Oberverwaltungsgericht Berlin-Brandenburg
12. Senat

Oberverwaltungsgericht Berlin-Brandenburg, Hardenbergstr. 31, 10623 Berlin

Rechtsanwälte
Geulen & Klinger
Schaperstraße 15
10719 Berlin

Aktenzeichen (Bitte stets angeben) Ihr Zeichen
OVG 12 N 164/20

Durchwahl
030 90149-8722
Intern 9149-8722

Datum
17. November 2020

Sehr geehrte Rechtsanwälte,

in der Verwaltungsstreitsache

Arne Semsrott ./. Bundesrechtsanwaltskammer

erhalten Sie ein Doppel des Schriftsatzes vom 12. November 2020 mit der Bitte um Stellungnahme binnen acht Wochen.

Mit freundlichen Grüßen
Auf Anordnung
Schumann
Die Geschäftsstelle

Dieses Schreiben ist ohne Unterschrift gültig, weil es mit einer Datenverarbeitungsanlage erstellt wurde.

222

avocado rechtsanwälte

avocado rechtsanwälte thurn-und-taxis-platz 6 60313 frankfurt

An das
Oberverwaltungsgericht Berlin-Brandenburg
- 12. Senat -
Hardenbergstraße 31
10623 Berlin

per beA

frankfurt, den	12.11.2020
unser zeichen:	31798-20/VO
durchwahl:	069.913.301.132
direktfax:	069.913.301.120
direktmail:	j.voss@avocado.de

In der Verwaltungsstreitsache

Arne Semsrott

gegen

Bundesrechtsanwaltskammer

- OVG 12 N 164/20 -

wegen: Anspruch nach dem IFG

übergeben wir wie im Schriftsatz vom 22. September 2020 angekündigt in der Anlage die streitgegenständlichen Dokumente. Ein Teil der Dokumente ist ohne Schwärzungen beigefügt, die übrigen Dokumente mit Schwärzungen bestimmter Seiten oder Passagen.

voßstraße 20 10117 **berlin**
t +49 [0]30 8848080 f +49 [0]30 88480884
berlin@avocado.de

nextower
thurn-und-taxis-platz 6 60313 **frankfurt**
t +49 [0]69 9133010 f +49 [0]69 91330119
frankfurt@avocado.de

neuer wall 46 20354 **hamburg**
t +49 [0]40 46897980 f +49 [0]40 468979899
hamburg@avocado.de

spichernstraße 75-77 50672 **köln**
t +49 [0]221 390710 f +49 [0]221 3907129
koeln@avocado.de

prinz-ludwig-palais
türkenstraße 7 80333 **münchen**
t +49 [0]89 55059560 f +49 [0]89 550595629
muenchen@avocado.de

rond point schuman 6 box 5 1040 **bruxelles**
t +32 [0]2 7423200 f +32 [0]2 7347671
bruxelles@avocado.de
www.avocado.de

avocado rechtsanwälte:
berger, figgen, gerhold, kaminski, voß
rechtsanwälte part mbb
die partnerschaft sowie deren partner sind
im partnerschaftsregister des amtsgerichts
berlin-charlottenburg unter pr 331 b eingetrage
salary partner, counsel, of counsel und associat
sind nicht partner der partnerschaftsgesellschaf

bankkonten:
commerzbank ag
iban-nr.: de42 5008 0000 0092 4234 00
swift-bic: dresdeff500

hypovereinsbank
iban-nr: de86 5032 0191 0008 2666 11
swift-bic: hyvedemm430

anderkonto
hypovereinsbank
iban-nr: de11 5032 0191 0008 2666 03
swift-bic: hyvedemm430

anderkonto
commerzbank ag
iban-nr.: de16 5008 0000 0091 7503 00
swift-bic: dresdeff500

ust-id-nr. de 814 17 29 76

Bei den Schwärzungen ist die Beklagte zugunsten des Klägers so restriktiv wie möglich vorgegangen. Sie hat sich dabei an der Entscheidung des Oberverwaltungsgerichts Berlin-Brandenburg in der Sache „OVG 12 N 104/20" sowie an der Begründung des erstinstanzlichen Urteils orientiert, welche bestimmte Schwärzungen für zulässig erachtet haben.

Die Beklagte hat über das erstinstanzliche Urteil hinausgehend nur solche Passagen zusätzlich geschwärzt, bei denen eindeutig von einer Offenlegung aufgrund eines der bereits im Schriftsatz vom 22. September 2020 dargelegten Ausnahmetatbestände abzusehen ist, oder bei denen es sich um personenbezogene Daten handelt. Legt man die Argumentation des Verwaltungsgerichts Berlin zugrunde, waren auch diese weiteren Passagen zu schwärzen. Dies hat das Verwaltungsgericht Berlin in seiner Entscheidung jedoch zu Unrecht verkannt. Zumindest hätte das Verwaltungsgericht Berlin dann die Beklagte zu einer aus seiner Sicht gebotenen Substantiierung ihres Vortrags auffordern müssen. Stattdessen hat das Verwaltungsgericht Berlin entgegen § 86 Abs. 1 u. 3 VwGO nicht darauf hingewirkt, dass die Beklagte ggf. erforderliche tatsächliche Angaben ergänzt oder weitere für die Feststellung und Beurteilung des Sachverhalts wesentliche Erklärungen zur Substantiierung der geheimhaltungsbedürftigen Inhalte abgibt. Deshalb wendet sich die Beklagte mit ihrem Antrag auf Zulassung der Berufung gegen die im Urteil ausgesprochene Verpflichtung zur im Übrigen vollständig ungeschwärzten Offenlegung der streitgegenständlichen Dokumente (s. im Einzelnen hierzu nachfolgend unter Ziffer I.).

Die Vorlage der geschwärzten Dokumente sowie die zugehörigen nachfolgenden Erläuterungen sind in diesem Zulassungsverfahren zu berücksichtigten. Das Vorbringen der Beklagten ist weder gemäß den §§ 128a Abs. 1, 87b Abs. 2 VwGO präkludiert noch in sonstiger Weise verspätet. Das Verwaltungsgericht Berlin hat die Beklagte insbesondere nicht gemäß § 87b Abs. 2 VwGO aufgefordert, zu bestimmten Vorgängen Tatsachen anzugeben oder Beweismittel zu bezeichnen oder Urkunden etc. vorzulegen. Die mit diesem Schriftsatz vorgelegten geschwärzten Dokumente und ihre Erläuterungen erweitern auch nicht die mit Schriftsatz vom 22. September 2020 geltend gemachten Zulassungsgründe, sondern präzisieren und detaillieren diese lediglich in zulässiger Weise (s. im Einzelnen hierzu nachfolgend unter Ziffer II.).

Im Einzelnen:

I. Zu den Dokumenten im Einzelnen

1. Vollständig ungeschwärzt vorgelegte Dokumente

Die Beklagte legt angesichts der Tatsache, dass der Testbericht des Sicherheitsaudits der SEC Consult sich mittlerweile frei zugänglich im Internet findet und bereits von einer auf IT-Themen spezialisierten Internetseite kommentiert wurde, den Testbericht des Sicherheitsaudits der SEC Consult ungeschwärzt vor.

Darüber hinaus legt die Beklagte in Ansehung der Entscheidung des Oberverwaltungsgerichts Berlin-Brandenburg in der Sache „OVG 12 N 104/20" folgende Vertragsbestandteile des Erstellungsvertrags gegenüber dem Kläger vollständig ungeschwärzt offen:

- Anlage Nr. 1 des Erstellungsvertrags – Kontextspezifikation (Anhang 1 zu Anlage 1)
- Anlagen Nr. 2 b) bis Nr. 2 e) des Erstellungsvertrags
- Anlage Nr. 5 des Erstellungsvertrags – Musterformular zum Änderungsverfahren EVB-IT Erstellungsvertrag
- Anlage Nr. 7 des Erstellungsvertrags – Sonderregelung zur Vertraulichkeit
- Anlage Nr. 11 des Erstellungsvertrags – Sonderregelung zur Teilabnahme, zu Freigabeerklärungen und zur Abnahme
- Anlage Nr. 12 des Erstellungsvertrags – Zahlungsplan
- Anlage Nr. 14 des Erstellungsvertrags – Musterformular zum Leistungsnachweis EVB-IT Erstellungsvertrag.

Alle weiteren Dokumente werden nur mit bestimmten Schwärzungen offengelegt.

Dabei ist die Beklagte jedoch zugunsten des Klägers so restriktiv wie möglich vorgegangen. Sie hat nur die Passagen geschwärzt, bei denen eindeutig von einer Offenlegung aufgrund eines der im Schriftsatz vom 22. September 2020 dargelegten Ausnahmetatbestände abzusehen ist, oder bei denen es sich um personenbezogene Daten handelt.

Zudem hat sich die Beklagte an der Begründung des erstinstanzlichen Urteils orientiert, welches bestimmte Schwärzungen für zulässig erachtet hat. Das Verwaltungsgericht Berlin hat im erstinstanzlichen Urteil keine weiteren Schwärzungen angeordnet, obwohl weitere Abschnitte der betreffenden Dokumente mit denselben Argumenten hätten geschwärzt werden müssen, mit denen bestimmte Schwärzungen angeordnet wurden. Dies hat das Verwaltungsgericht Berlin jedoch verneint, weil nach seiner Auffassung die Beklagte ihren Vortrag dazu nicht hinreichend substantiiert habe.

In diesem Fall hätte es aber gemäß § 86 Abs. 1 u. 3 VwGO Hinweise zur Beseitigung von Unklarheiten und Unstimmigkeiten geben müssen. Denn wenn nach Auffassung des Verwaltungsgerichts Berlin gemäß dem Vortrag der Beklagten bestimmte Informationen zwar grundsätzlich unter die Ausnahmetatbestände des IFG fallen, der Beklagtenvortrag jedoch zur Feststellung der Voraussetzungen bezüglich bestimmter Seiten oder Passagen der streitgegenständlichen Dokumente nicht ausreichte, dann hätte es die Beklagte gemäß § 86 Abs. 1 u. 3 VwGO darauf hinweisen müssen (BVerfG NJW 1994, 848, 849 – diese Entscheidung des Bundesverfassungsgerichts bezieht sich zwar auf die Vorschriften der ZPO zur richterlichen Hinweispflicht, wird aber auch für das Verständnis der richterlichen Hinweispflicht gemäß § 86 Abs. 3 VwGO herangezogen, vgl. u.a. Schoch/Schneider/Bier/Dawin, 38. EL Januar 2020, VwGO § 86 Rn. 139, 140).

Ein Gericht darf eine Klage z.B. nicht als unschlüssig abweisen, weil es den Sachvortrag für unsubstantiiert hält, ohne zuvor darauf hinzuweisen und Gelegenheit zu geben, in angemessener Frist auf den Hinweis zu reagieren (BVerfG NJW 1994, 848, 849; BGH NJW 1988, 3154, 3156; BGH NJW-RR 1993, 569; BGH NJW-RR 1998, 1377 ; BGH NJW 1999, 418, 421).

Dem kann auch nicht entgegengehalten werden, dass das Verwaltungsgericht von einem entsprechenden Hinweis absehen durfte, weil die Beklagte anwaltlich vertreten war. Hat der Rechtsanwalt einen Gesichtspunkt übersehen, ist er nach ständiger Rechtsprechung darauf hinzuweisen, es sei denn, er durfte auf seine Ansicht nicht vertrauen (BGH NJW 1989, 717, 718; BGH NJW-RR 1993, 569). Das bedeutet aber nicht, dass ein Hinweis an eine anwaltlich vertretene Partei nur dann erteilt werden muss, wenn diese auf die Richtigkeit ihrer Rechtsauffassung vertrauen durfte und mit der Gegenmeinung des Gerichts nicht zu rechnen brauchte. Vielmehr entfällt die Hinweispflicht des Gerichts erst dort, wo

einer anwaltlich vertretenen Partei die Mängel ihres Vortrags oder ihrer Antragstellung zweifellos bewusst sind (BVerfG NJW 1991, 2823; BGH WM 1977, 1201, 1203).

Das war hier aber gerade nicht der Fall:

Das Verwaltungsgericht Berlin übersandte der Beklagten die Erwiderung des Klägers vom 2. Januar 2019 auf deren ausführliche Klagerwiderung mit Verfügung vom 7. Januar 2019 lediglich „zur Kenntnisnahme". Danach bat das Verwaltungsgericht Berlin mit Verfügung vom 27. Mai 2020 nur noch um Mitteilung, ob Einverständnis mit einer Entscheidung ohne mündliche Verhandlung besteht (§ 101 Abs. 2 VwGO).

Sofern also das Verwaltungsgericht Berlin den diesbezüglichen Vortrag der Beklagten im erstinstanzlichen Verfahren für unsubstantiiert gehalten hat, hätte es gemäß § 86 Abs. 3 VwGO darauf hinwirken müssen, dass die Beklagte ggf. erforderliche tatsächliche Angaben ergänzt oder weitere für die Feststellung und Beurteilung des Sachverhalts wesentliche Erklärungen insbesondere zur Substantiierung der geheimhaltungsbedürftigen Inhalte abgibt.

Deshalb wendet sich die Beklagte mit ihrem Antrag auf Zulassung der Berufung gegen die im Urteil ausgesprochene Verpflichtung zur im Übrigen vollständig ungeschwärzten Offenlegung der streitgegenständlichen Dokumente.

2. Penetrationstests von Atos – Report und Präsentationen

a) Report zum Penetrationstest

Der Report zum Penetrationstest vom 29.04.2016 wird mit Schwärzungen in nur geringem Umfang offengelegt:

Deckblatt, S. 1:

Bei den geschwärzten Namen und E-Mail-Adressen von Mitarbeitern von Atos handelt es sich um personenbezogene Daten, die gemäß § 5 Abs. 1 IFG nicht offenzulegen sind. Das Informationsinteresse des Klägers an diesen Informationen ist als

sehr zu gering zu bewerten und überwiegt somit nicht das Interesse der benannten Personen am Ausschluss des Informationszugangs, da es sich bei der betreffenden Personen weder um gewählte Amtsträger noch um sonstige in der Öffentlichkeit stehende Personen handelt.

Inhaltsverzeichnis, S. 2:

Im Inhaltsverzeichnis ist die Überschrift der Ziffer 4.1.1 geschwärzt. Die Überschrift enthält bereits Informationen zum Server-Aufbau, welche die IT-Sicherheit des beA-Systems gefährden könnten. Die Überschrift bezieht sich zudem auf die Seite 7, die bereits nach dem erstinstanzlichen Urteil des Verwaltungsgerichts Berlin nicht offenzulegen ist. Entsprechend ist sie zu schwärzen.

Ziffer 2, S. 4 (Auftragsdetails):

Die Ausführung zum Deckblatt (S. 1) gelten entsprechend für die hier vorgenommene Schwärzung von Namen, E-Mail Adressen und Telefonnummern von Mitarbeitern der Beklagten sowie von Atos.

Ziffer 3.2, S. 6:

Auf dieser Seite ist ein Hinweis auf die interne Aufgabenverteilung zwischen Atos und einem Subunternehmer geschwärzt. Die Information würde Rückschlüsse auf die Projektorganisation und die Zusammenarbeit zwischen Atos und dem Subunternehmen zulassen. Diese Informationen sind als Betriebs- und Geschäftsgeheimnisse von Atos zu schwärzen.

Ziffer 4, 4.1, 4.1.1, S. 7:

Die Inhalte dieser Seite können nicht offengelegt werden. Hierzu verweist die Beklagte zunächst auf den Tenor und insbesondere auf die Urteilsbegründung des erstinstanzlichen Urteils des Verwaltungsgerichts Berlin vom 14.07.2020 (S. 10). Auf der Seite 7 sind die detaillierten technischen Server-Informationen (z.B. Informationen zu Server Name, Set-Cookie, Content-Type, Error-Report Details) enthalten, so dass ohne Schwärzung die IT-Sicherheit des beA-Systems gefährdet ist. Zudem enthält die Seite Programmiercode, welcher ein Betriebs- und Geschäftsgeheimnis

von Atos ist und auch nach dem erstinstanzlichen Urteil nicht offenzulegen ist (s. dort S. 10).

Ziffer 4.1.2, S. 8 (Informationen auf Fehlerseite):

Gleiches gilt für die Inhalte der letzten Zeile in dieser Tabelle, die ebenfalls technische und daher IT-sicherheitsrelevante Details zu den Fehlern enthalten (z.B. Informationen zu Transaction ID, Violation Category, Violations Log). Zudem enthält auch dieser Abschnitt Programmiercode, welcher als Betriebs- und Geschäftsgeheimnis von Atos nicht offenzulegen ist (vgl. erstinstanzliches Urteil, a.a.O.).

Ziffer 4.2.1, S. 9 und 10 (Fremdes UntrustedCertificate wird akzeptiert):

Bei den hier geschwärzten Passagen sind ebenfalls aus Gründen der IT-Sicherheit geheimhaltungsbedürftige Daten betroffen (z.B. Informationen zu Content-Type, Cookies, SOAPAction, User-Agent, Host, Connection, Content-Length, Certificate Hierarchy, Script-Transport-Security etc.). Zudem enthalten die geschwärzten Abbildungen Programmiercode, welcher ein Betriebs- und Geschäftsgeheimnis von Atos ist (vgl. erstinstanzliches Urteil, a.a.O.).

Ziffer 4.2.2, S. 11 (Denial of Service Angriff möglich):

Die letzte Zeile in der Tabelle wurde aus Gründen der IT-Sicherheit geschwärzt, weil sich dort eine Detailinformation zur konkreten Fehlerquelle befindet.

Selbst wenn Fehler behoben sind, geben die vorstehend beschriebenen Informationen vertiefte Einblicke in die Sicherheitsarchitektur des beA. Es bestünde bei einer Veröffentlichung die Gefahr, dass auch zukünftig Angriffe auf das beA zumindest erleichtert werden.

Ziffer 4.4, S. 13 und 14 (Durchgeführte Testszenarien):

In diesem Abschnitt werden die durchgeführten Testszenarien angelehnt an einen bestimmten Testing Guide dargestellt und detailliert beschrieben. Den Testing Guide kann Atos unabhängig vom beA bei allen IT-Projekten und Software-Entwicklungen

einsetzen, es handelt sich dabei um exklusives technisches Spezialwissen. Diese Informationen sind (auch nach dem erstinstanzlichen Urteil, a.a.O.) somit als Betriebs- und Geschäftsgeheimnisse von Atos zu schwärzen.

b) Präsentation Testbericht Atos – Inkrement 3 & Gesamtintegration

Die Präsentation zum Testbericht Atos vom 09.05.2016 wird mit den im Folgenden erläuterten Schwärzungen vorgelegt:

Folie 1:

Auf der ersten Folie ist aus Gründen des Datenschutzes gemäß § 5 Abs. 1 IFG der Name des bei Atos beschäftigten Autors der Präsentation geschwärzt. Das Informationsinteresse des Klägers an diesen Informationen ist als sehr zu gering zu bewerten und überwiegt somit nicht das Interesse der benannten Person am Ausschluss des Informationszugangs. Dies entspricht auch dem erstinstanzlichen Urteil, wonach derartige personenbezogene Daten ebenfalls zu schwärzen waren.

Dateien auf Folien 8, 9, 11, 12, 18, 19, 21, 22, 24 und 28:

Die auf den aufgeführten Folien verlinkten Dateien werden nicht offengelegt. Die meisten der Hyperlinks leiten auf einen internen Server von Atos weiter. Dies ergibt sich auch aus Folie 3, 4. Spiegelstrich, s. dort: „Alle eingebetteten Informationen und Verweise beziehen sich auf den Testdokumentationsstand aus dem HP ALM der Atos (Projekt „beA")." Die dort verlinkten Dokumente befinden sich somit nicht in den Akten der Beklagten, weshalb sie nicht dem Anspruch des Klägers auf Zugang unterliegen. Zudem sind diese Hyperlinks nicht mehr aufrufbar, weshalb die Beklagte nicht mehr nachvollziehen kann, auf welche Dokumente ursprünglich verlinkt war. Diese Hyperlinks auf Dokumente befinden sich auf den Folien 8, 9, 11, 12, 18, 19, 21, 22 und 24.

Auf den Folien 11 (jeweils rechts neben den geschwärzten Hyperlinks), 12 (rechts oben neben dem geschwärzten Hyperlink), 18 (unter dem geschwärzten Hyperlink), 19 (unter dem

geschwärzten Hyperlink rechts), 21 (unter dem geschwärzten Hyperlink rechts) und 22 (rechts oben neben dem geschwärzten Hyperlink) sind zusätzlich auch Dokumente eingebunden, die ebenfalls geschwärzt wurden. Diese in die Präsentation eingebundenen Dateien enthalten umfangreiche und detaillierte Darstellungen der zum damaligen Zeitpunkt durchgeführten, fehlgeschlagenen und noch offenen Tests, der dabei gefundenen Fehler sowie einen umfangreichen Ausschnitt der Atos-internen Testprotokolle.

Die umfassende und sehr detailgetreue Darstellung der durchgeführten Tests lässt eindeutige Rückschlüsse auf die konkrete Architektur des beA zu, welche selbst für die Nutzer nicht ersichtlich ist. Eine vergleichbare Architektur kann Atos bei IT-Projekten, insbesondere im Justizsektor, wieder verwenden. Es handelt sich daher um Betriebs- und Geschäftsgeheimnisse.

Zusätzlich enthalten diese Dateien genaue Informationen über die Art und Weise der Programmierung und interne Abhängigkeiten im System. Die Offenlegung dieser Informationen würde Angreifern die Identifizierung von etwaigen künftigen Schwachstellen im beA erleichtern. Daher können diese Dateien aus Gründen der IT-Sicherheit nicht veröffentlicht werden.

Auch lassen die detaillierten Informationen über die durchgeführten Tests, die Art der Darstellung dieser Tests und die dargestellten Reaktionen von Atos genaue Rückschlüsse auf die Teststrategie von Atos zu. Die Teststrategie von Atos ist für Nutzer des beA nicht ersichtlich und kann bei künftigen anderen IT Projekten in gleicher Art und Weise oder leicht angepasst von Atos wieder verwendet werden. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Geschäfts- und Betriebsgeheimnisse von Atos.

Schließlich war die Teststrategie im Vergabeverfahren ausdrücklich angefordert und unterschied sich in den Angeboten der einzelnen Bieter. Sie war somit ein Kernelement der Vergabeentscheidung und unterliegt damit der vergaberechtlichen Verschwiegenheit.

PDF-Dateien auf Folie 25:

Bei den ersten beiden eingebundenen PDF-Dateien handelt es sich um den vollständig offengelegten Testbericht des Sicherheitsaudits der SEC Consult sowie den teilweise offengelegten Report Penetrationstest (s. hierzu Ziffer I.2.a) dieses Schriftsatzes). Aus diesem Grund werden die Dokumente im Zusammenhang mit der Präsentation nicht erneut offengelegt.

Bei den unteren drei eingebundenen PDF-Dateien handelt es sich um umfangreiche und detaillierte Herstellerinformationen zu von Atos eingesetzten Standardprodukten. Diese Informationen können nicht offengelegt werden.

Die Idee an bestimmten Stellen auf den Einsatz von Standardlösungen zu setzen und Subunternehmer einzubinden, prägt die architektonische Lösung von Atos und unterscheidet den Lösungsvorschlag von den Angeboten der anderen Bieter. Die Informationen unterliegen damit der vergaberechtlichen Verschwiegenheit.

Die Informationen lassen des Weiteren eindeutige Rückschlüsse auf die konkrete Architektur des beA zu, welche für Nutzer nicht ersichtlich ist. Die Architektur kann Atos bei künftigen IT-Projekten, insbesondere im Justizsektor, wieder verwenden. Es handelt sich daher um Betriebs- und Geschäftsgeheimnisse. Zudem können Mitbewerber von Atos aus den genauen Informationen über die eingesetzten Standardprodukte klare Rückschlüsse auf die Kalkulation von Atos ziehen. Auch aus diesem Grund sind die Informationen als Betriebs- und Geschäftsgeheimnisse zu bewerten.

c) Präsentation Testbericht Atos – Tests zur Release-Version 1.0.3

Die Präsentation zum Testbericht Atos vom 19.01.2017 wird mit den im Folgenden erläuterten Schwärzungen vorgelegt:

Folie 1:

Auf der ersten Folie ist aus Gründen des Datenschutzes gemäß § 5 Abs. 1 IFG der Name des bei Atos beschäftigten Autors der

Präsentation geschwärzt. Das Informationsinteresse des Klägers an diesen Informationen ist als sehr zu gering zu bewerten und überwiegt somit nicht das Interesse der benannten Person am Ausschluss des Informationszugangs, s.o.

Folie 9:

Der Web-Link zum Testplan auf Folie 9 wurde entfernt. Der Hyperlink leitet auf einen internen Server von Atos weiter. Die dort enthaltenen Dokumente befinden sich somit nicht in den Akten der Beklagten, weshalb sie nicht dem Anspruch des Klägers auf Zugang unterliegen. Zudem ist der Hyperlink nicht mehr aufrufbar, weshalb die Beklagte nicht mehr nachvollziehen kann, auf welche Dokumente ursprünglich verlinkt war.

d) Präsentation Testbericht Atos – Tests zur Release-Version 1.1

Die Präsentation zum Testbericht Atos vom 14.06.2017 wird mit den im Folgenden erläuterten Schwärzungen vorgelegt:

Folie 1:

Auf der ersten Folie ist aus Gründen des Datenschutzes gemäß § 5 Abs. 1 IFG der Name des bei Atos beschäftigten Autors der Präsentation geschwärzt. Das Informationsinteresse des Klägers an diesen Informationen ist als sehr zu gering zu bewerten und überwiegt somit nicht das Interesse der benannten Person am Ausschluss des Informationszugangs, s.o.

Folie 9:

Der Web-Link zum Testplan auf Folie 9 wurde entfernt. Der Hyperlink leitet auf einen internen Server von Atos weiter. Die dort enthaltenen Dokumente befinden sich somit nicht in den Akten der Beklagten, weshalb sie nicht dem Anspruch des Klägers auf Zugang unterliegen. Zudem ist der Hyperlink nicht mehr aufrufbar, weshalb die Beklagte nicht mehr nachvollziehen kann, auf welche Dokumente ursprünglich verlinkt war.

3. Erstellungsvertrag

Die Bestandteile des Erstellungsvertrags werden mit den im Folgenden erläuterten Schwärzungen offengelegt:

a) EVB-IT Erstellungsvertrag

Ziffer 4.1, S. 9 bis 11 (Überlassung von Standardsoftware gegen Einmalvergütung):

In der Liste zu Ziffer 4.1 „Überlassung von Standardsoftware gegen Einmalvergütung auf Dauer (Verkauf)" hat die Beklagte zu Recht einige der eingesetzten Standardprodukte sowie die hierfür mit Atos vereinbarten Preise für die Produkte geschwärzt. Sie beruft sich hierbei zu Recht sowohl auf die vergaberechtliche Vertraulichkeit als auch auf Betriebs- und Geschäftsgeheimnisse von Atos. Die in der Liste der Standardsoftware aufgeführten Produkte lassen Rückschlüsse auf die Systemarchitektur sowie die Datenbankstruktur zu. Hierbei handelt es sich um eine individuelle Lösung, die Atos der Beklagten im Vergabeverfahren präsentiert und für die sie den Zuschlag erhalten hat.

Ziffer 5.1.1, S. 16 (Störungsbeseitigung):

In der Ziffer 5.1.1 ist ebenfalls ein eingesetztes Standardprodukt genannt, das die Beklagte zu Recht geschwärzt hat. Die Benennung dieses Produktes lässt Rückschlüsse auf die Systemarchitektur und damit Geschäftsgeheimnisse von Atos zu.

S. 27 (Unterschriften):

Darüber hinaus hat die Beklagte aus Gründen des Datenschutzes gemäß § 5 Abs. 1 IFG lediglich auf Seite 27 die Namen und Unterschriften der Vertragsunterzeichner geschwärzt. Das Informationsinteresse des Klägers an diesen Informationen ist als sehr zu gering zu bewerten und überwiegt somit nicht das Interesse der benannten Personen am Ausschluss des Informationszugangs.

b) **Anlage Nr. 1 – Leistungsbeschreibung**

Titelblatt, S. 1:

Der Name des Ansprechpartners der Beklagten ist aus Gründen des Datenschutzes gemäß §5 Abs. 1 IFG auf dem Titelblatt geschwärzt. Das Informationsinteresse des Klägers an diesen Informationen ist als sehr zu gering zu bewerten und überwiegt somit nicht das Interesse der benannten Person am Ausschluss des Informationszugangs.

Ziffer 2.10.2, S. 76 bis 78 (Support):

Auf S. 76 befinden sich umfangreiche Definitionen der Störungsprioritäten, welche geschwärzt wurden. Auf S. 77 bis 79 wurden die konkret einzuhaltenden Reaktions- und Fehlerbehebungszeiten geschwärzt. Diese Informationen lassen zumindest für Branchenkenner eindeutige Rückschlüsse auf die einzelnen Kalkulationen von Atos zu. Somit waren diese Abschnitte als Betriebs- und Geschäftsgeheimnisse von Atos zu schwärzen.

c) **Anlage Nr. 2 – Umsetzungskonzept des Auftragnehmers**

Folgende Informationen wurden zu Recht von der Beklagten geschwärzt:

S. II:

Die Namen und Kontaktdaten der Ansprechpartner von Atos und der Beklagten wurden geschwärzt. Es handelt sich um personenbezogene Daten, die nicht offenzulegen sind, denn das Informationsinteresse des Klägers an diesen Informationen ist als sehr zu gering zu bewerten und überwiegt nicht das Interesse der benannten Personen am Ausschluss des Informationszugangs.

S. 1 bis S. 18:

Bezüglich der Schwärzung dieses Abschnitts verweist die Beklagte zunächst auf den Tenor und die Urteilsbegründung des erstinstanzlichen Urteils des Verwaltungsgerichts Berlin vom 14.07.2020 (S. 13 und S. 14). Die in dem Abschnitt dargestellten

Informationen beinhalten Betriebs- sowie Geschäftsgeheimnisse von Atos und sind gemäß § 6 Abs. 2 IFG nicht zu veröffentlichen.

Diese geschwärzten Seiten enthalten folgende Informationen:

- Bereiche des beA und der Entwicklung des beA, in denen Produkte des Subunternehmers Governikus eingesetzt wurden: Es ist allgemein bekannt, dass Atos Governikus als Subunternehmer eingesetzt hat. Allerdings ist es Alleinstellungsmerkmal des Atos-Lösungsansatzes, in welchen Bereichen Produkte oder Individualentwicklungen von Governikus eingesetzt wurden. Dadurch unterscheidet sich der Lösungsvorschlag von Atos von den Lösungsvorschlägen von anderen Teilnehmern am Vergabeverfahren. Die Offenlegung lässt Rückschlüsse auf die architektonische Lösung von Atos zu, gibt Hinweise auf die Kalkulation und unterliegt zudem der vergaberechtlichen Verschwiegenheit;

- Einsatz von bestimmten weiteren Standardprodukten und Komponenten, der auf die Gesamtarchitektur des beA-Systems schließen lässt: Die Idee, an bestimmten Stellen auf den Einsatz von Standardlösungen zu setzen und Subunternehmer einzubinden, prägt die architektonische Lösung von Atos und lässt auch Rückschlüsse darauf zu, wie Atos in vergleichbaren Projekten vorgeht, die auch und gerade in der Justiz immer wieder neu ausgeschrieben werden. Zudem lassen diese Informationen Rückschlüsse auf die Kalkulation von Atos zu;

- Individuelle Vorgehensweise von Atos bei der Durchführung von Pilottests, Entwicklertests, Tests des Oberflächenprototyps, Integrationstests, Teil-Integrationstest und Technischen Tests: Die Ausführungen enthalten Darstellungen der Testphasen inklusive konkreten Beschreibungen dieser Testphasen. Zusätzlich stellt Atos in dem Abschnitt dar, wie sie plante Testkanzleien einzusetzen und in welcher Testumgebung einzelne Tests durchgeführt werden sollen. Die Beklagte hatte im Vergabeverfahren ausdrücklich nach dem konkreten Testkonzept gefragt. Jeder Bieter hat dazu eigene, voneinander unterscheidbare

Ausführungen gemacht, welche die Vergabeentscheidung beeinflussten. Die Ausführungen fallen damit unter die vergaberechtliche Verschwiegenheit. Es handelt sich zudem um ein Betriebs- bzw. Geschäftsgeheimnis, wie Atos in solchen Fällen die Entwicklung vornimmt und mit welchen konkreten Methoden Atos von ihr entwickelte Software testet. Des Weiteren ermöglichen das Testvorgehen und die von Atos im Einzelnen vorgeschlagene Zeitpläne Rückschlüsse auf die konkrete Kalkulation. Da die übrigen Bieter nach wie vor Mitbewerber von Atos sind, sind diese Informationen nach wie vor als Betriebs- und Geschäftsgeheimnisse relevant. Hierbei ist zudem besonders zu berücksichtigen, dass der Kreis der IT-Anbieter im Justizumfeld vergleichsweise klein ist, die Bieter deshalb regelmäßig an denselben Vergabeverfahren teilnehmen und das Vorgehen untereinander laufend genau beobachten.

- Einzelheiten zum Projektplan von Atos und zur konkreten Vorgehensweise bei der Erstellung des beA und dem geplanten technischen Durchstich, durch die sich das Angebot von Atos von anderen Angeboten im Vergabeverfahren unterscheidet: Diese Informationen unterliegen der vergaberechtlichen Verschwiegenheit. Der Projektplan und die Informationen zur konkreten Vorgehensweise lassen im dargestellten Detaillierungsgrad Branchenkennern Rückschlussmöglichkeiten auf die Kalkulation von Atos, den Einsatz von Personalressourcen und das Entwicklungsvorgehen zu. Sie sind somit auch Betriebs- und Geschäftsgeheimnisse von Atos.

- Informationen, die Rückschlüsse auf das Zuschneiden der einzelnen Inkremente zulassen: Der genaue Zuschnitt der Inkremente unterscheidet die von Atos angebotene Lösung gegenüber den Mitbietern. Somit unterliegt diese Angabe dem vergaberechtlichen Verschwiegenheitsgebot.

- Informationen über angeforderte Mitwirkungsleistungen der Beklagten in ihrer Eigenschaft als Auftraggeber, die sich zum Teil deutlich von den in der Leistungsbeschreibung enthaltenen Mitwirkungsleistungen unterscheiden: Diese Informationen lassen Rückschlüsse auf das

Entwicklungsvorgehen und die Projektplanung, insbesondere auf das aus Sicht von Atos erforderliche Zusammenarbeitsmodell, zu. Aus diesen Informationen können Branchenkenner auch Rückschlüsse auf den Ressourceneinsatz bei Atos ziehen. Dies zählt folglich zum individuellen Entwicklungsvorgehen und damit zu Betriebs- und Geschäftsgeheimnissen.

- Informationen über die von Atos geplante Projektstruktur und interne Projektsteuerung (inklusive Angaben zum Lenkungsausschuss, zum Projektausschuss, zur Projektleitung, zum Qualitätsmanager und zum Servicemanager): Diese Angaben unterscheiden sich von denen der Mitbieter und lassen Rückschlüsse auf das Vorgehen gerade bei dieser speziellen Anwendung zu. Bei ähnlichen Angeboten gerade aus dem Justizbereich wird erfahrungsgemäß wieder auf diese Projektstruktur zurückgegriffen, so dass diese Information ein Betriebs- und Geschäftsgeheimnis von Atos darstellt. Außerdem sind Rückschlüsse auf den konkreten Personaleinsatz und damit auf die Kalkulation möglich.

- Gliederung und Inhalt des von Atos eingesetzten Projekthandbuchs sowie eine ausführliche Darstellung des Atos-interne Regelwerks zum Projektvorgehen: Da es sich um ein Standard-Projekthandbuch und das standardisierte Vorgehen von Atos handelt, wird sie diese Informationen in vergleichbaren Projekten wiederverwenden. Die Beschreibung gibt sehr detailliert Aufschluss über das Projektvorgehen bei Atos und die speziell bei Atos standardisierten Prozesse sowie eine Erklärung, wie diese Standards an das konkrete Projekt angepasst werden. Es handelt sich somit um Geschäfts- und Betriebsgeheimnisse von Atos.

- Projektplan einschließlich detaillierter Angaben zu den Meilensteinen: Der Projektplan beschreibt das gesamte Vorgehen, der Personaleinsatz und die Kalkulation von Atos. Der Projektplan war wesentliches Entscheidungskriterium im Vergabeverfahren für die Beklagte, so dass er zum einen unter die vergaberechtliche Verschwiegenheit fällt und zum

anderen Geschäfts- und Betriebsgeheimnisse von Atos enthält.

Das Verwaltungsgericht Berlin hat zu Recht entschieden, dass die vorstehenden Informationen nicht offenzulegen sind. Auf Grundlage dieser Argumentation waren aber auch die im Folgenden aufgeführten Passagen zu schwärzen. Dies hat das Verwaltungsgericht Berlin in seiner Entscheidung zu Unrecht verkannt.

Ziffer 1f), S. 19 und 20 (Aktualisierung der Kontextspezifikation und Realisierung der Nachvollziehbarkeit zwischen Umsetzungsfeinkonzept und Kontextspezifikation):

Hierunter beschreibt Atos im Detail ihr Vorgehen, individualisiert ihre Lösung und benennt die eingesetzten Werkzeuge und ihren Umgang mit diesen Werkzeugen.

Die geschwärzten Passagen enthalten deshalb Geschäfts- und Betriebsgeheimnisse von Atos.

Ziffer 2), S. 21 und 22 (Eckpunkte für den Anforderungsbereich „Nachrichten"):

Atos beschreibt in den geschwärzten Abschnitten die Teilkomponente Nachrichtensystem, das fachliche Datenmodell sowie fachliche Aspekte und Funktionen für die Umsetzung der Anforderungen im Bereich „Nachrichten" einschließlich ihres speziellen Vorgehens. Es handelt sich dabei um Betriebs- und Geschäftsgeheimnisse von Atos.

Ziffer 2d), S. 40 (Fristeneinhaltung zu Spitzenzeiten):

In den geschwärzten Passagen skizziert Atos eine Lösungsidee zur Sicherstellung der rechtzeitigen Nachrichtenübermittlung zu Zeiten, in denen das beA stark in Anspruch genommen wird. Die Lösungsidee wurde bislang nicht umgesetzt, die Beklagte behält sich eine künftige Umsetzung jedoch ausdrücklich vor. Die von Atos präsentierte Lösung unterschied sich deutlich von den Vorschlägen der Mitbewerber und hat zur Vergabeentscheidung beigetragen. Die Passage unterliegt somit der vergaberechtlichen Verschwiegenheit. Zudem ist nicht ausgeschlossen, dass auch Atos

diese Idee in einem anderen Projekt der Justiz oder von sonstigen Auftraggebern wieder aufgreifen könnte. Jede Plattform, die Datentransfers zwischen Nutzern ermöglicht, hat vergleichbare Probleme mit der rechtzeitigen Übermittlung von Daten bei großer Auslastung. Entsprechend kann die Lösungsidee von Atos für eine große Zahl künftiger Projekte wieder verwendet werden. Sie ist daher als Geschäfts- und Betriebsgeheimnis nicht offenzulegen.

Ziffer 2g), S. 46 (Unterstützung bei dem Führen einer Handakte in Papierform oder elektronischer Form):

In dem Abschnitt beschreibt Atos die konkrete Lösungsidee wie das beA beim Dokumentenmanagement und Archivieren hilft. Hier gilt das Vorstehende entsprechend, so dass auch diese Passagen geheimhaltungsbedürftig und daher zu schwärzen sind.

Ziffer 3), S. 49 und 50 (Lösung für den Anforderungsbereich „Administration"):

Die geschwärzten Angaben unter „Systemverwaltung" und „Postfachverwaltung" wurden nicht in dieser Form umgesetzt und könnten von Atos für weitere Kommunikationssysteme als Idee dienen. Sie sind daher als Geschäfts- und Betriebsgeheimnisse von Atos zu bewerten.

In den restlichen geschwärzten Abschnitten wird bezüglich der Administration der Standardsoftware eines bestimmten Drittherstellers eine Lösungsidee vorgestellt, die Atos nicht umgesetzt hat. Es ist aber möglich, dass Atos in einem weiteren Projekt gemeinsam mit dem Dritthersteller diese Idee erneut präsentieren und sie umsetzen wird. Die Passage ist daher als Betriebs- und Geschäftsgeheimnis von Atos geheimhaltungsbedürftig.

Ziffer 3a), S. 51 bis 53 (Übermittlung neu erstellter Benutzerdaten):

In der geschwärzten Passage zur „Zustellung der Benachrichtigung (Zugangsdaten)" skizziert Atos eine Lösung, die ebenfalls nicht umgesetzt wurde. Atos wird diese Idee ggf. in einem anderen Projekt wieder aufgreifen, da vergleichbare Probleme bei den meisten IT-Projekten zu lösen sind. Die Informationen zu dieser

Lösung sind als Betriebs- und Geschäftsgeheimnisse von Atos geheimhaltungsbedürftig.

Die geschwärzten Ausführungen von Atos zum „Registrierungsprozess" wurden im Rahmen der Entwicklung mit Atos komplett neu erarbeitet. Die hier dargestellte Lösung wurde nicht umgesetzt. Die Lösung kann oder wird jedoch in vergleichbaren Projekten zum Einsatz kommen. Somit kann sie hier als Geschäfts- und Betriebsgeheimnis von Atos nicht offengelegt werden.

Dies gilt gleichermaßen für die geschwärzte Passage unter dem Schaubild auf S. 53, da sich dies ebenfalls auf den Registrierungsprozess bezieht.

Ziffer 3d), S. 62 und S. 63 (Arten von Authentifizierungsmerkmalen):

Die geschwärzten Passagen verweisen auf den Einsatz eines Produkts eines Drittherstellers. Dieser Verweis erlaubt Rückschlüsse auf Details der Architektur des beA-Systems. Dies ist aus Gründen der IT-Sicherheit geheim zu halten. Zusätzlich erlaubt die Information genaue Rückschlüsse auf die Kalkulation von Atos und ist somit als Betriebs- und Geschäftsgeheimnis zu schwärzen.

Die darunter aufgeführten Mitwirkungspflichten der Beklagten waren ebenfalls zu schwärzen. Die Kenntnis darüber lässt einerseits Schlüsse auf die Vorgehensweise von Atos zu. Andererseits lässt sich die Kalkulation von Atos nachvollziehen, wenn Konkurrenten erfahren, welche Mitwirkungsleistungen Atos von der Beklagten erwartet. Entsprechend beinhaltet der Abschnitt Betriebs- und Geschäftsgeheimnisse von Atos.

Ziffer 3e), S. 64 und 65 (Abgleich mit den jeweiligen Verzeichnissen):

Das geschwärzte Schaubild beschreibt die Architektur des Abgleichs der Verzeichnisdaten im beA. Diese Architektur ist für die Nutzer des Systems nicht ersichtlich. Solche Verzeichnisse werden grundsätzlich bei geschlossenen Kommunikationssystemen genutzt, so dass deren Architektur bei künftigen IT Projekten von Atos eingesetzt werden kann und somit ein Geschäfts- und

Betriebsgeheimnis darstellt. Dies gilt auch für die unter dem Schaubild geschwärzten spezifischen Erläuterungen.

Der geschwärzte Abschnitt auf S. 65 enthält Informationen darüber, inwiefern ein von Atos eingesetzter Subunternehmer mit der vorgeschlagenen Lösung und der dabei eingesetzten Architektur bereits praktische Erfahrungen in anderen IT-Projekten hat. Diese Information ist ein Betriebs- und Geschäftsgeheimnis des Subunternehmers von Atos.

Ziffer 4), S. 67 und 68 (Monitoring):

Das Monitoring wurde von Atos als Individualentwicklung umgesetzt. Diese Lösung wird von Atos auf den S. 67 und 68 detailliert beschrieben. Ohne eine Schwärzung würden Architekturüberlegungen des beA-Systems offenbart, die für die Nutzer nicht ersichtlich sind und auf die auch in anderen Projekten von Atos zurückgegriffen werden könnte. Die Beschreibung war somit als Geschäfts- und Betriebsgeheimnis von Atos zu schwärzen.

Ziffer 5), S. 72 (S.A.F.E.-Domäne BRAK):

Die geschwärzte Passage beschreibt die spezielle Umsetzungslösung von Atos in Bezug auf Schnittstellen zur BRAK, die für den Anwender des beA-Systems nicht ohne weiteres erkennbar ist und unterfällt damit zumindest der vergaberechtlichen Verschwiegenheitsverpflichtung. Dies stellt zudem auch ein Geschäfts- und Betriebsgeheimnis von Atos dar.

Ziffer 5a), S. 73 und 74 (barrierefreier Zugang):

Die hierunter auf S. 73 geschwärzten Passagen enthalten detaillierte Beschreibungen der Architektur des beA insbesondere im Hinblick auf die barrierefreie Nutzung der beA-Oberfläche, der in diesem Zusammenhang einzusetzenden Standardprodukte, der Webtechnologie, die die Lösung von Atos gegenüber anderen Lösungen im Vergabeverfahren individualisiert, sowie der konkreten Umsetzung. Die Konkretisierung des Angebots durch Atos unterliegt der vergaberechtlichen Verschwiegenheit. Die restlichen Informationen, wie in diesem und vergleichbaren Fällen vorgegangen wird, sind als Geschäfts- und Betriebsgeheimnisse von Atos zu bewerten.

Die auf S. 74 geschwärzten Inhalte betreffen ein anderes, dort konkret benanntes Projekt von Atos, in dem Barrierefreiheit eine Rolle spielte, sowie Beispiele für konkret geplante Umsetzungen. Es ist davon auszugehen, dass Atos diese Vorgehensweise auch in anderen Projekten nutzen wird, da Barrierefreiheit unabhängig vom beA bei allen IT-Projekten ein großes Thema ist. Auch hier liegt deshalb ein Geschäfts- und Betriebsgeheimnis vor, dessen Offenlegung Atos schaden würde.

Ziffer 5b), S. 75 und 76 (Ergonomieziele):

Die geschwärzten Aussagen sowie das Schaubild darunter benennen das konkret eingesetzte Prozessmodell zur Erreichung der geforderten Ergonomieziele und beschreiben detailliert das Vorgehen von Atos zur Umsetzung dieses Modells. Nach welchem Prozessmodell Atos sein Angebot in Bezug auf die geforderten Ergonomieziele gestaltet hat, unterliegt der vergaberechtlichen Verschwiegenheit. Es ist zudem ein Geschäfts- und Betriebsgeheimnis von Atos wie das gewählte Modell im Einzelfall umgesetzt werden soll, da Atos vergleichbare Systeme bei anderen IT-Projekten verwendet und sie den Vertragspartnern exklusiv zur Verfügung stellt. Bzgl. des Schaubilds verweisen wir zudem auf den Tenor und die Urteilsbegründung des erstinstanzlichen Urteils des Verwaltungsgerichts Berlin vom 14.07.2020 (S. 13 und S. 14).

Ziffer 5c), S. 78 bis 80 (Styleguide):

Die geschwärzten Abschnitte in diesem Bereich enthalten detaillierte Beschreibungen der Vorschläge von Atos bezüglich des Designs, des Stils und der Positionierung des Dialog-Bereichs. Die Vorschläge von Atos wurden in der Form im beA letztendlich nicht umgesetzt. Entsprechend kann Atos die Lösungsideen bei künftigen IT Projekten wieder verwenden. Es handelt sich um Betriebs- und Geschäftsgeheimnisse von Atos.

Ziffer 5d), S. 81 (Zugriff durch externe Systeme):

Die geschwärzten Inhalte benennen die konkrete Vorgehensweise von Atos bei der Entwicklung. Zudem wird die Architektur der gewählten Lösung beschrieben Für den Anwender ist die Funktionsweise nicht erkennbar. Daher handelt es sich um ein

Geschäfts- und Betriebsgeheimnis von Atos. Außerdem betrifft die Lösung einen sicherheitsrelevanten Bereich.

Zudem sind am Seitenende geschwärzte Hinweise von Atos an die Beklagte für Regelungen mit den Kanzleisoftware-Herstellern enthalten, wodurch sich die Lösung von den Lösungen anderer Bieter unterscheidbar machte, so dass hier auch die vergaberechtliche Vertraulichkeit zu wahren ist.

Ziffer 5e), S. 82 und 83 (Schnittstellentechnologie):

Die geschwärzten Inhalte beschreiben im Detail die Verfahrensweise und die einzusetzenden Technologien für die Schnittstellen zu Kanzleisoftwareprodukten. Diese Informationen sind allein schon aus Sicherheitsgründen geheim zu halten; zugleich sind sie Geschäfts- und Betriebsgeheimnisse von Atos.

Ziffer 5f), S. 84 bis 86 (Schnittstellendefinitionen):

Die geschwärzten Passagen beschreiben detailliert die von Atos eingesetzte Technologie, den Einsatz spezieller Tools sowie die einzelnen Funktionsweisen der Schnittstellen. Die vorstehenden Ausführungen zu den Schwärzungen auf den S. 82 und 83 gelten deshalb hier entsprechend. Die Beklagte beruft sich zu Recht auf die Geheimhaltungsbedürftigkeit derartiger Informationen.

Ziffer 5g), S. 87 und 88 (Gewährleistung einer sicheren Kommunikation):

Die im zweiten Absatz geschwärzte Passage enthält interne Informationen aus den technischen Arbeitsgruppen der Justiz, mit denen Atos Gespräche geführt hatte. Diese Kenntnisse von Atos sind Geschäfts- und Betriebsgeheimnisse und unterliegen zudem der vergaberechtlichen Verschwiegenheit.

Die weiteren Schwärzungen auf S. 87 und 88 betreffen von Atos eingesetzte Software-Komponenten, die Rückschlüsse auf die Architektur zulassen, detaillierte Beschreibungen der Architektur sowie einen systeminternen Vorschlag, der die Lösung von Atos unterscheidbar macht von anderen Lösungsvorschlägen und der so ggf. auch in anderen Systemen einsetzbar ist. Deshalb handelt es sich um Geschäfts- und Betriebsgeheimnisse von Atos.

Gleiches gilt für die Schwärzung auf S. 88, letzter Absatz. Dort nennt Atos ein bestimmtes einzusetzendes Produkt und beschreibt dessen Eigenschaften. Dies lässt ebenfalls Rückschlüsse auf die Architektur zu.

Ziffer 5h), S. 89 (Integration von Daten in die S.A.F.E.-Infrastruktur):

Hier wird ebenfalls ein von Atos eingesetztes Produkt beschrieben, so dass dies als Geschäfts- und Betriebsgeheimnisse von Atos zu schwärzen ist.

Ziffer 5i), S. 91 (Integration von Daten in die S.A.F.E.-Infrastruktur):

Auch hier wird ein von Atos eingesetztes Produkt konkret benannt. Daher ist dies als Geschäfts- und Betriebsgeheimnisse von Atos zu schwärzen.

Ziffer 5j), S. 92 (Ablösung des BRAV durch die S.A.F.E.-Domain):

Die Beschreibung der beabsichtigten Vorgehensweise zur Datenmigration sowie die Details der vorgeschlagenen Lösung sind als Geschäfts- und Betriebsgeheimnisse von Atos zu schwärzen.

Ziffer 5k), S. 93 und 94 (Übergabe von Daten der Kammersoftwareprodukte):

Der individuelle Lösungsvorschlag von Atos im letzten Absatz auf S. 93 zur Übergabe von Daten der Kammersoftwareprodukte stellt ebenfalls ein zu schwärzendes Geschäfts- und Betriebsgeheimnis von Atos dar. Gleiches gilt für das Schaubild auf S. 94 (oben) und die darunter folgende geschwärzte Beschreibung der diesbezüglichen Architektur.

Ziffer 5l), S. 95 und 96 (Autorisierung und Authentifizierung der Benutzer):

Die geschwärzten Passagen auf den S. 95 und 96 (einschließlich des Schaubilds auf S. 96) benennen und beschreiben den Einsatz und die Funktionsweise eines bestimmten Standard-Produkts, das Rückschlüsse auf die Gesamtarchitektur zulässt, so dass ein Geschäfts- und Betriebsgeheimnis vorliegt. Sie enthalten zudem sicherheitsrelevante Informationen.

Ziffer 6), S. 98 bis 100 (Anforderungsbereich Informationssicherheit):

Die Schwärzungen auf S. 98 enthalten Angaben zu den Funktionalitäten und den genauen Verfügbarkeiten und Reaktionszeiten einer von Atos von einem Subunternehmen dazugekauften Software-Lösung. Diese Produktinformationen zählen zu den Geschäfts- und Betriebsgeheimnissen des Subunternehmens. Zudem zählt die Information, welche Lösung Atos genau zugekauft hat zum Spezialwissen von Atos zur Durchführung derartiger Projekte und ist somit auch ein Geschäftsgeheimnis von Atos.

Die Schwärzungen auf S. 99 beinhalten jeweils konkrete Produkte, die Atos bei der Leistungserbringung einsetzen möchte. Die Information, welche Produkte bei einem solchen IT-Projekt sinnvoll eingesetzt werden können, ist Spezialwissen von Atos, welches Mitbewerbern bei möglichen künftigen IT-Ausschreibungen einen Vorteil verschaffen könnte. Entsprechend sind diese Angaben als Geschäfts- und Betriebsgeheimnisse von Atos geschwärzt. Weiterhin ermöglicht die Information über konkret eingesetzte Produkte genaue Rückschlüsse auf die Kalkulation von Atos und ist auch aus diesem Grund als Geschäftsgeheimnis von Atos zu bewerten.

Die Schwärzung auf S. 100 enthält eine sicherheitsrelevante Beschreibung des Systemverhaltens des beA. Die beschriebenen Funktionalitäten können nicht veröffentlicht werden, da diese Informationen ggf. für den Versuch eines Angriffs auf das System verwendet werden könnten.

Ziffer 6a), S. 101 und 102 (Erfüllung der Sicherheitsziele):

Die erste Schwärzung im 1. Unterpunkt auf S. 101 beinhaltet die Nennung eines konkreten von Atos zur Leistungserbringung eingesetzten Produkts. Die Information, welche Produkte bei einem solchen IT-Projekt sinnvoll eingesetzt werden können, ist Spezialwissen von Atos, welches Mitbewerbern bei möglichen künftigen IT-Ausschreibungen einen Vorteil verschaffen könnte. Entsprechend sind diese Angaben als Geschäfts- und Betriebsgeheimnisse von Atos geschwärzt. Weiterhin ermöglicht die Information über konkret eingesetzte Produkte genaue

Rückschlüsse auf die Kalkulation von Atos und ist auch aus diesem Grund als Geschäftsgeheimnis von Atos zu bewerten.

Die weitere Schwärzung im 1. Unterpunkt sowie die Schwärzungen im 2. und 3. Unterpunkt auf S. 101 beinhalten sicherheitsrelevante Aspekte des beA-Systems. Konkret wird dargestellt, wie die Ver- und Entschlüsselung der Datenbanken funktioniert und ein unberechtigter Zugriff verhindert wird. Zudem wird die eingesetzte Lösung zur Absicherung der Verbindung zwischen Kanzleisoftware und beA sowie bei der Kommunikation des beA mit Drittsystemen dargestellt. Diese Informationen sind weiterhin für die Sicherheit des Systems relevant und könnten von einem Angreifer ggf. missbraucht werden. Entsprechend können die Informationen nicht veröffentlicht werden.

Die Schwärzung im zweiten Punkt (oben auf S. 102) beinhaltet eine Beschreibung der im System automatisierten Überprüfung der Integrität von Journalen gegenüber Manipulationen. Diese Beschreibung könnte von einem Angreifer ggf. zur Manipulation der Journale benutzt werden und ist somit als sicherheitsrelevant für das System einzustufen. Zusätzlich enthält der Abschnitt die Information über eine eingesetzte Software-Lösung. Die Information welche Software-Lösung bei einem derartigen Projekt für die Sicherstellung der Integrität der Datenbestände sinnvoll eingesetzt werden kann ist Spezialwissen von Atos, welches Mitbewerbern bei möglichen künftigen IT-Ausschreibungen einen Vorteil verschaffen könnte. Zudem könnte die Information Rückschlüsse auf die Kalkulation von Atos ermöglichen. Daher sind diese Informationen als Geschäftsgeheimnisse von Atos zu bewerten.

Die Schwärzung im fünften Punkt (unten S. 102) stellt dar, wie das System gegen unbefugte Manipulationsversuche geschützt ist. Diese Information ist sicherheitsrelevant für das beA und könnte unter Umständen von Angreifern missbraucht werden. Daher kann die Information nicht herausgegeben werden.

<u>Ziffer 6b), S. 104 (Authentifizierungsmittel):</u>

Die Schwärzungen in diesem Abschnitt betreffen namentliche Nennungen von Vertragspartnern von Atos sowie konkret eingesetzten Software-Lösungen von Drittanbietern. Die

Informationen, welche Software-Lösungen bei einem solchen IT-Projekt sinnvoll eingesetzt werden können, sowie welche Drittanbieter verlässliche Vertragspartner sind, sind Spezialwissen von Atos, welches Mitbewerbern bei möglichen künftigen IT-Ausschreibungen einen Vorteil verschaffen könnte. Entsprechend sind diese Angaben als Geschäfts- und Betriebsgeheimnisse von Atos geschwärzt. Weiterhin ermöglichen diese Informationen über konkret eingesetzte Produkte genaue Rückschlüsse auf die Kalkulation von Atos und sind auch aus diesem Grund als Geschäfts- und Betriebsgeheimnisse von Atos zu bewerten.

Ziffer 6c), S. 105 und 106 (erstes Anmelden eines Benutzers):

Die Schwärzungen in dieser Ziffer betreffen Vorschläge von Atos für einen Erstregistrierungsprozess der Postfachbesitzer und der Nutzer. Diese Vorschläge wurden später so nicht umgesetzt. Das bedeutet, dass der vorgeschlagene Weg den Nutzern des beA nicht bekannt ist und von Atos in einem späteren vergleichbaren Projekt erneut verwendet werden könnte. Die Vorschläge könnten von Mitbewerbern bei einer künftigen IT-Ausschreibung kopiert werden. Die Informationen sind somit als Geschäftsgeheimnisse von Atos unkenntlich zu machen.

Ziffer 6e), S. 109 und 110 (manipulationsfreier und geheimer Nachrichtentransport):

Die Schwärzung im dritten Absatz auf der S. 109 beinhaltet die Nennung eines konkreten von Atos zur Leistungserbringung eingesetzten Produkts. Die Information, welches Produkt bei einem solchen IT-Projekt für den Authentifizierungsvorgang sinnvoll eingesetzt werden kann, ist Spezialwissen von Atos, welches Mitbewerbern bei möglichen künftigen IT-Ausschreibungen einen Vorteil verschaffen könnte. Entsprechend ist diese Angabe als Geschäftsgeheimnis von Atos geschwärzt. Weiterhin ermöglicht die Information über konkret eingesetzte Produkte genaue Rückschlüsse auf die Kalkulation von Atos und ist auch aus diesem Grund als Geschäftsgeheimnis von Atos zu bewerten.

Die Schwärzung im unteren Bereich der S. 109 beinhaltet eine genaue Beschreibung des beim beA eingesetzten Verfahrens zur Sicherstellung der Ende-zu-Ende-Verschlüsselung beim Nachrichtenexport. Diese Information ist weiterhin

sicherheitsrelevant für das beA und könnte von einem Angreifer ggf. beim Versuch des unberechtigten Zugriffs auf Nachrichten missbraucht werden. Daher kann die Information nicht veröffentlicht werden.

Die Schwärzung am Ende von S. 110 beinhaltet das eingesetzte Verfahren zur Absicherung der Kommunikation von Komponenten des beA untereinander. Die Kenntnis über das genau verwendete Verfahren könnte ein Angreifer ggf. missbrauchen. Entsprechend können diese sicherheitsrelevanten Informationen nicht veröffentlicht werden.

Ziffer 6g), S. 112 und 113 (stabiles Reaktionsverhalten):

Die Schwärzung oben auf S. 112 enthält den Namen eines von Atos eingesetzten Produktes. Die Information, welches Produkt bei einem solchen IT-Projekt für den Authentifizierungsvorgang sinnvoll eingesetzt werden kann, ist Spezialwissen von Atos, welches Mitbewerbern bei möglichen künftigen IT-Ausschreibungen einen Vorteil verschaffen könnte. Entsprechend ist diese Angabe als Geschäftsgeheimnis von Atos geschwärzt. Weiterhin ermöglicht die Information über konkret eingesetzte Produkte genaue Rückschlüsse auf die Kalkulation von Atos und ist auch aus diesem Grund als Geschäftsgeheimnis von Atos zu bewerten.

Die Schwärzungen in der Mitte der S. 112 (Grafik), unten auf S. 112 und auf S. 113 bis vor „Herausforderungen" enthalten detaillierte Darstellungen und Beschreibungen des wesentlichen Systemaufbaus des beA. Der dargestellte Aufbau zeigt den wesentlichen Kern des beA-Systems, der für den Anwender nicht ersichtlich ist. Die dargestellten Informationen sind sicherheitsrelevant und könnten ggf. für Angriffe auf die Verfügbarkeit des Systems missbraucht werden. Zudem beinhalten sie konkrete Informationen zu dem von Atos erstellten Angebot und unterliegen somit der vergaberechtlichen Verschwiegenheit. Weiterhin beinhaltet die Darstellung Geschäfts- und Betriebsgeheimnisse von Atos, da Atos die vorgeschlagene Architektur des beA auch bei künftigen Ausschreibungen vorschlagen kann.

Die Schwärzungen in der unteren Hälfte von S. 113 enthalten Informationen zum Aufbau des beA zur Sicherstellung der Ende-zu-

Ende-Verschlüsselung von Nachrichten bei gleichzeitiger Übertragung großer Nachrichten auf den Server von vielen Nutzern. Die dargestellten Informationen sind sicherheitsrelevant und könnten ggf. für Angriffe auf die Verfügbarkeit des Systems missbraucht werden. Zudem beinhalten sie konkrete (für die Nutzer nicht ersichtliche) Informationen zu dem von Atos erstellten Angebot und unterliegen somit der vergaberechtlichen Verschwiegenheit. Weiterhin beinhaltet die Darstellung Geschäfts- und Betriebsgeheimnisse von Atos, da Atos die vorgeschlagene Architektur des beA auch bei künftigen Ausschreibungen vorschlagen kann.

Ziffer 6h), S. 115 (Minimierung Datenverlust):

Bei der Schwärzung oben auf S. 115 (vor „Skalierbarkeit und Ausfallsicherheit der Lösung") handelt es sich um eine Beschreibung der Lösungsarchitektur hinsichtlich einer möglichst effizienten Speicherung von neuen bearbeiteten Nachrichten durch Atos. Die dargestellten Maßnahmen sind für Nutzer nicht direkt einsehbar und können von Atos bei künftigen ähnlichen IT-Projekten ebenfalls verwendet werden. Die Informationen können somit als Geschäftsgeheimnisse von Atos nicht herausgegeben werden.

Bei der Schwärzung im Abschnitt „Skalierbarkeit und Ausfallsicherheit der Lösung" auf S. 115 handelt es sich um eine Beschreibung der Betriebsarchitektur, die nicht nur für das beA-System, sondern auch für vergleichbare Systeme genutzt werden kann. Die dargestellten Maßnahmen zur Ausfallsicherheit der Lösung sind von Nutzern nicht direkt einsehbar und somit als Geschäfts- und Betriebsgeheimnisse von Atos geschützt.

Ziffer 7), S. 116 (Anforderungsbereich „Dokumentation"):

Die Schwärzung auf S. 116 beinhaltet die Beschreibung des Verfahrens bei Atos zur Erstellung und Gliederung von Dokumenten sowie generell zur Durchführung von Kundenprojekten. Diese Informationen zu internen Arbeitsabläufen könnten von Mitbewerbern bei künftigen Ausschreibungen zum Nachteil von Atos verwendet werden und stellen somit Geschäfts- und Betriebsgeheimnisse von Atos dar.

Ziffer 7a), S. 118 (Vorgehensweise zur Erstellung der Dokumentationen):

In dem geschwärzten Abschnitt stellt Atos das Verfahren zur Erstellung und Gliederung von Dokumenten sowie generell zur Durchführung von Kundenprojekten detailliert dar. Dies umfasst unter anderem eine genaue Darstellung der verschiedenen Projektabschnitte, der jeweiligen Beteiligung verschiedener Funktionen an den Abschnitten, die Definition des Zielbilds der Dokumentation sowie einen Prüfprozess. Diese Informationen zu internen Arbeitsabläufen und Betriebsinterna könnten von Mitbewerbern bei künftigen Ausschreibungen zum Nachteil von Atos verwendet werden und stellen somit Geschäfts- und Betriebsgeheimnisse von Atos dar.

Ziffer 7c) S. 123 (Gliederung der Betriebsdokumentation)

Die geschwärzten Stellen geben wieder, welche Komponenten eines Drittanbieters konkret bei der Entwicklung des beA zum Einsatz kommen sollten. Die Information, welche konkreten Drittanbieter-Komponenten Atos einsetzte, lassen Rückschlüsse auf die Kalkulation von Atos zu. Außerdem gehört es zum Spezialwissen von Atos, welche Produkte und Komponenten sich bei der Durchführung eines solchen Projekts am besten eignen. Die Information war somit als Betriebs- und Geschäftsgeheimnis zu schwärzen.

Ziffer 7f), S. 130 und 131 (Funktionsweise der Online-Hilfe):

Die geschwärzten Bereiche in dieser Ziffer sind beispielhafte Entwürfe für Benutzeroberflächen der Online-Hilfe, die in der Form im beA nicht umgesetzt wurden. Da die meisten IT-Projekte die eine oder andere Art von Online-Hilfe beinhalten, können diese Entwürfe von Atos ganz oder in Teilen bei künftigen IT-Ausschreibungen mit eingereicht werden und sind somit Geschäfts- und Betriebsgeheimnisse von Atos.

Ziffer 7g), S. 134 (Fortschreibung und Bearbeitung der Online-Hilfe):

Die geschwärzten Bereiche in dieser Ziffer sind beispielhafte Entwürfe für Benutzeroberflächen der Online-Hilfe, die in der Form im beA nicht umgesetzt wurden. Da die meisten IT-Projekte die ein

oder andere Art von Online-Hilfe beinhalten, können diese Entwürfe von Atos ganz oder in Teilen bei künftigen IT-Ausschreibungen mit eingereicht werden und sind somit Geschäfts- und Betriebsgeheimnisse von Atos.

Ziffer 9), S. 141 (Anforderungsbereich „Maßnahmen zur Inbetriebnahme"):

Die Schwärzung in dieser Ziffer beinhaltet eine Darstellung der Qualifikation und Erfahrungswerte der für Tests zuständigen Mitarbeiter bei Atos. Diese Informationen sind Betriebsinterna und somit Betriebsgeheimnisse von Atos.

Ziffer 9a), S. 143 bis 146 (Vorgehen bei der Definition, Durchführung und Dokumentation von Testfällen):

Die Schwärzungen der Bullet Points auf S. 143 beinhalten eine Darstellung des geplanten Testaufbaus von Atos, insbesondere eine Definition der Testfälle sowie die Herangehensweise von Atos an diese Testfälle. Die Teststrategie von Atos ist für Nutzer des beA nicht ersichtlich und kann bei künftigen anderen IT Projekten in gleicher Art und Weise oder leicht angepasst von Atos wieder verwendet werden. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Betriebsgeheimnisse von Atos und unterliegen zudem der vergaberechtlichen Verschwiegenheit.

Die Schwärzung im vorletzten Absatz auf S. 143 beinhaltet den Namen einer von Atos eingesetzten IT-Lösung. Die Information, welches Produkt bei einem solchen IT-Projekt als Testmanagement-Tool sinnvoll eingesetzt werden kann, ist Spezialwissen von Atos, welches Mitbewerbern bei möglichen künftigen IT-Ausschreibungen einen Vorteil verschaffen könnte. Entsprechend ist diese Angabe als Geschäftsgeheimnis von Atos geschwärzt. Weiterhin ermöglicht die Information über konkret eingesetzte Produkte genaue Rückschlüsse auf die Kalkulation von Atos und ist auch aus diesem Grund als Geschäftsgeheimnis von Atos zu bewerten.

Die Schwärzung im letzten Absatz auf S. 143 sowie auf S. 144 oben bis zum Abschnitt „Durchführung von Testfällen" beinhaltet eine Grafik und eine genauere Beschreibung zum Verfahren von Atos zur Bestimmung und Einordnung von Testfällen und der entsprechend notwendigen Tests für einzelne Bereiche der Software. Die dargestellte Teststrategie von Atos ist für Nutzer des beA nicht ersichtlich und kann bei künftigen anderen IT Projekten in gleicher Art und Weise oder leicht angepasst von Atos wieder verwendet werden. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Betriebsgeheimnisse von Atos und unterliegen zudem der vergaberechtlichen Verschwiegenheit.

Die Schwärzungen im Abschnitt „Durchführung von Testfällen" auf den S. 144 und 145 beschreiben das genaue Testvorgehen von Atos. Dabei ist in drei Grafiken beispielhaft dargestellt wie Atos plant die Testfortschritte zu verfolgen, sowie die Fehler zu erfassen und deren Entwicklung zu dokumentieren. Die dargestellte Teststrategie von Atos ist für Nutzer des beA nicht ersichtlich und kann bei künftigen anderen IT Projekten in gleicher Art und Weise oder leicht angepasst von Atos wieder verwendet werden. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Betriebsgeheimnisse von Atos und unterliegen zudem der vergaberechtlichen Verschwiegenheit. Zusätzlich können informierte Leser aus den Abbildungen und den Bildunterschriften ableiten, welche Tools Atos zur Durchführung und Dokumentation der Tests verwendet. Auch diese Information ist ein Geschäftsgeheimnis von Atos, da es Spezialwissen darstellt, welche IT-Lösungen für Tests bei einem derartigen IT-Projekt besonders geeignet sind.

Die Schwärzungen im Abschnitt „Dokumentation von Testfällen" auf den S. 145 und 146 beschreiben genau die Dokumentation von Tests durch Atos. Dabei wird in zwei Grafiken beispielhaft dargestellt, wie Atos plant die Testfortschritte zu dokumentieren.

Die Teststrategie von Atos ist für Nutzer des beA nicht ersichtlich und kann bei künftigen anderen IT Projekten in gleicher Art und Weise oder leicht angepasst von Atos wieder verwendet werden. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Geschäfts- und Betriebsgeheimnisse von Atos und unterliegen zudem der vergaberechtlichen Verschwiegenheit. Zusätzlich ergibt sich aus dem Text und den Abbildungen, welche Tools Atos zur Dokumentation der Tests verwendet. Auch diese Information ist ein Geschäftsgeheimnis von Atos, da es Spezialwissen darstellt, welche IT-Lösungen für Tests bei einem derartigen IT-Projekt besonders geeignet sind.

Ziffer 9b), S. 147 und 148 (Smoketests, Whitebox-Tests, Blackbox-Tests, Integrations- und Lasttests):

Die Schwärzungen in dieser Ziffer enthalten konkrete Beschreibungen des Testvorgehens von Atos inklusive der Definition verschiedener Testphasen und der Darstellung welche Testmethoden und Testtypen in den jeweiligen Phasen eingesetzt werden. Die Beschreibungen werden durch zwei Grafiken unterstützt. Die dargestellte Teststrategie von Atos ist für Nutzer des beA nicht ersichtlich und kann bei künftigen anderen IT Projekten in gleicher Art und Weise oder leicht angepasst von Atos wieder verwendet werden. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Geschäfts- und Betriebsgeheimnisse von Atos und unterliegen zudem der vergaberechtlichen Verschwiegenheit.

Ziffer 9c), S. 149 und 151 (Standard-Vorgehen zur Fehlerbehebung):

Die Schwärzung im ersten Abschnitt auf S. 149 beinhaltet den Namen einer von Atos eingesetzten Software-Lösung zu einer effizienten Kommunikation zwischen allen Beteiligten bei der Entwicklung. Die Information, welches Produkt bei einem solchen

IT-Projekt als Kommunikationsplattform sinnvoll eingesetzt werden kann, ist Spezialwissen von Atos, welches Mitbewerbern bei möglichen künftigen IT-Ausschreibungen einen Vorteil verschaffen könnte. Entsprechend ist diese Angabe als Geschäftsgeheimnis von Atos geschwärzt. Weiterhin ermöglicht die Information über konkret eingesetzte Produkte genaue Rückschlüsse auf die Kalkulation von Atos und ist auch aus diesem Grund als Geschäfts- und Betriebsgeheimnis von Atos zu bewerten.

Die beiden geschwärzten Grafiken auf S. 149 und 151 enthalten genaue Darstellungen des Test- und Fehlerbehebungsprozesses sowie des vorgesehenen Fehlerlebenszyklusses. Die dargestellte Teststrategie von Atos ist für Nutzer des beA nicht ersichtlich und kann bei künftigen anderen IT Projekten in gleicher Art und Weise oder leicht angepasst von Atos wieder verwendet werden. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Betriebsgeheimnisse von Atos und unterliegen zudem der vergaberechtlichen Verschwiegenheit.

Ziffer 9d), S. 152 und 153 (Auswertung der Tests):

Die Schwärzungen in diesem Abschnitt enthalten eine detaillierte Beschreibung des Vorgehens von Atos bei Tests, inklusive einer Darstellung der üblichen Fehlerbeschreibungen, der Fehleranalyse und -bewertung, dem Vorgehen zur künftigen Fehlervermeidung sowie eines Feedback-Prozesses. Die dargestellte Teststrategie von Atos ist für Nutzer des beA nicht ersichtlich und kann bei künftigen anderen IT Projekten in gleicher Art und Weise oder leicht angepasst von Atos wieder verwendet werden. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Betriebsgeheimnisse von Atos und unterliegen zudem der vergaberechtlichen Verschwiegenheit.

Ziffer 9e), S. 154 bis 156 (Pilottests zu den Oberflächen sowie die Tests mit den Kanzleien und der Justiz):

Die Schwärzungen in diesem Abschnitt enthalten eine detaillierte Beschreibung der Integrationstests und Pilottests. Die Beschreibung enthält konkrete Informationen zur Testplanung (inklusive einer Grafik zu Meilensteinen bzgl. der Tests), zur Durchführung der Oberflächentests, der Testung der Schnittstellen zur Justiz (inklusive der Beteiligung der Justiz an diesen Tests) und der Testphase mit Kanzleien. Diese Informationen enthalten eine Auskunft auf konkret im Vergabeverfahren gestellte Fragen zu den Tests, insbesondere zum Integrationstest, die auf die Bewertung des Angebots Einfluss hatten und unterliegen somit der vergaberechtlichen Verschwiegenheitsverpflichtung. Das dargestellte Vorgehen kann ohne große Änderungen auf alle Entwicklungsprojekte von IT-Systemen übertragen werden und ist somit nicht nur für das beA relevant. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Geschäfts- und Betriebsgeheimnisse von Atos.

Ziffer 9g), S. 158 (Unterstützung der Inbetriebnahme):

Die Schwärzung im Abschnitt „Unterstützung bei der Inbetriebnahme" beschreibt konkret, wie Atos die Beklagte bei der Inbetriebnahme des Systems unterstützt und welche Zeiträume hierfür eingeplant sind. Die Unterstützung bei der Inbetriebnahme ist bei allen IT-Projekten vergleichbar und somit unabhängig vom beA von Bedeutung. Die Angaben von Atos zum konkreten Vorgehen sind als Spezialwissen von Atos Betriebsgeheimnisse und somit nicht herauszugeben.

In der Schwärzung unten auf S. 158 findet sich eine detaillierte Beschreibung mit welchen Maßnahmen die Unterstützung der Beklagten erfolgen soll. Diese Beschreibung lässt Rückschlüsse auf das Entwicklungs- und Testvorgehen von Atos zu. Damit handelt es sich bei den Informationen in diesem Abschnitt um Betriebsgeheimnisse von Atos, da es sich nicht um beA-spezifische Maßnahmen handelt. Das dargestellte Vorgehen kann ohne große Änderungen auf alle Entwicklungsprojekte von IT-Systemen übertragen werden.

Ziffer 9h), S. 159 bis 161 (Tests für die Prüfung der Ausfallsicherheit und zur Wiederherstellung des Regelbetriebs):

Die Schwärzungen auf S. 159 enthalten eine Grafik und eine Tabelle die jeweils detailliert die Systemarchitektur des beA beschreiben. Die beim beA eingesetzte Systemarchitektur ist – jedenfalls in der Detailtiefe – für Nutzer des beA nicht ersichtlich. Der genaue Aufbau der Systemarchitektur des beA ist sicherheitsrelevant und kann nicht veröffentlicht werden. Zudem handelt es sich dabei um ein Betriebsgeheimnis von Atos, da Atos bei künftigen IT-Projekten die Grundstruktur des Aufbaus ebenfalls einsetzen kann.

Die Schwärzungen auf S. 160 sowie oben im ersten Absatz auf S. 161 beinhalten eine genaue Beschreibung des Vorgehens von Atos bei Ausfalltests. Die dargestellte Teststrategie von Atos ist für Nutzer des beA nicht ersichtlich und kann bei künftigen anderen IT Projekten in gleicher Art und Weise oder leicht angepasst von Atos wieder verwendet werden. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Betriebsgeheimnisse von Atos und unterliegen zudem der vergaberechtlichen Verschwiegenheit.

Die Schwärzung auf S. 161 unter der Überschrift „Rahmenbedingungen" beinhaltet eine Aufzählung der Voraussetzungen an die Tests und Anforderungen an Mitwirkungsleistungen der Beklagten. Daraus lassen sich einerseits Rückschlüsse auf die Kalkulation von Atos ziehen, welche ein Geschäftsgeheimnis von Atos ist. Andererseits ist die Teststrategie von Atos für Nutzer des beA nicht ersichtlich und kann bei künftigen anderen IT Projekten in gleicher Art und Weise oder leicht angepasst von Atos wieder verwendet werden. Somit könnten Mitbewerber von Atos die Informationen dazu verwenden, sich bei künftigen IT-Ausschreibungen einen Vorteil gegenüber Atos zu verschaffen, indem sie die Teststrategie kopieren oder ihr eigenes Angebot auf die Teststrategie von Atos anpassen. Die Informationen sind somit Geschäfts- und Betriebsgeheimnisse von Atos und unterliegen zudem der vergaberechtlichen Verschwiegenheit.

Ziffer 10), S. 162 (Anforderungsbereich „Softwarepflege und Wartung"):

Die Schwärzungen enthalten eine Beschreibung des internen Standards bei Atos für das Release von Software-Lösungen sowie für die Erbringung von Support-Leistungen. Diese Standards gelten bei Atos für alle IT-Projekte, unabhängig vom beA. Somit können diese Informationen über interne Standards bei künftigen IT-Ausschreibungen den Mitbewerbern von Atos Vorteile verschaffen, da sie ihre eigenen Angebote darauf anpassen können. Die Informationen über diese Standards sind somit als Geschäfts- und Betriebsgeheimnisse von Atos zu bewerten.

Ziffer 10a), S. 163 (Release-Planung und deren Aktualisierung):

Die Schwärzungen in diesem Abschnitt enthalten eine detaillierte Beschreibung des Release-Managements sowie eine grafische Darstellung des Releasezyklusses bei Atos. Diese Standards gelten bei Atos für alle IT-Projekte, unabhängig vom beA. Somit können diese Informationen über interne Standards bei künftigen IT-Ausschreibungen den Mitbewerbern von Atos Vorteile verschaffen, da sie ihre eigenen Angebote darauf anpassen können. Die Informationen über diese Standards sind somit als Geschäfts- und Betriebsgeheimnisse von Atos zu bewerten.

Ziffer 10b), S. 165 (Third-Level-Support):

Die geschwärzten Abschnitte enthalten konkrete Darstellungen des von Atos angebotenen Third-Level-Support, inklusive eines Vorschlags von Atos für die Zusammenarbeit zwischen Atos und der Beklagten im Rahmen des Third-Level-Supports. Diese von Atos vorgeschlagenen Lösungen zum Third-Level-Support sind für die Nutzer des beA nicht einsehbar und können von Atos bei künftigen IT-Ausschreibungen in der Form ebenfalls in das Angebot integriert werden. Somit sind die von Atos dargestellten konkreten Vorschläge zum Third-Level-Support als Betriebsgeheimnis von Atos zu bewerten. Zudem lassen die Vorschläge zum genauen Umfang des Third-Level-Supports und der Zusammenarbeit mit der Beklagten klare Rückschlüsse auf die Kalkulation von Atos zu und sind somit auch Geschäfts- und Betriebsgeheimnisse von Atos.

Ziffer 10c), S. 166 (Umsetzung von Changes, Service-Requests und die Problembehandlung als Third-Level-Support):

Der geschwärzte Abschnitt enthält eine genaue Beschreibung der internen Vorgänge bei Atos bei der Bearbeitung von Service Requests. Diese internen Vorgänge sind von Nutzern des beA nicht einsehbar und können unabhängig vom beA für alle größeren IT-Projekte bei Atos eingesetzt werden. Entsprechend handelt es sich dabei um Betriebsgeheimnisse von Atos, die nicht herausgegeben werden können.

Ziffer 11), S. 167 und 168 (Anforderungsbereich „Erweiterungen"):

Die Schwärzungen in diesem Abschnitt enthalten detaillierte Hinweise auf die beim beA verwendete Systemarchitektur sowie eingesetzte Methoden, die bei Atos nicht nur für beA, sondern für alle IT-Projekte eingesetzt werden. Diese Informationen könnten somit bei künftigen IT-Ausschreibungen von Mitbewerbern ggf. zum Nachteil von Atos eingesetzt werden. Sie sind als Betriebsgeheimnisse von Atos somit zu schwärzen.

Ziffer 11a), S. 169 bis 171 (Änderbarkeit/Erweiterbarkeit des Systems):

In den geschwärzten Abschnitten beschreibt Atos detailliert verschiedene bei Atos eingesetzte Modelle zum Qualitätsmanagement, zur Softwareentwicklung und zum Einsatz von Unit-Tests. Zudem sind zwei Abbildungen geschwärzt, welche die Beschreibungen bildlich untermalen und die von Atos zum Qualitätsmanagement verwendeten Programme zeigen. Diese Informationen sind Spezialwissen von Atos, das für die Nutzer des beA nicht ersichtlich ist, Die eingesetzten Standards zur Qualitätssicherung, Entwicklung und Testung verwendet Atos nicht nur beim beA, sondern bei allen IT-Projekten. Entsprechend sind die Informationen als Betriebsgeheimnisse von Atos zu schwärzen.

Ziffer 11b), S. 172 und 173 (Übergabe in ein neues Umfeld):

In den geschwärzten Abschnitten beschreibt Atos detailliert das übliche Vorgehen bei der Entwicklung von individuellen Software-Lösungen für Kunden unter Darstellung der einzelnen Prozessschritte, der jeweils eingesetzten Standards, der

Zusammenarbeit zwischen den Bereichen und mit dem jeweiligen Kunden. Die Beschreibung wird von zwei Abbildungen bildlich unterstützt. Diese Informationen sind Spezialwissen von Atos, das für die Nutzer des beA nicht ersichtlich ist. Die beschriebenen Prozesse verwendet Atos nicht nur beim beA, sondern bei allen IT-Projekten. Entsprechend sind die Informationen als Betriebsgeheimnisse von Atos zu schwärzen.

d) Anlage Nr. 2 a) – Zusatzvereinbarung für öffentliche Auftraggeber zum Vertriebsvertrag für Full Use Programme

Die Anlage 2 a) wird bis auf die Namen und Unterschriften auf der letzten Seite vollständig offengelegt. Bei den Namen und Unterschriften handelt es sich um personenbezogene Daten, die gemäß § 5 Abs. 1 IFG nicht offengelegt werden. Das Informationsinteresse des Klägers an diesen Informationen ist als sehr zu gering zu bewerten und überwiegt somit nicht das Interesse der benannten Personen am Ausschluss des Informationszugangs.

e) Anlage Nr. 3 a) – Verhandlungsprotokoll vom 16.09.2014

Anlage Nr. 3 a) enthält das Protokoll der Verhandlungen zwischen der Beklagten und Atos vom 16.09.2014. In der Verhandlung besprachen Atos und die Beklagte den Einsatz verschiedener Standardsoftware-Produkte sowie Open Source-Software bei der Entwicklung des beA. Insbesondere wurde diskutierte, in welchem Umfang und unter welchen Voraussetzungen Atos diesbezüglich Lizenzen auf die Beklagte übertragen kann und muss. Dabei wurden insbesondere auch die Vertragsverhältnisse von Atos zu diversen Dienstleistern thematisiert sowie die Frage, welche Leistungen von Atos direkt oder aber von einem Drittanbieter erbracht werden. Zudem wurden Einzelheiten zur Hinterlegung des Quellcodes als Insolvenzschutz für die Beklagte diskutiert. Weiterhin wurde über die folgenden Themen verhandelt: Reaktionszeiten von Atos bei Ausfällen, Beistellungsleistungen der Beklagten, die Migration des beA, Einzelheiten zur Abnahme, inhaltliche Klarstellungen zum Sicherheitskonzept, den Reaktionszeiten und dem Aufbau des beA. Anschließend wurden die Auswirkungen der besprochenen Themen

auf das Preisblatt verhandelt und abschließend der weitere Zeitplan festgelegt.

Die Anlage Nr. 3 a) enthält Geschäfts- und Betriebsgeheimnisse von Atos und kann daher insgesamt nicht offengelegt werden. In dem Verhandlungsgespräch wurde das Angebot von Atos konkretisiert, entsprechend unterliegt das Protokoll zudem der Verschwiegenheitsverpflichtung aus §§ 105, 55 BHO, Ziffer 2.3.2 und 3.1.1 VV zu § 55 BHO i.V.m. § 14 Abs. 3 VOL/A, § 3 Nr. 4 IFG.

Die den Bietern gestellten Fragen waren in den Verhandlungsgesprächen mit den einzelnen Bietern unterschiedlich. Auch die Protokolle wurden für alle Bieter getrennt und individuell erstellt, d.h. die Beklagte hat die Verhandlungsgespräche anhand der Angebote individuell vorbereitet, so dass sich für jeden Bieter unterschiedliche Fragen stellten. Aus einer Veröffentlichung der gestellten Fragen und des Verhandlungsverlaufs könnten Mitbewerber von Atos Vergleiche zu ihren eigenen Angeboten und Verhandlungsgesprächen ziehen und sich das Wissen für künftige Vergabeverfahren zunutze machen. Somit unterliegt das komplette Verhandlungsprotokoll der vergaberechtlichen Verschwiegenheit.

Die Anlage enthält zunächst sehr konkrete Informationen darüber, wie Atos sich in Verhandlungen bei der Ausschreibung großer IT-Projekte verhält. Diese Information kann von Mitbewerbern oder künftigen Auftraggebern bei künftigen Ausschreibungen zu Lasten von Atos verwendet werden und ist somit ein Geschäftsgeheimnis von Atos.

Zudem lässt die in der Anlage dargestellte Verhandlung in Bezug auf den Einfluss der besprochenen Leistungsänderungen auf das Preisblatt sehr genaue Rückschlüsse auf die Kalkulation und Preisgestaltung von Atos zu. Mitbewerber und künftige Auftraggeber von Atos könnten diese Informationen bei künftigen Ausschreibungen zu ihrem Vorteil nutzen. Insbesondere wäre es für Atos bei künftigen Aufträgen nur schwer in Verhandlungen durchzusetzen, schlechtere Bedingungen anzubieten, als bei diesem Projekt. Daher handelt es sich dabei um Geschäfts- und Betriebsgeheimnisse von Atos.

Weiterhin enthält die Anlage präzise Informationen zu bei der Entwicklung eingesetzten Softwarelösungen und den Vertragsverhältnissen zwischen Atos und Drittanbietern. Die Information, welche Dienstleister und welche Softwareprodukte bei einem solchen IT-Projekt besonders geeignet sind ist Spezialwissen von Atos und könnte von Mitbewerbern bei künftigen IT-Ausschreibungen sowie bei Verhandlungen mit Drittanbietern verwendet werden, um sich einen Vorteil zu verschaffen. Entsprechend handelt es sich dabei um Betriebs- und Geschäfts- und Betriebsgeheimnisse von Atos.

Zudem ergeben sich aus dem Protokoll klare Hinweise zu der Architektur des beA, die für Nutzer im front-end nicht ersichtlich sind. Diese Informationen, wie Atos das Portal aufgebaut hat sind Betriebsgeheimnisse von Atos.

f) Anlage Nr. 3 b) – Verhandlungsprotokoll vom 15.08.2014

Die Anlage Nr. 3 b) enthält das Verhandlungsprotokoll zwischen Atos und der Beklagten vom 15.08.2014. In der Verhandlung ging es um das konkrete Umsetzungskonzept von Atos, insbesondere um Sicherheitsaspekte des geplanten Systems. Die verhandelten Sicherheitsfragen betrafen dabei den Kern der Sicherheitsarchitektur. Im Einzelnen ging es um die genaue Ausgestaltung der Verschlüsselung verschiedener Bereiche des Systems, den Einsatz von bestimmter Drittanbieter-Software, Lösungsvorschlägen von Atos zu Problemen des Nachrichtenversands im beA, konkret durchzuführende Tests, Fragen zum Release-Management und der Fehlerbehebung sowie um konkrete Nachfragen zum Preisblatt.

Entsprechend kann das Protokoll nicht herausgegeben werden. Der Inhalt der Verhandlung unterliegt der vergaberechtlichen Verschwiegenheit. Zudem hat Atos im Rahmen der Verhandlung Geschäfts- und Betriebsgeheimnisse sowie Informationen, die auch heute noch sicherheitsrelevant für das System sind, mitgeteilt.

Die den Bietern gestellten Fragen waren in den Verhandlungsgesprächen mit den einzelnen Bietern unterschiedlich. Auch die Protokolle wurden für alle Bieter getrennt

und individuell erstellt. Aus einer Veröffentlichung der gestellten Fragen und des Verhandlungsverlaufs könnten Mitbewerber von Atos Vergleiche zu ihren eigenen Angeboten und Verhandlungsgesprächen ziehen und sich das Wissen für künftige Vergabeverfahren zunutze machen. Somit unterliegt das komplette Verhandlungsprotokoll der vergaberechtlichen Verschwiegenheit.

Die Anlage Nr. 3 b) enthält zunächst sehr detaillierte Informationen darüber, wie Atos sich in Verhandlungen bei der Ausschreibung großer IT-Projekte verhält. Diese Information kann von Mitbewerbern oder Auftraggebern bei künftigen Ausschreibungen zu Lasten von Atos verwendet werden und ist somit ein Geschäftsgeheimnis von Atos.

Zudem lässt die in der Anlage dargestellte Verhandlung in Bezug auf den Einfluss der besprochenen Konkretisierungen des Angebots und der direkten Besprechung von Nachfragen zum Preisblatt sehr genaue Rückschlüsse auf die Kalkulation und Preisgestaltung von Atos zu. Mitbewerber und künftige Auftraggeber von Atos könnten diese Informationen bei künftigen Ausschreibungen zu ihrem Vorteil nutzen. Insbesondere wäre es für Atos bei künftigen Aufträgen nur schwer in Verhandlungen durchzusetzen, schlechtere Bedingungen anzubieten als bei diesem Projekt. Daher handelt es sich dabei um Geschäfts- und Betriebsgeheimnisse von Atos.

Weiterhin enthält die Anlage präzise Informationen zu bei der Entwicklung eingesetzten Softwarelösungen und den Vertragsverhältnissen zwischen Atos und Drittanbietern. Die Information, welche Dienstleister und welche Softwareprodukte bei einem solchen IT-Projekt besonders geeignet sind, ist Spezialwissen von Atos und könnte von Mitbewerbern bei künftigen IT-Ausschreibungen sowie bei Verhandlungen mit Drittanbietern verwendet werden, um sich einen Vorteil zu verschaffen. Daher handelt es sich dabei um Geschäfts- und Betriebsgeheimnisse von Atos.

Des Weiteren ergeben sich aus dem Protokoll klare Hinweise zu der Architektur des beA, die für Nutzer im front-end nicht ersichtlich sind. Diese Informationen, wie Atos das Portal aufgebaut hat, sind Betriebsgeheimnisse von Atos.

Der Kern der Verhandlung betraf zudem verschiedene essentielle Sicherheitsaspekte des beA. Die besprochenen Vorschläge und Lösungsmöglichkeiten wurden großenteils im beA umgesetzt und sind somit weiterhin sicherheitsrelevant und können nicht veröffentlicht werden.

g) Anlage Nr. 4 – Preisblatt

Atos legt in den ausgefüllten Abschnitten des Preisblatts seine Kalkulation und die genaue Berechnung des Gesamtpreises offen. Es ist jeweils angegeben, in welchem Umfang Atos mit einzelnen Leistungen kalkuliert, sowie der konkrete Preis, den Atos hierfür verlangt.

Die Angaben von Atos zu den einzelnen Preiskomponenten lassen sehr genaue Rückschlüsse auf die Kalkulation von Atos zu. Diese Informationen sind Spezialwissen von Atos, welches von Mitbewerbern oder Auftraggebern bei künftigen IT-Ausschreibungen ggf. zum Nachteil von Atos verwendet werden kann. Einerseits können Mitbewerber aus den Informationen ableiten, wie Atos ein derartiges Projekt kalkuliert und künftig die eigene Kalkulation ähnlich gestalten. Andererseits könnten Mitbewerber aus den Informationen zur Kalkulation von Atos Rückschlüsse auf künftige Angebote von Atos bei Ausschreibungen von IT-Projekten ziehen und diese gezielt unterbieten. Daher sind die Informationen als Geschäfts- und Betriebsgeheimnisse von Atos zu bewerten. Zudem unterliegen sie als Teil des Angebots von Atos der Verschwiegenheitsverpflichtung aus §§ 105, 55 BHO, Ziffer 2.3.2 und 3.1.1 VV zu § 55 BHO i.V.m. § 14 Abs. 3 VOL/A, § 3 Nr. 4 IFG.

h) Anlage Nr. 6 – Sonderregelung zum Quellcode

Die Schwärzungen zu Beginn der Anlage enthalten Namen von Vertragspartnern von Atos, bzw. von einer von Atos bei der Auftragserfüllung verwendeten Standardsoftware.

Diese Informationen können Rückschlüsse auf die Kalkulation von Atos geben, da Mitbewerber daraus recht genau ableiten können, welche Kosten für Atos in Bezug auf die eingesetzten Dienstleister angefallen sind. Sie sind somit Geschäfts- und Betriebsgeheimnisse von Atos.

Zudem gehört es zum Spezialwissen von Atos, welche Softwarelösungen und welche Drittanbieter für bestimmte Spezialbereiche am besten geeignet sind. Diese Information würde Mitbewerbern bei künftigen IT-Ausschreibungen einen Vorteil verschaffen und ist als Betriebsgeheimnis von Atos zu bewerten.

Die Schwärzung im ersten Absatz von Ziffer 3 enthält eine genaue Benennung und Beschreibung der Bestandteile der von Atos eingesetzten Software-Lösung. Die sonstigen Schwärzungen in Ziffer 3 enthalten ebenfalls klare Hinweise auf die eingesetzten Software-Lösungen von Atos. Die Information, welche Software-Lösungen für die Erbringung der geforderten Leistungen am besten geeignet sind, ist Spezialwissen von Atos, welches den Mitbewerbern bei anderen IT-Ausschreibungen Vorteile bringen könnte (siehe oben).

i) Anlage Nr. 8 – Sonderregelung zu Verzug und Vertragsstrafe

Die geschwärzten Satzteile enthalten genauen Angaben zur Höhe der ausgehandelten Vertragsstrafe.

Diese Information zeigt, wie Atos bei derartigen großen IT-Projekten verhandelt und stellt somit Spezialwissen von Atos dar, welches Mitbewerbern bei künftigen Ausschreibungen von IT-Projekten einen Vorteil verschaffen würde. Die Frage, in welcher Höhe eine Vertragsstrafe für den Anbieter wirtschaftlich akzeptabel ist und vom Auftraggeber akzeptiert wird, ist bei IT-Großprojekten für Anbieter schwer zu beantworten. Bei Herausgabe der konkreten Höhe würden die Mitbewerber von Atos hier von den jahrelangen Erfahrungen von Atos profitieren.

Zudem lassen die Informationen zur genauen Vertragsstrafe zusammen mit den anderen herausgegebenen Informationen klare Rückschlüsse auf die Kalkulation von Atos zu. Dies würde es

Mitbewerbern ermöglichen, bei künftigen IT-Ausschreibungen das Angebot von Atos genauer voraussehen zu können und dies bei ihren eigenen Angeboten zu berücksichtigen.

j) Anlage Nr. 9 – Sonderregelung zur Sicherheitsleistung

Die geschwärzten Satzteile enthalten genauen Angaben zur Höhe der ausgehandelten Vertragserfüllungs- und Mängelhaftungssicherheit. Diese Information zeigt, wie Atos bei derartigen großen IT-Projekten verhandelt und stellt somit Spezialwissen von Atos dar, welches Mitbewerbern bei der Ausschreibung von künftigen IT-Projekten einen Vorteil verschaffen könnte. Wie hoch die Sicherheit sein muss, damit der Auftraggeber mit ihr einverstanden ist, sie aber dennoch für den Anbieter wirtschaftlich vertretbar bleibt, ist bei Ausschreibungen von IT-Großprojekten eine schwer zu beantwortende Frage für Anbieter. Mitbewerber könnten hier von den Erfahrungen von Atos profitieren.

Zudem lassen diese Informationen zusammen mit den anderen herausgegebenen Informationen klare Rückschlüsse auf die Kalkulation von Atos zu. Ein wichtiger Teil der Berechnungsgrundlage für ein Angebot sind die Kosten für die zu stellenden Sicherheiten. Diese ließen sich für Konkurrenten von Atos aus der genauen Höhe der ausgehandelten Sicherheiten zurückrechnen.

Dies würde es Mitbewerbern ermöglichen, bei künftigen IT-Ausschreibungen das Angebot von Atos genauer voraussehen zu können und dies bei ihren eigenen Angeboten zu berücksichtigen.

k) Anlage Nr. 10 – Sonderregelung zur Auftragsdatenverarbeitung und Fernwartung von Software

Die Anlage 10 inklusive der Änderungsvereinbarung zu Anlage 10 und dem Anhang 1 zu Anlage 10 enthalten die Vereinbarung zur Auftragsdatenverarbeitung zwischen Atos und der Beklagten, welche Anlässlich der Geltung der Regelungen der EU Datenschutz-

Grundverordnung 2018 geschlossen wurde. Die Anlage 10 wird komplett offengelegt; lediglich die Unterschriften unter den beiden Verträgen sowie die in Anhang 1 zu Anlage 10 auf S. 4 aufgeführten weisungsberechtigten Personen bei der Beklagten sowie Weisungsempfänger bei Atos wurden aus Gründen des Datenschutzes geschwärzt. Das Informationsinteresse des Klägers an diesen Informationen ist als sehr zu gering zu bewerten und überwiegt somit nicht das Interesse der benannten Personen am Ausschluss des Informationszugangs.

l) Anlage Nr. 13 – Mitwirkungsleistungen des Auftraggebers

In der Anlage stellt Atos detailliert für jede genau bezeichnete Projektphase und die dazugehörigen Leistungen von Atos die notwendigen Mitwirkungsleistungen der Beklagten dar. Daraus ergeben sich auch Informationen über detaillierte Arbeitsabläufe von Atos, wie beispielsweise zum Zeitpunkt und der Durchführung von Pilottests oder der Erstellung des Online-Hilfssystems. Für die Mitwirkungsleistungen der Beklagten gibt Atos zudem eine konkrete Frist oder einen Termin für die Erbringung dieser Mitwirkungsleistung an.

Die Anlage besteht vollständig aus Betriebs- und Geschäftsgeheimnissen von Atos.

Aus der Anlage ist die geplante Konzeption des Projekts mit einzelnen Projektphasen, der zeitlichen Planung dieser Phasen und der jeweils in den Phasen zu erbringenden Leistungen ersichtlich. Diese Informationen können einerseits konkrete Rückschlüsse auf die Kalkulation von Atos ermöglichen, indem Mitbewerber sehen, welche Fristen für welche Leistungen von Atos eingeplant sind. Zusätzlich wirken sich die geforderten Mitwirkungsleistungen der Beklagten ebenfalls direkt auf die Kalkulation aus. Andererseits zeigt die Anlage sehr detailliert auf, wie Atos ein solches IT-Großprojekt plant und welche Arbeitsabläufe bei einem solchen Projekt durchgeführt werden. Diese Information stellt Spezialwissen von Atos dar und könnte von Mitbewerbern bei künftigen IT-Ausschreibungen zum eigenen Vorteil verwendet werden.

Zudem ist für die Informationen aus der Anlage die vergaberechtliche Verschwiegenheitsverpflichtung aus §§ 105, 55 BHO, Ziffer 2.3.2 und 3.1.1 VV zu § 55 BHO i.V.m. § 14 Abs. 3 VOL/A, § 3 Nr. 4 IFG einschlägig, da die übermittelten Informationen zum Angebot von Atos gehören.

II. Berücksichtigung im Zulassungsverfahren

Die Vorlage der geschwärzten Dokumente sowie die vorstehenden Erläuterungen in diesem Schriftsatz sind im Zulassungsverfahren zu berücksichtigten.

1. Keine Präklusion gemäß den §§ 128a Abs. 1, 87b Abs. 2 VwGO

Das Vorbringen der Beklagten ist nicht gemäß den §§ 128a Abs. 1, 87b Abs. 2 VwGO präkludiert.

Sie hat zwar die geschwärzten Dokumente nicht bereits im erstinstanzlichen Verfahren vorgelegt. Jedoch hat das Verwaltungsgericht Berlin

- weder gemäß § 86 Abs. 3 VwGO darauf hingewirkt, dass die Beklagte ggf. erforderliche tatsächliche Angaben ergänzt oder weitere für die Feststellung und Beurteilung des Sachverhalts wesentliche Erklärungen abgibt,

- noch die Beklagte im Sinne von § 87b Abs. 2 VwGO aufgefordert, zu bestimmten Vorgängen Tatsachen anzugeben oder Beweismittel zu bezeichnen oder Urkunden etc. vorzulegen.

Insbesondere erhielt die Beklagten auch keine Aufforderung unter Fristsetzung und mit einer Belehrung gemäß § 87b Abs. 3 Nr. 3 VwGO über die Folgen einer Fristversäumung verbunden (VGH Kassel NVwZ- RR 1998, 208). Eine solche Aufforderung hätte bezogen auf den jeweiligen Einzelfall konkret abgefasst (BVerwGE 51, 188), inhaltlich bestimmt und verständlich sein müssen (BFH NJW 1995, 2511).

Dies ist im erstinstanzlichen Verfahren nicht geschehen, so dass die Beklagte auch im Berufungsverfahren und insbesondere auch in diesem Zulassungsverfahren nicht präkludiert ist (vgl. BVerwGE 51, 188).

2. Fristgerechte Geltendmachung der Zulassungsgründe

Die mit diesem Schriftsatz vorgelegten geschwärzten Dokumente mit den zugehörigen Erläuterungen sind in diesem Zulassungsverfahren zu berücksichtigen. Sie detaillieren lediglich die mit Schriftsatz vom 22. September 2020 geltend gemachten Zulassungsgründe.

Dies ist auch zulässig, denn die Darlegung eines Zulassungsgrundes kann auch nach dem Ablauf der Darlegungsfrist des § 124a Abs. 4 S. 4 VwGO insoweit noch ergänzt werden, als der konkrete Zulassungsgrund bereits in offener Frist den Mindestanforderungen entsprechend dargelegt worden ist (OVG Lüneburg NVwZ-RR 2009, 360).

Die Beklagte hat in ihrem Schriftsatz vom 22. September 2020 fristgerecht die Zulassungsgründe geltend gemacht und die zu ihrer Begründung genannten Gesichtspunkte den Mindestanforderungen entsprechend vorgetragen.

Diese Mindestanforderungen an die Geltendmachung der Zulassungsgründe werden durch die ständige Rechtsprechung des Bundesverfassungsgerichts deutlich. Danach verbietet Art. 19 Abs. 4 GG eine Auslegung und Anwendung des § 124a VwGO, die die Beschreitung des eröffneten Rechtswegs in einer unzumutbaren, aus Sachgründen nicht mehr zu rechtfertigenden Weise erschwert (vgl. BVerfGE 78, 88 [98 f.] = NVwZ 1988, 718; BVerfGE 96, 27 [39] = NJW 1997, 2163; BVerfGE 104, 220 [231 f.] = NJW 2002, 2456 = NVwZ 2002, 1370 L; BVerfG NVwZ 2011, 546).

Das Zulassungsverfahren soll gerade nicht das Berufungsverfahren vorwegnehmen (BVerfG NVwZ 2000, 1163 (1164); 2009, 515 (516); 2010, 634 (641)) und muss auch seinerseits innerhalb einer angemessenen Verfahrensdauer zu einem Abschluss gebracht werden (BVerfG NVwZ 2011, 486, 492). Deshalb dürfen an die Begründung eines Zulassungsantrags nicht dieselben Anforderungen gestellt werden wie an die spätere Berufungsbegründung, für die zusätzliche Zeit zur Verfügung steht (BVerfGE 151, 173 Rn. 29).

Das ist im hiesigen Zulassungsverfahren vor allem auch deshalb von besonderer Bedeutung, weil

- zum einen das Verwaltungsgericht Berlin im erstinstanzlichen Verfahren keinerlei Aufforderungen im Sinne der §§ 86 Abs. 3, 87b Abs. 2 VwGO an die Beklagte gerichtet hat (s.o. Ziffer 1.), und

- zum anderen die Prüfung der jeweiligen Passagen auf ihre Geheimhaltungsbedürftigkeit hin und die entsprechenden Schwärzungen aufgrund des großen Umfangs und der Komplexität in der kurzen Zeit schlichtweg nicht möglich ist.

Die Beklagte hat für die Prüfung und Umsetzung der in Ziffer I. dargestellten Schwärzungen bis zum 11. November 2020 weit über 55 Personentage benötigt. Vor allem angesichts der im Vergleich zu anderen Behörden und Institutionen geringeren Personalausstattung der Beklagten wäre es unzumutbar von ihr zu verlangen, innerhalb der Begründungsfrist des § 124a VwGO sämtliche Passagen aller streitgegenständlichen Dokumente im Einzelnen auf das Erfordernis einer Schwärzung hin zu prüfen und dies im Schriftsatz vom 22. September 2020 darzulegen.

In diesem Sinne hat sich das Bundesverfassungsgericht zu einer verfassungswidrigen Ablehnung der Berufungszulassung (BVerfG NVwZ 2011, 546) wie folgt geäußert:

> „... Vor diesem Hintergrund dürfen an die Darlegung eines Zulassungsgrundes keine überspannten Anforderungen gestellt werden. Insbesondere ist der in § 124 II Nr. 1 VwGO enthaltene Zulassungsgrund der ernstlichen Zweifel an der Richtigkeit des erstinstanzlichen Urteils immer schon dann erfüllt, wenn der Kl. im Zulassungsverfahren einen einzelnen tragenden Rechtssatz oder eine einzelne erhebliche Tatsachenfeststellung mit schlüssigen Gegenargumenten in Frage gestellt hat (vgl. BVerfGE 110, 77 [83] = NJW 2004, 2510; BVerfG[2. Kammer des Ersten Senats], NVwZ 2000, 1163 = NJW 2000, 3776 L)."
> *(Unterstreichung hinzugefügt)*

Danach liegen schlüssige Gegenargumente bereits dann vor, wenn der Antragsteller (hier: die Beklagte) substantiiert rechtliche oder tatsächliche Umstände aufzeigt, aus denen sich die gesicherte Möglichkeit ergibt, dass die erstinstanzliche Entscheidung unrichtig ist. Dies muss bei Unklarheiten

nach Zulassung der Berufung während des sich anschließenden Berufungsverfahrens im Rahmen der Amtsermittlung geklärt werden (BVerfG NVwZ 2011, 546):

> „Es ist nicht zulässig, diese Prüfung ins Zulassungsverfahren vorzuverlagern und damit die eigentlich erforderliche Beweisaufnahme zu umgehen (vgl. auch BVerfG [2. Kammer des Ersten Senats], NJW 2010, 1062 Rdnr. 22)."

Vor dem Hintergrund dieser Rechtsprechung genügt folglich für die gesicherte Möglichkeit einer erstinstanzlichen Fehlentscheidung, dass die Beklagte hier das verwaltungsgerichtliche Urteil tragende Tatsachenfeststellungen mit schlüssigen Gegenargumenten in Frage gestellt hat (BVerfG NVwZ 2011, 546).

Genau diese Voraussetzungen hat die Beklagte mit ihrem Schriftsatz vom 22. September 2020 erfüllt. Sie hat fristgerecht die Zulassungsgründe geltend gemacht und die zu ihrer Begründung genannten Gesichtspunkte vorgetragen (vgl. auch BVerwG NVwZ 2003, 490 (491); BayVerfGH BayVBl. 2006, 430; OVG Münster NVwZ 1997, 1224; VGH München BeckRS 2012, 48390). Sie hat eindeutig in Bezug auf die in § 124 Abs. 2 VwGO aufgeführten Zulassungsgründe auf den hier zu entscheidenden Fall bezogen und aus sich heraus verständlich in rechtlicher sowie tatsächlicher Hinsicht näher erläutert, aus welchen Gründen sie jeweils welchen der geltend gemachten Zulassungsgründe für gegeben erachtet (VGH Kassel NVwZ 1998, 755; BeckRS 2013, 52718; OVG Lüneburg NVwZ-RR 2009, 360; OVG Magdeburg NVwZ-RR 2009, 136; OVG Münster NVwZ 1997, 1224), und dargelegt, aus welchen Gründen die von ihr angeführten Zulassungsgründe erfüllt sein sollen (OVG Bln-Bbg NVwZ 2011, 1533).

Die Beklagte hat insbesondere in ihrem Schriftsatz vom 22. September 2020 unter Ziffer III.1. im Einzelnen und konkret bezogen auf die jeweiligen Dokumente begründet, weshalb gemäß § 124 Abs. 2 VwGO ernstliche Zweifel an der Richtigkeit des erstinstanzlichen Urteils bestehen.

In diesem Schriftsatz wurde zu jedem der Dokumente (zum Teil anhand mehrerer Beispiele) dargelegt und begründet, nach welchen Kriterien Schwärzungen vorzunehmen sind, d.h. die Verurteilung zur vollständigen Offenlegung bzw. zur Offenlegung mit Schwärzungen in geringerem Umfang des betreffenden Dokuments zu Unrecht erfolgte.

Dies gilt insbesondere für Anlagen Nr. 2, Nr. 3a, Nr. 3b und Nr. 4 zum Erstellungsvertrag, deren Inhalte zum Kern des Angebots von Atos gehörten und die eng miteinander zusammenhängen.

Die Beklagte hat im Gegensatz zu einer vom OVG Lüneburg zu Recht abgelehnten Berufungszulassung (NVwZ-RR 2009, 360) die Zulassungsgründe selbstständig ausdrücklich dargelegt und ihnen dann jeweils diejenigen Elemente seiner Kritik an der erstinstanzlichen Entscheidung klar zugeordnet.

Die Beklagte hat somit mit ihrem Schriftsatz vom 22. September 2020 die Anforderungen an eine Zulassungsbegründung hinreichend erfüllt. Mit diesem ergänzenden Schriftsatz werden die Zulassungsgründe in zulässiger Weise präzisiert und detailliert.

Die vorgelegten geschwärzten Dokumente sowie die Erläuterungen zu den Schwärzungen sind daher zu berücksichtigen.

Jan Peter Voß

Rechtsanwalt

Anlagen

berlin
dr. klaus greb[17], saskia barth[7],
dr. arne glöckner, sarina böll

frankfurt dr. christian berger,
jan peter voß, dr. udo a. zietsch[1,7],
dr. johannes weisser ll.m. (usa), thomas dick,
dr. thorsten lieb[5], dr. jörg michael voß ll.m.,
ralph w. hummel[9],
dr. arno maier-bridou ll.m. (cornell university)[3,13,14],
jürgen heilbock ll.m. (georgetown university)[18],
lars-henning behrens ll.m.[1,14], ralf schulten,
thomas hopf, nina horbach[1], christiane leffers[11],
nathalie maier-bridou d.e.a (paris panthéon-sorbonne) ll.m.[13],
ric kessler ll.m.[3], dr. giselher rüpke mcl (university of chicago)[4,6],
of. dr. thomas wilmer[10], nora matthaei ll.m. (university of cape town), dr. dennis geissler[16],
theresa viegener ll.m. (university of aberdeen, scottland), dr. lukas ströbel, lucia Patrizzi,
martha wettschereck[19]

hamburg dr. ulrich leo[8]

köln dr. ralf kaminski, markus figgen,
dr. thomas gerhold, dr. ulrich leo,
barbara schramm[5], dr. norbert windeln ll.m.[3],
markus melcher ll.m., matthias schleifenbaum ll.m.,
dr. rebecca schäffer mji, claudia dorfmüller,
justus heldt, dr. sonja röder m.b.s., bianca grewe,
sarina böll, dr. gregor caspar ischebeck,
dr. tim langmaack ll.m.eur, demis tarampouskas,
nils-alexander weng, jan laboranowitsch llm., dr. wolfgang kräber[17],
dr. thomas rummler[10], adrianus de kruiff

münchen dr. dennis geissler, dr. udo a. zietsch[1,8],
dr. klaus greb[17], markus melcher ll.m.

brüssel markus figgen,
dr. thomas gerhold, dr. rebecca schäffer mji
dr. thorsten lieb[5]

1 auch notar mit amtssitz in frankfurt am main
2 auch fachanwalt für miet- und wohnungseigentumsrecht
3 auch fachanwältin/fachanwalt für arbeitsrecht
4 auch fachanwalt für verwaltungsrecht
5 auch fachanwältin/fachanwalt für gewerblichen rechtsschutz
6 privatdozent
7 auch mediatorin/mediator
8 zweigstelle
9 auch steuerberater
10 nicht als rechtsanwalt zugelassen
11 auch wirtschaftsmediatorin/-mediator (ihk)
12 auch fachanwalt für bau- und architektenrecht
13 auch avocat à la cour (paris)
14 auch fachanwalt für handels- und gesellschaftsrecht
15 auch fachanwalt für insolvenzrecht
16 auch fachanwalt für transport- und speditionsrecht
17 auch fachanwalt für vergaberecht
18 auch attorney-at-law (new york)
19 auch fachanwältin für familienrecht

Anlage 9 Vertrag

Anlage zu Ziffer 17.5 EVB-IT Erstellungsvertrag

Kombinierte Vertragserfüllungs- und Mängelhaftungssicherheit

Der Auftragnehmer hinterlegt bei Abschluss des EVB-IT Erstellungsvertrages den als Sicherheit vereinbarten Geldbetrag gemäß § 18 Abs. 5 VOL/B oder übergibt dem Auftraggeber eine unbefristete Bürgschaft eines deutschen Kreditinstituts oder eines vergleichbaren Kreditinstituts aus einem Mitgliedsstaat der EU in der vereinbarten Höhe. Der Auftragnehmer verzichtet auf die Einreden der Aufrechenbarkeit, der Anfechtbarkeit und der Vorausklage, auf die Einrede der Aufrechenbarkeit jedoch nur soweit, wie die Gegenforderung nicht unbestritten oder nicht rechtskräftig festgestellt ist. Auf die Einrede der Anfechtbarkeit wird zudem nur soweit verzichtet, wie kein Fall des § 123 BGB (Anfechtung wegen arglistiger Täuschung) vorliegt.

Die kombinierte Vertragserfüllungs- und Mängelhaftungssicherheit beträgt hinsichtlich der Vertragserfüllung [redacted] und hinsichtlich der Mängelhaftung [redacted] des Erstellungspreises[1]*. Der Auftraggeber kann eine Anpassung verlangen, wenn sich der Auftragswert* gegenüber dem Erstellungspreis* erhöht. Eine Anpassung ist erstmalig bei einer Erhöhung um [redacted] und im Übrigen in angemessenen Schritten möglich.

Die Sicherheit dient als Vertragserfüllungssicherheit der Absicherung sämtlicher Ansprüche des Auftraggebers aus der Erstellung der Software bis zur Abnahme, insbesondere für Ansprüche wegen Pflichtverletzungen des Auftragnehmers, aus Vertragsstrafe und ungerechtfertigter Bereicherung. Ist eine Teilabnahme oder die Gesamtabnahme erfolgt, dient die Sicherheit auch der Absicherung sämtlicher Mängelansprüche aus der Erstellung der Software. Die Sicherheit ist unverzüglich nach Ablauf der Verjährungsfristen für Mängelansprüche der Software und nach Erfüllung der bis dahin erhobenen Ansprüche auch auf Erstattung von Überzahlungen und Schadensersatz an den Auftragnehmer zurückzugeben.

Bürgschaften können auch durch andere Bürgen als deutsche Kreditinstitute oder vergleichbare Kreditinstitute aus einem Mitgliedsstaat der EU gestellt werden, sofern der Auftraggeber den Bürgen zuvor als tauglich anerkannt hat.

[1] Die mit * versehenen Begriffe werden in den EVB IT Erstellungs-AGB definiert.

Vereinbarung

betreffend den „Vertrag über die Verarbeitung personenbezogener Daten im Auftrag" (Erstellung) und den „Vertrag über die Verarbeitung personenbezogener Daten im Auftrag" (Betrieb)

für

die Erstellung und den Betrieb des besonderen elektronischen Anwaltspostfachs („**beA**")

zwischen

der **Bundesrechtsanwaltskammer**
Littenstraße 9
10179 Berlin
- nachstehend „**BRAK**" genannt -

und

der **Atos Information Technology GmbH**
Otto-Hahn-Ring 6
81739 München
- nachstehend „**Atos**" genannt -

- gemeinsam nachstehend „**Vertragsparteien**" oder „**Parteien**" genannt -

Die BRAK und Atos haben

- am 24.09.2014 einen EVB-IT Erstellungsvertrag betreffend die Realisierung eines Systems zum Betrieb des besonderen elektronischen Anwaltspostfachs („**Erstellungsvertrag**") und
- am 25.02.2015/17.04.2015 einen Vertrag über den Betrieb des besonderen elektronischen Anwaltspostfachs („**Betriebsvertrag**")

abgeschlossen.

Bisherige Bestandteile der vorstehenden Verträge sind u. a.

- ein Vertrag über Auftragsdatenverarbeitung als Anhang 1 zur Anlage 10 des Erstellungsvertrages und
- ein Vertrag über Auftragsdatenverarbeitung als Anhang 1 zur Anlage 11 des Betriebsvertrages.

Die Parteien sind sich darüber einig, dass

- der als Anlage beigefügte Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (Erstellung) als Anhang 1 zur Anlage 10 an die Stelle des bisher bestehenden Vertrags über Auftragsdatenverarbeitung tritt und damit Teil des zwischen den Vertragspartnern abgeschlossenen Erstellungsvertrages ist, und
- der als Anlage beigefügte Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (Betrieb) als Anhang 1 zur Anlage 11 an die Stelle des bisher bestehenden Vertrags über Auftragsdatenverarbeitung tritt und damit Teil des zwischen den Vertragspartnern Betriebsvertrags ist.

Der Erstellungsvertrag und der Betriebsvertrag gelten unverändert fort, soweit nicht in dieser Vereinbarung ausdrücklich abweichende Regelungen getroffen werden.

Anlagen:

- Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (Erstellung)
- Vertrag über die Verarbeitung personenbezogener Daten im Auftrag (Betrieb)

Unterschriften

Berlin, den 12.09.2018	München, den 18.09.2018
[redacted]	[redacted]
BRAK	Atos

Report 101500651
Externe Sicherheitsüberprüfung beA Webanwendung

Atos IT Solutions and Services GmbH

Durchgeführt von

SEC Consult
ADVISOR FOR YOUR INFORMATION SECURITY

Unternehmensberatung GmbH

Version:	**1.0**
Autor:	**I. Lorch**
Verantwortlich:	**I. Lorch**
Datum:	**18.12.2015**
Vertraulichkeitsstufe:	**Streng vertraulich**

Inhaltsverzeichnis

1 Management Summary

Im folgenden Kapitel finden Sie die Ergebnisse des Audits, sowie die von SEC Consult empfohlenen Maßnahmen.

1.1 Ergebnisse des Audits

Bei der externen Sicherheitsüberprüfung für das Unternehmen Atos IT Solutions and Services GmbH untersuchte SEC Consult die beA Webanwendung sowie dessen Client-Security Komponente und das zugehörige Backend (für die vollständige Auflistung der überprüften Systeme siehe Kap. 2.3).

Bei diesem konkreten Projekt wurde ein Timebox-Ansatz zur Ermittlung des Aufwands herangezogen. Dies bedeutet, dass SEC Consult nur die innerhalb der angegebenen Zeit gefundenen Schwachstellen dokumentieren kann. Alle Angriffe wurden aus der Sicht eines Außenstehenden durchgeführt und fanden mit eingeschränktem Wissen (zur Verfügung gestellte Dokumentationen siehe Kapitel 2.3) über interne Strukturen statt

Kapitel 1.2 zeigt dabei die empfohlenen Maßnahmen basierend auf den Ergebnissen des Audits auf.

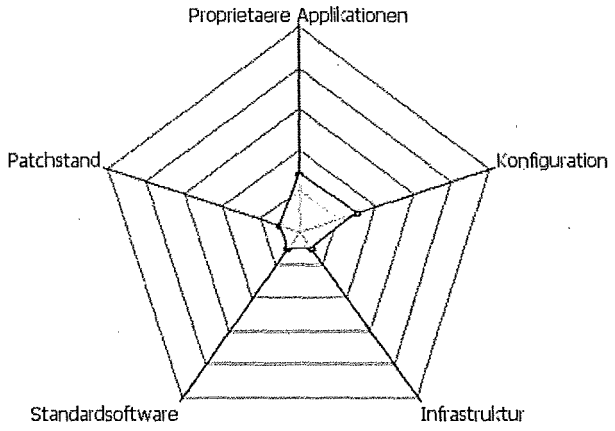
Die Testergebnisse zeigen, dass die beA Webanwendung sowie die Client-Security Komponente und das zugehörige Backend . Eine während der Sicherheitsüberprüfung identifizierte Schwachstelle wurde bereits während des Testzeitraums in kürzester Zeit behoben. Kleine Schwachstellen verbleiben u. a. noch im Bereich der Preisgabe von potentiell sensiblen Versionsinformationen der eingesetzten Software der Systeme.

1.1.1 Impact / Worst Case Szenarien

SEC Consult konnte während des Audits einzelne, für Webanwendungen typische Schwachstellen von geringem Risiko identifizieren.

1.1.2 Technische Risikobewertung

Anhand der Risikoeinschätzung von SEC Consult in fünf Dimensionen ergibt sich folgendes Risikoprofil:



Legende: Bewertung der einzelnen Dimensionen nach Schulnotensystem (1: geringes Risiko; 5: hohes Risiko)

- **Proprietäre Applikationen:** Hier ist ein leichter Ausschlag zu verzeichnen. Teile der gefundenen Schwachstellen befinden sich in der proprietären Webanwendung.
- **Patchstand:** In den Tests konnten keine Schwachstellen gefunden und ausgenutzt werden, die auf nicht eingespielte Sicherheitspatches zurückzuführen sind.
- **Standardsoftware:** In der eingesetzten Standardsoftware wurden keine sicherheitskritischen Fehler gefunden.
- **Konfiguration:** Die Konfiguration der Komponenten ist in den meisten Fällen einwandfrei. Leichte Konfigurationsmängel im verwendeten Applikationsserver wurden festgestellt.
- [redacted]

Es ergibt sich ein technisches Gesamtrisiko von **7,54 (Gering)**. Dies zeigt, dass die beA Webanwendung effektive Schutzmaßnahmen implementiert hat.

Disclaimer

Dieser Bericht ist streng vertraulich und nur für die interne, vertrauliche Verwendung beim Auftraggeber bestimmt. Der Empfänger verpflichtet sich, für die Geheimhaltung der streng vertraulichen Inhalte im Sinne der Organisation Sorge zu tragen. Der Empfänger übernimmt die Verantwortung für die weitere Verteilung des Dokuments.

Bei diesem konkreten Projekt wurde ein Timebox-Ansatz zur Ermittlung des Aufwands herangezogen. Dies bedeutet, dass SEC Consult lediglich innerhalb des vereinbarten Zeitfensters Schwachstellen identifizieren und dokumentieren kann. Aus diesem Grund kann aus der Überprüfung in diesem Projekt keinerlei Anspruch auf Vollständigkeit der in diesem Bericht dokumentierten Sicherheitslücken abgeleitet werden.

Des Weiteren stellt die Sicherheitsüberprüfung eine Augenblicksbetrachtung zum Zeitpunkt der Überprüfung dar. Eine Bewertung des zukünftigen Sicherheitsniveaus oder möglicher zukünftigen Risikoschwachstellen kann davon nicht abgeleitet werden.

Im Zuge des Audits wurden auf Systemen des Auftraggebers im Scope, falls erforderlich, lokale Dateien erstellt (z.B. temporäre Dateien, Log-Dateien, oder vom Auftragnehmer hochgeladene Programme zur Ausnutzung von etwaigen Schwachstellen). Dies geschieht, falls erforderlich, entweder manuell oder automatisiert durch Schwachstellenscanner. Diese Dateien wurden nach dem Audit soweit dem Auftragnehmer möglich entfernt. Eine vollständige Entfernung ist jedoch bedingt durch das Vorgehen in einem Sicherheitsaudit (z.B. fehlender Systemzugriff oder keine ausreichenden Rechte) nicht immer möglich. Es können daher ausgewählte dieser lokalen Dateien auch nach Beendigung des Auftrags vorhanden sein, die bei Bedarf vom Auftraggeber selbst zu entfernen sind.

1.2 Empfohlene Maßnahmen

Aufgrund der Ergebnisse der Sicherheitsüberprüfung hat SEC Consult folgende Maßnahmen als sinnvoll eingestuft.

1.2.1 Maßnahmen mit unmittelbarem Handlungsbedarf

1. **Behebung der in diesem Report aufgezeigten Sicherheitslücken.** Im Rahmen der Sicherheitsüberprüfung wurden mehrere Schwachstellen gefunden. Diese Schwachstellen sollten ehestmöglich behoben werden. Lösungsansätze für die einzelnen Lücken finden sich am Ende der jeweiligen Detailbeschreibung.

   Die Spezialisten von SEC Consult stehen Ihnen diesbezüglich gerne telefonisch oder vor Ort und „Hands on" im Zuge unserer „Care and Repair" – Services zur Verfügung.

1.2.2 Weiterführende Maßnahmen

1. **Abnahme Tests bei Eigenentwicklungen.** Jedes System sollte vor Produktivsetzung einer Sicherheitsüberprüfung unterzogen werden, die vom Umfang so gewählt werden sollte, dass kritische Applikationen gründlicher überprüft werden als weniger kritische. Da bei selbstentwickelten Applikationen der Source Code zur Verfügung steht, empfehlen sich für kritische Applikationen Glassbox Test bzw. Source Code Reviews. Durch die Durchführung vor Produktivsetzung wird das Risiko drastisch reduziert und eventuelle Down-Times vermieden.
2. **Zyklische externe Sicherheitsüberprüfungen.** Im Laufe der Zeit werden immer neue Schwachstellen und Angriffsvektoren bekannt auf die proprietäre Software nicht überprüft wurde. Eine zyklische Durchführung von externen Sicherheitsüberprüfungen kann auf mittlere Sicht das hohe Sicherheitsniveau einer Anwendung halten.
3. **Überprüfung der in diesem Test nicht berücksichtigten Systeme.** Die Sicherheit des Gesamtsystems ist in vielen Fällen vom schwächsten Glied abhängig. Selbst ein Server, der als nicht kritisch eingestuft wird, kann es einem Angreifer beispielsweise ermöglichen, über die Firewall hinwegzukommen und andere Systeme von intern zu attackieren. Daher ist es sinnvoll, in regelmäßigen Abständen den gesamten IP Range des Unternehmens zu testen.
4. **Source Code Audit von kritischen Applikationen.** Besonders kritische Applikationen, die beispielsweise wichtige Informationen verwalten, können mittels eines Source Code Audits besonders detailliert überprüft werden. So können auch Schwachstellen gefunden werden, die in einem Blackbox-Audit nur schwer zu finden sind.
5. **Stresstest der IT Infrastruktur und Applikationen zur Vorbeugung gegen (D)DoS Attacken.** Denial of Service bzw. Distributed Denial of Service Attacken können massive Schäden für Unternehmen verursachen. Mit Hilfe von Stresstests kann festgestellt werden, ob die Infrastruktur bzw. die Anwendungen solchen Angriffen standhalten können und ob die etablierten Prozesse für DoS Attacken funktionieren.

1.2.3 Notwendige Handlungen im Nachgang der Überprüfung

1. **Entfernen von Testkonten, welche für die Auditoren erstellt wurden.** Um den sicheren Betrieb der Systeme sicherzustellen, empfiehlt SEC Consult nicht mehr benötigte Accounts zu entfernen oder zu deaktivieren. Während der Tests wurden den Auditoren folgende Token zur Verfügung gestellt:

Typ	System	Kommentar
Chipkarte	test.bea-brak.de	beAcard188
Chipkarte	test.bea-brak.de	beA64card
Software-Token	test.bea-brak.de	Anna Mitarbeiter
Software-Token	test.bea-brak.de	Initial SystemverwalterStaging

2. **Entfernen von auditspezifischen Konfigurationsänderungen.** Nach Beendigung des Audits empfiehlt SEC Consult alle Test-spezifischen Änderungen wieder rückgängig zu machen. Folgende spezifische Änderungen wurden vorgenommen:
    - Freischaltung der SEC Consult IP-Range (92.60.14.128/26)

2 Vorgehensweise

Im folgenden Kapitel wird die Vorgehensweise, die SEC Consult bei der Sicherheitsüberprüfung anwendet, erläutert.

2.1 Testmethode

SEC Consult führt Penetrationstests durch, um die Sicherheit eines Gesamtsystems oder einzelner Systemkomponenten zu überprüfen. Die Tools, Methoden und Techniken, die von SEC Consult eingesetzt werden, fallen in die folgenden drei Kategorien:

1

Für das Unternehmen Atos IT Solutions and Services GmbH wurde ein Penetrationstest an der externen Webanwendung beA durchgeführt. Dabei , um eventuellen Angriffen widerstehen zu können. Alle Angriffe wurden aus der Sicht eines Außenstehenden durchgeführt und fanden mit eingeschränktem Wissen über interne Strukturen statt (siehe Kapitel 2.3).

2.2 Durchgeführte Testklassen

Details zur Risikobewertung können in Kapitel 2.5 nachgelesen werden. Die beA Webanwendung sowie das zugehörige Backend und die Client-Security Anwendung wurden, sofern die Services es erlaubten, auf folgende Fehlerklassen getestet:

2.2.1 Server-Konfiguration

	Konfigurationsfehler	
	Ausnutzbare Konfigurationsfehler für verschiedene Arten von Server-Software	
Angriffsvektor	Getestet[1]	Ausnutzbar[2]
Enumeration von Server-Inhalten	JA	NEIN
Ausnutzung von Default-Accounts	JA	NEIN
Enumeration von Benutzeraccounts	JA	NEIN
Ausnutzung gefährlicher Protokollfeatures	JA	NEIN
Ausnutzung nicht ausreichend gesetzter Berechtigungen	JA	NEIN
Ausnutzung von ungeschützter Funktionalität	JA	NEIN
Enumeration von Server-internen Informationen	JA	NEIN
Sammeln von Informationen über System- oder Fehlermeldungen	JA	JA
Erraten von Passwörtern	JA	NEIN

[1] Der Ergebnisbericht enthält gegebenenfalls auch Quellcodeauszüge frei erhältlicher Tools und Exploits von Drittherstellern.

	Konfigurationsfehler		
	Ausnutzbare Konfigurationsfehler für verschiedene Arten von Server-Software		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Mitlesen unverschlüsselter, sensitiver Daten		JA	NEIN
Weitere Angriffsvektoren			

2.2.2 Patch Level

	Server Patch-Level		
	Diese Schwachstellenklasse bezieht sich auf bekannte Lücken, die mit automatischen Tools identifiziert werden können.		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Ausnutzung öffentlich bekannter Sicherheitslücken		JA	NEIN
Weitere Angriffsvektoren			

2.2.3 Standard-Software und proprietäre Applikationen

	Authentisierungsfehler		
	Fehler in der Authentisierung von Benutzern der Anwendung		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Umgehen der Authentisierung		JA	NEIN
Weitere Angriffsvektoren			

	Autorisierungsfehler		
	Ein unautorisierter oder unberechtigter Benutzer kann auf geschützte Objekte zugreifen		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Zugriff auf geschützte Funktionalität		JA	NEIN
Zugriff auf geschützte Ressourcen		JA	NEIN
Weitere Angriffsvektoren			

	Ausgabe von Informationen		
	Der Angreifer kann interne Informationen über die Anwendung oder die Serverumgebung sammeln		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Ausnutzen von Dateiendungsverarbeitungen		JA	NEIN
Sammeln von Informationen über Entwickler-Kommentare		JA	NEIN
Sammeln von Informationen über System- oder Fehlermeldungen		JA	NEIN
Lesen von Sampledateien oder alten, unreferenzierten Files		JA	NEIN
Weitere Angriffsvektoren			

	Interpreter Injection / Eingabe-Validierung		
	Die Anwendung übergibt nicht validierte Parameter an einen Interpreter, gefährliche Library-Funktionen oder OS-APIs		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Zugriff auf das Dateisystem		JA	NEIN
Code Injection		JA	NEIN
Command Injection		JA	NEIN
Format String Injection		JA	NEIN
IMAP/SMTP Injection		JA	NEIN
LDAP Injection		JA	NEIN
ORM Injection		JA	NEIN
Overflowing Character Buffers		JA	NEIN
Path Traversal		JA	NEIN
SQL Injection		JA	NEIN
SSI Injection		JA	NEIN
XML Injection		JA	NEIN
XPath Injection		JA	NEIN
Weitere Angriffsvektoren			

	State -/ Session-Management-Fehler		
	State- oder Session Status wird von der Anwendung nicht richtig gehandhabt.		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Ermittlung von Session-Identifikatoren		JA	NEIN
Ausnutzung von Problemen im State-Management		JA	NEIN
Weitere Angriffsvektoren			

	Unsichere Funktionalität (Minimalprinzip)		
	Die Applikation bietet Funktionalität, die zu Sicherheitsproblemen führt.		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Ausnutzung von Sample-Anwendungen		JA	NEIN
Upload beliebiger Files		JA	NEIN
Weitere Angriffsvektoren			

	Unsicheres Management vertrauenswürdiger Daten		
	Vertrauenswürdige oder interne Daten können vom Angreifer verändert werden.		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Manipulation applikationsinterner Daten am Client		JA	NEIN

Lesen applikationsinternen oder vertraulicher Daten am Client		JA	NEIN
Weitere Angriffsvektoren			

	Unsichere Algorithmen		
	Der Einsatz unsicherer Algorithmen erlaubt die Kompromittierung sensitiver Informationen		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Ausnutzung schwacher Verschlüsselungsalgorithmen		JA	NEIN
Ausnutzung schwacher Zufallszahlengeneratoren		JA	NEIN
Weitere Angriffsvektoren			

	Verwundbarkeit durch Denial-of-Service		
	Das Service kann durch den Angreifer unbenutzbar gemacht werden.		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Aufbrauchen limitiert verfügbarer Ressourcen		NEIN	NEIN
Aussperren von Benutzeraccounts		JA	NEIN
Weitere Angriffsvektoren			

	Verwundbarkeit gegenüber client-seitigen Attacken (Web Browser)		
	Diese Schwachstellenklasse bezieht sich auf Webapplikationen. Benutzer der Anwendung werden zum Ziel dieser Angriffe.		
Angriffsvektor		Getestet[1]	Ausnutzbar[2]
Cross-Site Request Forgery (XSRF)		JA	NEIN
HTML Injection / Cross-Site Scripting (XSS)		JA	NEIN[3]
HTTP Response Splitting / header injection		JA	NEIN
Frame Spoofing		JA	NEIN
Session Fixation		JA	NEIN
Weitere Angriffsvektoren			

[1]Getestet: Der Angriffsvektor wurde in dieser Überprüfung von SEC Consult getestet.

[2]Ausnutzbar: Der Angriffsvektor wurde in dieser Überprüfung als ausnutzbare Schwachstelle identifiziert.

[3]Hier existiert ein theoretischer Angriffsvektor, welcher jedoch aufgrund von Beschränkungen aktuell nicht ausnutzbar ist (siehe Kapitel 5.1.5).

2.3 Umfang und Zeitplan

Von 07.12.2015 bis 18.12.2015 fand eine externe Sicherheitsüberprüfung statt, bei der es galt Sicherheitslücken in einer Teststellung der beA Webanwendung des Unternehmens Atos IT Solutions and Services GmbH zu finden. SEC Consult testete dabei das System mit der folgenden IP Adresse:

- 185.62.147.189 (test.bea-brak.de)

Ebenfalls Teil der Sicherheitsüberprüfung waren das Backend der beA Webanwendung sowie die zugehörige Client-Security Anwendung.

Für die Sicherheitsüberprüfung wurden folgende Dokumentationen und Hilfsmittel zur Verfügung gestellt:

- Umsetzungsfeinkonzept beA-System (Version 3.1, 14.01.2015)
- beA Client-Security – Kryptographische Funktionen für elektronische Nachrichten
- Zwei Chipkarten (beAcard188, beA64card) + kompatibles Chipkartenlesegerät
- Zwei Software-Token (Anna Mitarbeiter, Initial SystemverwalterStaging)

2.4 Disclaimer

Dieser Bericht ist streng vertraulich und nur für die interne, vertrauliche Verwendung beim Auftraggeber bestimmt. Der Empfänger verpflichtet sich, für die Geheimhaltung der streng vertraulichen Inhalte im Sinne der Organisation Sorge zu tragen. Der Empfänger übernimmt die Verantwortung für die weitere Verteilung des Dokuments.

Bei diesem konkreten Projekt wurde ein Timebox-Ansatz zur Ermittlung des Aufwands herangezogen. Dies bedeutet, dass SEC Consult lediglich innerhalb des vereinbarten Zeitfensters Schwachstellen identifizieren und dokumentieren kann. Aus diesem Grund kann aus der Überprüfung in diesem Projekt keinerlei Anspruch auf Vollständigkeit der in diesem Bericht dokumentierten Sicherheitslücken abgeleitet werden.

Des Weiteren stellt die Sicherheitsüberprüfung eine Augenblicksbetrachtung zum Zeitpunkt der Überprüfung dar. Eine Bewertung des zukünftigen Sicherheitsniveaus oder möglicher zukünftigen Risikoschwachstellen kann davon nicht abgeleitet werden.

Im Zuge des Audits wurden auf Systemen des Auftraggebers im Scope, falls erforderlich, lokale Dateien erstellt (z.B. temporäre Dateien, Log-Dateien, oder vom Auftragnehmer hochgeladene Programme zur Ausnutzung von etwaigen Schwachstellen). Dies geschieht, falls erforderlich, entweder manuell oder automatisiert durch Schwachstellenscanner. Diese Dateien wurden nach dem Audit soweit dem Auftragnehmer möglich entfernt. Eine vollständige Entfernung ist jedoch bedingt durch das Vorgehen in einem Sicherheitsaudit (z.B. fehlender Systemzugriff oder keine ausreichenden Rechte) nicht immer möglich. Es können daher ausgewählte dieser lokalen Dateien auch nach Beendigung des Auftrags vorhanden sein, die bei Bedarf vom Auftraggeber selbst zu entfernen sind.

2.5 Einzelrisikobewertung

Alle gefundenen Sicherheitsrisiken wurden mit einem Risk-Score bewertet. Dieser Risk-Score wird in einer Risiko-Matrix ermittelt, die sich aus Wahrscheinlichkeit und Schwere zusammensetzt. Die Wahrscheinlichkeit bezeichnet dabei die Wahrscheinlichkeit mit der ein Angreifer den Fehler findet und ausnutzen kann. Die Schwere bezieht sich auf den Schweregrad der Lücke und ihre Auswirkungen. Da der Schweregrad das Risiko wesentlich stärker beeinflusst als die Wahrscheinlichkeit, fließt er quadriert in die Gleichung ein.

Durch die Multiplikation von Wahrscheinlichkeit und Quadrat der Schwere ergibt sich der Risk-Score, der eine sehr differenzierte Einschätzung des Risikos, das durch eine Sicherheitslücke entsteht, erlaubt.

Schwere / Wahrscheinlichkeit	1	4	9	16	25
1	1	4	9	16	25
2	2	8	18	32	50
3	3	12	27	48	75
4	4	16	36	64	100
5	5	20	45	80	125

Um eine einfache textuelle Beschreibung des Risikos zu ermöglichen, wurden die Risk-Scores in vier Kategorien unterteilt:

Risk-Score	Bewertung
1 – 10	gering
11 – 24	mittel
25 – 60	groß
61 – 125	kritisch

2.6 Gesamtrisikobewertung

Um ein Gesamtrisiko für ein System, ein Netzwerk oder ein ganzes Unternehmens angeben zu können, müssen die Einzelrisiken aufsummiert werden. Eine einfache Addition ist jedoch nicht möglich, da dies nicht dem wirklichen Verhalten einzelner Schwachstellen zueinander entspricht. Zwei Schwachstellen, von denen das gleiche Risiko ausgeht, bedeuten gemeinsam nicht das doppelte Risiko.

Daher wird zum Summieren der Einzelrisiken die energetische Summenformel angewandt:

$$10\lg(10^{R_1/10}+10^{R_2/10}+\ldots+10^{R_n/10}) = R_{gesamt}$$

R ... Einzelrisiko
R_{gesamt} ... Gesamtrisiko

3 Schwachstellenübersicht

Aus dem Securityaudit ergibt sich für das Unternehmen Atos IT Solutions and Services GmbH folgende Auflistung an Schwachstellenklassen:

Risikobewertung	Anzahl der Schwachstellenklassen
Gering	2
Mittel	0
Groß	0
Kritisch	0
Gesamt	**2**

3.1 Gesamtrisiko pro System

Die folgende Tabelle enthält eine Risikowertung für jedes Einzelsystem, auf dem Sicherheitsrisiken identifiziert wurden.

System	Einsatzbereich	Risiko
test.bea-brak.de (185.62.147.189)	Web	Gering (7,54)
Gesamt	-	**Gering (7,54)**

3.2 Einzelrisiken

Die folgende Liste enthält eine Aufzählung aller gefundenen Sicherheitslücken.

Sicherheitslücke	System	Risiko	Seite
Limitiertes nicht-permanentes Cross-Site Scripting	test.bea-brak.de (185.62.147.189)	Gering (4,00)	16
Information Disclosure	test.bea-brak.de (185.62.147.189)	Gering (5,00)	19
Autorisierungsfehler	test.bea-brak.de (185.62.147.189)	Behoben	23
Gesamt	-	**Gering (7,54)**	-

4 Gefundene Schwachstellenklassen

Im folgenden Kapitel werden Schwachstellenklassen, die beim Unternehmen Atos IT Solutions and Services GmbH im Zuge des Security Audits gefunden wurden, erläutert.

4.1 Information Disclosure Schwachstellen

Fehlermeldungen, Kommentare und andere Informationen in statischen oder dynamisch generierten Webinhalten, aber auch Default- und individuelle Komponenten eines heterogenen Systems, enthalten oft Informationen, die für den Endbenutzer nicht sichtbar sein sollten. Unter diesen Bereich fallen folgende Klassen:

- Allgemeine Information Disclosure: Verwendete Softwareprodukte und deren Version. Benutzerinformationen und Login-Daten. Namen verwendeter Systemkomponenten. Defaultkomponenten verwendeter Systeme sind aktiviert und liefern sensible Informationen.

4.2 Cross-Site Scripting / -Tracing Schwachstellen

Mittels Cross-Site Scripting (XSS) Attacken werden clientseitige Scripte (JavaScript, VB-Script, etc.) mit Hilfe von Fehlern in Webapplikationen in den Webbrowser potentieller Opfer geschleust. XSS Angriffe werden sehr oft dazu benutzt, um Authentifizierungstoken (Session IDs) zu stehlen, können aber je nach Funktionalität der Applikation auch dazu benutzt werden, Inhalte von Webauftritten zu verändern oder den Webbrowser anderer Benutzer fernzusteuern.

Um Cross-Site Scripting zu verhindern, müssen spezielle Zeichen wie ", ', < oder > in der Benutzerausgabe durch ihre HTML Äquivalente (`&quot;`, `&#39;`, `&lt;`, `&gt;`) ersetzt werden. Besser jedoch ist es, einen Whitelist-Ansatz zu wählen, bei welchem im Benutzerinput nur jene Zeichen erlaubt werden, die unbedingt notwendig sind. Beispielsweise sollte ein Eingabeformularfeld nur Ziffern erlauben, wenn eine Postleitzahl einzugeben ist. Dabei ist darauf zu achten, dass diese Überprüfung serverseitig durchgeführt wird und sich nicht nur auf Felder in Formularen beschränkt.

Die in diesem Audit identifizierte Cross-Site Scripting Schwachstelle ist von geringem Risiko, da die Anzahl der für Scripte einsetzbare Zeichen stark begrenzt ist.

5 Detailanalyse

In diesem Kapitel werden die einzelnen Angriffe und die gefundenen Sicherheitslücken detailliert erläutert. Zudem werden Best Practices für eine sichere Einsatzumgebung der beA Webanwendung empfohlen.

5.1 test.bea-brak.de (185.62.147.189)

5.1.1 Allgemein

Auf dem Host `test.bea-brak.de` läuft die beA Webanwendung in einer Testumgebung. Im Zuge der Sicherheitsüberprüfung wurde diese, sowie dessen Client-Security Komponente und das zugehörige Backend überprüft. Dabei wurden unter anderem die Anwendungen decompiliert, analysiert und modifiziert sowie die Kommunikation zwischen diesen analysiert und manipuliert um Schwachstellen zu identifizieren.

Die eingesetzte TLS Transportverschlüsselung weist ein weit überdurchschnittliches Sicherheitsniveau auf. Aktuell befinden sich noch drei nicht Perfect Forward Secrecy unterstützende Chiffren im Einsatz, welche zur weiteren Steigerung des Sicherheitsniveau deaktiviert werden können.

5.1.2 Whois Information

Die Whois Information wird für jede IP Adresse aus der Permission to Attack überprüft, um sicherzustellen, dass diese auch dem Unternehmen oder dessen Vertragspartner gehört, welche auditiert werden. Die nachfolgende Tabelle stellt die öffentlich in Datenbanken verfügbare Whois Information dar.

```
inetnum:        185.62.147.0 - 185.62.147.255
netname:        BRAK-BEA
descr:          Bundesrechtsanwaltskammer Service BEA
country:        DE
admin-c:        ON936-RIPE
tech-c:         MS11367-RIPE
status:         ASSIGNED PA
mnt-by:         MOSAIC-MNT
mnt-by:         SBS-MNT
source:         RIPE
```

5.1.3 Portscan Ergebnisse

Portnummer	Protokoll	Service	Version
443	TCP	HTTP/SSL	-

Bitte beachten Sie, dass die unter Service bzw. Version beschriebenen Werte **nicht** dem realen Service entsprechen müssen.

5.1.4 Best Practices: Schutz der Einsatzumgebung der beA Webanwendung

Um die Sicherheit des Gesamtsystems zu gewährleisten ist es notwendig, dass der Schutz der Einsatzumgebung der beA Webanwendung am lokalen Computer sichergestellt wird. Dazu werden dem Benutzer der beA Webanwendung folgende ‚Best Practices' empfohlen:

Anti-Virus Software

Ein Virenscanner stellt sicher, dass sich auf einem Rechner keine bösartige Software wie Viren, Malware und Trojanische Pferde befindet. Dabei sollte der eingesetzte Computer regelmäßig vollständig von der Anti-Virus Software untersucht werden. Bei der Übertragung von Daten auf den lokalen Computer (z.B. Downloads oder USB-Sticks) muss mit Hilfe der Anti-Viren Software sichergestellt werden, dass diese keine bösartige Software enthalten.

Firewall

Die Netzwerkverbindung sollte vor Angriffen von außen geschützt werden. Dazu sollten geeignete Schutzmaßnahmen wie eine Firewall installiert sein. Handelsübliche Router bieten diese zumeist bereits an. Ist dies nicht der Fall, sollte lokal am Computer auf welchem die beA Webanwendung eingesetzt wird eine Softwarefirewall installiert werden.

Betriebssystem- / Software Updates

Um die Sicherheit des eingesetzten Betriebssystems und der Software zu gewährleisten, sollten diese regelmäßigen Updates unterzogen werden. Wo/Wenn immer möglich sollten automatische Updates aktiviert sein: Dabei ist darauf zu achten dass die automatischen Updates vom System auch wirklich automatisch (d.h. ohne Nachfrage/Zutun des Nutzers) installiert werden.

Schutz vor unbefugtem Zugriff

Es muss sichergestellt werden, dass keine Unbefugten Zugriff auf den eingesetzten Computer erhalten. Beim Verlassen des Computers sollte dieser Heruntergefahren oder mit einem Passwort gesperrt werden. Bei Abwesenheit müssen zusätzliche Schutzmaßnahmen wie das Verschließen des Raumes getroffen werden, um einen unbefugten Zugriff sowie Manipulation der Hardware zu verhindern.

Passwortsicherheit

Es sind hinreichend komplexe Passwörter einzusetzen. Passwörter sollten mindestens aus 8 Zeichen und 3 der 4 möglichen Zeichenklassen (Groß-, Klein, Ziffern und Sonderzeichen) bestehen und regelmäßig geändert werden. Des Weiteren muss sichergestellt werden, dass die eingesetzten Passwörter geheim bleiben und keinen Unbefugten bekannt werden.

Browsersicherheit

Zum Schutz des eingesetzten Computers sollte der Browser immer in seiner aktuellsten Version eingesetzt und mit Updates versorgt werden. Des Weiteren dürfen keine Plugins oder Addons aus unbekannten Quellen ausgeführt oder installiert werden.

5.1.5 Limitiertes nicht-permanentes Cross-Site Scripting

Ein Skript der Webapplikation gibt ungefilterten User-Input aus. Dies führt zu einer Cross-Site Scripting-Schwachstelle. Beim nicht-permanenten Cross-Site Scripting kann HTML- oder JavaScript-Code über einen speziellen Link auf der Webseite eingeschleust werden. Das JavaScript des Angreifers wird im Browser des Opfers im Kontext der angegriffenen Webseite ausgeführt, wenn das Opfer über den speziellen Link (z.B. aus Phishing-Emails) auf die Webseite gelangt. Die Schwachstelle kann vom Angreifer ausgenutzt werden, um Eingaben von Benutzern der Webseite mitzulesen (Keylogger-Attacken), Inhalte der Webseite zu verändern oder auf andere Seiten umzuleiten.

In diesem speziellen Fall ist die Möglichkeit die Schwachstelle auszunutzen jedoch, auf Grund der begrenzten Zeichenanzahl (max. 10 Zeichen) welche im verwundbaren Parameter zulässig sind, stark begrenzt. Trotzdem sollte die Schwachstelle behoben werden, so dass eventuelle Konfigurationsänderungen, z.B. das Erhöhen der zulässigen Zeichenanzahl, keine Auswirkungen auf die Sicherheit des Systems haben.

5.1.5.1 Proof-of-Concept

Beim Aufruf der folgenden URL wird der eingefügte JavaScript Code ausgeführt. Der Payload `';open()//` öffnet dabei beispielhaft einen neuen Tab/Pop-Up:

```
https://test.bea-brak.de/bea/index.xhtml?dswid=';open()//&jfwid=9999
```

Die Abbildung zeigt, dass beim Aufruf der URL der eingeschleuste JavaScript Payload ausgeführt und ein neuer Browsertab geöffnet wurde:

Abbildung 1: Eingeschleuster JavaScript Payload wird ausgeführt und öffnet einen neuen Tab.

5.1.5.2 Lösung

Alle Benutzer-Ein- und Ausgaben müssen einer strikten Ein- und Ausgabeüberprüfung unterzogen werden. Bei derartigen Überprüfungen sind Whitelist-Methoden den Blacklist-Methoden unbedingt vorzuziehen. Es wird empfohlen, beispielsweise in Parametern oder Eingabefeldern, welche nur numerischen Input aufweisen können (z.B. IDs, Postleitzahlen, usw.), nur die Eingabe von Zahlen zu erlauben. Dabei ist es wichtig, diese Überprüfung serverseitig durchzuführen, da clientseitige Maßnahmen umgangen werden können.

Um Cross-Site Scripting zu verhindern, müssen zusätzlich spezielle Zeichen wie z.B. [;()"´`,<>/\'=] in der Benutzerausgabe durch ihre HTML Äquivalente (", ', <, >, ...) ersetzt werden. Auf keinen Fall dürfen nur bestimmte HTML-Tags wie z.B. <script> gefiltert werden, da es zahlreiche andere Methoden gibt, Cross-Site Scripting auszunutzen bzw. derartige Filter zu umgehen.

5.1.5.3 Risiko Matrix

Schwere / Wahrscheinlichkeit	**1**	**4**	**9**	**16**	**25**
1	1	4	9	16	25
2	2	8	18	32	50
3	3	12	27	48	75
4	4	16	36	64	100
5	5	20	45	80	125

Schwere: Bezeichnet den Schweregrad des Fehlers (1...leicht - 25...sehr schwer).
Wahrscheinlichkeit: Bezeichnet die Wahrscheinlichkeit, mit der die Lücke von einem Angreifer ausgenutzt wird (1...unwahrscheinlich - 5...sehr wahrscheinlich).

5.1.5.4 Risiko Klassifizierung

Wahrscheinlichkeit	Die Schwachstelle ist leicht zu entdecken. Für die erfolgreiche Ausnutzung dieser ist jedoch Benutzer-Interaktion (z.B. das Besuchen einer präparierten Webseite oder das Klicken auf einen Link) erforderlich.
Schwere	Auf Grund der begrenzten Zeichenanzahl (max. 10 Zeichen) welche im verwundbaren Parameter zulässig sind, ist die Schwere als gering einzuschätzen.
Risiko	Gering (4)
ÖNORM A 7700	Kapitel 7: Behandlung von Benutzereingaben Kapitel 8: Behandlung von Datenausgaben

5.1.6 Information Disclosure

Über Information-Disclosure Schwachstellen kann ein Angreifer an Daten und Informationen über ein System gelangen, die bei weiteren Angriffen wesentliche Hilfen darstellen. Dazu gehört beispielsweise die Ausgabe von Versionsnummern. In vielen Fällen können bestimmte Schwachstellen nicht ohne weiteres Wissen über das System ausgenutzt werden. Information Disclosures erleichtern die Ausnutzung solcher Schwachstellen.

5.1.6.1 Proof-of-Concept

Der Aufruf der folgenden URL hat einen Fehler zur Folge, welcher die eingesetzte JBoss Version preisgibt:

```
https://test.bea-brak.de/bea/settings/RES_NOT_FOUND
```

Die Response des Servers mit detaillierten Informationen über die eingesetzt JBoss Version sieht wie folgt aus:

```
HTTP/1.1 404 Not Found
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Date: Tue, 08 Dec 2015 09:32:27 GMT
Strict-Transport-Security: max-age=15724800
X-Expires-Orig: None
Cache-Control: max-age=0, must-revalidate, private
Content-Length: 1114

<html><head><title>JBoss Web/7.5.9.Final-redhat-1 - JBWEB000064: Error
report</title><style><!--H1 {font-family:Tahoma,Arial,sans-
serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-
family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-
size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-
color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-
serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-
serif;color:white;background-color:#525D76;} P {font-
family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A
{color : black;}A.name {color : black;}HR {color : #525D76;}--></style>
</head><body><h1>JBWEB000065: HTTP Status 404 -
/bea/settings/RES_NOT_FOUND</h1><HR size="1"
noshade="noshade"><p><b>JBWEB000309: type</b> JBWEB000067: Status
report</p><p><b>JBWEB000068: message</b>
<u>/bea/settings/RES_NOT_FOUND</u></p><p><b>JBWEB000069: description</b>
<u>JBWEB000124: The requested resource is not available.</u></p><HR size="1"
noshade="noshade"><h3>JBoss Web/7.5.9.Final-redhat-1</h3></body></html>
```

Der Aufruf der folgenden URL mit den Sonderzeichen `">` im Parameter `text` hat einen Fehler zur Folge,

welcher die eingesetzte EdaWeb Version sowie einen Stack Trace preisgibt:

```
https://test.bea-brak.de/xwiki/bin/view/Main/Search?text=">&f_type=DOCUMENT&f_locale=de&f_locale=&r=1
```

Die Response des Servers mit detaillierten Versionsinformationen über EdaWeb sowie Stack Traces sieht wie folgt aus:

```
HTTP/1.1 500 Internal Server Error
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=utf-8
Content-Language: en
Date: Tue, 15 Dec 2015 10:50:18 GMT
Connection: close
Strict-Transport-Security: max-age=15724800
Set-Cookie: citrix_ns_id=YrfpVilY4ZkQNslbt9KF6zzzWXQ0006; Domain=.bea-brak.de; Path=/; HttpOnly
X-Expires-Orig: None
Cache-Control: max-age=0, must-revalidate, private
Content-Length: 2939

<!DOCTYPE html><html><head><title>EdaWeb/3.0.24 - Error report</title><style type="text/css">H1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} H2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} H3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} BODY {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} B {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} P {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;}A {color : black;}A.name {color : black;}.line {height: 1px; background-color: #525D76; border: none;}</style> </head><body><h1>HTTP Status 500 - Invalid URL [http://test.bea-brak.de/xwiki/bin/view/Main/Search?text=&amp;quot;&amp;gt;&amp;amp;f_type=DOCUMENT&amp;amp;f_locale=de&amp;amp;f_locale=&amp;amp;r=1]</h1><div class="line"></div><p><b>type</b> Exception report</p><p><b>message</b> <u>Invalid URL [http://test.bea-brak.de/xwiki/bin/view/Main/Search?text=&amp;quot;&amp;gt;&amp;amp;f_type=DOCUMENT&amp;amp;f_locale=de&amp;amp;f_locale=&amp;amp;r=1]</u></p><p><b>description</b> <u>The server encountered an internal error that prevented it from fulfilling this request.</u></p><p><b>exception</b></p><pre>javax.servlet.ServletException: Invalid URL [http://test.bea-brak.de/xwiki/bin/view/Main/Search?text=&amp;quot;&amp;gt;&amp;amp;f_type=DOCUMENT&amp;amp;f_locale=de&amp;amp;f_locale=&amp;amp;r=1]
```

```
      org.xwiki.resource.servlet.RoutingFilter.constructExtendedURL(RoutingFil
ter.java:193)
      org.xwiki.resource.servlet.RoutingFilter.doFilter(RoutingFilter.java:100
)
</pre><p><b>root
cause</b></p><pre>org.xwiki.resource.CreateResourceReferenceException:
Invalid URL [http://test.bea-
brak.de/xwiki/bin/view/Main/Search?text=&quot;&gt;&amp;f_type=DOCUMENT&amp;f_
locale=de&amp;f_locale=&amp;r=1]
      org.xwiki.url.ExtendedURL.&lt;init&gt;(ExtendedURL.java:124)
      org.xwiki.resource.servlet.RoutingFilter.constructExtendedURL(RoutingFil
ter.java:191)
      org.xwiki.resource.servlet.RoutingFilter.doFilter(RoutingFilter.java:100
)
</pre><p><b>root cause</b></p><pre>java.net.URISyntaxException: Illegal
character in query at index 56: http://test.bea-
brak.de/xwiki/bin/view/Main/Search?text=&quot;&gt;&amp;f_type=DOCUMENT&amp;f_
locale=de&amp;f_locale=&amp;r=1
      java.net.URI$Parser.fail(URI.java:2848)
      java.net.URI$Parser.checkChars(URI.java:3021)
      java.net.URI$Parser.parseHierarchical(URI.java:3111)
      java.net.URI$Parser.parse(URI.java:3053)
      java.net.URI.&lt;init&gt;(URI.java:588)
      java.net.URL.toURI(URL.java:939)
      org.xwiki.url.ExtendedURL.&lt;init&gt;(ExtendedURL.java:122)
      org.xwiki.resource.servlet.RoutingFilter.constructExtendedURL(RoutingFil
ter.java:191)
      org.xwiki.resource.servlet.RoutingFilter.doFilter(RoutingFilter.java:100
)
</pre><p><b>note</b> <u>The full stack trace of the root cause is available
in the EdaWeb/3.0.24 logs.</u></p><hr
class="line"><h3>EdaWeb/3.0.24</h3></body></html>
```

5.1.6.2 Lösung

Der Server sollte so konfiguriert sein, dass dem Benutzer keine technischen Fehlermeldungen/Informationen angezeigt werden. Debugging Output oder detaillierte Fehlermeldungen sollten in einer Produktivumgebung deaktiviert sein. Es wird empfohlen, nur einen Fehlercode ohne zusätzliche Systeminformationen anzuzeigen.

5.1.6.3 Risiko Matrix

Schwere / Wahrscheinlichkeit	**1**	**4**	**9**	**16**	**25**
1	1	4	9	16	25
2	2	8	18	32	50
3	3	12	27	48	75
4	4	16	36	64	100
5	**5**	20	45	80	125

Schwere: Bezeichnet den Schweregrad des Fehlers (1...leicht - 25...sehr schwer).
Wahrscheinlichkeit: Bezeichnet die Wahrscheinlichkeit, mit der die Lücke von einem Angreifer ausgenutzt wird (1...unwahrscheinlich - 5...sehr wahrscheinlich).

5.1.6.4 Risiko Klassifizierung

Wahrscheinlichkeit	Die Wahrscheinlichkeit, dass die Schwachstellen von einem Angreifer entdeckt werden, wird als hoch eingeschätzt.
Schwere	Es handelt sich um Information Disclosure Schwachstellen, die nicht zur direkten Kompromittierung des Systems führen. Die erhaltenen Informationen können jedoch vom Angreifer bei späteren Attacken verwertet werden.
Risiko	Gering (5)
ÖNORM A 7700	Kapitel 10: System- und Fehlermeldungen

5.1.7 Autorisierungsfehler

Autorisierungsfehler erlauben es einem Angreifer unbefugt auf Ressourcen oder Funktionen zuzugreifen, für welche er nicht berechtigt ist. Durch Ausnutzen einer solchen Schwachstelle könnte ein Angreifer auf sensible Daten anderer Benutzer zugreifen. Über den Parameter `msgid` wird im Nachrichteneingang und den Entwürfen die zu betrachtende/bearbeitende Nachricht identifiziert. Einem Angreifer war es möglich diesen Parameter zu manipulieren und somit beschränkten Zugriff auf Informationen über Nachrichten anderer Benutzer zu erhalten.

Folgende Informationen über fremde Nachrichten konnten eingesehen werden:

- Absender
- Empfänger
- Eigenes Aktenzeichen
- Aktenzeichen der Justiz
- Nachrichtentyp
- Gesendet-, Empfangen-, Zugegangen-Datum
- Dateiname, Name und Größe angehängter Dateien

Die hier beschriebene Schwachstelle wurde am Fr. 11.12.2015 an das Unternehmen Atos IT Solutions and Services GmbH gemeldet und von den Entwicklern behoben. Ein Recheck am Mo. 14.12.2015 zeigte, dass die **Schwachstelle behoben ist.**

5.1.7.1 Proof-of-Concept

Die folgenden beiden URLs sind Beispiele für den Aufruf von Nachrichten sowie Entwürfen. Durch das Abändern des Parameters `msgid` war es möglich auf Informationen über die Nachrichten anderer Benutzer zuzugreifen:

```
https://test.bea-brak.de/bea/messages/view/view.xhtml?post-
boxid=100757&msgid=106877&dswid=1870
https://test.bea-brak.de/bea/messages/create/createMes-
sage.xhtml?msgid=107628&dswid=3500
```

Der folgende Screenshot zeigt, welche Informationen ein authentifizierter Benutzer über die Nachricht mit der `msgid` 106892 eines anderen Benutzers einsehen konnte. Die Client-Security Anwendung verhinderte einen Zugriff auf den Inhalt der Nachricht, jedoch waren große Teile der Metadaten der Nachricht für einen unberechtigten Benutzer immer noch ersichtlich:

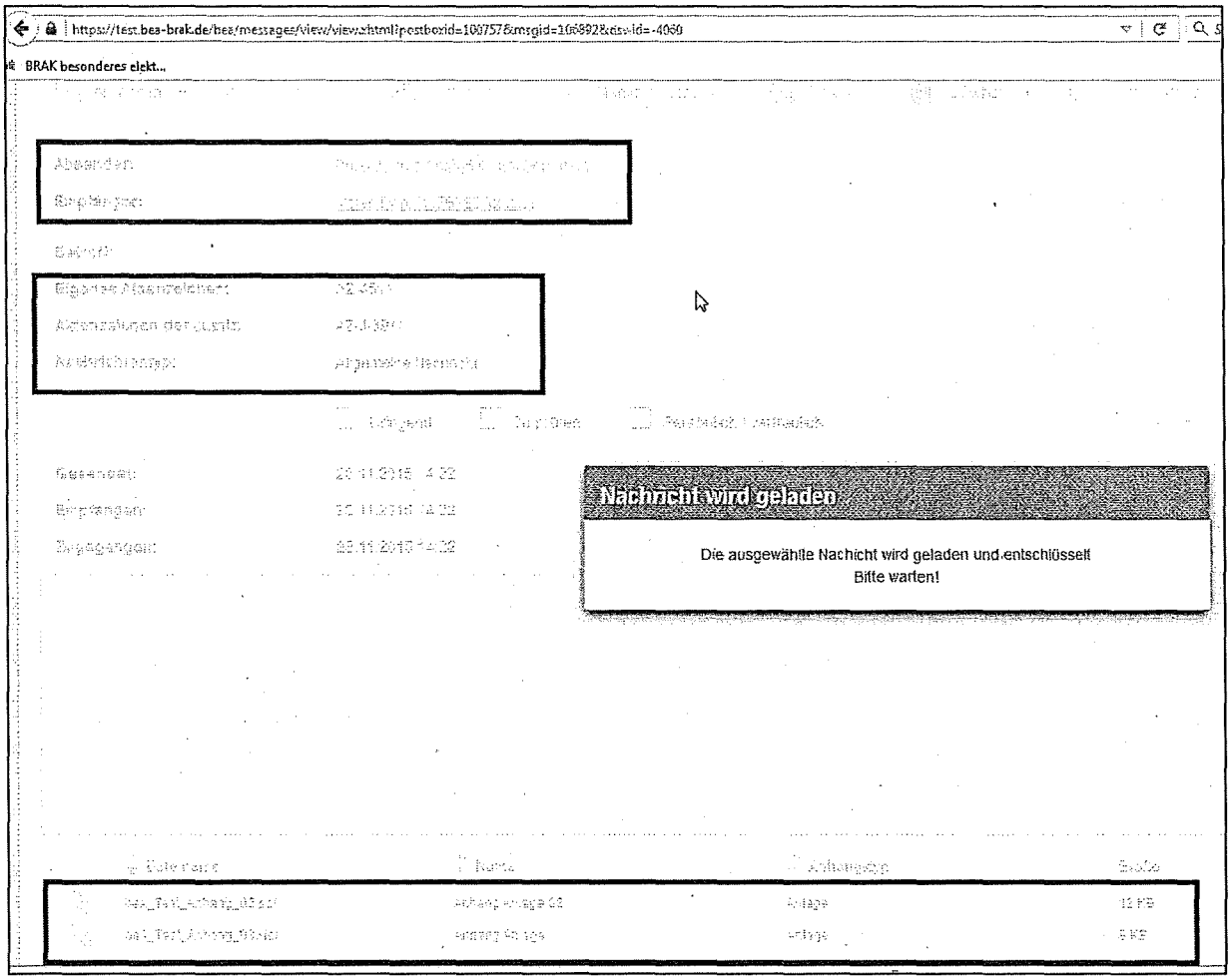


Abbildung 2: Meta-Informationen, welche ein nicht autorisierter Benutzer über Nachrichten anderer Benutzer einsehen konnte.

6 Version History

Version	Datum	Status/Änderungen	Erstellt von	Verantwortlich
1.0	18.12.2015	Finale Version	I. Lorch	I. Lorch

Vertrag

über die Verarbeitung personenbezogener Daten im Auftrag

zwischen

der Bundesrechtsanwaltskammer BRAK,
Littenstraße 9, 10179 Berlin

- nachstehend „Auftraggeber" genannt -

und

Atos Information Technology GmbH,

Am Studio 16, 12489 Berlin

- nachstehend „Auftragsverarbeiter" genannt -

Präambel:

Dieser Vertrag über die Verarbeitung personenbezogener Daten im Auftrag tritt als Anhang 1 zur Anlage 10 an die Stelle des bisher bestehenden Vertrags über Auftragsdatenverarbeitung und ist damit Teil des zwischen den Vertragspartnern abgeschlossenen EVB-IT Erstellungsvertrages vom 24.09.2014.

§ 1 Gegenstand der Auftragsverarbeitung

(1) Der Auftraggeber beauftragt den Auftragsverarbeiter wie folgt:

> Realisierung eines Systems zum Betrieb des besonderen elektronischen Anwaltspostfachs sowie dessen Wartung und Pflege

Im Rahmen dieses Auftrages verarbeitet der Auftragsverarbeiter personenbezogene Daten, die er vom Auftraggeber zur Verfügung gestellt bekommt oder im Auftrag des Auftraggebers selbst erhebt.

(2) Die Leistungserbringung erfolgt ausschließlich auf Anforderung und nach Vorgabe des Auftraggebers auf Grundlage des EVB-IT Erstellungsvertrages vom 24.09.2014 einschließlich seiner Anlagen und sämtlicher, z.B. im Rahmen von Änderungsverfahren, getroffenen Zusatzvereinbarungen (nachfolgend als „**Hauptvertrag**“ bezeichnet).

(3) Die Leistungserbringung erfolgt ausschließlich auf Anforderung und nach Weisung des Auftraggebers auf Grundlage des Hauptvertrags.

(4) Gegenstand des Hauptvertrags sind nicht die Nutzung oder Verarbeitung von personenbezogenen Daten durch den Auftragsverarbeiter. Jedoch ist im Zuge der Leistungserbringung des Auftragsverarbeiters als Dienstleister im Bereich der Wartung, des Supports bzw. Administration der Software ein Zugriff auf personenbezogene Daten nicht ausgeschlossen.

(5) Bei der Art der personenbezogenen Daten handelt es sich z.B. um

- Namen
- Kontaktdaten
- Geburtsdaten
- Mitgliedsdaten
- Zugangsdaten der Sicherungsmittel

(6) Der Kreis der Betroffenen umfasst

- Rechtsanwälte und ihre Mitarbeiter
- Vorstände, Geschäftsführung und Mitarbeiter der Rechtsanwaltskammern
- Präsidium, Geschäftsführung und Mitarbeiter des Auftraggebers
- Systemadministratoren
- Richter, Rechtspfleger und Beschäftigte in den Gerichten der Länder und des Bundes
- Richter und Mitarbeiter Anwaltsgerichte
- Mitarbeiter der Landesjustizverwaltungen
- Mitarbeiter in Landes- und Bundesministerien
- Präsidien und Geschäftsführung anderer Berufskammern

§ 2 Pflichten des Auftraggebers

Der Auftraggeber bleibt für die Beurteilung der Zulässigkeit der Datenerhebung, -verarbeitung oder -nutzung sowie für die Wahrung der Rechte der Betroffenen verantwortlich.

§ 3 Weisungsrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, in folgendem Umfang Weisungen gegenüber dem Auftragsverarbeiter zu erteilen.

Besteht die Auftragsverarbeitung in der Zurverfügungstellung von Software oder IT-Tools auf Rechnern des Auftragsverarbeiters, erfolgen die Weisungen auch durch Befehlseingaben entsprechend der Funktionalitäten der zur Verfügung gestellten Software oder des IT-Tools.

(2) Der Auftraggeber erteilt alle Weisungen, die zur Erfüllung des Auftrags notwendig sind, in schriftlicher Form. Mündliche Weisungen sind unverzüglich in schriftlicher Form zu bestätigen. Die schriftliche Form wird durch E-Mails oder elektronische Befehlseingaben gewahrt.

(3) Weisungen, die zu einer Änderung oder Ergänzung des Gegenstands der Auftragsverarbeitung führen, sind gemeinsam abzustimmen und entsprechend § 1 dieses Vertrages schriftlich festzuhalten.

(4) Erfolgt die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter ohne Weisung des Verantwortlichen, weil das Recht der Europäischen Union oder eines Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, ihn zu dieser Verarbeitung verpflichtet, wird der Auftragsverarbeiter dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mitteilen, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(5) Weisungsberechtigte Personen des Auftraggebers sind:

- [redacted]
- [redacted]
- [redacted]

Weisungsempfänger beim Auftragsverarbeiter sind:

- [redacted]
- [redacted]

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner bei Auftraggeber und/oder Auftragsverarbeiter wird dem Vertragspartner unverzüglich ein Nachfolger oder Vertreter schriftlich mitgeteilt.

§ 4 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der datenschutzrechtlichen Pflichten des Auftragsverarbeiters einschließlich der beim Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, die der Auftragsverarbeiter treffen muss, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Zu diesem Zweck ist der Auftraggeber insbesondere berechtigt, Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen, sowie sich durch Stichprobenkontrollen und sonstige Vor-Ort-Kontrollen von der Einhaltung dieser Vereinbarung durch den Auftragsverarbeiter in dessen Geschäftsbetrieb zu überzeugen. Stichprobenkontrollen und sonstige Vor-Ort-Kontrollen sind in der Regel rechtzeitig beim Auftragsverarbeiter anzumelden. Der Auftraggeber kann von Überprüfungen vor Ort absehen, wenn ihm der Auftragsverarbeiter geeignete Zertifikate, Prüfberichte oder ähnliche Dokumente über die von ihm getroffenen technischen und organisatorischen Maßnahmen zur Verfügung stellt und ihm dadurch die Einhaltung der dort dokumentierten Maßnahmen zum Datenschutz nachweist.

(2) Der Auftraggeber informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse oder der technischen und organisatorischen Maßnahme feststellt.

(3) Der Auftraggeber und der Auftragsverarbeiter arbeiten auf Anfrage des Auftraggebers mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

§ 5 Hauptpflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter ist verpflichtet, personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers zu verarbeiten. Er hat personenbezogene Daten unverzüglich zu berichtigen, zu löschen und zu sperren, wenn der Auftraggeber dies in einer Weisung verlangt. Berichtigungen, Löschungen oder Sperrungen von Daten, die im Auftrag verarbeitet werden, erfolgen durch den Auftragsverarbeiter nur nach Weisung des Auftraggebers, es sei denn, der Auftragsverarbeiter ist zur Berichtigung, Löschung oder Sperrung dieser Daten gesetzlich verpflichtet. Verlangt ein Betroffener direkt vom Auftragsverarbeiter die Berichtigung oder Löschung seiner Daten, leitet der Auftragsverarbeiter dieses Ersuchen unverzüglich an den Auftraggeber weiter.

(2) Dem Auftragsverarbeiter ist es untersagt, die ihm überlassenen Daten für andere Zwecke zu verarbeiten oder ohne Wissen des Auftraggebers Kopien oder Duplikate zu erstellen. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber erstellt oder genutzt werden, müssen als Datenträger des Auftraggebers besonders gekennzeichnet und fortlaufend aktualisiert werden. Eingang und Ausgang werden dokumentiert. Die vorstehende Regelung gilt auch für nicht-digitale Datenträger entsprechend.

(3) Der Auftragsverarbeiter ist nicht berechtigt, bei Durchführung seiner vertraglichen Pflichten aus dem Hauptvertrag gezielt auf personenbezogene Daten oder sonstige Betriebsdaten des Auftraggebers zuzugreifen. Sollte ein Zugriff auf personenbezogene Daten des Auftraggebers unerlässlich sein, um die Leistungen aus dem Hauptvertrag erfüllen zu können, beschränkt der Auftragsverarbeiter seinen Zugriff auf das absolut notwendige Maß. Er darf solche personenbezogenen Daten des Auftraggebers nur soweit notwendig auf eigene Rechner übertragen und dort verarbeiten. Die Datenübertragung ist nach dem jeweiligen Stand der Technik zu verschlüsseln. Diese Daten dürfen ausschließlich für den Zweck der Erfüllung der Leistungen aus dem Hauptvertrag verwendet werden. Er ist verpflichtet,

solche Daten nach Durchführung der entsprechenden Leistung aus dem Hauptvertrag unverzüglich zu löschen, spätestens mit Beendigung dieses Vertrages. Dem Auftraggeber steht ein Weisungsrecht zu, wie der Auftragsverarbeiter mit solchen personenbezogenen Daten und sonstigen Betriebsdaten des Auftraggebers zu verfahren hat. Auf Weisung des Auftraggebers sind solche Daten umgehend zu löschen oder auf die Rechner rückzuübertragen. Der Auftragsverarbeiter stellt sicher, dass keine Datenübermittlung an andere Stellen durch den Auftragsverarbeiter erfolgt.

(4) Der Auftragsverarbeiter ist verpflichtet, die Weisungen des Auftraggebers innerhalb seiner Prozesse zu dokumentieren.

(5) Der Auftragsverarbeiter hat ein Löschkonzept vorzuhalten und unmittelbar sicherzustellen, dass die Rechte auf Auskunft und auf Berichtigung sowie, soweit aufgrund datenschutzrechtlicher Bestimmungen vorgeschrieben, auf Vergessenwerden und Datenportabilität erfüllt werden können. Dieser Absatz gilt nur, soweit die betroffenen personenbezogenen Daten auch tatsächlich vom Auftragsverarbeiter auf seinen eigenen Rechnern gespeichert werden.

(6) Der Auftragsverarbeiter hat die datenschutzrechtlichen Grundsätze bei der Verarbeitung personenbezogener Daten einzuhalten sowie die Sicherheit herzustellen, die zum Schutz personenbezogener Datenerforderlich ist. Er ist insbesondere verpflichtet, in seinem Verantwortungsbereich alle technischen und organisatorischen Maßnahmen zu treffen, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen ggf. unter anderem ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten, sofern möglich;

b) die Fähigkeit, die Vertraulichkeit, die Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicher zu stellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere der Stand der Technik, die Implementierungskosten, die Art, der Umfang und die

Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmäßig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden.

Zu diesem Zwecke vereinbaren die Parteien in Anlage 1 zu diesem Vertrag die technischen und organisatorischen Maßnahmen, die erforderlich sind, um ein angemessenes Schutzniveau beim Auftragsverarbeiter sicher zu stellen.

Dem Auftragsverarbeiter ist es gestattet, alternative adäquate technische und organisatorische Maßnahmen aufgrund des technischen Fortschritts und der Weiterentwicklung umzusetzen. Dabei darf das Schutzniveau der in Anlage 1 zu diesem Vertrag vereinbarten technischen und organisatorischen Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind dem Auftraggeber schriftlich mitzuteilen und einvernehmlich in einer geänderten Anlage 1 schriftlich festzuhalten.

(7) Der Auftragsverarbeiter verpflichtet sich, dem Auftraggeber auf Anforderung alle zur Überprüfung der technischen und organisatorischen Maßnahmen notwendigen Angaben zur Verfügung zu stellen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen. Der Nachweis von technischen und organisatorischen Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch die Einhaltung genehmigter Verhaltensregeln, mittels derer die Anwendung der datenschutzrechtlichen Bestimmungen präzisiert wird, die datenschutzrechtliche Zertifizierung nach einem genehmigten Zertifizierungsverfahren durch eine akkreditierte Zertifizierungsstelle, aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren) oder eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(8) Der Auftragsverarbeiter sichert zu, dass die Daten des Auftraggebers von den sonstigen Datenbeständen des Auftragsverarbeiters strikt getrennt verarbeitet und gespeichert werden. Eine Vermischung der Daten des Auftraggebers mit sonstigen Datenbeständen des Auftragsverarbeiters muss während der gesamten Dauer dieses Vertrages ausgeschlossen sein. Sofern der Auftragsverarbeiter Daten des Auftraggebers für die Ausführung dieses Vertrages nicht mehr benötigt, wird er den Auftraggeber hiervon benachrichtigen und nach Rücksprache mit dem Auftraggeber nicht mehr benötigte Datenbestände löschen. Die Einzelheiten dazu werden die Parteien zu gegebener Zeit festlegen.

§ 6 Mitwirkungspflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter hat an der Erstellung der Verarbeitungsverzeichnisse des Auftraggebers, die die Auftragsverarbeitung nach § 1 betreffen, mitzuwirken, insbesondere die hierfür erforderlichen Angaben dem Auftraggeber mitzuteilen.

(2) Der Auftragsverarbeiter unterstützt den Auftraggeber des Weiteren bei dessen Einhaltung der Pflichten betreffend die Sicherheit personenbezogener Daten, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehört insbesondere die Unterstützung bei den Pflichten des Auftraggebers,

- ein angemessenes Schutzniveaus durch technische und organisatorische Maßnahmen sicherzustellen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen, sowie
- Datenschutz-Folgenabschätzungen und
- vorherige Konsultationen mit der Aufsichtsbehörde durchzuführen,

soweit dies jeweils die vertragsgegenständliche Auftragsverarbeitung betrifft.

(3) Der Auftragsverarbeiter sichert zu, dass er bei Datenaudits des Auftraggebers mitwirkt. Werden hierbei Fehler oder Unregelmäßigkeiten festgestellt, wird der Auftraggeber dies dem Auftragsverarbeiter schriftlich mitteilen. Der Auftragsverarbeiter ist verpflichtet, Fehler oder Unregelmäßigkeiten unverzüglich zu beheben.

(4) Der Auftragsverarbeiter ist im Zusammenhang mit der vertragsgegenständlichen Auftragsverarbeitung verpflichtet, den Auftraggeber bei der Beantwortung von Anträgen auf Wahrnehmung von Rechten der betroffenen Personen sowie bei der Einhaltung der Pflichten den Auftraggeber nach den jeweils einschlägigen datenschutzrechtlichen Vorschriften zu unterstützen.

(5) Soweit der Auftraggeber einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragsverarbeiter ausgesetzt ist, hat ihn der Auftragsverarbeiter nach besten Kräften zu unterstützen. Der Auftragsverarbeiter wird den Auftraggeber insbesondere bei der Erfüllung von dessen Melde- und Informationspflichten gegenüber Aufsichtsbehörden und Betroffenen bei Verletzungen des Schutzes personenbezogener Daten unterstützen sowie dem Auf-

traggeber in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung stellen.

§ 7 Hinweis- und Mitteilungspflichten des Auftragsverarbeiters

(1) Sofern der Auftragsverarbeiter der Ansicht ist, dass eine Weisung des Auftraggebers gegen Datenschutzvorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. In diesem Fall ist der Auftragsverarbeiter berechtigt, die Durchführung der entsprechenden Datenverarbeitung solange auszusetzen, bis der Auftraggeber die Weisung bestätigt oder abändert.

(2) Der Auftragsverarbeiter wird den Auftraggeber unverzüglich schriftlich in Kenntnis setzen, sollten im Herrschaftsbereich des Auftragsverarbeiters personenbezogene Daten, die der Auftragsverarbeiter für den Auftraggeber verarbeitet, entgegen den Bestimmungen dieses Vertrages oder der einschlägigen Datenschutzvorschriften verarbeitet werden, verloren gehen oder Dritte auf diese personenbezogenen Daten zugegriffen haben.

(3) Des Weiteren wird der Auftragsverarbeiter den Auftraggeber unverzüglich über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde informieren, soweit sie sich auf diese Auftragsverarbeitung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragsverarbeiter ermittelt.

§ 8 Örtliche Beschränkung der Datenverarbeitung

(1) Die Verarbeitung und Nutzung der Daten findet ausschließlich im Gebiet der Bundesrepublik Deutschland oder in einem Mitgliedsstaat der Europäischen Union statt. Eine Datenverarbeitung in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum findet nur statt, soweit keine Daten betroffen sind, die Privatgeheimnisse im Sinne von § 203 StGB darstellen, die unter den Beschlagnahmeschutz des § 97 StPO fallen oder die unter die anwaltliche Verschwiegenheitspflicht fallen. Jede darüber hinaus gehende Verlagerung in ein Drittland bedarf der vorherigen schriftlichen Zustimmung des Auftraggebers und darf nur erfolgen, wenn zusätzlich zu den Voraussetzungen des vorstehenden Satzes die besonderen Voraussetzungen der einschlägigen datenschutzrechtlichen Vorschriften, insbesondere die Vorschriften zu Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen, erfüllt sind.

(2) Falls ein Unterauftragsverarbeiter beauftragt werden soll, gelten die vorstehenden Anforderungen auch für den Unterauftragsverarbeiter zusätzlich zu § 9 dieses Vertrages.

§ 9 Unterauftragsverarbeiter

(1) Die Beauftragung von Unterauftragsverarbeitern ist nur mit vorheriger schriftlicher Zustimmung des Auftraggebers zugelassen. Die Zustimmung kann nur erteilt werden, wenn der Auftragsverarbeiter Namen und Anschrift des Unterauftragsverarbeiters schriftlich mitteilt. Außerdem muss der Auftragsverarbeiter sicherstellen, dass er den Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig ausgewählt hat. Der Auftragsverarbeiter hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragsverarbeiter auch gegenüber Unterauftragsverarbeitern gelten. Insbesondere muss der Auftraggeber berechtigt sein, Kontrollen vor Ort beim Unterauftragsverarbeiter durchzuführen oder durch Dritte durchführen zu lassen. Zudem hat der Auftragsverarbeiter die Einhaltung der Pflichten durch den Unterauftragsverarbeiter regelmäßig zu überprüfen und das Ergebnis dieser Überprüfungen dem Auftraggeber mitzuteilen, soweit dies für die hierin vereinbarte Auftragsverarbeitung relevant ist.

(2) Die Weiterleitung von Daten des Auftraggebers durch den Auftragsverarbeiter an einen Unterauftragsverarbeiter ist erst zulässig, wenn diesem in einem Vertrag dieselben Datenschutzpflichten auferlegt werden, die in diesem Vertrag zwischen dem Auftraggeber und dem Auftragsverarbeiter festlegt sind, wobei insbesondere hinreichende Nachweise dafür erbracht werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen beim Unterauftragsverarbeiter so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der anwendbaren datenschutzrechtlichen Vorschriften erfolgt. Kommt der Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragsverarbeiter gegenüber dem Auftraggeber für die Einhaltung der Pflichten dieses Unterauftragsverarbeiters.

(3) Der Auftragsverarbeiter unterrichtet den Auftraggeber umgehend bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf Datenschutzverletzungen oder andere Unregelmäßigkeiten die sich beim Unterauftragsnehmer bei der Verarbeitung von Daten des Auftraggebers ereignen.

(4) Der Auftragsverarbeiter ist auch ohne schriftliche Zustimmung des Auftraggebers berechtigt, Dritte mit Nebenleistungen, die nicht direkt mit der beauftragten Datenverarbeitung in Zusammenhang stehen, zur Unterstützung bei der Auftragsdurchführung in Anspruch zu nehmen (wie z.B. Telekommunikationsleistungen, Wartung, Pflege und Benutzerservice der eingesetzten Software, Reinigungsdienste, Prüfungs- und Entsorgungsleistungen bezüglich der verwendeten Daten und Datenträger). Der Auftragsverarbeiter ist allerdings verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch mit

diesen Dritten eine schriftliche Vereinbarung zu treffen, die den gesetzlichen datenschutzrechtlichen Vorgaben und Pflichten des Auftragsverarbeiters entsprechen. Der Auftragsverarbeiter gewährt dem Auftraggeber bei Bedarf zu Kontrollzwecken Einsicht unter Berücksichtigung etwaiger vertraglicher Vertraulichkeitsvereinbarungen in die entsprechenden Vertragspassagen.

§ 10 Rückgabe oder Löschung von Daten und Datenträgern

(1) Nach Abschluss des Auftrags oder früher nach Aufforderung durch den Auftraggeber wird der Auftragsverarbeiter alle personenbezogenen Daten und sämtliche in seinen Besitz gelangten Datenträger, Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, nach Wahl des Auftraggebers entweder an diesen zurückgeben oder datenschutzgerecht löschen oder vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll einer Löschung ist dem Auftraggeber auf dessen Anforderung hin vorzulegen.

(2) Etwaige gesetzliche Aufbewahrungsfristen bleiben hiervon unberührt. Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragsverarbeiter entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

§ 11 Besondere Vertraulichkeitsvereinbarung; Pflicht zur Wahrung des Datengeheimnisses

(1) Der Auftragsverarbeiter sichert die Wahrung der Vertraulichkeit bei der Verarbeitung personenbezogener Daten zu. Er verpflichtet sich, sicherzustellen, dass die ihm unterstellen Personen, die Zugang zu personenbezogenen Daten des Auftraggebers haben, diese Daten ausschließlich auf Weisung des Auftraggebers verarbeiten. Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben sowie das Datengeheimnis und, soweit einschlägig, das Fernmeldegeheimnis wahren. Der Auftragsverarbeiter darf ausschließlich Personen einsetzen, die sich ihm gegenüber schriftlich zur Vertraulichkeit verpflichtet haben. Die Verschwiegenheitspflicht erstreckt sich auch auf die dem Auftragsverarbeiter bekannt gewordenen sonstigen Betriebs- und Geschäftsdaten des Auftraggebers. Diese Verschwiegenheitspflicht setzt nicht voraus, dass Daten als vertraulich gekennzeichnet sind. Schaltet der Auftragsverarbeiter Unterauftragsverarbeiter ein, muss er zudem sicherstellen, dass auch diese Unterauftragsverarbeiter und die ihnen unterstellten Personen personenbezogene Daten ausschließlich auf Weisung des Auftraggebers verarbeiten und sich zur Vertraulichkeit im vorstehend vereinbarten Umfang verpflichtet haben.

(2) Der Auftragsverarbeiter verwendet die Daten, überlassene Datenträger und Unterlagen sowie sämtliche hiervon gefertigten Kopien oder Reproduktionen nicht für andere als die gemäß diesem Auftrag definierten Zwecke und verwahrt diese in einer Weise, dass sie Dritten nicht zugänglich sind und gibt diese nicht an Dritte weiter. Auf Verlangen des Auftraggebers hat der Auftragsverarbeiter unverzüglich sämtliche in seiner Verfügungsmacht befindlichen Datenträger des Auftraggebers sowie jegliche Kopien oder Reproduktionen hiervon an den Auftraggeber zurückzugeben oder datenschutzgerecht zu vernichten und dies dem Auftraggeber schriftlich zu bestätigen.

(3) Die datenschutzkonforme Vernichtung von Test- und Ausschussmaterial, sofern dieses anfällt, übernimmt der Auftragsverarbeiter standardmäßig. In besonderen vom Auftraggeber zu bestimmenden Fällen erfolgt eine Aufbewahrung bzw. Übergabe.

(4) Vorbehaltlich zwingender gesetzlicher Regelungen verpflichtet sich der Auftragsverarbeiter, weder das Vorhandensein noch den Inhalt bestimmter Daten Dritten zu offenbaren.

(5) Soweit keine anderweitigen gesetzlichen oder vertraglichen Verpflichtungen zur Vertraulichkeit bestehen, entfällt die Vertraulichkeitsverpflichtung gemäß den vorstehenden Bestimmungen, soweit:

- Daten öffentlich bekannt sind oder werden, ohne dass dies auf eine rechts- oder vertragswidrige Handlung des Auftragsverarbeiters zurückzuführen ist oder
- der Auftraggeber Daten gegenüber dem Auftragsverarbeiter schriftlich zur anderweitigen Nutzung freigegeben hat.

(6) Der Auftragsverarbeiter bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind.

Der Auftragsverarbeiter sichert zu, dass er die bei der Durchführung der Auftragsverarbeitung beschäftigten Mitarbeiter und jede sonstige dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht. Der Auftragsverarbeiter überwacht die Einhaltung der hier angegebenen datenschutzrechtlichen Vorschriften.

(7) Auskünfte an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger schriftlicher Zustimmung durch den Auftraggeber erteilen.

§ 12 Eigentums- und Nutzungsrechte

(1) Durch diesen Vertrag werden dem Auftragsverarbeiter keine Nutzungsrechte an den Daten des Auftraggebers gewährt, die über die vertragsgemäße Erfüllung der Auftragsverarbeitung hinausgehen.

(2) Die Daten des Auftraggebers sowie alle von ihm übergebenen Datenträger bleiben im Eigentum des Auftraggebers. Dem Auftragsverarbeiter stehen daran keine Zurückbehaltungsrechte zu.

§ 13 Haftung

(1) Der Auftragsverarbeiter trägt die Darlegungs- und Beweislast dafür, dass er vor Beginn sowie während der gesamten Dauer der Auftragsverarbeitung für den Auftraggeber die Umsetzung der technischen und organisatorischen Maßnahmen, wie in Anlage 1 dieses Vertrages vereinbart, sowie die Einhaltung aller sonstigen ihm in seiner Eigenschaft als Auftragsverarbeiter obliegenden datenschutzrechtlichen Pflichten sichergestellt hat.

(2) Für den Ersatz von Schäden, die ein Betroffener wegen eines Verstoßes gegen datenschutzrechtliche Vorschriften oder, soweit einschlägig, gegen das Fernmeldegeheimnis als auch wegen einer unzulässigen oder unrichtigen Datenverarbeitung im Rahmen des Auftragsverarbeitungsverhältnisses erleidet, ist im Verhältnis zum Auftraggeber der Auftragsverarbeiter verantwortlich, es sei denn, der Auftragsverarbeiter hat die unzulässige oder unrichtige Datenverarbeitung nicht zu vertreten. Dem Auftraggeber stehen insoweit vertragliche Regressansprüche gegen den Auftragsverarbeiter zu, sollte der Auftraggeber den Betroffenen dieser Schäden entschädigen müssen.

(3) Im Falle einer Verletzung seiner Pflichten aus diesem Vertrag haftet der Auftragsverarbeiter entsprechend den gesetzlichen Regelungen nach Art. 82 DSGVO.

§ 14 Beginn und Dauer des Vertrags; Kündigung

(1) Dieser Vertrag beginnt mit Unterzeichnung durch beide Parteien und gilt für die Dauer des EVB-IT Erstellungsvertrages vom 24.09.2014, ohne dass jedoch für den Auftraggeber eine tatsächliche Verpflichtung zur regelmäßigen Abnahme von Leistungen entsteht.

(2) Das Recht jeder Partei zur fristlosen Kündigung aus wichtigem Grund bleibt unberührt. Der Auftraggeber kann insbesondere den Vertrag jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß des Auftragsverarbeiters gegen diese Vereinbarung vorliegt, wenn der Auftragsverarbeiter eine

Weisung nicht ausführt oder wenn der Auftragsverarbeiter Kontrollen durch den Auftraggeber vertragswidrig ganz oder teilweise verweigert.

(3) Auch nach einer Kündigung dieses Vertrages oder eines einzelnen Auftragsverarbeitungsverhältnisses gelten die hierin vereinbarten Bestimmungen für die Abwicklung des gekündigten Auftragsverarbeitungsverhältnisses oder dieses Vertrages solange fort, bis diese vollständig rückabgewickelt und die Daten des Auftraggebers auf ihn zurückübertragen sind.

§ 15 Datenschutzbeauftragter des Auftragsverarbeiters

(1) Der Auftragsverarbeiter sichert zu, dass er einen fachkundigen und zuverlässigen Datenschutzbeauftragten bestellt hat. Der nachstehende Mitarbeiter ist beim Auftragsverarbeiter als Beauftragter für den Datenschutz bestellt: Josef Beck

(2) Ein Wechsel des Datenschutzbeauftragten ist dem Auftraggeber unverzüglich schriftlich mitzuteilen.

§ 16 Schlussbestimmungen

(1) Ergänzungen und Änderungen dieses Vertrags bedürfen der Schriftform. Dies gilt auch für einen etwaigen Verzicht auf dieses Schriftformerfordernis.

(2) Sollte Eigentum des Auftraggebers beim Auftragsverarbeiter durch Maßnahmen Dritter, etwa durch Pfändung, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragsverarbeiter den Auftraggeber unverzüglich und vor Eintritt dieser Maßnahmen zu verständigen.

(3) Es besteht bei den Vertragsparteien Einigkeit darüber, dass „Allgemeine Geschäftsbedingungen" des Auftragsverarbeiters auf diesen Vertrag keine Anwendung finden.

(4) Erweist sich eine Bestimmung dieses Vertrages als unwirksam, so berührt dies die Wirksamkeit der übrigen Bestimmungen des Vertrags nicht. Beide Vertragsparteien sind in diesem Falle verpflichtet, unverzüglich in eine nachträgliche Zusatzbestimmung einzuwilligen, die nach Sinn und Zweck der unwirksamen Bestimmung am nächsten kommt.

(5) Sollten Widersprüche zwischen Bestimmungen dieses vorliegenden Dokuments und übrigen Vertragsdokumenten bestehen, gehen die Bestimmungen des vorliegenden Dokuments den übrigen Vertragsdokumenten vor.

(6) Rechtswahl, Gerichtsstandsvereinbarung

Für diesen Vertrag gilt das Recht des Landes, in dem der Auftraggeber seinen Sitz hat, unter Ausschluss der Regelungen des internationalen Privatrechts.

Alleiniger Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist, vorbehaltlich eines etwaigen ausschließlich gesetzlichen Gerichtsstandes, der Sitz des Auftraggebers. Der Auftraggeber ist berechtigt, einen Rechtsstreit auch am gesetzlichen Gerichtsstand anhängig zu machen.

(7) Anlage 1 ist wesentlicher Bestandteil dieses Vertrages.

Berlin, 12.09.2018

Ort / Datum

[redacted]

Auftraggeber

Berlin, 18.09.2018

Ort / Datum

[redacted]

Auftragsverarbeiter

Anlage 1

Technische und organisatorische Maßnahmen bei der Auftragsverarbeitung

Die nachfolgenden Maßnahmen zur Gewährleistung der Sicherheit bei der Verarbeitung personenbezogener Daten stellen Mindestanforderungen dar, die eingehalten werden müssen. Weitergehende Maßnahmen, die zu einem höheren Schutzniveau führen, können im Ermessen und zu Lasten des Auftragsverarbeiters eingeführt werden. Maßnahmen, die dem technischen Fortschritt unterliegen, können ebenfalls im Ermessen und zu Lasten des Auftragsverarbeiters eingeführt werden, sofern das geforderte Schutzniveau nicht unterschritten wird.

1. Sicherstellung von Verfügbarkeit und Belastbarkeit

1.1 Verfügbarkeitskontrolle

Durch Brand- und Wasserschäden, Blitzschlag oder Stromausfall oder aber Diebstahl und Sabotage können Datenbestände in Gefahr geraten. Dass in diesen Fällen kein Datenverlust eintritt soll die Verfügbarkeitskontrolle sicherstellen.

Der Schutz vor zufälliger Zerstörung kann hauptsächlich über die Einhaltung entsprechender Brandschutzvorschriften und durch zusätzliche Hardware zur unterbrechungsfreien Stromversorgung und Netzwerksicherheit sichergestellt werden. Mit den entsprechenden Vorkehrungen und Zusatzsoftware können EDV-Systeme beispielsweise im Falle eines plötzlichen Stromausfalles noch so lange weiterbetrieben werden, bis ein kontrolliertes Abschalten möglich ist. Hierdurch können sowohl Datenverlust als auch Hardwareschäden vermieden werden.

Unter die Verfügbarkeitskontrolle fallen aber auch Maßnahmen zur Datensicherung, also die klassischen Backup- und Datenspiegelungslösungen. In welchen Intervallen solche Datensicherungen durchgeführt werden müssen, hängt immer von der Art der Daten, der Veränderungshäufigkeit und der Wichtigkeit der Daten für das Unternehmen ab. Für alle Datensicherungen gilt aber, dass auch die erstellte Sicherung vor Zerstörung und Diebstahl gesichert sein muss. Sicherungskopien dürfen daher nie im gleichen Gebäude oder Brandabschnitt wie das Datenverarbeitungssystem aufbewahrt werden. Vielmehr ist zu empfehlen, die Datensicherung entweder direkt auf einem Server an einem anderen Standort zu erstellen, oder Datenträger mit Datensicherungen entsprechend an einem ausgelagerten Ort aufzubewahren.

Die folgenden Maßnahmen zur Verfügbarkeitskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

[illegible]
Es existiert ein Brandschutzkonzept, bestehend aus Brandmeldern, Brandschutztüren und lokalen Feuerlöschern.
Eine unterbrechungsfreie Stromversorgung (USV) für die Server-Systeme ist vorhanden.
Die Serverräume sind klimatisiert.
Es existiert ein schriftliches Datensicherheitskonzept.
Für jedes geschäfts- oder sicherheitskritische System ist entsprechend dem Gefährdungspotential ein redundantes System vorhanden.
Daten werden redundant an 2 Standorten gehalten.
Serverfestplatten werden regelmäßig gespiegelt.
Es erfolgen regelmäßige Tests der erstellten Backups (Test der restore-Funktion).
Virenscanner und Firewall werden regelmäßig kontrolliert und aktualisiert.
Es existiert ein Notfallplan bei Ausfall der Systeme. Dieser wird in regelmäßigen Abständen als Testszenario durchgespielt und die Ergbenisse protokolliert.

1.2 Sicherstellung der Belastbarkeit

Es sind hinreichende Rechen- und Serverkapazitäten einzusetzen, so dass die Funktionsfähigkeit auch bei starkem Zugriff bzw. starker Auslastung gewährleistet ist.

Die folgenden Maßnahmen zur Sicherstellung der Belastbarkeit müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Überwachung der Auslastung anhand von Monitoringdaten
Kapazitätsanpassung bei Überschreitung von vereinbarten Schwellwerten

2. Sicherstellung der Integrität

2.1 Weitergabekontrolle

Die Weitergabekontrolle betrifft im Grunde zwei verschiedene Szenarien. Zum einen wird auf die Sicherung der Übertragungswege von personenbezogenen Daten - gleich ob per Datenträger oder elektronisch - abgezielt. Zum anderen betrifft die Weitergabekontrolle die Revisionsfähigkeit von Datenübermittlungsvorgängen an unternehmensfremde Dritte.

Hinsichtlich des ersten Szenarios müssen Maßnahmen getroffen werden, um zu verhindern, dass Unbefugte während eines Übertragungsvorgangs Zugriff – gleich welcher Art – auf personenbezogene Daten haben. Umfasst werden dabei aber nicht nur die elektronische Übermittlung, sondern beispielsweise auch die Verbringung eines Back-Up-Datenträgers in einen Archivraum. In jedem Fall der Datenübermittlung sind entsprechende Sicherheitsmaßnahmen zu treffen. Dies umfasst auch die Weitergabe von Daten an den Auftragsverarbeiter.

Das zweite Szenario verlangt eine „vorbeugende" Dokumentation darüber, welche Empfänger personenbezogene Daten durch Datenübertragung erhalten sollen. Die Regelung verlangt dabei keine ständige Protokollierung sämtlicher Datenübertragungen, sondern vielmehr soll nur die vorgesehene Übermittlung dokumentiert werden. Für diese Dokumentation müssen alle Übermittlungsadressaten inklusive der an sie zu übermittelnden Datenmenge bezeichnet werden. Des Weiteren müssen die möglichen Übermittlungen in zeitlicher Hinsicht (Beginn und Ende der Übermittlung) überprüfbar sein. Die entsprechenden Dokumentationsunterlagen müssen auch für Dritte einsehbar und in einem entsprechend allgemein lesbaren Format vorhanden sein.

Folgende Maßnahmen zur Weitergabekontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

[illegible]
Die Daten des Auftraggebers werden vom Auftragsverarbeiter nur nach vorheriger schriftlicher Weisung an Dritte weitergegeben.
Es wird durch entsprechende Regelungen (z.B. durch die Einschränkung des Personenkreises, die Datenträger erstellen können und regelmäßige Kontrollen dieser Einschränkung) sichergestellt, dass keine Daten des Auftraggebers unbefugt weitergegeben werden.
Insofern im Rahmen der Auftragsdurchführung Daten weitergegeben werden müssen, erfolgt eine Weitergabe der Daten wenn möglich ausschließlich in anonymisierter Form oder aber es erfolgt eine Verschlüsselung der Daten vor der Weitergabe (z.B. MIME, PGP Standard). Daten werden gemäß dem Stand der Technik verschlüsselt.
Der Transport von Datenträgern erfolgt bei Bedarf durch sichere Transportbehälter (Versiegelung). Bei Ablieferung erfolgt eine Identitätsprüfung des Empfängers.
Es erfolgt eine Dokumentation der Übermittlung.

2.2 Eingabekontrolle

Wie bereits weiter oben erwähnt, ergibt es immer auch Sinn zu protokollieren, wer wann auf welche Daten zugreift, und was verändert wird. Die Maßnahmen

zur Eingabekontrolle sollen genau das sicherstellen. Mit ihnen soll sich jederzeit ermitteln lassen, wer bestimmte Daten erstellt hat, was der Inhalt dieser Daten war und ist und wann die Erstellung bzw. Änderung vorgenommen wurde. So soll ermittelt werden können, wer für falsche oder unvollständige Daten verantwortlich zeichnet. Nicht gespeichert werden dürfen dabei aber die gelöschten oder veränderten Daten an sich. Es obliegt den Unternehmen wie die Identifizierung des „Datenurhebers" umgesetzt wird. Es ist dabei nicht erforderlich, dass sich diese bereits direkt aus dem Datenverarbeitungssystem ergibt. Ausreichend ist beispielsweise auch eine Identifizierungsmöglichkeit über Eingangskontrollbücher oder Schichtpläne.

Zu beachten ist, dass mit der Anfertigung von Eingabeprotokollen eine neue Sammlung personenbezogener Daten entsteht, die als solche behandelt werden muss. Bei einer automatisierten Erstellung sollte daher darauf geachtet werden, dass sich einzelne Einträge auch nur automatisiert wieder ermitteln lassen.

Folgende Maßnahmen zur Eingabekontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Der Auftragsverarbeiter muss Zugangsregelungen und Benutzerberechtigungen im Einsatz haben, mit denen die Identifizierung aller Benutzer und Datenstationen im System möglich ist.
Aktivitäten auf den Systemen müssen über Protokoll-Funktionen nachvollziehbar sein.
Die entsprechenden Protokolle werden für einen festgelegten Zeitraum aufbewahrt.
Zugriff auf diese Protokolle haben definierte Personen (z.B.: Datenschutzbeauftragte und IT-Sicherheitsbeauftragte). Die Protokolldateien sind gegen unbefugte Nutzung und Veränderung gesichert.

3. Sicherstellung der Vertraulichkeit

3.1 Zutrittskontrolle

Die Zutrittskontrolle verlangt Maßnahmen, die Unbefugten den körperlichen Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehren. Es muss also verhindert werden, dass unbefugte Personen überhaupt die Möglichkeit des Zutritts zu Datenverarbeitungsanlagen haben. Die Zutrittskontrolle soll aber nicht nur einen unbefugten Zutritt, sondern auch eine Zerstörung von EDV-Anlagen verhindern.

Die Zutrittsberechtigungen sind daher immer genau festzulegen und zu dokumentieren. Dies gilt insbesondere auch für unternehmensfremde Personen wie

Wartungstechniker (denen immer Begleitpersonen an die Seite gestellt werden sollten) oder das Reinigungspersonal. Zur Zutrittskontrolle gehören aber auch alle Maßnahmen, die ein gewaltsames Eindringen verhindern.

Eine effektive Zutrittskontrolle ist in der Regel nur durch eine Kombination von verschiedenen ineinandergreifenden Maßnahmen möglich.

Folgende Maßnahmen zur Zutrittskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Die Sicherung des Betriebsgeländes erfolgt durch: • Umzäunung • Sichtkontrollen und Gästelisten am Empfang/Pförtner • außerhalb der Betriebszeiten Überwachung durch einen Wachdienst • Betrieb von Überwachungseinrichtungen wie Alarmanlagen und Video-/Monitorüberwachung.
Der Brandschutz wird sichergestellt durch: • Brandschutztüren • lokale Feuerlöscher • Brand- bzw. Rauchmeldern mit Direktaufschaltung zur Feuerwehr.
Schlüssel und andere Türöffnungssysteme (z.B. Magnetkarten) werden ausschließlich personenbezogen ausgegeben und protokolliert.
Es existiert ein mehrstufiges Sicherheits- und Schließkonzept für besonders schützenswerte Räume. Die Schlüsselausgabe erfolgt nur an einen eingeschränkten Personenkreis und wird protokolliert.
Die Serverräume sind durch stets verschlossene Sicherheits- und Brandschutztüren von den übrigen Räumen abgetrennt.
Die TK-Anlage ist von den übrigen Räumen abgetrennt.

3.2 Zugangskontrolle

In Abgrenzung zur „räumlichen" Zutrittskontrolle müssen Maßnahmen der Zugangskontrolle die Benutzung von Datenverarbeitungsanlagen durch unbefugte Personen verhindern. Es muss hier eine Identifikation der Nutzer und Prüfung der Berechtigungen erfolgen, um eine unzulässige Kenntnisnahme oder gar eine Änderung oder Löschung von personenbezogenen Daten zu verhindern.

Folgende Maßnahmen zur Zugangskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Es werden ausschließlich individuelle, persönliche Benutzerkennungen angewendet und keine Gruppenpasswörter genutzt.

Maßnahmen
Es existiert eine systemseitige und mittels Arbeitsanweisung festgelegte Passwortregelung: • Es werden mindestens 8 Zeichen und ein entsprechender Zeichenmix verwendet. • Das Passwort wird regelmäßig gewechselt (z.B. nach 3 Monaten).
Es erfolgt eine systemseitige Einschränkung der Passwortwahl, damit z.B. bereits verwendete Passwörter nicht abwechselnd genutzt werden können.
Es gibt eine systemseitige Zugangssperre bei mehr als 3 Anmeldeversuchen.
Es erfolgt eine systemseitige Bildschirmsperre bei Pausen mit Passwort Aktivierung.
Der Zugang zu den Systemen (An- und Abmeldung) wird protokolliert.
Es existieren verschiedene Berechtigungsstufen und Zuteilung dieser auf die Nutzer.
Es ist eine Firewall und ein Virenscanner installiert. Gemäß Checklisten und Protokollen werden regelmäßige Updates und Sicherheitspatches installiert, um das Schutzniveau hoch zu halten.
Für die IT-Systeme werden Administratoren eingesetzt. Diese nutzen spezielle Passwortkonventionen. Die Administratorenarbeit wird systemseitig protokolliert.
Fernwartung erfolgt unter Verwendung eines Virtual Private Networks (VPN).

3.3 Zugriffskontrolle

Mitarbeiter des Auftragsverarbeiters und Dritte mit entsprechenden Berechtigungen dürfen nur auf Daten zugreifen, die für die Erbringung der Dienstleitung relevant und erforderlich sind. Bei der Zugriffskontrolle geht es daher darum, die berechtigten Zugriffe auf Daten insoweit zu beschränken als es für die zugreifenden Personen möglich und nötig ist.

Die verschiedenen Berechtigungen können dabei den Zugriff auf bestimmte Teile des Netzwerkes, bestimmte Programme und/oder bestimmte Bearbeitungsrechte (Leserechte, Druckrechte, Veränderungsrechte) regeln. Darüber hinaus bietet es sich an, berechtigte Zugriffe zu protokollieren, um später nachvollziehen zu können, wer wann auf welche Daten zugegriffen und diese eventuell verändert hat.

Folgende Maßnahmen zur Zugriffskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Es existiert ein rollenbasiertes Berechtigungskonzept (verschieden Berechtigungsstufen) für die Zugriffe der Mitarbeiter auf Daten. Die Rechteverwaltung erfolgt durch Administratoren.
Die Clear Desk Policy des Auftragsverarbeiters wird eingehalten.
Es erfolgt eine restriktive Rechte-Vergabe auf Basis eines „Need-to-know" Ansatzes.

[illegible]
Die Berechtigungsvergabe wird regelmäßig überprüft, protokolliert und die Protokolle werden für einen festgelegt Zeitraum aufbewahrt.
Es erfolgt eine organisatorische Trennung von Administration und Betrieb/Anwendung.
Der Zugang zu den Systemen (An- und Abmeldung) wird protokolliert und die Zugriffsprotokolle werden periodisch ausgewertet.
Insofern externe Datenträger für die Speicherung von Kundendaten genutzt werden, werden diese Datenträger, die Daten des Auftraggebers enthalten, gemäß dem Stand der Technik verschlüsselt. Die Aufbewahrung findet in gesicherten Räumen statt.
Datenschutzgerechte Datenträgerentsorgung. Die physikalische Vernichtung erfolgt gemäß DIN 66399 mindestens in Sicherheitsstufe 3
Die Vernichtung von Ausdrucken mit personenbezogenen Daten des Auftraggebers erfolgt durch entsprechende Aktenvernichter (cross cut).

4. Sicherstellung von Nichtverkettbarkeit durch Zweckbestimmung

4.1 Verwendungszweckkontrolle/Trennungskontrolle

Zu unterschiedlichen Zwecken erhobene personenbezogene Daten müssen natürlich auch getrennt gespeichert und ausgewertet werden. Diesem Erfordernis wird das Datentrennungsgebot gerecht, welches organisatorische und technische Maßnahmen zur Datentrennung verlangt.

Getrennt werden müssen beispielsweise Mitarbeiter- und Kundendaten, oder auch die Daten verschiedener Kunden bei einem Auftragsverarbeiter. Eine physikalische Trennung (verschiedene Datenträger) ist jedoch nicht immer umsetzbar oder wirtschaftlich sinnvoll. Es ist daher ausreichend wenn die Daten logisch getrennt voneinander gespeichert werden. Dafür ist es ausreichend wenn die Daten beispielsweise nur über verschiedene Zugangsdaten erreichbar sind.

Folgenden Maßnahmen zur Trennungskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

[illegible]
Sofern keine dedizierten Systeme für genau einen Kunden zum Einsatz kommen, müssen die genutzten Systeme mandantenfähig sein.
Zur Sicherstellung des Produktivbetriebs ist das Entwicklungssystem vollständig von den Produktivsystemen getrennt. Ein Austausch findet ausschließlich im für die Verarbeitung erforderlichen Rahmen und Umfang statt (Programmdateien, Parameterdateien, etc.)

4.2 Pseudonymisierung

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Folgende Maßnahmen zur Pseudonymisierung müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Anonymisierte Kennungen, welche nur mit Hilfe einer separaten Datenbank auflösbar sind.
Überwiegender Einsatz von Serverkennungen, die Rückschlüsse auf die Funktion verbergen.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Datenschutz-Management

Das Datenschutz-Management gibt organisatorische Maßnahmen vor, die für die Gewährleistung eines rechtskonformen Umgangs mit personenbezogenen Daten ergriffen werden müssen.

Das Datenschutz-Management besteht im Wesentlichen aus der Audit Funktion (lfd. Bestandsaufnahme existierender Datenschutzprozesse), der Governance Funktion (Steuerung des Datenschutzes) sowie der Awareness Funktion (Aufklärung / Information der Mitarbeiter) und beinhaltet u.a. folgende Prozesse:

- interne Prüfungen vor Beginn neuer Verarbeitungen personenbezogener Daten,
- schriftliche Richtlinien („Datenschutzstrategien") zur Gewährleistung der Grundsätze zur Datenqualität, Unterrichtung, Sicherheit und Betroffenenrechte,
- ständige Aktualisierung von Verarbeitungsverzeichnissen,
- Bestellung eines Datenschutzbeauftragten,
- Durchführung von Mitarbeiterschulungen,

- Beschwerde- und Data-Breach-Management (s. ergänzend Ziffer 5.2).

Folgenden Maßnahmen zum Datenschutz-Management müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet worden und sind gemäß DS-GVO, Artikel 29 und 32 (4) angewiesen, personenbezogene Daten nur auf Anweisung des Verantwortlichen zu verarbeiten.
Der Auftragnehmer führt jährlich Schulungen durch, um das Datenschutzbewusstsein der eingesetzten Mitarbeiter jährlich zu stärken.
Die technischen und organisatorischen Maßnahmen zum Datenschutz gemäß DS-GVO, Artikel 32, werden im Rahmen der ISO-Zertifizierung regelmäßig überprüft.

5.2 Incident-Response-Management

Es müssen IT-Sicherheitskonzepte und Notfallpläne für das Vorgehen beim Ausfall von IT-Systemen sowie für den Fall schwerwiegender Datenschutzverstöße existieren.

Des Weiteren ist eine abgestufte Meldepflicht von Datenpannen an Aufsichtsbehörden und Betroffene vorgesehen. Grundsätzlich muss jede Datenpanne der zuständigen Aufsichtsbehörde gemeldet werden, es sei denn, dass sie „voraussichtlich nicht zu einem Risiko" des Betroffenen führt. Die Meldung der Datenpanne muss innerhalb von 72 Stunden bei der zuständigen Aufsichtsbehörde stattfinden. Ein Überschreiten der Frist ist nur in begründeten Fällen möglich. Die Meldungen haben u.a. die Art der Datenpanne, die Kategorien von betroffenen Daten, die Anzahl der Betroffenen und der Datensätze, eine Einschätzung der Folgen für den Betroffenen sowie die Maßnahmen zur Ursachenbeseitigung bzw. zur Schadensminimierung beim Betroffenen zu umfassen.

Es ist daher ein Incident-Response-Management vorzuhalten, dass die vorstehenden Anforderungen erfüllt.

Folgenden Maßnahmen zum Incident-Response-Management müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Auftretende Security Ereignisse werden nach einem „ITIL Best Practice" angelehnten Betriebsverfahren bearbeitet, um möglichst zeitnah einen störungsfreien Betrieb wiederzuer-

Maßnahmen
langen.
Security Incidents werden zeitnah überwacht und analysiert. Abhängig von der Art des Ereignisses nehmen an deren Bearbeitung zuständige und notwendige Service Teams und Spezialisten teil.

6. Datenschutzfreundliche Voreinstellungen

Für IT-Systeme sind sog. „datenschutzfreundliche Voreinstellungen" vorzunehmen. Es werden technische Spezifikationen als Grundmodus abverlangt, die vor allem dem Gebot der Datenminimierung Rechnung tragen. Im jeweiligen IT-System ist die Wahl der Voreinstellungen auf das für den jeweiligen Verarbeitungszweck Erforderliche zu begrenzen.

Das Gebot datenschutzfreundlicher Voreinstellungen erstreckt sich auf

- die Menge der erhobenen personenbezogenen Daten,
- den Umfang ihrer Verarbeitung,
- ihre Speicherfristen und
- ihre Zugänglichkeit (Zugangsbeschränkungen).

Folgenden Maßnahmen zu datenschutzfreundlichen Voreinstellungen müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

Maßnahmen
Die Menge der personenbezogenen Daten wird z. B. dadurch minimiert, dass personenbezogene Daten in Logfiles nur sehr restriktiv eingesetzt werden.
Transparenz in Bezug auf die Funktionen und die Verarbeitung Daten wird dadurch hergestellt, dass dargestellt wird, welche Daten für welche Funktion innerhalb der Software verwendet werden.
Daten werden so früh wie möglich gelöscht oder anonymisiert.
Die Zugriffsmöglichkeiten auf Daten wird auf das notwendige Maß minimiert

6.1 Auftragskontrolle

Die Auftragskontrolle soll sicherstellen, dass sich der Auftragsverarbeiter auch an die Weisungen des Auftraggebers hält und Datenverarbeitung nur innerhalb dieser Weisungen stattfindet. Denn allein die Weisungsgebundenheit führt dazu,

dass eine Weitergabe von Daten an den Auftragsverarbeiter nicht als Weitergabe an Dritte gewertet wird, welche zustimmungsbedürftig wäre.

Die Auftragskontrolle verlangt deshalb nach in Art und Umfang verhältnismäßigen Maßnahmen, welche sicherstellen, dass das Übermitteln, Speichern, Nutzen, Verändern und Löschen personenbezogener Daten nur nach Vorgabe des Auftraggebers beim Auftragsverarbeiter erfolgen kann. Zum einen hat also der Auftragsverarbeiter die Weisungen des Auftraggebers einzuhalten, zum anderen muss der Auftraggeber dafür Sorge tragen, dass seine Weisungen verständlich und umsetzbar sind und auch befolgt werden.

Die Weisungen können dabei in jeder Form erteilt werden, es empfiehlt sich jedoch eine Form zu wählen, die zum einen Irrtümer vermeidet und später ordentliche Nachweise ermöglicht. In der Praxis lassen sich diese Erfordernisse am besten über die Nutzung von Formularen (schriftlich oder elektronisch) bei der Auftragserteilung umsetzen. In den Weisungen sollte immer auch enthalten sein, welche Daten wie übermittelt werden sollen.

Erfolgte Maßnahmen sind sowohl vom Auftraggeber, als auch vom Auftragsverarbeiter ständig auf ihre Umsetzung zu überprüfen und gegebenenfalls zu verbessern.

Folgende Maßnahmen zur Auftragskontrolle müssen mindestens durch den Auftragsverarbeiter umgesetzt werden:

[illegible]
Es werden detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung, Nutzung, Wartung, usw. personenbezogener Daten des Auftraggebers, sowie über deren Zweckbindung im Vertrag festgehalten.
Die Erteilung von Weisungen erfolgt in schriftlicher oder elektronischer Form. Mündliche Weisungen sind nur in begründeten Ausnahmefällen zulässig und müssen unverzüglich schriftlich von Auftraggeber bestätigt werden.
Während der Durchführung der beauftragten Dienstleistung erfolgt eine Kontrolle der Auftragsausführung. Für die Kontrolle der Auftragsausführung wird ein gemäß ITIL „Best Practice" beschriebenes Change Vorgehen praktiziert. Dementsprechend ist nur ein zuvor autorisierter Kundenvertreter berechtigt, einen Change freizugeben.
Eine genehmigte Weitergabe an Dritte (Subunternehmer) ist nur zulässig, wenn die Zusammenarbeit in einem entsprechenden Vertrag geregelt ist und die Schutzmaßnahmen des Subunternehmers die gleichen Kriterien wie die des Auftragsverarbeiters erfüllen. Die Subunternehmer werden in regelmäßigen Abständen sowie bei besonderen Vorkommnissen auf die Einhaltung des Schutzniveaus überprüft.

Dieses Werk ist eine Übersetzung aus dem Englischen.

GNU General Public License (GPL), Version 2.0

- Die aktuelle Version der GNU GPL, Version 3.0
- Was ist bei einer möglichen Lizenzverletzung zu tun
- Übersetzungen der GNU GPL, Version 2.0
- GNU GPL, Version 2.0: Häufig gestellte Fragen
- Die GNU GPL, Version 2.0, ist in weiteren Formaten abrufbar (auf Englisch): Nur Text, Texinfo, LaTeX, Nur HTML (autonom), Docbook

---

Inhalt

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by

others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

> **a)** You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
> **b)** You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
> **c)** If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works

based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

> **a)** Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
> **b)** Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
> **c)** Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of what it does.
Copyright (C) yyyy  name of author

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA  02110-1301, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w'.  This is free software, and you are welcome
to redistribute it under certain conditions; type `show c'
for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Copyright-Hinweis siehe oben.

Report Penetrationstest

beA-Kanzleisoftware-Schnittstelle

Auftraggeber: [redacted]

Version:	*1.0*
Datum:	*29.04.2016*
Status:	***Final***
Seitenanzahl:	*21*
Klassifizierung:	*Vertraulich*

Autor: [redacted]
E-Mail: [redacted]*@atos.net*
Atos IT Solutions and Services GmbH

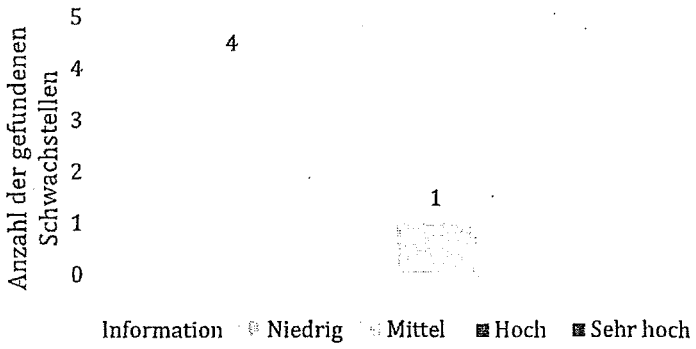
Inhaltsverzeichnis

1 Management Summary

Für die Applikation beA-Kanzleisoftware-Schnittstelle wurde im Zeitraum vom 14.03.2016 bis 22.03.2016 ein Penetrationstest durchgeführt. Ziel des Penetrationstests war die Überprüfung der SOAP Schnittstelle beA-Kanzleisoftware-Schnittstelle auf Schwachstellen der OWASP Top 10 und Schwächen im Rollen- und Rechtemodell.

Die beA-Kanzleisoftware Schnittstelle ermöglicht es Herstellern von Kanzleisoftware Lösungen den Zugriff auf das beA in Ihre Produkte zu integrieren. Die Kanzleisoftware-Schnittstelle besteht aus einer fachlichen Schnittstelle zum Zugriff auf Postfächer und Nachrichten und einem dazugehörigen optionalen Toolkit, welches die Ver- und Entschlüsselung von Nachrichten und von Anhängen durchführt und die Signaturerstellung und Prüfung anbietet.

Grundsätzlich ergaben sich aus dem Penetrationstest 1 Schwachstelle mit mittlerer Kritikalität und 4 Informationen.



Zusammenfassung der gefundenen Schwachstellen

Die Bewertung der gefundenen Schwachstellen erfolgt aus rein technischer Sicht auf Basis des CVSS Base Score.

Maßnahmen sollten sein, dass Schwachstellen mit der Kritikalität „Sehr hoch" und „Hoch" umgehend bereinigt werden müssen, während Schwachstellen mit der Kritikalität „Mittel" bereinigt werden sollten.
Des Weiteren wäre es sinnvoll die als „Niedrig" eingestuften Schwachstellen ebenfalls zu bereinigen.

Die Applikation ist anfällig für Denial-of-Service Angriffe. Durch eine hohe Anzahl automatisch generierter Requests kann die Erreichbarkeit des Servers temporär unterbrochen werden.

Das untrustedCertificate, welches mit dem Webservice Aufruf getConfiguration abgerufen wird, kann ausgetauscht werden. Dadurch ist eine erfolgreicher Man-in-the-Middle möglich.

Verschiedene Fehlerseiten beinhalten Informationen, wie z.B. Server Version oder möglichen Entry Points.

Die TLS Verschlüsselungskonfiguration konnte aus dem Atos-Netz heraus nicht getestet werden. Diese sollte vor der Produktivsetzung auf mögliche Schwachstellen untersucht werden.

2 Auftragsdetails

Untersuchungsgegenstand und überprüfte Komponenten:

- Name der Applikation
  - Applikation: beA-Kanzleisoftware-Schnittstelle
  - URL: https://test.bea-brak.de
  - Webservice: beAPortType
- Ziel des Penetrationstests
  - Penetrationstest OWASP Top 10
  - Überprüfung Rollen- und Rechtemodell
- Out of Scope
  - Denial of Service
- Testzeitraum
  - 14.03.2016– 22.03.2016
- Benutzerkonten, Rollen und Rechte
  - Zertifikat: [redacted]
  - Zertifikat: [redacted]
  - Zertifikat: [redacted]
- Verwendete Quell IP Adresse:
  - IP Adresse: Atos Intranet
- Rahmenbedingungen
  - Der Penetrationstest wurde aus dem Atos Intranet durchgeführt.
  - Der CVSS Temporal und Environmental Score finden keine Anwendung bei der Gewichtung der Schwachstellen.

Auftraggeber:

- [redacted]@atos.net, +49 [redacted]

Auditor:

- [redacted]@atos.net, +49 [redacted]

3 Schwachstellenübersicht

Entsprechend der international anerkannten Organisation „National Vulnerability Database (NVD) of the National Institute of Technology (NIST)" wird die empfohlene Bewertung des Risikos anhand der CVSS v3.0 Base Score Metrik entsprechend der folgenden Tabelle angegeben.

Risikobewertung	CVSS Score
Sehr hoch	9,0-10
Hoch	7,0 - 8,9
Mittel	4,0 - 6,9
Niedrig	0,1 - 3,9
Information	0

3.1 Übersicht nach Schwachstellenkategorien

	CVSS Score				
Schwachstelle	**Info**	**Niedrig**	**Mittel**	**Hoch**	**Sehr hoch**
Information Gathering					
Server Version wird auf Fehlerseite preisgegeben	0				
Informationen auf Fehlerseite	0				
Configuration and Deployment Management Testing					
Fremdes UntrustedCertificate wird akzeptiert	0				
Denial of Service Angriff möglich			5		
Identity Management Testing					
Authentication Testing					
Authorization Testing					
Session Management Testing					
Input Validation Testing					
Testing for Error Handling					
Testing for weak Cryptography					
Verschlüsselungskonfiguration konnte nicht getestet werden	0				
Business Logic Testing					
Client Side Testing					

3.2 Zusammenfassung der Empfehlungen

In diesem Kapitel werden die empfohlenen Maßnahmen gesammelt aufgelistet bzw. zusammengefasst. Ziel ist es, sich schnell einen Überblick über die nötigen Schutzmaßnahmen verschaffen zu können. Die einzelnen genaueren Beschreibungen der Maßnahmen werden jeweils den betreffenden
Schwachstellen beigefügt.

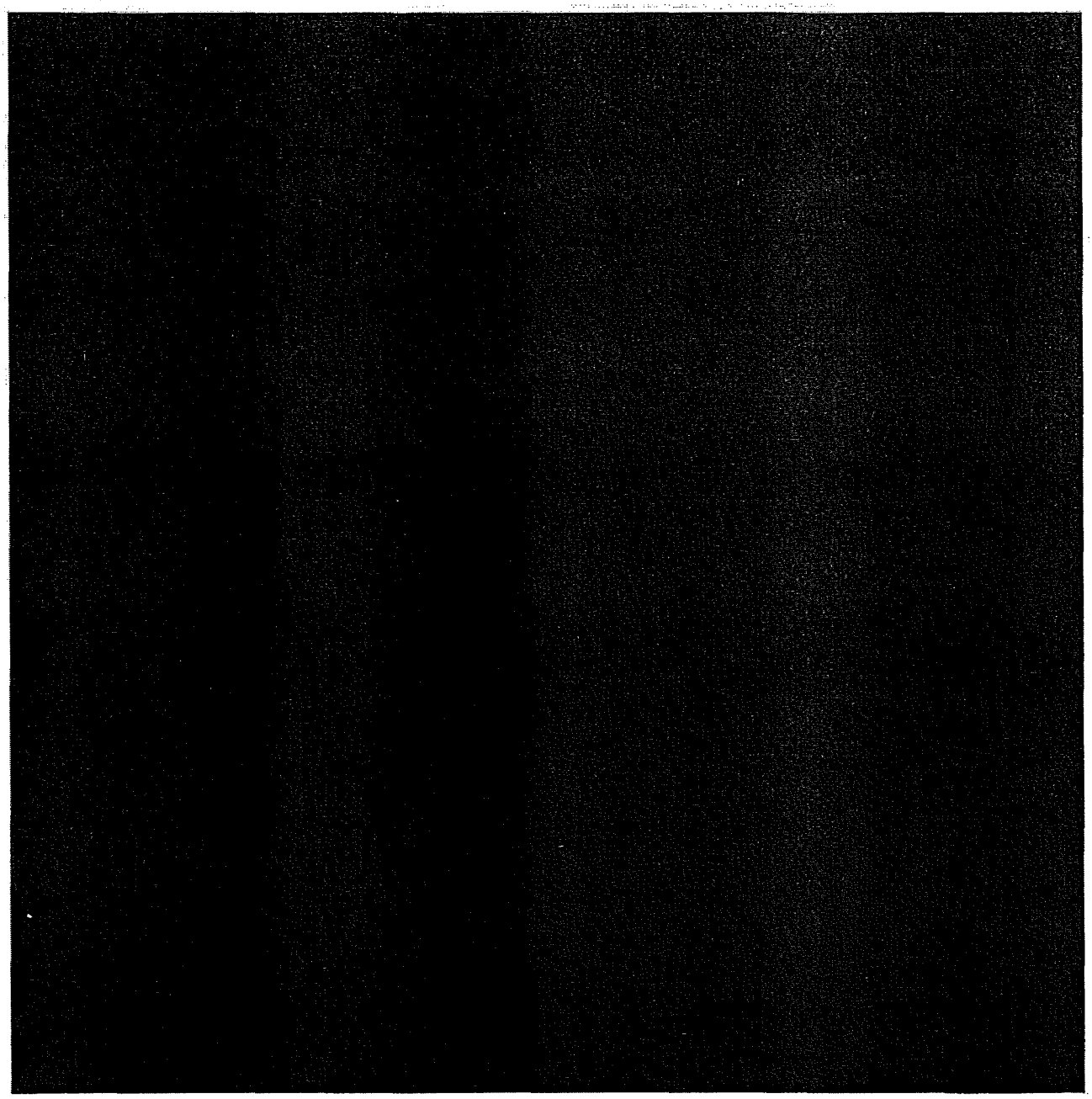
Folgende Maßnahmen werden vorgeschlagen:

1. Gegen DoS-Angriffe sollte ein entsprechender Schutzmechanismus realisiert werden, z.B. Requestlimitierung auf Benutzer.
2. Falsche Zertifikate sollten auf [redacted] erkannt und geblockt werden.
3. Fehlerseiten sollten bereinigt werden und unnötige Informationspreisgaben entfernt werden
4. Die Verschlüsselungskonfiguration sollte vor Produktivsetzung auf mögliche Schwachstellen überprüft werden.

Für die Priorisierung von Maßnahmen zur Reduktion von potentiellen Schwachstellen ist nicht nur die bloße Anzahl von Schwachstellen entscheidend. Viel wichtiger ist die Kritikalität der Schwachstellengruppen – also das Schadenspotential das entsteht, wenn eine Schwachstelle ausgenutzt werden würde. Z.B. sind eine fehlende Authentifizierung oder ein Standardpasswort kritischer zu bewerten als die Schwachstelle eines veralteten Verschlüsselungsalgorithmus.

4 Durchgeführte Tests und Ergebnisse

In den folgenden Unterkapiteln werden die Schwachstellen und Funde angelehnt an den OWASP Testing Guide gruppiert und detailliert dokumentiert.



4.1.2 Informationen auf Fehlerseite

Information

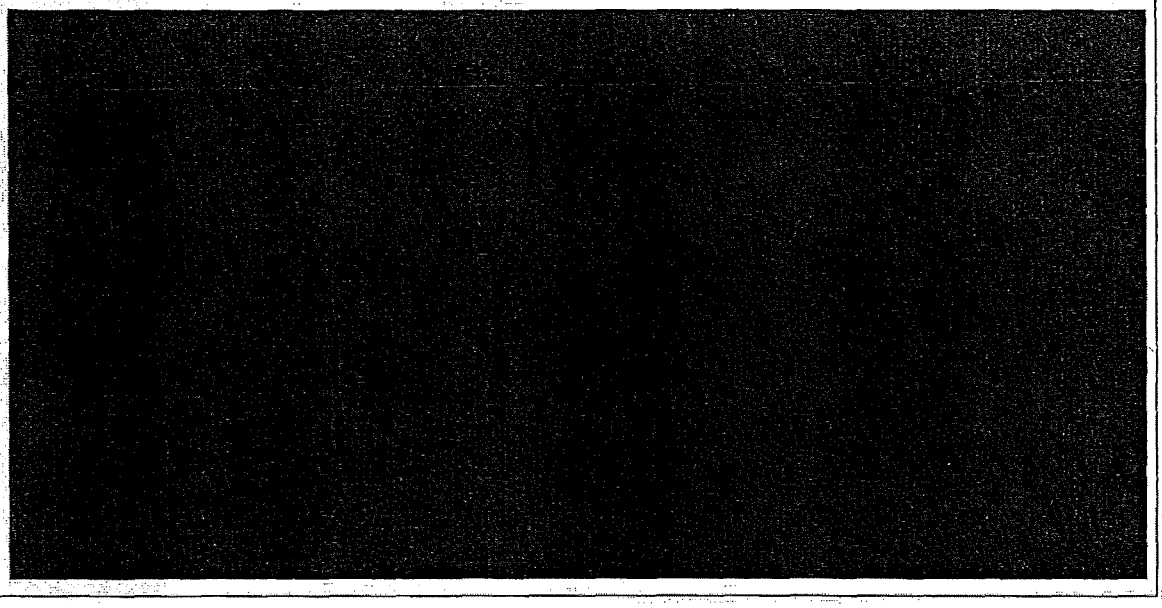
0
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N

Die Applikation soll nur über ein vorgeschaltetes Proxy System (oder Load Balancer) erreichbar sein. Über den Aufruf von mindestens einer URL antwortet das System mit einem Verweis auf das eigentlich verwendete Back-End- oder ein anderes System. Ein Angreifer kann mit dem Wissen um die zugrunde liegenden Back-End Systeme sein Angriffe zielgerichteter durchführen.

Wenn Systeme hinter Load Balancern oder Proxies betrieben werden, sollten sämtliche Verweise von IP Adressen oder FQDN auf die vorgeschalteten LoadBalancer/Proxies zeigen.

https://test.bea-brak.de/bea/BeAPortType/forgot_password.%7Bpb

Die o.g. URL verursacht bei Eingabe eine Fehlerseite, welche einige Informationen, u.a. eine IP-Adresse enthält.



4.2 Configuration and Deployment Management Testing

4.2.1 Fremdes UntrustedCertificate wird akzeptiert

Information

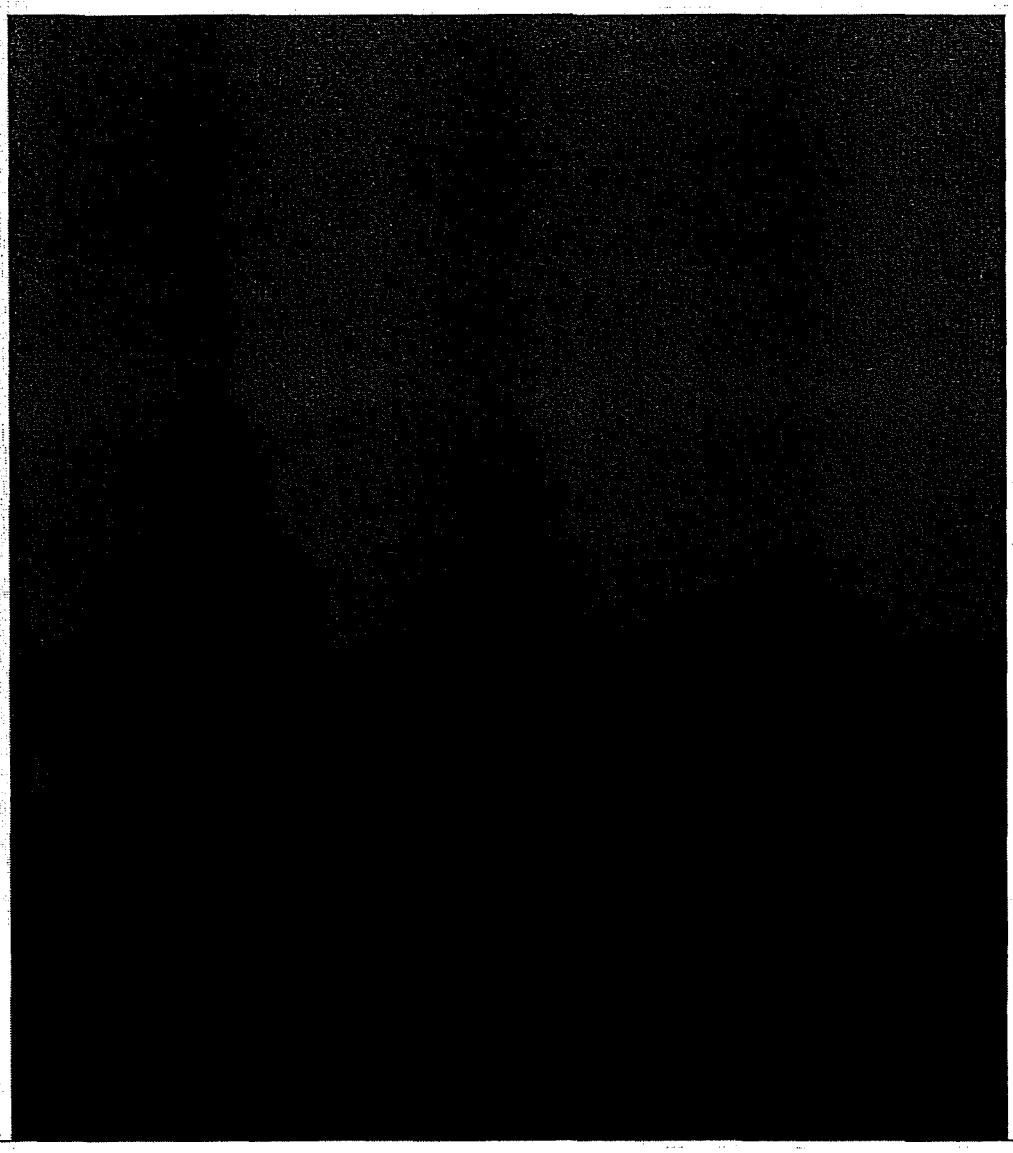
0
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N

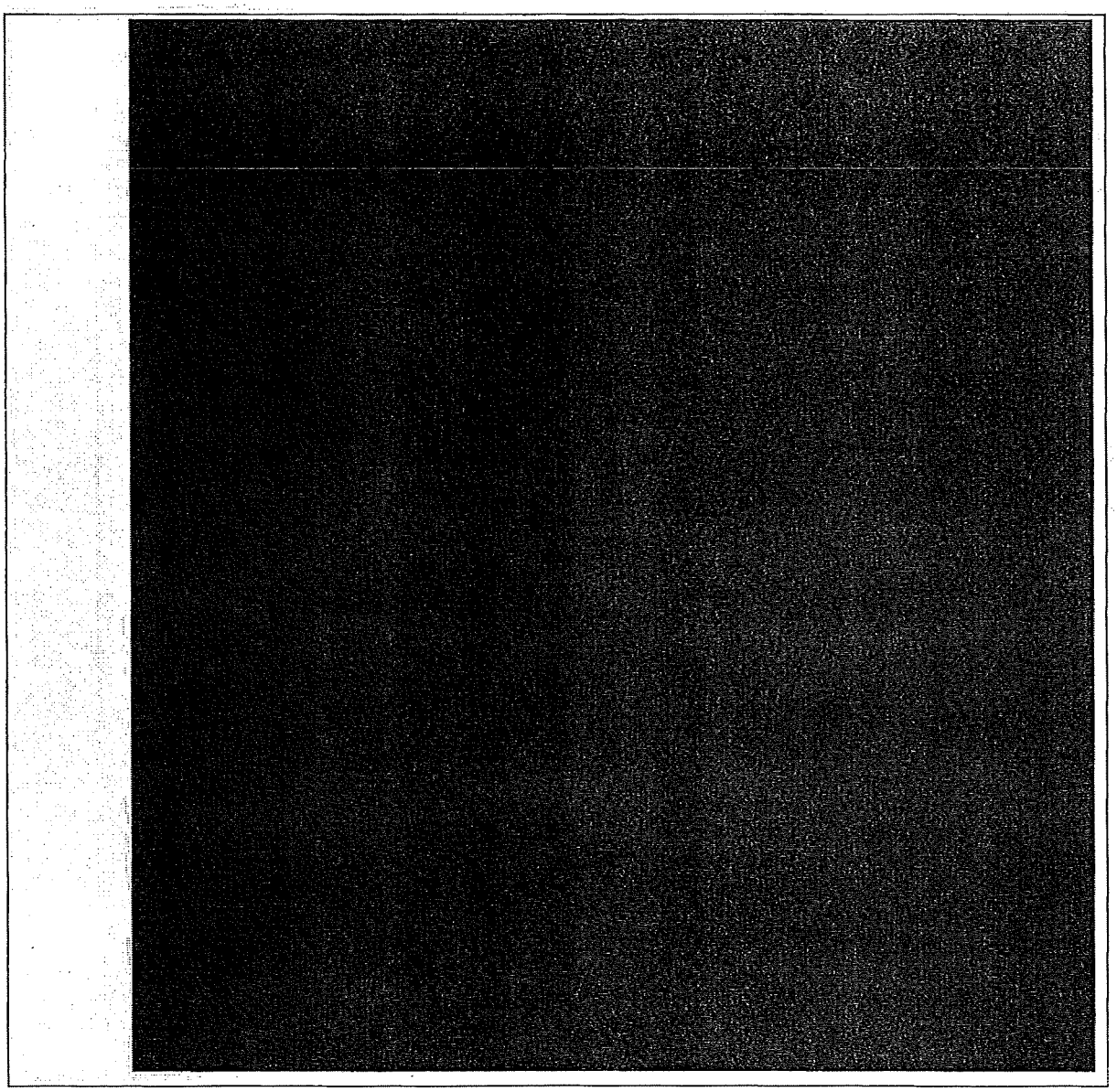
Das mit dem Webservice getConfiguration angefragte untrustedCertificate kann durch eine Man-in-the-Middle Angriff ausgetauscht werden. Während des Tests konnte in der Server Response zu diesem Webservice das ursprüngliche untrustedCertificate gegen das Zertifikat der Man-in-the-Middle Software ausgetauscht werden, welches auch dem Java-Keystore hinzugefügt wurde. Governikus lässt die Anmeldung zu und der Traffic kann durch die Software mitgelesen werden.

Hinweis:
Da es sich bei diesem Finding um einen Angriff auf die Clientinstanz handelt und der SOAP Webservice selbst keine Verwundbarkeit aufweist, wird dieser Befund lediglich als „Information" bewertet.

Auf Governikus-Seite sollte ein entsprechender Whitelisting-Ansatz realisiert werden, der das Einfügen eines solchen Zertifikates verhindert.

getConfiguration





4.2.2 Denial of Service Angriff möglich

Mittel

5
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:L

Das Backend-System kann durch Denial of Service Angriffe temporär außer Betrieb gesetzt werden. Während des Tests ist das aufgefallen, als ein automatischer Scanner die Applikationsstruktur auf mögliche Schwachstellen untersuchen sollte und zu diesem Zweck eine große Anzahl an Requests an das System gesendet hat. Nach kurzer Zeit hat das System nicht mehr reagiert und konnte nicht mehr erreicht werden. Angreifer haben dadurch die Möglichkeit, für möglicherweise schwerwiegende Systemausfälle zu sorgen.

Das System sollte einen entsprechenden Schutz gegen solche Denial of Service Angriffe aufweisen. Beispielsweise könnten Benutzer, von denen eine ungewöhnlich hohe Anzahl an Requests kommt, anhand der IP gesperrt werden.

https://test.bea-brak.de

Nach kurzer Verwendung eines automatischen Scanners war das Backendsystem temporär nicht mehr erreichbar.

[redacted]

4.3 Testing for weak Cryptography

4.3.1 Verschlüsselungskonfiguration konnte nicht getestet werden

Information

0
CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:N

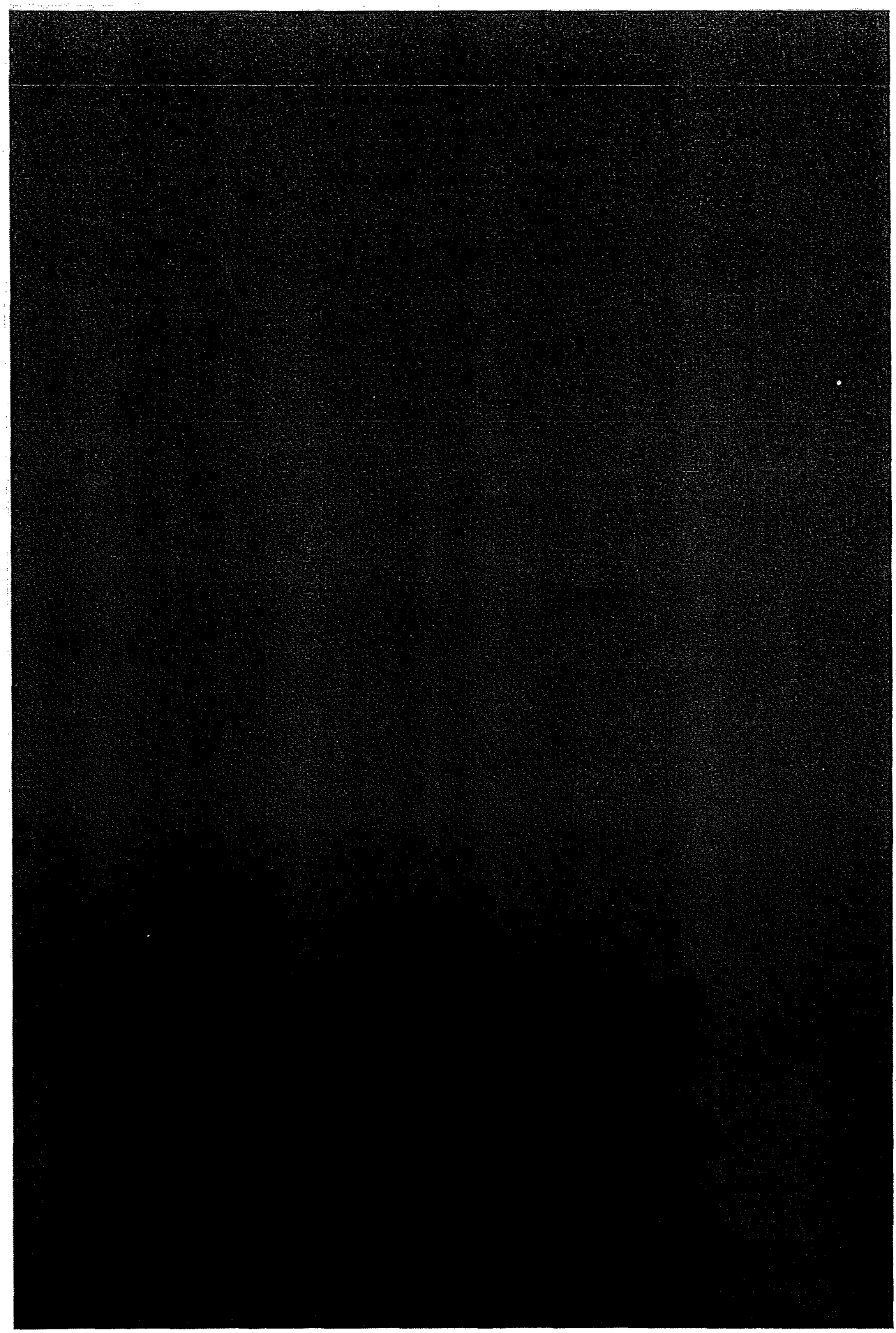
Zum Aufbau abgesicherter Verbindungen und zum Verschlüsseln der Datenübertragung kann Secure Sockets Layer (SSL) bzw. Transport Layer Security (TLS) eingesetzt werden. Bei der sicheren Kommunikation zwischen einem Client und Server, können mittels SSL/TLS unterschiedliche Technologien, Algorithmen und Zertifikatstypen verwendet werden. Einige der Algorithmen, die zur Verschlüsselung und Signierung eingesetzt werden können, sind jedoch veraltet bzw. kompromittiert. Ein Angreifer kann Schwachstellen in veralteten Algorithmen dazu verwenden, um die Vertraulichkeit und Integrität der Kommunikation zu verletzen.

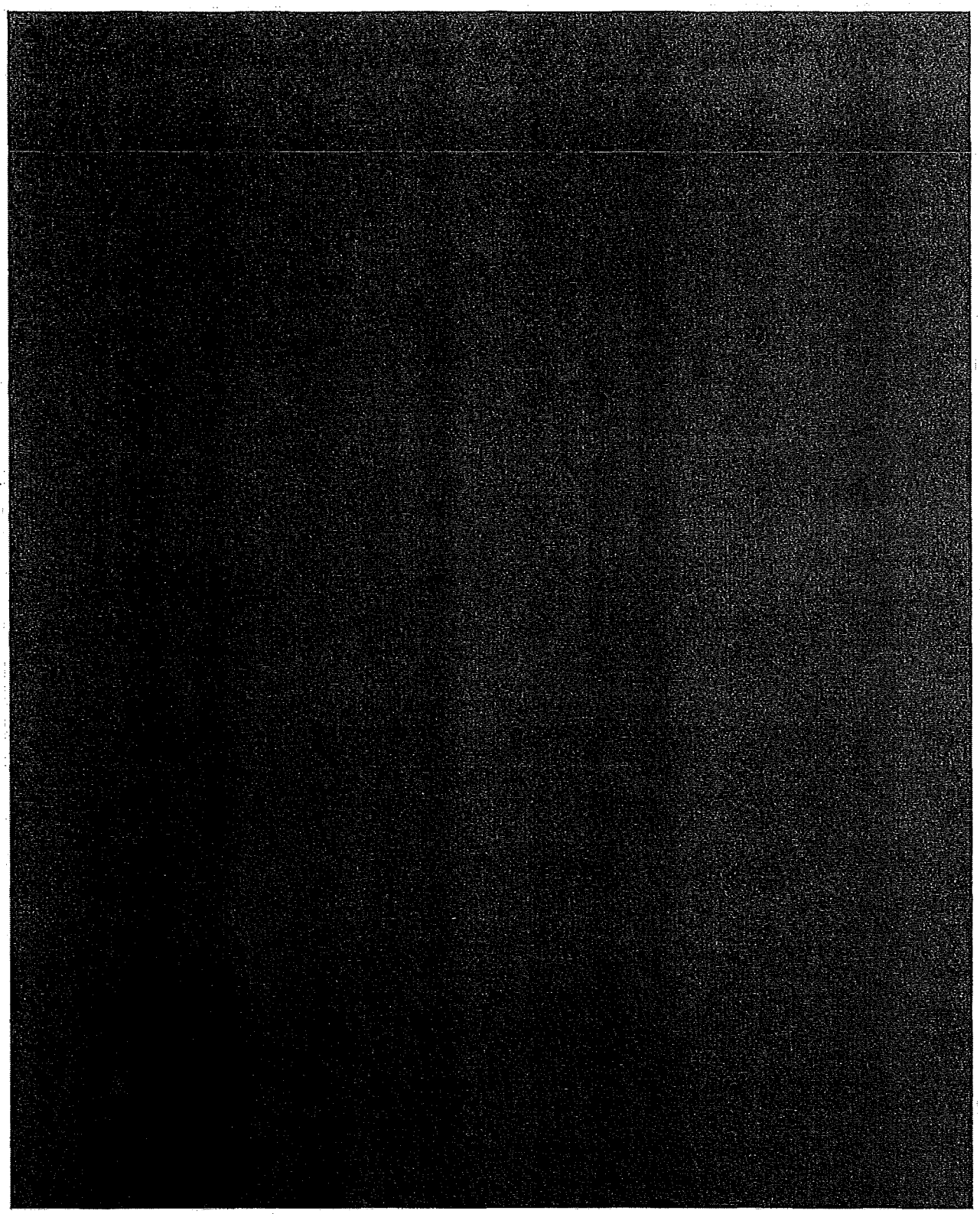
Hinweis:
Es war nicht möglich, die eingestellte Serverkonfiguration auf unsichere Verschlüsselungsalgorithmen zu testen.

Vor Produktivsetzung sollte der entsprechende Server erneut geprüft und die Konfiguration ggf. angepasst werden.

https://test.bea-brak.de

4.4 Durchgeführte Testszenarien

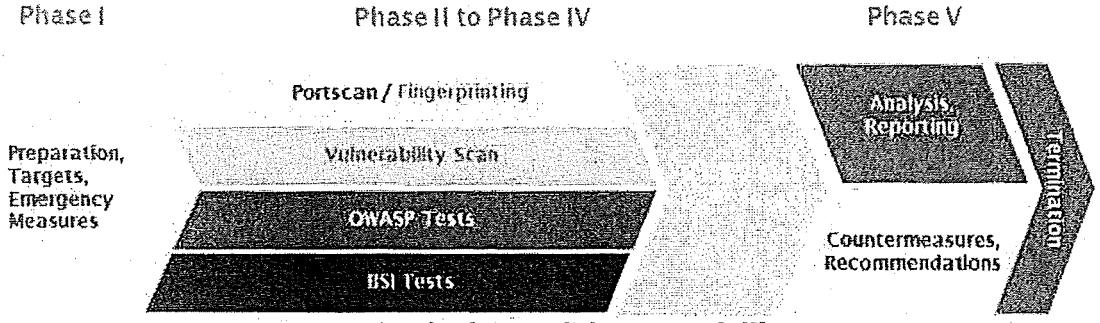




5 Allgemeine Informationen

5.1 Test Durchführung

Grundsätzlich sind die Penetrationstests für Web-Applikationen an den OWASP1 Testing Guide angelehnt, welcher ein großes und effizientes Spektrum für die Überprüfung dieser Services bietet.



Test Methodology (Phasenmodell)

Phase 1:
Bevor die eigentlichen Tests und Scans beginnen, müssen zunächst in Phase 1 die entsprechenden rechtlichen Bedingungen und weitere Anforderungen sowie der genaue Scope des Tests spezifiziert werden. Sind sämtliche organisatorischen Rahmenbedingungen ausgehandelt kann mit dem Start von Phase 2 begonnen werden.

Phase 2:
In diesem Abschnitt des Penetrationstests wird das Testobjekt durch erste Analysen wie Port-Scans und Foot-printing analysiert. Des Weiteren werden in dieser Phase automatisierte Scan-Tools zum Einsatz gebracht, um so viele Informationen wie möglich über das Testobjekt zu sammeln und um erste automatisierte Angriffe auf die Systeme durchzuführen. Auf Basis der Ergebnisse der eingesetzten Tools können erste potentielle Schwachstellen eruiert werden, welche dann von den Tools bereits aktiv ausgenutzt werden. Auf Basis dieser Informationen und der Analyse aus Phase 3 werden dann weitere manuelle Attacken in Phase 4 ausgeführt.

Phase 3:
Es werden die entsprechenden Scan-Ergebnisse ausgewertet und analysiert. Dabei werden zum einen die bereits durch die Tools ausgeführten Angriffe ersichtlich und zum anderen können die gesammelten Informationen der Scans für die Ausführung von manuellen Angriffen in Phase 4 genutzt werden.

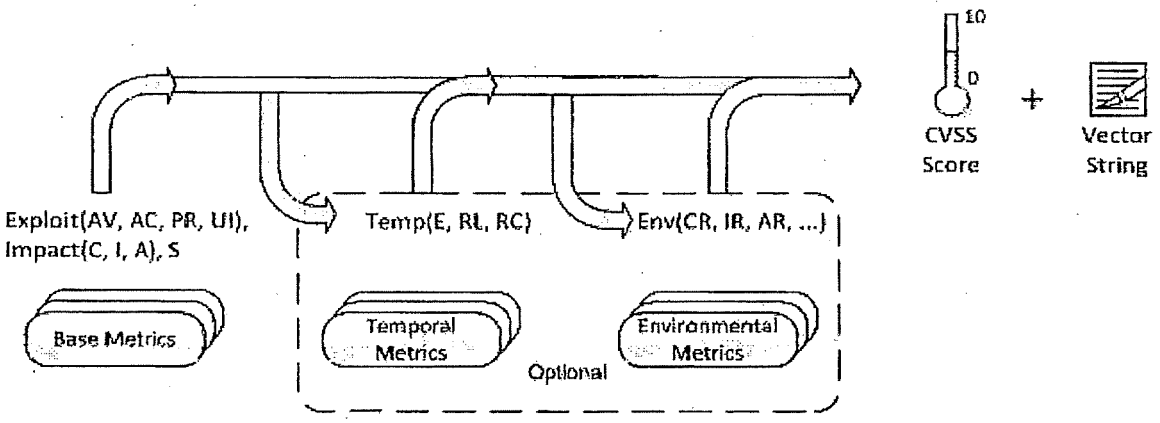
Phase 4:
Basierend auf den Scan-Ergebnissen aus Phase 2 sowie der genaueren Analyse in Phase 3 werden dann weitere manuelle Attacken auf das Testobjekt durchgeführt. In dieser Phase wird versucht Schwachstellen auszunützen um beispielsweise Angriffe für die Erweiterung von Rechten (Privilege Escalation) oder zur generellen Überprüfung von Rechten (Access Control) durchzuführen. Zusätzlich werden weitere Angriffe wie XSS oder SQL-Injection durchgeführt.

Phase 5
Abschließend werden die gefundenen Schwachstellen und Funde basierend auf dem CVSSv3 bewertet und dokumentiert. Dabei werden die Wahrscheinlichkeit der Ausnutzung sowie schwere der Schwachstelle und weitere Parameter einbezogen, um einen entsprechenden Risk Score zu generieren.

[1] Das Open Web Application Security Project (OWASP) ist eine offene Community mit dem Ziel, Unternehmen und Organisationen zu unterstützen, sichere Anwendung zu entwickeln, zu kaufen und zu warten. https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf

5.2 Common Vulnerability Scoring System (CVSS)

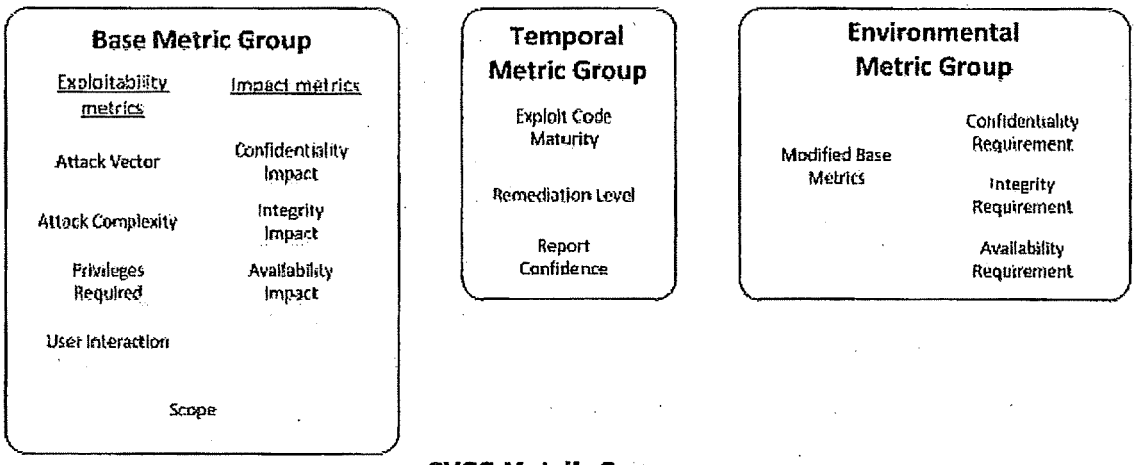
Software, Hardware und Firmware Schwachstellen stellen ein kritisches Risiko für jede Organisation dar die ein Computer Netzwerk betreibt, dabei sind diese schwer zu kategorisieren und abzuschätzen. CVSS2 bietet einen Weg die grundlegenden Charakteristiken von Schwachstellen zu erfassen und deren Schweregrad durch einen numerischen Score darzustellen. Weiterhin wird der Score auch textuell dargestellt. Der Score kann als qualitative Repräsentation (Information, niedrig, mittel, hoch, sehr hoch) übersetzt werden um Unternehmen zu helfen ihre Schwachstellen-Management-Prozesse richtig zu priorisieren und zu bewerten.



CVSS Metriken und Formeln

Die Bewertung einer Schwachstelle erfolgt anhand von drei Kategorien:

- Base Metric - Eigenschaften, die sich im Lauf der Zeit nicht ändern
- Temporal Metric - Eigenschaften, die sich im Lauf der Zeit ändern können
- Environmental Metric - Eigenschaften, die sich auf das Umfeld eines Systems beziehen



CVSS Metrik Gruppen

Atos verwendet für die Bewertung einer Schwachstelle die Base Metric Group. Die Temporal Metric Group und Environmental Metric Group finden keine Anwendung bei der Gewichtung der gefundenen Schwachstellen.

Die folgenden Kapitel beschreiben für das allgemeine Verständnis den Aufbau und Anwendung der Bases Metric Group.

[2] CVSS - Common Vulnerability Scoring System
http://www.first.org/cvss

5.2.1 Base Metric Group

Die Base Metric Group repräsentiert die wesentlichen Charakteristiken einer Schwachstelle die konstant über eine bestimmte Zeit und über die Benutzerumgebung hinaus vorhanden sind. Sie ist aus der Exploitability Metric, der Impact Metric und dem Scope zusammengesetzt.

5.2.1.1 Exploitability Metrics

Die Exploitability Metrics zeigt die Charakteristik der angreifbaren Komponenten der Schwachstelle. Daher sollte jede der unten gelisteten Exploitability Metrics relativ zu den angreifbaren Komponenten gewertet werden und die Eigenschaften der Schwachstelle wiederspiegeln die zu einem erfolgreichen Angriff führen.

Attack Vector (AV)

Diese Metrik beschreibt die Umstände unter denen eine Schwachstelle ausnutzbar ist. Der Wert dieser Metrik wird größer je weiter entfernt (logisch und physisch) der Angreifer sein kann um die schwache Komponente auszunutzen. Es besteht die Annahme, dass die Anzahl von potentiellen Angreifern einer Schwachstelle die vom Internet ausnutzbar ist größer ist, als die Anzahl potentiellen Angreifer die die Schwachstelle nur durch physischen Zugang zu einem Gerät ausnutzen können, wodurch ein höherer Score entsteht. Die Liste von möglichen Werten ist in den folgenden Punkten aufgeführt.

- Network (N)

  Eine Schwachstelle die über einen Netzwerkzugang ausnutzbar ist bedeutet, dass die angreifbare Komponente an den Network Stack gebunden und der Zugriff über OSI Layer 3 (Netzwerk-Schicht) stattfindet. Eine solche Schwachstelle wird oft „remotely exploitable" genannt. Ein Beispiel für einen Netzwerk Angriff ist ein Angriff der einen denial of service (DoS) durch senden eines speziell erstellten TCP Pakets über das öffentliche Internet (z.B. CVE 2004 0230) auslöst.

- Adjacent (A)

  Eine Schwachstelle die mit benachbartem Netzwerkzugang ausnutzbar ist meint, dass die angreifbare Komponente an den Network Stack gebunden ist, der Angriff aber auf dasselbe geteilte physikalische (z.B. Bluetooth, IEEE 802.11) oder logische (z.B. Lokales IP Subnet) Netzwerk limitiert ist und nicht über OSI Layer 3 hinweg (z.B. Router) durchgeführt werden kann. Ein Beispiel für einen Adjacent Angriff wäre eine ARP (IPv4) oder neighbor discovery (IPv6) Flooding, die zu einem denial of service auf dem lokalen LAN Segment führt. Siehe auch CVE 2013 6014.

- Local (L)

  Eine Schwachstelle die durch lokalen Zugang ausnutzbar ist bedeutet, dass die angreifbare Komponente nicht an den Network Stack gebunden ist, und der Angreifer durch read/write/execute Fähigkeiten agiert. In manchen Fällen muss der Angreifer auch lokal eingeloggt sein um die Schwachstelle auszunutzen. Andernfalls ist die Schwachstelle womöglich auf Interaktion mit dem User angewiesen um eine bösartige Datei auszuführen.

- Physical (P)

  Bei einer Schwachstelle die durch physikalischen Zugang ausnutzbar ist, muss der Angreifer die angreifbare Komponente physikalisch manipulieren. Physikalische Interaktion kann kurz (z.B. evil maid attack) oder dauerhaft sein. Ein Beispiel einer solchen Attacke ist eine Kaltstartattacke die einem Angreifer Zugang zu Schlüsseln der Festplattenverschlüsselung gewährt, nachdem er physikalischen Zugang zum System hat. Ein weiteres Beispiel sind periphere Angriffe wie z.B. Firewire/USB Direct Memory Access Angriffe.

Attack Complexity (AC)

Diese Metrik beschreibt die Bedingungen die existieren müssen um die Schwachstelle auszunutzen, auf die der Angreifer aber keinen Einfluss hat. Wie unten beschrieben, können solche Umstände mehr Informationen über das Ziel, das Vorhandensein von bestimmten Systemkonfigurationen oder Berechnungsfehler benötigen. Wichtiger Weise schließt die Bewertung dieser Metrik zur Ausnutzung der Schwachstelle jeglichen Bedarf an Interaktionen des Users aus. Der Wert dieser Metrik ist höher je einfacher der Angriff ist. Die Liste von möglichen Werten ist in den folgenden Punkten aufgeführt.

- Low (L)

  Spezielle Bedingungen oder Voraussetzungen für den Zugang existieren nicht. Ein Angreifer kann einen reproduzierbaren Erfolg gegen die angreifbare Komponente erwarten.

- High (H)

  Eine erfolgreiche Attacke hängt von den Bedingungen über die Kontrolle des Angreifers hinaus ab. So kann ein erfolgreicher Angriff nicht beliebig gelingen, sondern erfordert Aufwand des Angreifers bei der Vorbereitung oder muss erfolgen noch bevor ein erfolgreicher Angriff gegen die angreifbare Komponente erwartet wird.

Privileges Required (PR)

Diese Metrik beschreibt eine Ebene der Privilegien die ein Angreifer haben muss, bevor er erfolgreich eine Schwachstelle ausnutzen kann. Der Wert dieser Metrik ist am höchsten wenn keine Privilegien benötigt werden. Die Liste von möglichen Werten ist in den folgenden Punkten aufgeführt.

- None (N)

  Der Angreifer ist vor dem Angriff unautorisiert und braucht daher keinen Zugang zu Einstellungen oder Dateien um seinen Angriff durchzuführen.

- Low (L)

  Der Angreifer ist mit Privilegien ausgestattet die ihm grundlegende Nutzerrechte verleihen und normalerweise nur Einstellungen und Dateien betreffen die dem Nutzer gehören. Alternativ richtet ein Angreifer mit niedrigen Privilegien nur Schaden an nicht sensiblen Ressourcen an.

- High (H)

  Der Angreifer ist mit Privilegien ausgestattet die ihm signifikante (z.B. administrative) Kontrolle über die angreifbare Komponente geben und Einstellungen oder Dateien in der gesamten Komponente betreffen.

User Interaction (UI)

Diese Metrik beschreibt die Bedingungen für den Benutzer und nicht die des Angreifers, die nötig sind um erfolgreich eine Komponente angreifen zu können. Sie legt fest ob eine Schwachstelle allein durch den Angreifer oder nur mit Hilfe eines anderen Benutzers (oder eines vom Benutzer initiierten Prozesses) ausnutzbar ist. Der Wert dieser Metrik ist am größten wenn keine Interaktion eines anderen Benutzers nötig ist. Die Liste von möglichen Werten ist in der untenstehenden Tabelle aufgeführt.

- None (N)

  Die Schwachstelle kann ausgenutzt werden ohne notwendige Interaktion mit einem anderen Benutzer.

- Required (R)

  Die erfolgreiche Ausnutzung der Schwachstelle benötigt Aktionen eines Benutzers. Ein Beispiel wäre ein Exploit das nur während einer Installation einer Applikation als Systemadministrator erfolgreich wäre.

5.2.1.2 Scope

Eine wichtige Eigenschaft die von CVSS v3.0 erfasst wird ist die Fähigkeit einer Schwachstelle in einer Softwarekomponente Ressourcen zu beeinflussen die über ihre Privilegien und Mittel hinausgehen.

Formal bezieht sich Scope auf die Sammlung von Privilegien, die von einer Gruppe definiert werden (z.B. einer Applikation, einem Betriebssystem oder einer Sandbox Umgebung), denen Zugang zu einer Ressource (z.B. Dateien, CPU, Speicher, etc.) gewährt wird. In manchen Fällen wird basierend auf vordefinierten Regeln oder Standards die Autorisierung einfach oder nur ungenügend kontrolliert. Zum Beispiel im Fall von Netzwerkverkehr der zu einem Netzwerk Switch gesendet wird. Der Switch akzeptiert den Netzwerkverkehr der an einem Ports ankommt und ist die Autorität die den Verkehrsfluss zu anderen Ports kontrolliert.

Wenn es durch eine Schwachstelle einer Softwarekomponente möglich ist, Ressourcen zu beeinflussen die von einer anderen Komponente verwaltet werden, hat ein Scope „change" stattgefunden.

Man kann sich einen Scope „change" wie das Ausbrechen aus einer Sandbox vorstellen. Ein Beispiel wäre eine Schwachstelle in einer Virtuellen Maschine, die es dem Angreifer ermöglicht Dateien auf dem Host OS zu löschen. In diesem Beispiel gibt es zwei separate Privilegien Gruppen. Eine Gruppe die Privilegien für die Virtuelle Maschine mit Benutzern durchsetzt und eine andere die Privilegien für das Hostsystem, in dem die Virtuelle Maschine läuft, definiert und durchsetzt.

Ein Scope „change" würde nicht auftreten, wenn z.B. eine Schwachstelle in Microsoft Word es einem Angreifer erlauben würde alle Systemdateien des Host OS zu kompromittieren, da dieselbe Autorität (Host OS) die Privilegien der Word-Instanz des Benutzers als auch den Zugriff auf Systemdateien durchsetzt.

Der Base Score ist am größten wenn ein Scope „change" stattgefunden hat. Die Liste von möglichen Werten ist in den folgenden Punkten aufgeführt.

- Unchanged (U)

  Eine ausgenutzte Schwachstelle kann nur Ressourcen beeinflussen, die von derselben Autorität verwaltet werden. Dabei sind die angreifbare Komponente und die beeinflusste Komponente dieselbe.

- Changed (C)

  Eine ausgenutzte Schwachstelle kann Ressourcen beeinflussen, die über die vorgesehenen Privilegien hinausgehen. In diesem Fall sind die angreifbare Komponente und die beeinflusste Komponente verschieden.

5.2.1.3 Impact Metrics

Die Impact Metrik bezieht sich auf die Eigenschaften der betroffenen Komponente. Egal ob eine erfolgreich ausgenutzte Schwachstelle, eine oder mehrere Komponenten betrifft, die Impact Metrik wird der Komponente entsprechend gewertet die den schwersten Schaden erlitten hat und die am direktesten mit dem Angriff in Verbindung gebracht werden kann. Deswegen sollten die Auswirkungen die ein Angreifer verursachen kann auf ein angemessenes Ergebnis beschränkt werden.

Wenn kein Scope „change" aufgetreten ist, sollte die Impact Metrik die Auswirkungen auf confidentiality, integrity und availability(CIA) der gefährdeten Komponente reflektieren. Wenn aber ein Scope „change" aufgetreten ist, sollte die Impact Metrik die Auswirkungen auf CIA der gefährdeten Komponente oder der betroffenen Komponente reflektieren, abhängig davon welche Komponente den größten Schaden erlitten hat.

Confidentiality Impact (C)

Diese Metrik misst die Auswirkungen auf die Vertraulichkeit der Informationen die von einer Softwarekomponente verwaltet werden. Vertraulichkeit bezieht sich auf den eingeschränkten Zugang zu Informationen und für ausschließlich autorisierte Benutzer, sowie die Unterbindung des Zugangs für unautorisierte Benutzer. Der Wert dieser Metrik erhöht sich mit steigendem Verlust an Vertraulichkeit bei der betroffenen Komponente. Die Liste von möglichen Werten ist in den folgenden Punkten aufgeführt.

- High (H)

  Es besteht ein totaler Verlust der Vertraulichkeit der dazu führt, dass alle Ressourcen in der betroffenen Komponente dem Angreifer offenbart werden. Es ist auch möglich, dass nur der Zugang zu einigen Informationen durch den Angriff erfolgt ist, diese jedoch kritisch sind und dadurch direkte und ernste Auswirkungen haben können. Dies wäre der Fall, wenn ein Angreifer beispielsweise das Passwort des Administrators oder private Verschlüsselungsschlüssel eines Web-Servers erbeuten würde.

- Low (L)

  Es besteht leichter Verlust der Vertraulichkeit. Der Angreifer erhält Zugang zu einigen Informationen, hat jedoch keinen Einfluss darauf welche oder wie viele Informationen er erbeuten kann oder die Anzahl bzw. die Art des Verlusts ist beschränkt. Die Offenlegung der Informationen durch den Angreifer bedeutet keinen ernsten und direkten Verlust an Vertraulichkeit für die betroffene Komponente.

- None (N)

  Es besteht kein Verlust der Vertraulichkeit bei der betroffenen Komponente.

Integrity Impact (I)

Diese Metrik misst die Auswirkungen auf die Integrität einer erfolgreich ausgenutzten Schwachstelle. Integrität bezieht sich auf die Vertrauenswürdigkeit und Nachvollziehbarkeit von Informationen. Der Wert dieser Metrik erhöht sich mit den Konsequenzen für die betroffene Komponente. Die Liste von möglichen Werten ist in den folgenden Punkten aufgeführt.

- High (H)

  Es besteht ein totaler Verlust der Integrität oder des Schutzes. Dies wäre der Fall, wenn der Angreifer alle Dateien die von der betroffenen Komponente geschützt werden verändern kann. Alternativ wäre dies der Fall wenn nur manche Dateien verändert werden können, dies aber zu direkten und ernsten Konsequenzen für die betroffene Komponente führen würden.

- Low (L)

  Veränderung von Daten ist möglich aber der Angreifer hat keine Kontrolle über die Konsequenzen einer Veränderung oder die Anzahl der Veränderungen ist beschränkt. Die Datenveränderung hat keinen direkten und ernsten Einfluss auf die betroffene Komponente.

- None (N)

  Es besteht kein Verlust der Integrität bei der betroffenen Komponente.

Availability Impact (A)

Diese Metrik misst den Einfluss auf die Verfügbarkeit der betroffenen Komponente, die aus einer erfolgreichen Ausnutzung einer Schwachstelle resultiert. Während die Confidentiality und Integrity Impact Metriken den Verlust von Vertraulichkeit und Integrität von Daten (z.B. Informationen, Dateien) die von der betroffenen Komponente benutzt werden betreffen, bezieht sich diese Metrik auf den Verlust der Verfügbarkeit der betroffenen Komponente selbst, wie etwa ein Netzwerkservice (z.B. Web, Datenbank, Email). Da Availability die Verfügbarkeit von Informationen und Ressourcen meint, schränken Angriffe die Bandbreite, Rechenleistung oder Speicherplatz verbrauchen die Verfügbarkeit der betroffenen Komponente ein. Der Wert dieser Metrik erhöht sich mit den Konsequenzen für die betroffene Komponente. Die Liste von möglichen Werten ist in den folgenden Punkten aufgeführt.

- High (H)

  Es besteht kompletter Verlust der Verfügbarkeit der dazu führt, dass es dem Angreifer möglich ist den Zugang zu Ressourcen der betroffenen Komponente komplett zu sperren. Dieser Zustand ist entweder während des Angriffes anhaltend oder dauerhaft auch nach dem Angriff vorhanden. Alternativ kann der Angreifer auch nur kurzfristig die Fähigkeit haben die Verfügbarkeit zu blockieren, was aber direkte und ernste Konsequenzen für die beeinflusste Komponente hat (z.B. kann der Angreifer keine bestehenden Verbindungen trennen aber neue Verbindungen verhindern oder er kann eine Schwachstelle die bei jedem erfolgreichen Angriff nur etwas Speicher reserviert wiederholt ausnutzen. Nach wiederholter Ausnutzung führt dies jedoch zum Ausfall des Service.).

- Low (L)

  Es besteht reduzierte Performance oder Unterbrechungen in der Verfügbarkeit von Ressourcen. Selbst wenn eine wiederholte Ausnutzung der Schwachstelle möglich ist, hat der Angreifer nicht die Möglichkeit einen Service für legitime Benutzer vollständig zu blockieren. Die Ressourcen der betroffenen Komponente sind entweder ständig, teilweise oder sporadisch vollständig verfügbar. Es bestehen jedoch keine direkten und ernsten Konsequenzen für die betroffene Komponente.

- None (N)

  Es besteht kein Einfluss auf die Verfügbarkeit der betroffenen Komponente.

5.2.2 Base Vectors

Der v3.0 Vektor String beginnt mit dem Label „CVSS" und einer numerischen Repräsentation der aktuellen Version „3.0". Es folgen Informationen über die Metriken in Form einer Reihe von abgekürzten Metrik Namen, einem „:" und dem entsprechenden Wert der Metrik in abgekürzter Form. Die Kurzformen wurden oben in dieser Spezifikation definiert (in Klammern nach jedem Metrik Namen und Metrik Wert). Die Metriken werden durch einen Schrägstrich „/" voneinander getrennt. In der folgenden Tabelle sind die abgekürzten Metrik Namen und die möglichen Werte zusammengefasst.

Metrik Name	Mögliche Werte	Metrik Name	Möglich Werte
Attack Vector, AV	[N,A,L,P]	Scope, S	[U,C]
Attack Complexity, AC	[L,H]	Confidentiality, C	[H,L,N]
Privileges Required, PR	[N,L,H]	Integrity, I	[H,L,N]
User Interaction, UI	[N,R]	Availability, A	[H,L,N]

Beispiel: Eine Schwachstelle mit folgenden Base Metrik Werten: „Attack Vector: Network, Attack Complexity: Low, Privileges Required: High, User Interaction: None, Scope: Unchanged, Confidentiality: Low, Integrity: Low, Availability. None" ohne spezifizierte Temporal oder Environmental Metriken würde folgenden Vektor produzieren:

CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N

Anlage 8 Vertrag

Anlage zu Ziffer 16 EVB-IT Erstellungsvertrag

Sonderregelung zu Verzug und Vertragsstrafe

Anstelle von Ziffer 9.3 EVB-IT Erstellungs-AGB wird Folgendes vereinbart:

Des Weiteren ist der Auftraggeber für den Fall der Überschreitung des vereinbarten Vertragserfüllungstermins[1]* berechtigt, für jeden Kalendertag, an dem sich der Auftragnehmer mit der Einhaltung des Vertragserfüllungstermins* in Verzug befindet, eine Vertragsstrafe in Höhe von [redacted] des Auftragswertes* zu verlangen. Satz 1 gilt auch für Überschreitungen von vereinbarten Teilabnahmeterminen. In diesem Fall berechnet sich die Vertragsstrafe nach dem auf die Teilleistung entfallenden Anteil am Auftragswert*. Insgesamt darf die Summe der aufgrund dieser Regelung zu zahlenden Vertragsstrafen jedoch nicht mehr als [redacted] des Auftragswertes* betragen.

Als **Teilabnahmetermin** gilt: Der Auftragnehmer muss das Umsetzungsfeinkonzept inkl. Styleguide sowie die Gliederungen spätestens acht Wochen nach Auftragserteilung zur Abnahme vorlegen (vgl. Ziffer 8 Vertrag). Weitere **Teilabnahmetermine** gibt es nicht.

Als **Vertragserfüllungstermin** gilt der in Ziffer 8 Vertrag genannte Termin.

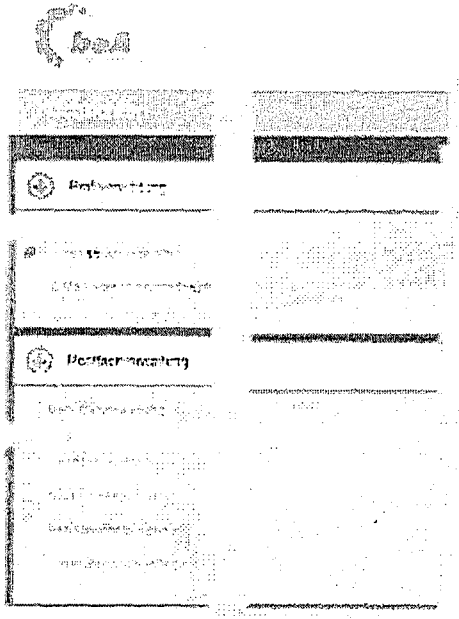
Die Vertragsstrafe für versäumte Teilabnahmetermine fällt nicht an, wenn der Vertragserfüllungstermin eingehalten wird oder aber der Vertragserfüllungstermin für nicht mehr als 14 Kalendertage überschritten wird.

Die Regelungen der Ziffer 9 EVB-IT Erstellungs-AGB gelten im Übrigen fort. Die fortgeltenden Regelungen in Ziffer 9 EVB-IT Erstellungs-AGB gelten auch für die Vertragsstrafenregelungen in dieser Anlage.

[1] Die mit * versehenen Begriffe werden in den EVB IT Erstellungs-AGB definiert

Atos

BUNDESRECHTSANWALTSKAMMER



Projekt beA

besonderes elektronisches Anwaltspostfach

Testbericht Atos

Inkrement 3 & Gesamtintegration

Version: 1.1
Datum: 09.05.2016
Autor: [redacted]

Inhalt

Informationen zum Bericht allgemein

Informationsstand / Dokumentationsumfang

- Basis für den Bericht sind die Testergebnisse mit dem Stand 04.05.2016 12:00 Uhr
- Zu dem Zeitpunkt sind nicht alle Tests der Atos abgeschlossen
- Wie mit den offenen Themen umgegangen wird, wird an entsprechender Stelle in diesem Bericht beschrieben
- Alle eingebetteten Informationen und Verweise beziehen sich auf den Testdokumentationsstand aus dem HP ALM der Atos (Projekt „beA“).
- Nicht alle Testergebnisse sind als Extrakt in diesen Report eingebettet, aufgrund des hohen Datenvolumens.
- Alle Informationen können im Einzelnen durch den Kunden versioniert und historisiert im HP ALM eingesehen werden.
- Bei Bedarf können weitere, ausgewählte Einzelbereiche in Form separater Extraktionen durch Atos bereitgestellt werden.

Atos

BUNDESRECHTSANWALTSKAMMER

Inhalte der Testphase - Übersicht

Zielsetzung

- Einzeltests zu Neufunktionalitäten des Inkrement 3
- Funktionale Komplett-Integration / Gesamtintegration des beA-Gesamtsystems
- Nicht-funktionale Tests (Security, Last, Ausfall)
- Abschließende Regression

Zeitraum

- Aug 2015 – Mai 2016

Voraussetzungen

- Finalisiertes UFK
- Bereitstellung der voll integrierten Testumgebung (STA)
- Bereitstellung der erforderlichen HW/SW-Token für die Tests
- Fixes zu allen Tickets aus Inkrement 1&2
- Komplette Lieferung alle Komponenten zum Teststart

Inhalt

Rückblick Inkrement 1 & 2

Zielsetzung

- Funktionaler Vortest der mit den Inkrementen 1 & 2 zur Verfügung gestellten beA-Funktionalitäten

Testbare Funktionalitäten aus Inkrement 1 & 2

- Einzelne beA Dialoge
- Integration Justiz
- BITV

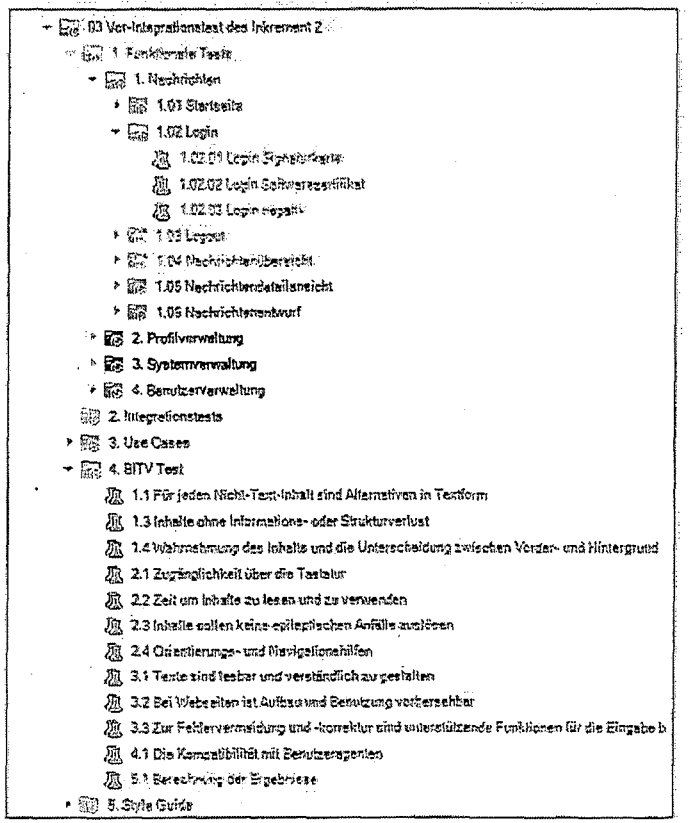
Meilensteine

08.04.2015	Testbeginn Inkrement 1
03.07.2015	Testende Inkrement 2

Berücksichtigung in Inkrement 3 & Gesamtintegration

- Funktionalitäten wurden über die Testfälle zur Gesamtintegration und im Rahmen der Regression berücksichtigt
- Es wurden aber nicht alle Tests in Breite und Tiefe wiederholt

Auszug aus dem HP ALM



Inhalt

Ergebnisse der Testphase - Zusammenfassung

Testergebnisse [redacted]

- Es wurden 1749 Testfälle[1] für diese Testphase spezifiziert und für eine Durchführung eingeplant
  - Erfolgreich bearbeitet (96%)
    - 1528 wurden erfolgreich durchgeführt
    - 156 Testszenarien wurden während der Durchführung als „nicht durchführbar" gestrichen
  - Mit Fehlern abgeschlossen (1%)
    - 17 Testfälle wurden mit Fehlern abgeschlossen
  - Noch zur Durchführung geplant (3%)
    - 48 Testfälle sind noch nicht durchgeführt worden

Übersicht zu festgestellten Auffälligkeiten [redacted]

- Es wurden 576 Auffälligkeiten[1] aus dem Test erfasst (aus Inkrement 1-3)
  - Erfolgreich bearbeitet (90%)
    - 524 Tickets wurden analysiert, behoben und erfolgreich geretestet
  - Noch offen für Inkrement 3 (3%)
    - 14 Tickets sind aktuell noch in der Analyse (kein Prio A&B)
  - Offen, aber nicht Scope von Inkrement 3 (7%)
    - 38 Tickets zur Bearbeitung nach Inkrement 3 deklariert

[1] *Extrakt der Zahlen aus dem HP (02.05.2016 gegen 18:00 Uhr) – Links zu den Quell-Reports eingefügt*

Ergebnisse der Regression - Zusammenfassung

Regression zu BzT [redacted]

- Es wurden 239 Testfälle (14% des Gesamttestsets) zur Durchführung innerhalb der Regression definiert
- In allen Funktionsbereichen der beA-Anwendung und der zugehörigen Komponenten wurden die Kernfunktionen erneut geprüft
  - Erfolgreich bearbeitet (97%)
    - 233 wurden erfolgreich durchgeführt
  - Nicht erfolgreich abgeschlossen (3%)
    - 6 Testfälle konnten nicht erfolgreich durchgeführt werden;Grund:
      - Offene Retests: Bereich SAFE-Connector (2)
      - Fehlende HW-Token: Registrierung Orga-Postfach (2); Registrierung Vertreter (2)

Übersicht zu festgestellten Auffälligkeiten [redacted]

- Keine offenen Fehler Prio A&B aus der Regression
- Fehler-Schwerpunkt lag auf den Komponenten beA-Anwendung, Client Security, SAFE-Connector

Offene Testfälle und gelieferte Fixes werden durch Atos zeitnah nachgetestet

Inhalt

Offene Punkte aus der Testphase - Testfälle

17 Testfälle wurden mit Fehlern abgeschlossen [redacted]

- Offene Tests ergeben sich u.a. aufgrund von:
  - Problemen an der BNotK-Schnittstelle (SAFE-Connector-Tests; BGH-Postfachanlage)
  - Fehlenden Testkarten (Orga-Postfächer; BGH-Postfächer; Abwickler)
  - Nachzutestende Fixes aus der BzT-Lieferung
- Tests sind u.a. fehlgeschlagen in den Bereichen
  - SAFE-BRAK
  - SAFE-Connector
  - beA Rollen & Rechte
- Zu jedem fehlgeschlagenen Testfall gibt es einen Defekt im HP ALM
  - Anhand der Folgefolie, mit der Detailsicht zu noch offenen Defekts, lässt sich die Kritikalität im Bezug auf die erwarteten Systemfunktionen zum Go Live bewerten

48 Testfälle sind noch nicht durchgeführt worden [redacted]

- Diese Tests werden nach BzT durchgeführt
- Sie ergeben sich aus letzten Änderungen am UFK, die im Breite und Tiefe geprüft werden, Schwerpunkt dabei:
  - Rollen und Rechte
  - Negativ-Szenarien

Offene Punkte aus der Testphase - Auffälligkeiten

14 Tickets sind aktuell noch in der Analyse [redacted]

- Kritikalität [redacted]
  - A: 0
  - B: 0
  - C: 14

Übersicht zu den offenen Prio A/B Fehlern, die eine SW-Anpassung erfordern [redacted]

- Keine

Inhalt

Risikobewertung / Zielerreichung / Mgmt Summary

Management Summary

- Alle funktionalen Bereiche des beA-Gesamtsystems wurden im Rahmen der abschließenden Regressionstests noch einmal geprüft
- Einige Tests in der Tiefe und in weiteren Test-Varianten zu Einzelfunktionen des beA-Systems, konnten bis zum BzT nicht abgeschlossen werden, waren aber auch nicht Bestandteil des Regressionstests
    - Die offenen Themen (Tests & Fehler) blockieren aber nicht BzT & Abnahmephase
    - Alle offenen Themen werden parallel zur Abnahmephase durch Atos abgeschlossen

Risiken

- Insbesondere durch Kombinationsmöglichkeiten bei Hard- und Software, eine große Nutzer-Anzahl, paralleles Arbeiten und die komplexe Sicherheitsarchitektur lassen sich nicht allen möglichen Test-Varianten definieren und durchführen. Abdeckungsrisiken ergeben sich dadurch für folgende Bereiche:
    - Lasttest über beA-Applikation ist nur eingeschränkt möglich (repräsentativ über die KSW-Schnittstelle realisiert)
    - Locking für ausgewählte Anwendungsfälle untersucht
    - Negativ-Szenarien in ausgewählten Funktionsbereichen definiert
    - Sonderfälle an der Kammerschnittstelle (ausgewählte Szenarien wurden von Kammervertretern geprüft)

Atos

BUNDESRECHTSANWALTSKAMMER

Inhalt

Detail: Testvoraussetzung & Testbasis

Testbasis

- Systemdokumentation
  - UFK mit seinen 8 Hauptbereichen
    1. beA System
    2. beA Anwendung
    3. beA Client Security
    4. beA HSM
    5. SAFE BRAK
    6. Intermediär BRAK
    7. beA Kanzleisoftware-Schnittstelle
    8. SAFE-Connector
  - Sonstige Anforderungen
    9. BITV
    10. Lastanforderungen aus der Betreiber-Ausschreibung
- Software
  - Liefergegenstände zu Inkrement 3 (Komplettsystem auf der STA-Umgebung, vgl. Release Notes)
- Testspezifikation zu Inkrement 3/Gesamtintegration
  - siehe Testprotokolle auf Folie «Detail: Testdurchführung – Übersicht»

Atos

BUNDESRECHTSANWALTSKAMMER

Inhalt

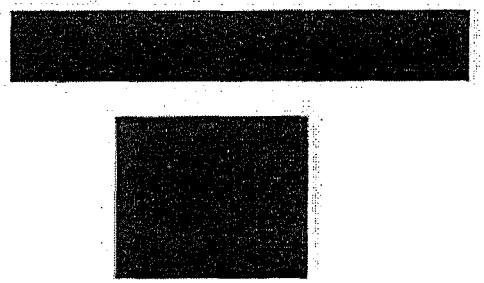
Detail: Testabdeckung - Übersicht

Übersicht der untersuchten Anforderungsbereiche

- Zu allen 10 Anforderungsbereichen (vgl. vorangegangene Folie) wurden Testszenarien definiert
  - Im HP ALM sind alle Testfälle mit zugehörigen UFK-Elementen verlinkt

- Nicht abgedeckte Anforderungselemente sind als „nicht im Test" im HP ALM (Modul Requirements) deklariert, u.a.
  - redundante Funktionsbeschreibungen
  - Kapitel ohne funktionalen Bezug
  - leere Kapitel des UFK
  - sowie nicht testbare Bereiche

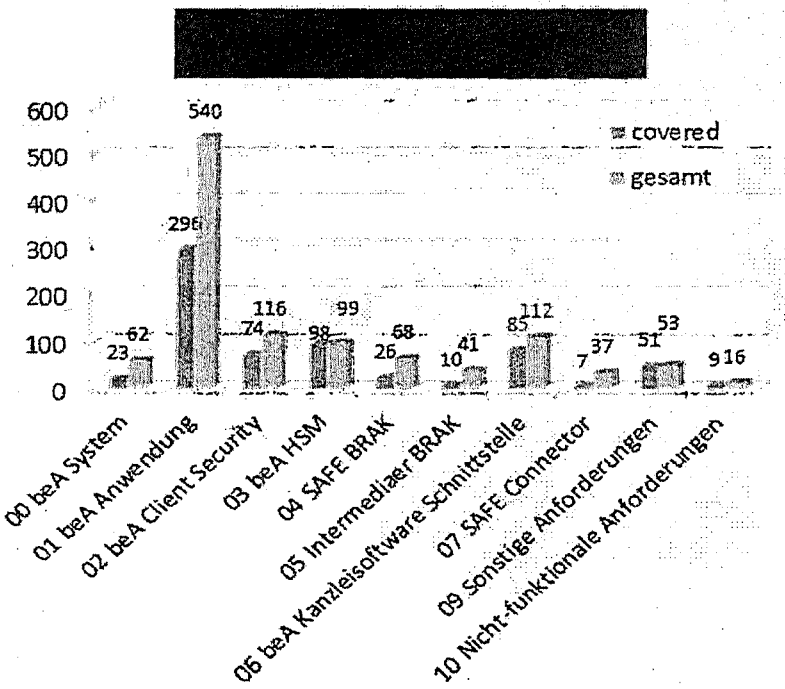
- Detailübersicht der Anforderungselemente (1144) inkl. Begründung, falls nicht im Test (Extrakt HP ALM)

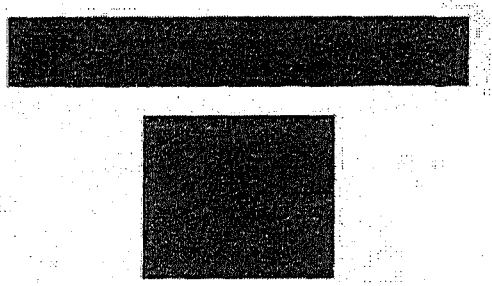


Detail: Testabdeckung - Übersicht

Abgedeckte Anforderungsbereiche

- Zu jedem testbaren Anforderungselement (679) gibt es mindestens ein Testszenario
- Pro Anforderungselement wurden funktionale und nicht-funktionale Anforderungen mittels gängiger Analyse-Methoden des ISTQB wie z.B. Grenzwert- o. Äquivalenzklassenanalyse untersucht
  - Im Ergebnis wurde je identifiziertem Szenario ein Testfall im HP ALM spezifiziert (Modul Test Plan) und mit dem jeweiligen UFK-Element im HP ALM verlinkt



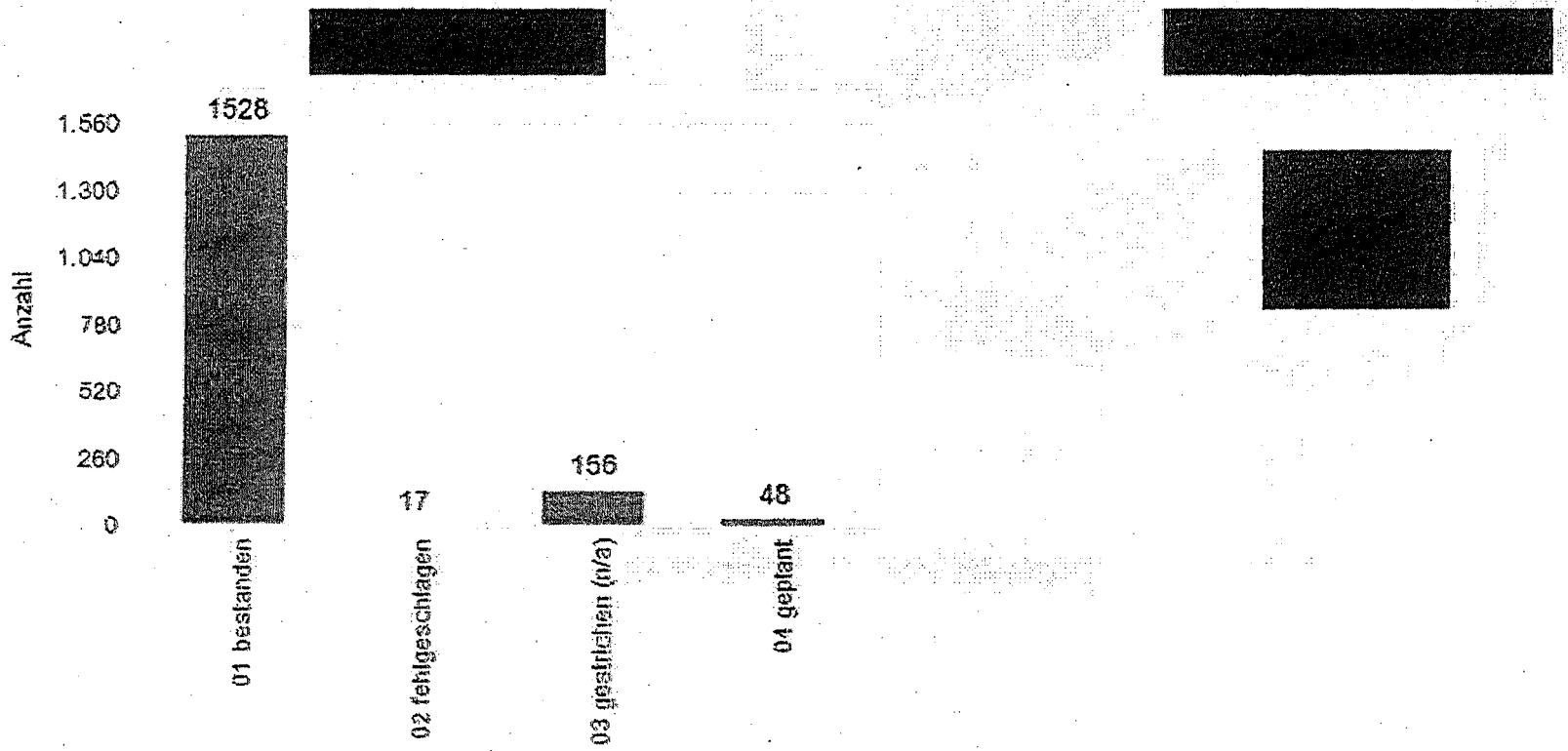


Inhalt

Detail: Testdurchführung - Übersicht

Zur Durchführung wurden die spezifizierten Testfälle (1749) in Testsets organisiert und 1-n Mal für Testdurchführungen geplant

- Ergebnisse im Detail (Extrakt HP ALM)



Detail: Testdurchführung - Übersicht

Alle Durchführungsprotokolle (Extrakt HP ALM)

Erklärung zum Teststatus im Detail

passed	Test erfolgreich durchgeführt ohne Einschränkungen
passed with exception	Test erfolgreich, aber mit geringer Abweichung zur Spezifikation (z.B. ein einzelner Schritt ist n/a)
n/a	Test kann nicht mehr, wie spezifiziert, durchgeführt werden (z.B. wegen UFK-Änderungen)
failed	Test konnte nicht erfolgreich durchgeführt werden
blocked	Testvoraussetzungen nicht erfüllt

Atos

BUNDESRECHTSANWALTSKAMMER

Inhalt

Detail: Nicht-funktionale Tests - Übersicht

Security-Tests

- Details auf der Folgefolie

Lasttests

- Konzept 1: Last erzeugt über die KSW-Schnittstelle (=Eingangskanal für 50% der beA-Nutzer)
  - repräsentative Bewertung des Lastverhaltens möglich
  - Szenarien
    - Nachrichtenversand intern
    - Nachrichtenversand an EGVP

[redacted]

- Konzept 2: Parallele Sessions auf die Login-Seite per Web-Simulator
  - bei halber Ziellast 2016 (7.000 Sessions/h pro Backend-Server) keine Auffälligkeiten
  - weiterer Tests mit Ziellast 2016 geplant für Durchführung im Mai

[redacted]

Ausfalltests

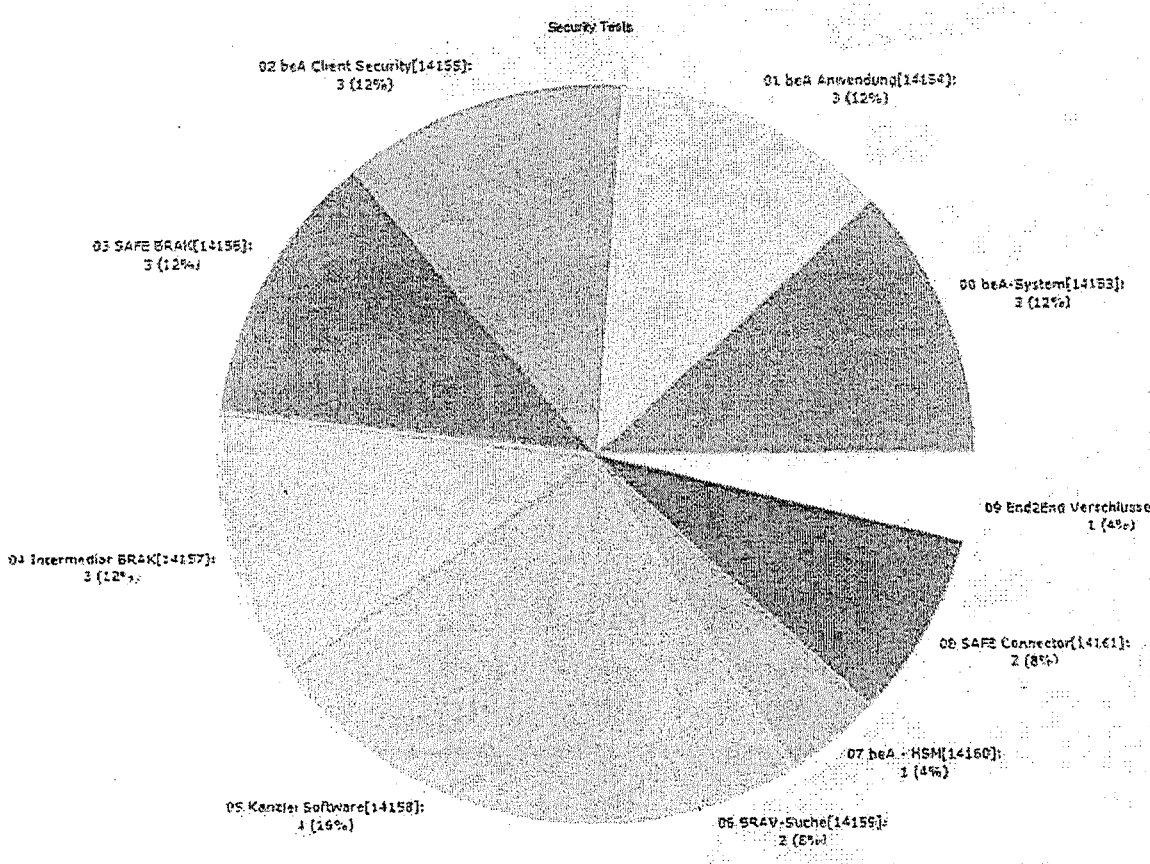
- Die Ausfalltests von Servern, Netzwerkkomponenten oder einem ganzen RZ wurden durch den Betreiber Atos MS mit Unterstützung des Testteams durchgeführt
- Die Dokumentation der Testergebnisse erfolgte über Atos MS

Atos

BUNDESRECHTSANWALTSKAMMER

Detail: Nicht-funktionale Tests – Security Tests

Übersicht zu durchgeführten Testfällen je Komponente



Prüfungen durch:

- Atos Pentests
- SecConsult Pentests
- Qualys SSL Labs Tests
- Governikus und Worldline Herstellertests

für Schwachstellen in:

- HW/SW-Architektur
- Authentifizierungskonzept
- Signaturmechanismen
- Ende-zu-Ende-Verschlüsselung

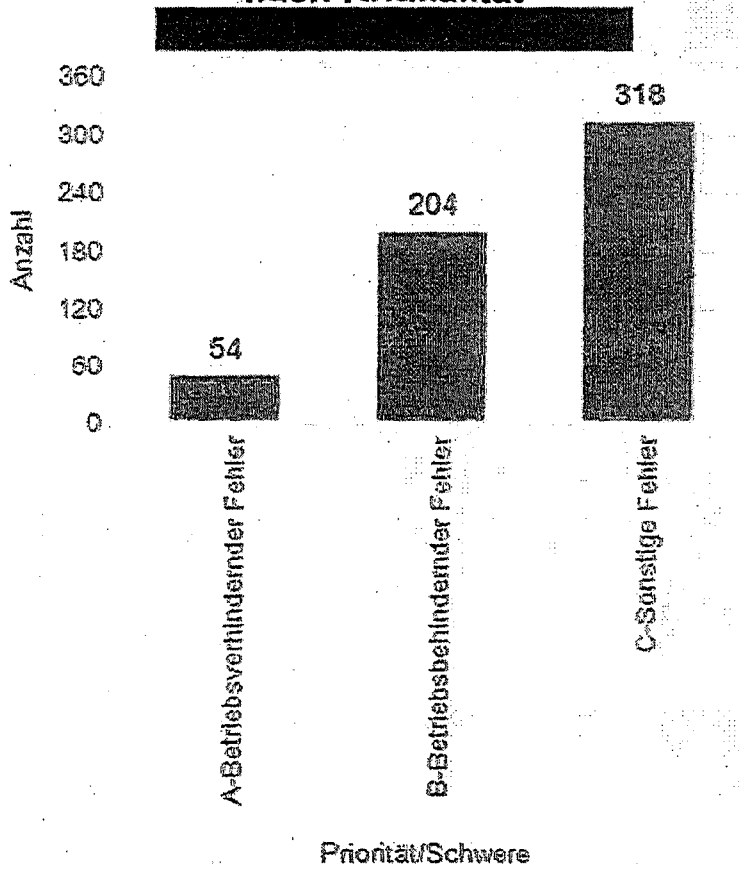
Fazit:

- Robustes System
- Offen: einen Prio C Defekt für DoS Angriffe Kanzlei-Software

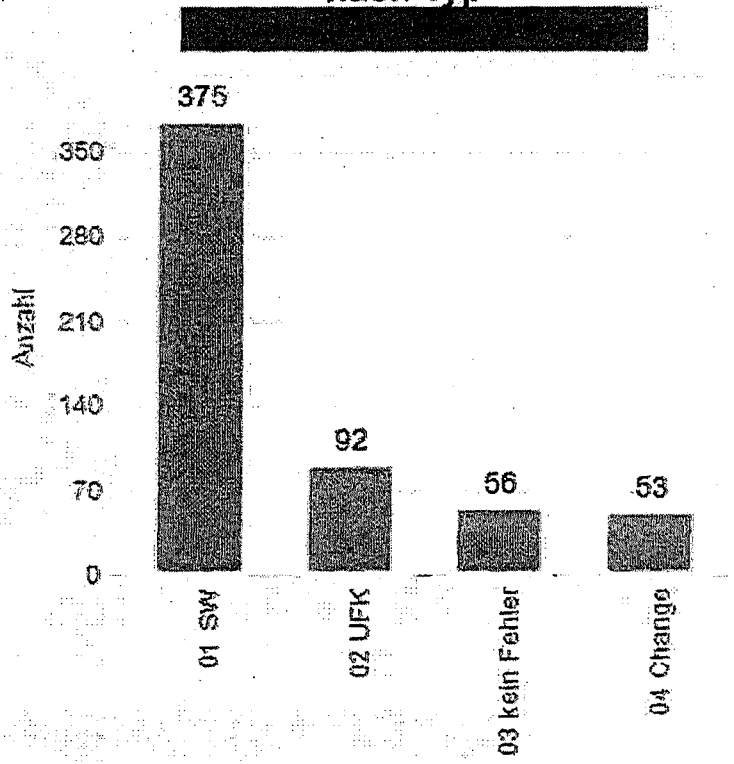
Inhalt

Detail: Festgestellte Auffälligkeiten - Grafik

Alle Fehler - Übergreifend Inkrement 1 – 3
nach Kritikalität

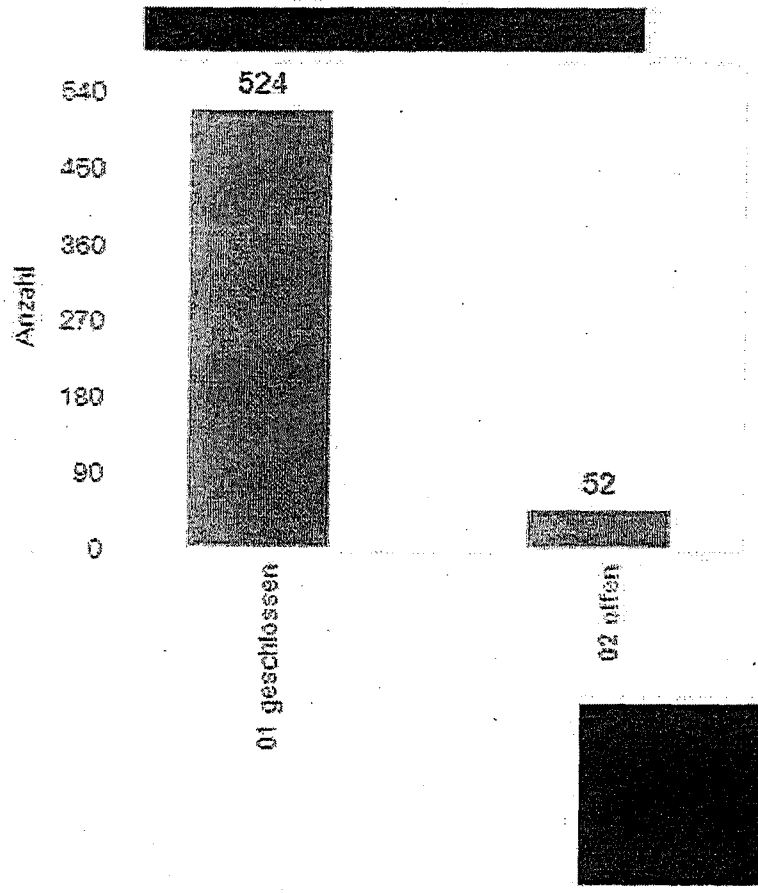


Alle Fehler - Übergreifend Inkrement 1 – 3
nach Typ

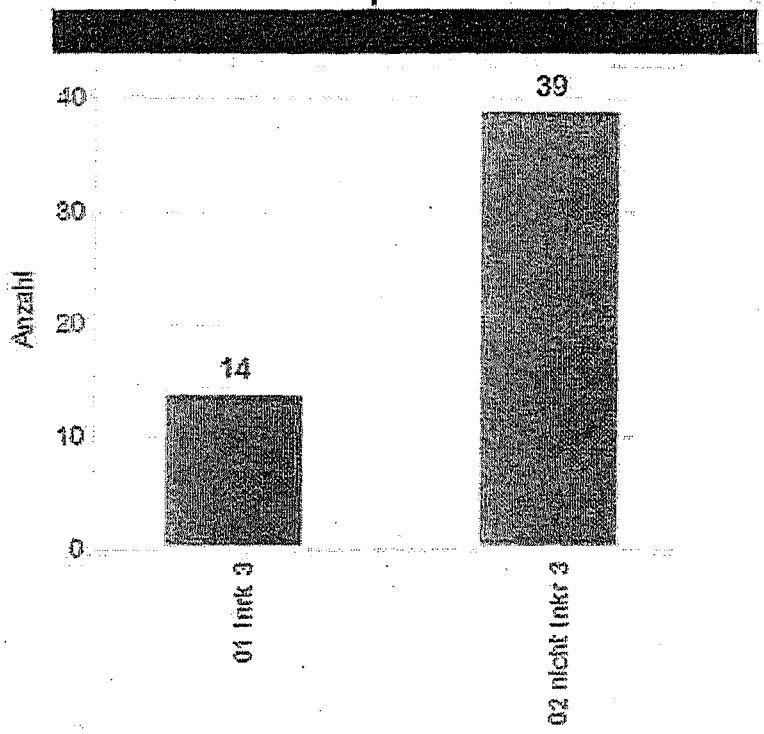


Detail: Festgestellte Auffälligkeiten - Übersicht

Alle Fehler - Übergreifend Inkrement 1 – 3 nach Status



OFFENE Fehler - Übergreifend Inkrement 1 – 3 nach Scope Inkrement 3



Atos

BUNDESRECHTSANWALTSKAMMER

Projekt beA

besonderes elektronisches Anwaltspostfach

Testbericht Atos

Tests zur Release-Version 1.1

Version des Testberichts: 1.1

Datum: 14.06.2017

Autor: [redacted]

Inhalt

Inhalte der Testphase - Übersicht

Informationsstand

- Basis für diesen Bericht sind die Testergebnisse mit dem Stand 14.06.2017 12:00 Uhr
- Zu dem Zeitpunkt sind alle Tests der Atos abgeschlossen

Zielsetzung

- Tests zu den Neufunktionalitäten/Funktionsänderungen mit „Version 1.1“

Neue Funktionaliäten in Version 1.1 sind

- Senden an (Default-)Verteilerlisten
- REQ-00021 REQ-00044 REQ-00045 REQ-00046 REQ-00063 REQ-00064
  REQ-00065 REQ-00074 REQ-00076 REQ-00087 REQ-00094 REQ-00096
  REQ-00097 REQ-00125 REQ-00129 REQ-00139 CCB-128 CCB-129

Inhalt

Ergebnisse der Testphase - Zusammenfassung

Testergebnisse

- Es wurden 16 komplexe Testfälle für diese Testphase spezifiziert und durchgeführt.
  - Ohne Fehler
    - 16
  - Mit Fehlern abgeschlossen
    - 0
  - Noch zur Durchführung geplant
    - 0 Testfälle sind noch nicht durchgeführt worden.

Inhalt

Offene Punkte aus der Testphase - Testfälle

Folgende Themen sollten noch nicht von der BRAK getestet werden:
Es können alle Themen getestet werden.

Inhalt

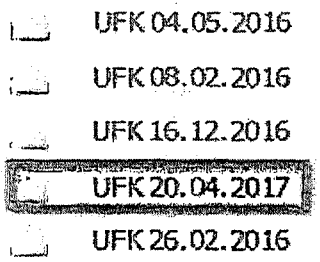
Atos

BUNDESRECHTSANWALTSKAMMER

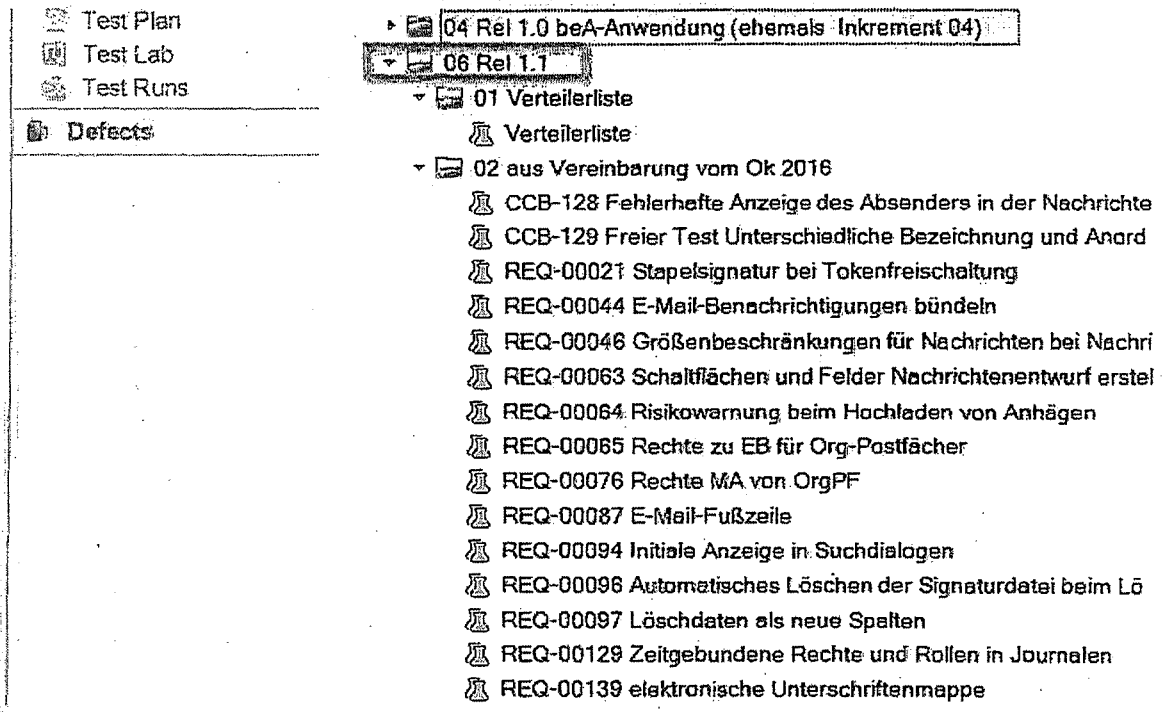
Detail: Testvoraussetzung & Testbasis

Testbasis

- UFK vom 20.04.2017



Testplan: Web-Link



beA Preisblatt

BUNDESRECHTSANWALTSKAMMER

Pos.	Bezeichnung Für sämtliche Mengenangaben besteht keine Abnahmeverpflichtung durch den AG.	Kapitalverweis auf die Leistungsbeschreibung	Menge pro Stück / PT	Menge Monate	Preis (netto) pro Stück	Preis (netto) monatlich	Summe Kosten pro Stück (netto)	Summe monatliche Kosten (netto)
1	Erarbeitung eines Umsetzungsfeinkonzeptes einschließlich der Abnahme durch den Auftraggeber (Festpreis)	2.1 Abschnitt D und 2.12	[redacted]		[redacted]		[redacted]	
2	Realisierung der beA Software, einschließlich aller Schnittstellen Angabe der Personentage und des Preises (Aufwand mit Obergrenze)	2.3, 2.5, 2.4, 2.5, 2.6 und 2.11.1 jeweils alle Abschnitte	[redacted]		[redacted]		[redacted]	
3	Ggf. eingesetzte Standardsoftware Angabe der Anzahl und des Gesamtpreises über alle Standardsoftware-Produkte	2.2, 2.3, 2.4, 2.5, 2.6 und 2.11.1 jeweils alle Abschnitte					[redacted]	
4	Ggf. eingesetzte vorbestehende Teile Angabe der Anzahl und des Gesamtpreises über alle Teile	2.2, 2.3, 2.4, 2.5, 2.6 und 2.11.1 jeweils alle Abschnitte						
5	Erarbeitung der Anwenderdokumentation und der Anwenderhilfe einschließlich der Abnahme durch den Auftraggeber (Festpreis)	2.7.1 Abschnitt B 2.7.3 alle Abschnitte	[redacted]		[redacted]		[redacted]	
6	Erarbeitung eines Styleguides für die Web-Oberfläche einschließlich der Abnahme durch den Auftraggeber (Festpreis)	2.7.1 Abschnitt A und 2.8.1 Abschnitt C	[redacted]		[redacted]		[redacted]	
7	Erarbeitung der technische Systemdokumentation einschließlich der Abnahme durch den Auftraggeber (Festpreis)	2.7.1 Abschnitt C	[redacted]		[redacted]		[redacted]	
8	Erarbeitung der Betriebsdokumentation, einschließlich einer Installationsdokumentation einschließlich der Abnahme durch den Auftraggeber (Festpreis)	2.7.1 Abschnitt D	[redacted]		[redacted]		[redacted]	
9	Erarbeitung des Sicherheitskonzeptes einschließlich der Abnahme durch den Auftraggeber (Festpreis)	2.7.1 Abschnitt E	[redacted]		[redacted]		[redacted]	
10	Erarbeitung des Einweisungskonzepts, mit allen aufgeführten Unterlagen einschließlich der Abnahme durch den Auftraggeber (Festpreis)	2.7.1 Abschnitt A und 2.8 Abschnitt A	[redacted]		[redacted]		[redacted]	
11	Erarbeitung der Testpläne und Testspezifikation einschließlich der Abnahme durch den Auftraggeber (Festpreis)	2.7.1 Abschnitt A und 2.8.1 Abschnitt A und B	[redacted]		[redacted]		[redacted]	
12	Pflegepauschale für die beA Software (bezogen auf die Leistungen in Position 2) es gelten die gestaffelten Reaktions- und Fehlerbeseitigungszeiten	2.10 und 2.10.1 alle Abschnitte		[redacted]		[redacted]		[redacted]
13	Pflegepauschale für die beA Software (bezogen auf die Leistungen in den Positionen 3 und 4) es gelten die gestaffelten Reaktions- und Fehlerbeseitigungszeiten	2.10 und 2.10.1 alle Abschnitte		[redacted]		[redacted]		[redacted]
14	Third-Level Support einschließlich der geforderten Service-Level für Kernteil	2.10.2, alle Abschnitte, besonders Abschnitt C		[redacted]		[redacted]		[redacted]
15	Third-Level Support einschließlich der geforderten Service-Level für Schnittstelle	2.10.2, alle Abschnitte, besonders Abschnitt C		[redacted]		[redacted]		[redacted]
16	Third-Level Support einschließlich der geforderten Service-Level für Bundesrak	2.10.2, alle Abschnitte, besonders Abschnitt C		[redacted]		[redacted]		[redacted]
17	Entwicklerstundensatz	2.9.2, 2.11 ohne 2.11.1	[redacted]		[redacted]		[redacted]	
18	Berater-Tagessatz	2.9.2, 2.11 ohne 2.11.1						
19	Reisekostenpauschale für durch den Auftraggeber veranlasste Reisen des Auftragnehmers zum Auftraggeber nach Berlin	2.9.2, 2.11 ohne 2.11.1						
	Summe		[redacted]					

Anlage 12 Vertrag

Anlage zu Ziffer 8 EVB-IT Erstellungsvertrag

Sonderregelung zum Zahlungsplan

Die Vergütung für die Erstellung des Umsetzungsfeinkonzepts nach Position 1 des Preisblatts wird mit der Abnahme des Umsetzungsfeinkonzepts fällig.

Die Vergütung für die Realisierung der beA-Software, einschließlich aller Schnittstellen, nach Position 2 des Preisblatts erfolgt in Höhe von 80 % der Summe aus Position 2 des Preisblatts in monatlichen Abschlägen nach Aufwand. Die Restzahlung ist nach Abnahme der Leistung fällig.

Die Vergütung für eingesetzte Standardsoftware nach Position 3 des Preisblatts wird mit Fälligkeit der jeweiligen Lizenzgebühren geleistet.

Die Vergütung für die in Positionen 5 bis 11 des Preisblatts beschriebenen Leistungen wird jeweils nach der Abnahme der Leistung entsprechend dem Umsetzungsfeinkonzept fällig.

RED HAT
ENTERPRISE AGREEMENT
GERMANY/AUSTRIA/SWITZERLAND

RED HAT
GESCHAFTSKUNDENVERTRAG
DEUTSCHLAND/OSTERREICH/SCHWEIZ

redhat.

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE PURCHASING AND/OR USING SOFTWARE OR SERVICES FROM RED HAT. BY USING RED HAT SOFTWARE OR SERVICES, CLIENT SIGNIFIES ITS ASSENT TO AND ACCEPTANCE OF THIS AGREEMENT AND ACKNOWLEDGES IT HAS READ AND UNDERSTANDS THIS AGREEMENT. AN INDIVIDUAL ACTING ON BEHALF OF AN ENTITY REPRESENTS THAT HE OR SHE HAS THE AUTHORITY TO ENTER INTO THIS AGREEMENT ON BEHALF OF THAT ENTITY. IF CLIENT DOES NOT ACCEPT THE TERMS OF THIS AGREEMENT, THEN IT MUST NOT USE RED HAT SOFTWARE OR SERVICES. THIS AGREEMENT INCORPORATES THOSE APPENDICES AT THE END OF THIS AGREEMENT.

BITTE LESEN SIE DIESEN VERTRAG VOR DEM KAUF UND/ODER DER NUTZUNG VON RED HAT SOFTWARE ODER SERVICELEISTUNGEN SORGFÄLTIG DURCH. DURCH DIE NUTZUNG DER RED HAT SOFTWARE ODER SERVICELEISTUNGEN ERKLÄRT DER KUNDE SEINE VERTRAGS-ANNAHME UND EINWILLIGUNG IN DEN VOR-LIEGENDEN VERTRAG UND BESTÄTIGT, DASS ER DIE BESTIMMUNGEN DIESES VERTRAGES GELESEN UND VERSTANDEN HAT. EINE IM NAMEN EINER JURISTISCHEN PERSON HANDELNDEN EINZELPERSON ERKLÄRT, DASS SIE ZUM ABSCHLUSS DES VORLIEGENDEN VERTRAGES IM NAMEN DIESER JURISTISCHEN PERSON BEFUGT IST. FALLS DER KUNDE SICH NICHT MIT DEN VORLIEGENDEN VERTRAGSBESTIMMUNGEN EINVERSTANDEN ERKLÄRT, IST ER NICHT BERECHTIGT, DIE RED HAT SOFTWARE ODER SERVICELEISTUNGEN ZU NUTZEN. DIESER VERTRAG SCHLIEßT DIE AM ENDE DES VERTRAGES ANGEFÜGTEN ANHÄNGE MIT EIN.

This Red Hat Enterprise Agreement, including all referenced appendices and documents located at URLs (the "Agreement"), is between Red Hat Limited, an Irish registered company, ("Red Hat") and the purchaser or user of Red Hat software and services who accepts the terms of this Agreement ("Client"). The effective date of this Agreement ("Effective Date") is the earlier of the date that Client signs or accepts this Agreement or the date that Client uses Red Hat's software or services.

Der Abschluss des vorliegenden Red Hat Geschäftskundenvertrages, einschließlich sämtlicher, durch Verweis auf die URLs angegebener Anhänge und Dokumente (der "VERTRAG") erfolgt zwischen Red Hat Limited, einer in Irland eingetragenen Gesellschaft, ("Red Hat") und dem Käufer oder Anwender der Red Hat Software und Serviceleistungen, der die Bestimmungen dieses VERTRAGES annimmt ("KUNDE"). Der vorliegende VERTRAG tritt mit Unterzeichnung bzw. Annahme oder mit Beginn der Nutzung der Red Hat Software oder Serviceleistungen durch den KUNDEN in Kraft, je nachdem, welches Datum früher eintritt ("DATUM DES INKRAFTTRETENS").

1. Scope of Agreement

1.1 Framework. This Agreement establishes a framework that will enable Red Hat to provide Software and Services to Client. "Software" means Red Hat Enterprise Linux, JBoss Enterprise Middleware and other software programs branded by Red Hat, its Affiliates and/or third parties including all modifications, additions or further enhancements delivered by Red Hat. The specific services (the "Services") and/or Software that Red Hat will provide to Client will be described in an Order Form, signed by the parties or otherwise accepted by Red Hat, which may consist of (a) one or more mutually agreed order forms, statements of work, work orders or similar transaction documents, or (b) an order placed by Client through Red Hat's online store accessible from a Red Hat website. The parties agree that the terms of this Agreement will govern all purchases and use by Client of Software and Services unless otherwise agreed by the parties in writing.

1. Umfang des VERTRAGES

1.1 Rahmenbedingungen. Der vorliegende VERTRAG schafft für Red Hat die Rahmenbedingungen für die Bereitstellung der SOFTWARE und SERVICES an den KUNDEN. "SOFTWARE" umfasst die Programme Enterprise Linux, JBoss Enterprise Middleware sowie sonstige, mit einem Warenzeichen von Red Hat, seinen VERBUNDENEN UNTERNEHMEN und/oder Dritten gekennzeichnete SOFTWARE, einschließlich sämtlicher von Red Hat zur Verfügung gestellter Modifikationen, Ergänzungen oder Weiterentwicklungen. Die dem KUNDEN von Red Hat bereitgestellten speziellen Serviceleistungen (die "SERVICES") und/oder SOFTWARE werden in einer ORDER FORM beschrieben, die von den Parteien unterzeichnet oder anderweitig von Red Hat angenommen wird und Folgendes beinhaltet: (a) eine oder mehrere gegenseitig vereinbarte ORDER FORMS, Leistungsbeschreibungen (Statement of Works), Work Orders oder ähnliche Transaktionsdokumente oder (b) einen vom KUNDEN über eine Red Hat Website im Online Store platzierten Auftrag. Die Parteien erklären ihr Einverständnis, dass der Erwerb und die Nutzung der SOFTWARE und SERVICES durch den KUNDEN den Bestimmungen des vorliegenden VERTRAGES unterliegen, sofern die Parteien nicht schriftlich etwas anderes vereinbaren.

1.2 **Affiliates.** Red Hat and Client agree that Affiliates of Client may acquire Software and Services from Red Hat or its Affiliates by entering an Order Form with Red Hat (or a Red Hat Affiliate) that incorporates the terms and conditions of this Agreement. The parties acknowledge that adjustments to the terms of this Agreement may be made in a particular Order Form (for example, to address disparate tax and/or legal regimes in other geographic regions). "Affiliate" means an entity that owns or controls, is owned or controlled by, or is under common control or ownership with a party, where "control" is the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 **VERBUNDENE UNTERNEHMEN.** Red Hat und der KUNDE vereinbaren, dass die VERBUNDENEN UNTERNEHMEN des KUNDEN die SOFTWARE und SERVICES von Red Hat (oder von einem seiner VERBUNDENEN UNTERNEHMEN) durch Unterzeichnung einer ORDER FORM erwerben können, in welchem die Bestimmungen des vorliegenden VERTRAGES mit eingebunden sind. Die Parteien vereinbaren, dass die Bestimmungen dieses VERTRAGES in bestimmten ORDER FORMS angepasst werden können, um z.B. unterschiedlichen Steuer- und/oder Rechtssystemen in anderen Ländern Rechnung zu tragen. "VERBUNDENES UNTERNEHMEN" bezeichnet ein Unternehmen, das über den Mehrheitsbesitz an einer Partei verfügt oder die Kontrolle über diese Partei ausübt, unter der Kontrolle oder im Mehrheitsbesitz dieser Partei steht oder zusammen mit dieser Partei unter der gemeinsamen Kontrolle bzw. im Mehrheitsbesitz eines anderen Unternehmens steht, wobei "Kontrolle" die mittelbare oder unmittelbare Verfügungsgewalt ist, einen beherrschenden Einfluss auf die Geschäftsführung und Richtlinien eines Unternehmens auszuüben, sei es durch den Besitz an stimmberechtigten Wertpapieren, per Vertrag oder anderweitig.

1.3 **Business Partners.** Red Hat has entered into agreements with other organizations ("Business Partners") to promote, market and support certain Software and Services. When Client purchases Software and Services through a Business Partner, Red Hat confirms that it is responsible for providing the Software and Services to Client under the terms of this Agreement. Red Hat is not responsible for (a) the actions of Business Partners, (b) any additional obligations Business Partners have to Client, or (c) any products or services that Business Partners supply to Client under any separate agreements between a Business Partner and Client.

1.3 **Geschäftspartner.** Red Hat hat hinsichtlich der SOFTWARE und SERVICES mit anderen Unternehmen ("GESCHÄFTSPARTNER") Verträge über Produktförderung, Vermarktung und Support abgeschlossen. Red Hat bestätigt, dass wenn der KUNDE die SOFTWARE und SERVICES über einen GESCHÄFTSPARTNER erwirbt, Red Hat die Verantwortung dafür übernimmt, dass dem KUNDEN die SOFTWARE und SERVICES gemäß den Bedingungen dieses VERTRAGES zur Verfügung gestellt werden. Red Hat übernimmt keine Verantwortung (a) für die Handlungen der GESCHÄFTSPARTNER, (b) für zusätzliche Verpflichtungen der GESCHÄFTSPARTNER gegenüber dem KUNDEN oder (c) für Produkte oder Serviceleistungen, die die GESCHÄFTSPARTNER dem KUNDEN unter gesondert zwischen ihnen abgeschlossenen Verträgen bereitstellen.

2. Obligations of the Parties

2. Verpflichtungen der Parteien

2.1 **On-Site Obligations.** If Red Hat personnel are working on Client's premises, then (a) Client will provide a safe and secure working environment for Red Hat personnel, and (b) Red Hat will comply with all reasonable workplace safety and security standards and policies, applicable to Client's employees, of which Red Hat is notified in writing by Client in advance.

2.1 **Verpflichtungen vor Ort.** Für den Fall, dass Mitarbeiter von Red Hat Arbeitsleistungen in den Geschäftsräumen des KUNDEN erbringen, sorgt der KUNDE dafür, dass das Personal von Red Hat eine sichere Arbeitsumgebung vorfindet, und Red Hat verpflichtet sich, sämtliche, für die Mitarbeiter des KUNDEN geltenden Sicherheitsrichtlinien und -vorschriften am Arbeitsplatz im vertretbaren Rahmen einzuhalten, über die Red Hat vom KUNDEN im Voraus schriftlich unterrichtet wird.

2.2 **Changes to Work and Delays.** Changes to the Services will be m Changes to Work and Delays. Changes to the Services will be made only through a written change order signed by both parties. In the event that (a) Client fails to timely fulfill its obligations under an Order Form, and this failure adversely impacts the provision of Services, or (b) events outside of either party's reasonable control cause a delay in or otherwise affect Red Hat's ability to perform its obligations under an Order Form, Red Hat will be entitled to appropriate relief, including adjusting the timing of its delivery of applicable Services.

2.2 **Änderung der Leistungen und Verzug.** Änderungen der SERVICES können nur durch einen schriftlichen, von beiden Parteien zu unterzeichnenden Änderungsauftrag erfolgen. Falls (a) der KUNDE seinen Verpflichtungen aus einer ORDER FORM nicht nachkommt und dadurch die Bereitstellung der SERVICES beeinträchtigt wird oder (b) nicht von den Parteien zu vertretende Ereignisse dazu führen, dass Red Hat seinen Verpflichtungen aus einer ORDER FORM nur verspätet nachkommen kann oder diese Ereignisse die Erfüllung der Verpflichtungen anderweitig beeinträchtigen, so kann Red Hat im vertretbaren Rahmen Abhilfe verlangen, einschließlich der zeitlichen Anpassung der jeweils bereitzustellenden SERVICES.

2.3 **Assistance.** Client may provide Red Hat access to Client

2.3 **Mitwirkung.** Der KUNDE gewährt Red Hat Zugang zu seinen

information, systems, and software ("Client Information"), and resources such as workspace, network access, and telephone connections as reasonably required by Red Hat in order to provide the Services. Client understands and agrees that (a) the completeness, accuracy of, and extent of access to, any Client Information provided to Red Hat may affect Red Hat's ability to provide Services, and (b) if reasonable access to Client Information is not provided, Red Hat will be relieved from providing any Services dependent upon such access. Client will obtain any third party consents necessary to grant Red Hat access to the Client Information that is subject to the proprietary rights of, or controlled by, any third party, or which is subject to any other form of restriction upon disclosure.

Informationen, Systemen und Softwareprogrammen ("KUNDENINFORMATIONEN") sowie zu Betriebsmitteln wie Arbeitsbereiche, Netzwerkzugang und Fernsprechanschlüsse, und zwar so, wie es für Red Hat angemessenerweise erforderlich ist, um die SERVICES zu erbringen. Der KUNDE ist darüber in Kenntnis, dass die Bereitstellung der SERVICES durch Red Hat von der Vollständigkeit, Richtigkeit und dem Umfang der Red Hat zur Verfügung gestellten KUNDENINFORMATIONEN abhängt und erklärt sein Einverständnis, dass Red Hat von der Verpflichtung zur Bereitstellung der SERVICES befreit wird, wenn ein angemessener Zugang zu den KUNDENINFORMATIONEN nicht gewährt wird. Für KUNDENINFORMATIONEN, die dem Eigentumsrecht oder der Kontrolle Dritter oder in anderer Weise einer eingeschränkten Offenlegung unterliegen, beschafft der Kunde die erforderlichen Genehmigungen Dritter, um Red Hat Zugang zu den KUNDENINFORMATIONEN zu gewähren.

3. Payment

3. Zahlung

3.1 Fees and Expenses. Fees for the Services (the "Fees") will be identified in an Order Form and are (a) due upon Red Hat's acceptance of an Order Form or, for renewal of Services, at the start of the renewal term, and (b) payable in accordance with Section 3.2. Fees are stated in Euro, must be paid in Euro, and, unless otherwise specified in writing, do not include out-of-pocket expenses, customs, duties or shipping costs. Client will reimburse Red Hat for all reasonable expenses Red Hat incurs in connection with the performance of Services. Client agrees to pay Red Hat the applicable Fees for each Unit. "Unit" is the measurement of Software or Service usage defined in the applicable Order Form. Any renewal of Subscription Services will be at the same price per Unit listed in the applicable Order Form. "Subscription Services" mean fee-bearing subscriptions for a defined period of time for a certain scope of Services.

3.1 Gebühren und Auslagen. Die Kosten für die SERVICES ("GEBÜHREN") werden in einer ORDER FORM angegeben und sind (a) bei Annahme der ORDER FORM durch Red Hat oder im Fall einer Verlängerung der SERVICES zu Beginn des Verlängerungszeitraums fällig und (b) gemäß den Bestimmungen in Absatz 3.2 zu zahlen. Die GEBÜHREN werden in Euro angegeben und sind in Euro zu entrichten. Sofern schriftlich nichts anderes vereinbart wurde, beinhalten die GEBÜHREN keine Auslagen, Zölle, Abgaben oder Frachtkosten. Der KUNDE erstattet Red Hat sämtliche Auslagen, die Red Hat in Verbindung mit der Bereitstellung der SERVICES entstehen und verpflichtet sich, die jeweiligen GEBÜHREN pro EINHEIT an Red Hat zu zahlen. "EINHEIT" ist das Maß zur Berechnung der in der jeweiligen ORDER FORM angegebenen SOFTWARE- oder SERVICEnutzung. Eine Verlängerung des SUBSCRIPTION SERVICE erfolgt zum gleichen Preis pro EINHEIT, der in der ORDER FORM angegeben ist. "SUBSCRIPTION SERVICE" bezeichnet kostenpflichtige Abonnements für einen festgelegten Zeitraum und SERVICEumfang.

3.2 Invoices

3.2 Rechnungen

3.2.1 If Client desires credit terms with respect to the payment of Fees, Client will reasonably cooperate with Red Hat in establishing and periodically re-confirming Client's credit-worthiness. If credit terms are provided to Client, Red Hat will invoice Client for the Fees upon Red Hat's acceptance of the applicable Order Form and upon acceptance of any future order. Unless otherwise specified in an Order Form and subject to Red Hat's approval of credit terms, Client will pay Fees and expenses, if any, no later than thirty (30) days from the date of each invoice; provided, however, that Fees for professional services, training, training credits and other service credits are due prior to delivery. Except as otherwise provided in this Agreement, any and all payments made by Client pursuant to this Agreement are non-refundable. Red Hat reserves the right to suspend or cancel performance of all or part of the Services and/or change its credit terms if actual payment has not been received within thirty (30) days of the invoice date.

3.2.1 Falls der KUNDE für die Zahlung der GEBÜHREN ein Zahlungsziel wünscht, ist er verpflichtet, Red Hat in vertretbarem Umfang bei der Feststellung und periodischen Rückbestätigung seiner Kreditwürdigkeit zu unterstützen. Wird dem KUNDEN ein Zahlungsziel eingeräumt, so stellt Red Hat die GEBÜHREN dem KUNDEN nach Annahme der jeweiligen ORDER FORM sowie nach Annahme aller zukünftigen Aufträge in Rechnung. Sofern in einer ORDER FORM nichts anderes angegeben ist und vorbehaltlich der Genehmigung der Zahlungsziele durch Red Hat, sind die ggf. anfallenden GEBÜHREN und Auslagen spätestens dreißig (30) Tage nach Rechnungsdatum vom KUNDEN zu zahlen, wobei jedoch vorausgesetzt wird, dass die GEBÜHREN für Professional Services,, Trainings sowie für Credits für Schulungen und sonstige Serviceleistungen vor der Bereitstellung fällig sind. Wenn in vorliegendem VERTRAG nichts anderes vereinbart wurde, sind die vom KUNDEN gemäß diesem VERTRAG geleisteten Zahlungen nicht zurückerstattungsfähig. Red Hat behält sich das Recht vor, die Bereitstellung der SERVICES auszusetzen oder einzustellen bzw. eine Änderung des Zahlungszieles vorzunehmen, falls zur Zahlung fällige Beträge nicht innerhalb von dreißig (30) Tagen nach Rechnungsdatum

eingegangen sind.

3.2.2 If Client is paying by credit card, Client (a) authorizes Red Hat to charge Client's credit card for the Services and for the amount due at the time of renewal of Subscription Services, and (b) agrees to provide updated credit card information to Red Hat for renewal purposes.

3.2.2 Bei Kreditkartenzahlung (a) erteilt der KUNDE Red Hat die Genehmigung, die SERVICES und den bei Verlängerung des SUBSCRIPTION SERVICE fälligen Betrag der Kreditkarte des KUNDEN zu belasten; (b) verpflichtet sich der KUNDE, Red Hat im Falle der Verlängerung die aktuellen Kreditkarteninformationen mitzuteilen.

3.3 **Taxes.** All Fees are exclusive of Taxes. Client will pay Red Hat an amount equal to any Taxes arising from or relating to this Agreement or an applicable Order Form which are paid by or are payable by Red Hat. "Taxes" means any form of sales, use, value added or other form of taxation and any fines, penalties, surcharges or interest, but excluding any taxes based solely on the net income of Red Hat. To the extent permitted by law, if Client is required to withhold or deduct any portion of the payments due to Red Hat, Client will increase the sum payable to Red Hat by the amount necessary so that Red Hat receives an amount equal to the sum it would have received had Client made no withholdings or deductions.

3.3 **Steuern.** Sämtliche GEBÜHREN verstehen sich ohne STEUERN. Der KUNDE zahlt an Red Hat den Betrag, der den von Red Hat auf Grund oder in Verbindung mit vorliegendem VERTRAG oder einer jeweiligen ORDER FORM gezahlten oder zahlbaren STEUERN entspricht. "STEUERN" bezeichnen sämtliche Mehrwert-, Umsatz-, Verbrauchs- und sonstige Steuern, einschließlich Buß- und Zwangsgelder, Strafgebühren und Zinsen, jedoch keine Steuern, die ausschließlich auf die Erträge von Red Hat erhoben werden. Falls der KUNDE verpflichtet ist, einen Teil der an Red Hat fälligen Zahlungsleistungen einzubehalten oder abzuziehen, so hat er den an Red Hat zahlbaren Betrag im rechtlich zulässigen Rahmen um den jeweils erforderlichen Betrag zu erhöhen, so dass Red Hat den Betrag erhält, der ohne Einbehaltung oder Abzug seitens des KUNDEN fällig gewesen wäre.

4. License and Ownership

4. Lizenz und Eigentum

4.1 **Software.** Each type of Software is governed by a license grant or an end user license agreement, which license terms are contained or referenced in the appendices to this Agreement or the applicable Order Form.

4.1 **Software.** Jede Art von SOFTWARE unterliegt der Gewährung einer Lizenz oder einer Endbenutzer-Lizenzvereinbarung, deren Bedingungen in den Anhängen dieses VERTRAGES oder in der jeweiligen ORDER FORM aufgeführt oder durch Bezugnahme enthalten sind.

4.2 **Freedom to Use Ideas.** Subject to Section 9 (Confidentiality) and Client's rights in Client Information and notwithstanding anything to the contrary contained in this Agreement or an Order Form, the ideas, methods, concepts, know-how, structures, techniques, inventions, developments, processes, discoveries, improvements and other information and materials developed in and during the course of any Order Form may be used by Red Hat, without an obligation to account, in any way Red Hat deems appropriate, including by or for itself or its clients or customers.

4.2 **Freie Verwertung von Ideen.** Vorbehaltlich der in Absatz 9 (Geheimhaltung) enthaltenen Bestimmungen und des Rechts des KUNDEN an seinen KUNDENINFORMATIONEN sowie ungeachtet anders lautender Bestimmungen in vorliegendem VERTRAG oder einer ORDER FORM ist Red Hat berechtigt, das im Zuge und Verlauf eines Auftrages erarbeitete Know-how und die entwickelten Ideen, Methoden, Konzepte, Strukturen, Verfahren, Erfindungen, Entwicklungen, Prozesse, Entdeckungen, Weiterentwicklungen und sonstige Informationen und Materialen ohne Rechenschaftspflicht in jeder geeigneten Form zu verwerten, einschließlich für sich selbst oder seine KUNDEN.

4.3 **Marks.** Unless expressly stated in an Order Form, no right or license, express or implied, is granted in this Agreement for the use of any Red Hat, Red Hat Affiliate, Client or third party trade names, service marks or trademarks, including, without limitation, the distribution of the Software utilizing any Red Hat or Red Hat Affiliate trademarks.

4.3 **Marken.** Sofern in einer ORDER FORM nicht ausdrücklich etwas anderes vereinbart wurde, werden mit vorliegendem VERTRAG weder ausdrücklich noch stillschweigend Rechte oder Lizenzen zur Verwertung von Handelsnamen, Dienstleistungsmarken oder Warenzeichen gewährt, die entweder Eigentum von Red Hat, eines mit Red Hat VERBUNDENEN UNTERNEHMENS, des KUNDEN oder Eigentum Dritter sind. Dies beinhaltet insbesondere auch die Weitergabe der SOFTWARE unter Verwendung der Warenzeichen von Red Hat oder von einem mit Red Hat VERBUNDENEN UNTERNEHMEN.

5. Reporting and Inspection

5. Reporting und Überprüfung

5.1 **Reporting.** Client will notify Red Hat (or the Business Partner from whom Client purchased Software or Services) promptly if the actual number of Units of Software or Services utilised by Client exceeds the number of Units for which Client has paid the applicable Fees. In its notice, Client will include the number of

5.1 **Reporting.** Der KUNDE ist verpflichtet, Red Hat (oder die GESCHÄFTSPARTNER, von denen der KUNDE die SOFTWARE oder SERVICES erworben hat) umgehend zu benachrichtigen, wenn die tatsächliche Anzahl der von ihm verwendeten EINHEITEN an SOFTWARE oder SERVICES die Anzahl der

additional Units and the date(s) on which such Units were first utilised. Red Hat (or the Business Partner) will invoice Client for the applicable Services for such Units and Client will pay for such Services no later than thirty (30) days from the date of invoice.

EINHEITEN überschreitet, für die der KUNDE die entsprechenden Gebühren bezahlt hat. Der KUNDE ist verpflichtet, in seiner Mitteilung die Anzahl der zusätzlichen EINHEITEN sowie das jeweilige Datum anzugeben, an dem diese EINHEITEN erstmals verwendet wurden. Red Hat (oder seine GESCHÄFTSPARTNER) stellen dem KUNDEN die entsprechenden SERVICES für diese EINHEITEN in Rechnung, und der KUNDE ist verpflichtet, diese spätestens dreißig (30) Tage nach Rechnungsdatum zu begleichen.

5.2 Inspection. During the term of this Agreement and for one (1) year thereafter, Red Hat or its designated agent may inspect Client's facilities and records to verify Client's compliance with this Agreement. Any such inspection will take place only during Client's normal business hours and upon no less than ten (10) days prior written notice from Red Hat. Red Hat will give Client written notice of any non-compliance, including the number of under-reported Units of Software or Services, and Client will have fifteen (15) days from the date of this notice to make payment to Red Hat for the applicable Services provided with respect to the underreported Units. If Client under-reports the number of Units utilised by more than five percent (5%) of the number of Units for which Client paid, Client will also pay Red Hat for the cost of such inspection.

5.2 Überprüfung. Red Hat oder ein von Red Hat beauftragter Vertreter ist während der Laufzeit dieses VERTRAGES und ein (1) Jahr darüber hinaus berechtigt, die Anlagen und Einrichtungen sowie die Unterlagen des KUNDEN daraufhin zu überprüfen, ob der vorliegende VERTRAG vom KUNDEN eingehalten wird. Eine solche Überprüfung findet nur während der gewöhnlichen Geschäftszeiten des KUNDEN statt und wird mindestens zehn (10) Tage vorher von Red Hat schriftlich angekündigt. Red Hat teilt dem KUNDEN jede Nichteinhaltung unter Angabe der Anzahl der nicht gemeldeten SOFTWARE und SERVICES mit. Ab dem Datum dieser Mitteilung hat der KUNDE fünfzehn (15) Tage Zeit, die Zahlungen für die jeweils bereitgestellten SERVICES für nicht gemeldete EINHEITEN an Red Hat zu leisten. Wenn die Anzahl der vom KUNDEN verwendeten, unangemeldeten EINHEITEN die Anzahl der von ihm gezahlten EINHEITEN um mehr als fünf Prozent (5%) überschreitet, hat er darüber hinaus die Kosten für eine derartige Überprüfung an Red Hat zu zahlen.

6. Term and Termination

6. Laufzeit und Beendigung

6.1 Term and Termination of Agreement. The term of this Agreement will begin on the Effective Date and will terminate at the expiration of ninety (90) days following written notice of termination given by one party to the other. Termination of this Agreement will not operate to terminate any Order Form and the terms and conditions of this Agreement will continue in full force and effect to the extent necessary to give effect to any Order Form in effect at the time of termination of this Agreement and until such time as the applicable Order Form expires or is terminated in accordance with Section 6.2 below.

6.1 Laufzeit und Beendigung des VERTRAGES. Die Laufzeit dieses VERTRAGES beginnt mit dem DATUM DES INKRAFTTRETENS und endet nach Ablauf von neunzig (90) Tagen nach schriftlicher Kündigung durch eine Partei. Die Kündigung des vorliegenden VERTRAGES bewirkt nicht die Kündigung einer ORDER FORM, und die Bedingungen dieses VERTRAGES bleiben weiterhin im erforderlichen Umfang verbindlich, um den zum Zeitpunkt der Kündigung dieses VERTRAGES gültigen Aufträgen bis zu deren Ablauf oder deren Kündigung gemäß nachstehendem Absatz 6.2 Rechtskraft zu verleihen.

6.2 Term and Termination of Order Form

6.2 Laufzeit und Beendigung einer ORDER FORM

6.2.1 The term of an Order Form begins on the date the Order Form is executed ("Order Form Effective Date") and continues for the term stated in the Order Form. Thereafter, the term for Subscription Services will automatically renew for successive terms of one (1) year each, unless either party gives written notice to the other of its intention not to renew at least sixty (60) days before the commencement of the next renewal term. Client must use any other Services set forth in an Order Form during the term specified in the Order Form or within one (1) year of the Order Form Effective Date, whichever is shorter; if unused, such Services will be forfeited.

6.2.1 Die Laufzeit einer ORDER FORM beginnt mit dem Datum der Ausfertigung ("GÜLTIGKEITSDATUM DER ORDER FORM") und gilt für den in der ORDER FORM angegebenen Zeitraum. Anschließend verlängert sich die Dauer der SUBSCRIPTIONS automatisch um die Dauer von jeweils einem (1) Jahr, sofern eine der Parteien gegenüber der jeweils anderen Partei nicht mindestens sechzig (60) Tage vor Beginn des nächsten Verlängerungszeitraums schriftlich kündigt. Der KUNDE muss alle weiteren in einer ORDER FORM aufgeführten SERVICES innerhalb des dort angegebenen Zeitraums oder innerhalb von einem (1) Jahr nach dem GÜLTIGKEITSDATUM DER ORDER FORM in Anspruch nehmen, je nachdem, welcher Zeitraum kürzer ist. Die SERVICES verfallen, falls sie nicht genutzt werden.

6.2.2 If Client or Red Hat materially breaches the terms of an Order Form, and such breach is not cured within thirty (30) days after written notice of the breach is given to the breaching party, then the other party may, by giving written notice of termination to the

6.2.2 Falls der KUNDE oder Red Hat in erheblicher Weise gegen die Bedingungen einer ORDER FORM verstoßen und diesen Verstoß nicht innerhalb von dreißig (30) Tagen beheben, nachdem die zuwiderhandelnde Partei schriftlich über den Verstoß informiert

breaching party, terminate the applicable Order Form and/or this Agreement; provided, however, that no cure period will be required for a breach of Section 9 of this Agreement (Confidentiality). The termination of an individual Order Form will not terminate any other Order Form or this Agreement unless otherwise specified in the written notice of termination. Without prejudice to any other right or remedy of Red Hat, in the event either party terminates an Order Form, Client will pay Red Hat (or the Business Partner from whom Client purchased such Software or Services) for all Services provided up to the effective date of termination.

wurde, ist die jeweils andere Partei berechtigt, den entsprechenden Auftrag und/oder den vorliegenden VERTRAG gegenüber der zuwiderhandelnden Partei schriftlich zu kündigen, wobei jedoch im Falle eines Verstoßes gegen Absatz 9 dieses VERTRAGES (Geheimhaltung) keine Nachbesserungsfrist gewährt werden muss. Sofern in der schriftlichen Kündigung nichts anderes angegeben wurde, bewirkt die Kündigung einer einzelnen ORDER FORM nicht die Kündigung einer anderen ORDER FORM oder des vorliegenden VERTRAGES. Ungeachtet sonstiger Red Hat zustehender Rechte oder Rechtsmittel ist der KUNDE im Falle der Kündigung einer ORDER FORM durch eine der Parteien verpflichtet, an Red Hat (oder an den GESCHÄFTSPARTNER, von dem der KUNDE die SOFTWARE oder SERVICES erworben hat) sämtliche bis zur Wirksamkeit der Kündigung bereitgestellten SERVICES zu zahlen.

6.3 **Survival.** If this Agreement or an Order Form is terminated for any reason, Sections 3, 4, 5.2, 6.3, 7, 8, 9, 10.2, 12, 13.1, and 13.5-13.15 of this Agreement (as the same are incorporated into each Order Form) will survive such termination.

6.3 **Geltung über das Vertragsende hinaus.** Sollte dieser VERTRAG oder eine ORDER FORM aus jedweden Gründen beendet werden, so bleiben die Absätze 3, 4, 5.2, 6.3, 7, 8, 9, 10.2, 12, 13.1 und 13.5 bis 13.15 dieses VERTRAGES (welche auch in jeder ORDER FORM enthalten sind) über die Beendigung hinaus wirksam.

7. Continuing Business

Nothing in this Agreement will preclude or limit Red Hat from providing software, materials, or services for itself or other clients, irrespective of the possible similarity of such software, materials or services to those that might be delivered to Client. The terms of confidentiality in Section 9 will not prohibit or restrict either party's right to develop, use or market products or services similar to or competitive with the other party; provided, however, that neither party is relieved of its obligations under this Agreement.

7. Fortführung der Geschäftstätigkeit

Red Hat wird durch vorliegenden VERTRAG in keinerlei Weise eingeschränkt oder daran gehindert, Softwareprogramme, Materialen oder Serviceleistungen entweder für sich selbst zu nutzen oder anderen KUNDEN zur Verfügung zu stellen, unabhängig von der Tatsache, ob dem KUNDEN möglicherweise ähnliche Softwareprogramme, Materialen oder Serviceleistungen bereitgestellt werden. Das Recht der Parteien, ähnliche Produkte oder Serviceleistungen wie die jeweils andere Partei bzw. Konkurrenzprodukte zu entwickeln, zu verwerten oder zu vermarkten, wird durch die Geheimhaltungsbestimmungen in Absatz 9 nicht eingeschränkt oder verwehrt. Jedoch werden hierdurch die Parteien nicht von Ihren jeweiligen Pflichten aus diesem VERTRAG befreit.

8. Limitation of Liability and Disclaimer of Damages

8.1 **Limitation of Liability.** **FOR ALL EVENTS AND CIRCUMSTANCES, RED HAT'S AND ITS AFFILIATES' AGGREGATE AND CUMULATIVE LIABILITY ARISING OUT OF OR RELATING TO THIS AGREEMENT AND ALL ORDER FORMS, INCLUDING WITHOUT LIMITATION ON ACCOUNT OF PERFORMANCE OR NON-PERFORMANCE OF OBLIGATIONS, REGARDLESS OF THE FORM OF THE CAUSE OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE), STATUTE OR OTHERWISE WILL BE LIMITED TO DIRECT DAMAGES AND WILL NOT EXCEED THE GREATER OF FORTY FIVE THOUSAND EURO (€45,000) OR THE AMOUNT THAT CLIENT PAID (OR IS PAYABLE) TO RED HAT UNDER THE APPLICABLE ORDER FORM GIVING RISE TO LIABILITY DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY.**

8.2 **Disclaimer of Indirect Damages.** **AND NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS AGREEMENT OR ANY ORDER FORM, IN NO EVENT WILL RED**

8. Haftungsbeschränkung und Ausschluss von Schadensersatz

8.1 **Haftungsbeschränkung.** **IN JEDEM FALL UND UNTER ALLEN UMSTÄNDEN HAFTEN RED HAT UND SEINE VERBUNDENEN UNTERNEHMEN AUF GRUND ODER IN VERBINDUNG MIT VORLIEGENDEM VERTRAG UND SÄMTLICHEN ORDER FORMS, INSBESONDERE AUF GRUND DER ERFÜLLUNG ODER NICHTERFÜLLUNG VON VERPFLICHTUNGEN UNABHÄNGIG VON DER ART DES KLAGEGEGENSTANDES, INSGESAMT UND KUMULATIV NUR FÜR DIREKTE SCHÄDEN. DIE HAFTUNG VON RED HAT UND SEINEN VERBUNDENEN UNTERNEHMEN IST – JE NACHDEM, WELCHER BETRAG HÖHER IST – AUF FÜNFUNDVIERZIGTAUSEND EURO (45.000 €) ODER AUF DEN BETRAG BESCHRÄNKT, DEN DER KUNDE IN DEN UNMITTELBAR VORANGEHENDEN ZWÖLF (12) MONATEN VOR ERSTMALIGEM EINTRETEN DES SCHADENSFALLS GEMÄß DEM DEN HAFTUNGSSFALL BETREFFENDEN ORDER FORM AN RED HAT GEZAHLT HAT ODER ZU ZAHLEN HAT.**

8.2 **Haftungsausschluss in Bezug auf indirekte Schäden.** **UNGEACHTET ABWEICHENDER BESTIMMUNGEN IN VORLIEGENDEM VERTRAG ODER EINER ORDER FORM**

HAT OR ITS AFFILIATES BE LIABLE TO CLIENT OR ITS AFFILIATES FOR: ANY CLAIM BASED UPON A THIRD PARTY CLAIM; ANY INCIDENTAL, CONSEQUENTIAL, SPECIAL, INDIRECT, EXEMPLARY OR PUNITIVE DAMAGES, WHETHER ARISING IN CONTRACT, TORT (INCLUDING NEGLIGENCE OR BREACH OF STATUTORY DUTY), MISREPRESENTATION OR OTHERWISE; OR FOR ANY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THIS AGREEMENT AND/OR ANY ORDER FORMS FALLING WITHIN THE FOLLOWING CATEGORIES:

(A) LOSS OF DATA;
(B) LOSS OF PROFITS;
(C) LOSS OF SAVINGS;
(D) LOSS OR INTERRUPTION OF SERVICE;
(E) LOSS OF BUSINESS OR ANTICIPATORY PROFITS;
(F) LOSS OF USE OR DOWNTIME;
(G) LOSS OF OR CORRUPTION TO DATA OR OTHER INFORMATION OR LOSS OR DAMAGE TO SOFTWARE;

EVEN IF RED HAT OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS AND/OR DAMAGE.

HAFTEN RED HAT UND SEINE VERBUNDENEN UNTERNEHMEN GEGENÜBER DEM KUNDEN ODER SEINEN VERBUNDENEN UNTERNEHMEN IN KEINEM FALL FÜR: ANSPRÜCHE AUF GRUND VON FORDERUNGEN DRITTER, ZUFÄLLIGE, INDIREKTE, SPEZIELLE ODER INDIREKT ENTSTANDENE ODER FOLGESCHÄDEN ODER FÜR STRAFSCHADENSERSATZ. DIES GILT UNABHÄNGIG DAVON, OB DIESE ANSPRÜCHE AUF GRUND DER VERTRAGLICHEN HAFTUNG, DER HAFTUNG AUS UNERLAUBTER HANDLUNG (EINSCHLIEßLICH FAHRLÄSSIGKEIT ODER VERLETZUNG DER RECHTSPFLICHT) ODER AUF GRUND FALSCHER DARSTELLUNGEN ODER ANDERWEITIG ENTSTEHEN. DES WEITEREN HAFTEN RED HAT UND SEINE VERBUNDENEN UNTERNEHMEN NICHT FÜR SCHÄDEN AUF GRUND ODER IN VERBINDUNG MIT VORLIEGENDEM VERTRAG BZW. EINER ORDER FORM, DIE DEN FOLGENDEN KATEGORIEN ZUZUORDNEN SIND:

(A) DATENVERLUST;
(B) GEWINNAUSFALL;
(C) ENTGANGENE EINSPARUNGEN;
(D) EINSTELLUNG ODER UNTERBRECHUNG DER SERVICELEISTUNGEN;
(E) GESCHÄFTSAUSFALL ODER VERLUST ERWARTETER GEWINNE;
(F) ENTGANGENER NUTZEN ODER AUSFALLZEITEN;
(G) VERLUST ODER BESCHÄDIGUNG DER DATEN ODER SONSTIGER INFORMATIONEN UND AUSFALL ODER BESCHÄDIGUNG DER SOFTWARE.

RED HAT ODER DIE MIT RED HAT VERBUNDENEN UNTERNEHMEN HAFTEN SELBST DANN NICHT, WENN SIE VON DER MÖGLICHKEIT EINES SOLCHEN VERLUSTES UND/ODER SCHADENS UNTERRICHTET WURDEN.

8.3 **Disclaimer of Direct Damages.** FOR THE AVOIDANCE OF DOUBT, THE TYPES OF LOSS AND/OR DAMAGE SPECIFIED IN SECTION 8.2 (A) TO (G) INCLUSIVE SHALL NOT CONSTITUTE DIRECT LOSS FOR THE PUPROSES OF THIS AGREEMENT AND/OR ANY ORDER FORM.

8.3 **Haftungsausschluss in Bezug auf direkte Schäden.** ZUR KLARSTELLUNG WIRD VORSORGLICH FESTGEHALTEN, DASS DIE IN ABSATZ 8.2 (A) BIS EINSCHLIEßLICH (G) GENANNTEN VERLUSTE, AUSFÄLLE ODER SCHÄDEN KEINE DIREKTEN VERLUSTE IM SINNE DIESES VERTRAGES BZW. EINER ORDER FORM DARSTELLEN.

8.4 **No Exclusion or Limitation of Liability.** NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT AND/OR ANY ORDER FORM, RED HAT DOES NOT EXCLUDE OR LIMIT LIABILITY FOR (A) PERSONAL INJURY OR DEATH TO THE EXTENT THAT SUCH INJURY OR DEATH RESULTS FROM THE NEGLIGENCE OR WILLFUL DEFAULT OF RED HAT, ITS AGENTS, SERVANTS, AFFILIATES, OR SUBCONTRACTORS; (B) ANY BREACH OF THE CONDITIONS OR WARRANTIES IMPLIED PURSUANT TO SECTION 12 OF THE SALE OF GOODS ACT 1893 AS AMENDED BY SECTION 10 OF THE SALE OF GOODS AND SUPPLY OF SERVICES ACT 1980; AND/OR (C) ANY FRAUDULENT MISREPRESENTATION UPON WHICH THE CLAIMING PARTY CAN BE SHOWN TO HAVE RELIED.

8.4 **Keine Haftungsbeschränkung bzw. kein Haftungsausschluss.** UNGEACHTET ABWEICHENDER BESTIMMUNGEN IN VORLIEGENDEM VERTRAG BZW. EINER ORDER FORM IST DIE HAFTUNG VON RED HAT IN FOLGENDEN FÄLLEN NICHT AUSGESCHLOSSEN ODER BESCHRÄNKT: (A) BEI PERSONENSCHÄDEN ODER TOD, SOFERN DER PERSONENSCHADEN ODER TODESFALL AUF FAHRLÄSSIGKEIT ODER VORSÄTZLICHE UNTERLASSUNG SEITENS RED HAT, SEINER BEVOLLMÄCHTIGTEN, ERFÜLLUNGSGEHILFEN, VERBUNDENEN UNTERNEHMEN ODER UNTERAUFTRAGNEHMER ZURÜCKZUFÜHREN IST; (B) BEI VERSTÖßEN GEGEN STILLSCHWEIGEND ANGENOMMENE BEDINGUNGEN UND KONKLUDENTE ZUSICHERUNGEN GEMÄß § 12 DES GESETZES BETREFFEND DEN VERKAUF VON WAREN VON 1893 [SALE OF GOODS ACT], IN DER UM § 10 ERGÄNZTEN FASSUNG DES GESETZES BETREFFEND DEN VERKAUF VON WAREN UND DIENSTLEISTUNGEN VON 1983 [SALE OF GOODS AND SUPPLY OF SERVICES ACT]; UND/ODER (C) IM FALLE ARGLISTIGER TÄUSCHUNG AUF DIE DIE SCHADENSERSATZ FORDERNDE PARTEI NACHGEWIESENERMAßEN VERTRAUT HAT.

9. Confidentiality

9.1 Obligations. During the term of this Agreement, both parties agree that (i) Confidential Information will be used only in accordance with the terms and conditions of this Agreement; (ii) each will use the same degree of care it utilises to protect its own confidential information, but in no event less than reasonable care; and (iii) the Confidential Information may be disclosed only to employees, agents and contractors with a need to know, and to its auditors and legal counsel, in each case, who are under a written obligation to keep such information confidential using standards of confidentiality not less restrictive than those required by this Agreement. Both parties agree that obligations of confidentiality will exist for a period of two (2) years following initial disclosure of the particular Confidential Information. "Confidential Information" means all information disclosed by either Red Hat or Client ("Disclosing Party") to the other party ("Recipient") during the term of this Agreement that is either (i) marked confidential or (ii) disclosed orally and described as confidential at the time of disclosure and subsequently set forth in writing, marked confidential, and sent to the Recipient within thirty (30) days following the oral disclosure.

9.2 Exclusions. Confidential Information will not include information which: (i) is or later becomes publicly available without breach of this Agreement, or is disclosed by the Disclosing Party without obligation of confidentiality; (ii) is known to the Recipient at the time of disclosure by the Disclosing Party; (iii) is independently developed by the Recipient without use of the Confidential Information; (iv) becomes lawfully known or available to the Recipient without restriction from a source having the lawful right to disclose the information; (v) is generally known or easily ascertainable by parties of ordinary skill in the business of the Recipient; or (vi) is software code in either object code or source code form that is licensed under an open source license. The Recipient will not be prohibited from complying with disclosure mandated by applicable law if, where reasonably practicable and without breaching any legal or regulatory requirement, it gives the Disclosing Party advance notice of the disclosure requirement.

10. Representations and Warranties

10.1 General Representations and Warranties. Red Hat represents and warrants that: (a) it will use reasonable skill and care in providing the Services; (b) the Services will be performed in a professional and workmanlike manner by qualified personnel; (c) it has the authority to enter into this Agreement with Client; and (d) to Red Hat's knowledge, Red Hat branded Software does not, at the time of delivery to Client, include malicious or hidden mechanisms or code for the purpose of damaging or corrupting the Software.

9. Geheimhaltung

9.1 Pflichten. Während der Laufzeit dieses VERTRAGES verpflichten sich beide Parteien, (i) VERTRAULICHE INFORMATIONEN ausschließlich gemäß den Bedingungen dieses VERTRAGES zu verwenden, (ii) VERTRAULICHE INFORMATIONEN mit der gleichen Sorgfalt zu behandeln, die sie für den Schutz ihrer eigenen VERTRAULICHEN INFORMATION anwenden, jedoch mindestens unter Einhaltung der angemessenen Sorgfaltspflicht und (iii) VERTRAULICHE INFORMATIONEN nur gegenüber den jeweiligen Wirtschaftsprüfern und Beratern sowie gegenüber denjenigen Mitarbeitern, Bevollmächtigten und Unternehmen offen zu legen, die diese Informationen benötigen, wobei die genannten Personen schriftlich zur Geheimhaltung unter Verwendung von Vertraulichkeitsrichtlinien zu verpflichten sind, die mindestens denjenigen des vorliegenden VERTRAGES entsprechen. Beide Parteien verpflichten sich, VERTRAULICHE INFORMATIONEN für einen Zeitraum von zwei (2) Jahren nach erstmaliger Offenlegung geheim zu halten. "VERTRAULICHE INFORMATIONEN" bezeichnen sämtliche von Red Hat oder dem KUNDEN ("OFFEN LEGENDE PARTEI") der jeweils anderen Partei ("EMPFÄNGER") während der Laufzeit dieses VERTRAGES offen gelegte Informationen, die entweder (i) als vertraulich gekennzeichnet sind oder (ii) unter Mitteilung der Vertraulichkeit mündlich offen gelegt wurden und anschließend schriftlich mit einem Vertraulichkeitsvermerk niedergelegt und dem EMPFÄNGER innerhalb von dreißig (30) Tagen nach der mündlichen Offenlegung zugestellt wurden.

9.2 Ausnahmen. VERTRAULICHE INFORMATIONEN sind keine Informationen, die (i) öffentlich zugänglich sind oder werden, ohne gegen den vorliegenden VERTRAG zu verstoßen, oder die von der OFFEN LEGENDEN PARTEI ohne Verpflichtung zur Geheimhaltung weitergegeben werden, (ii) dem EMPFÄNGER zum Zeitpunkt der Offenlegung durch die OFFEN LEGENDE PARTEI bereits bekannt sind, (iii) vom EMPFÄNGER unabhängig, ohne Verwendung der VERTRAULICHEN INFORMATIONEN erarbeitet werden, (iv) dem EMPFÄNGER auf rechtmäßigem Wege uneingeschränkt durch Dritte zugänglich oder bekannt gemacht werden, die rechtmäßig zur Offenlegung der Informationen befugt sind, (v) der Allgemeinheit bekannt sind oder in der Branche des EMPFÄNGERS von Personen mit normalen Fähigkeiten leicht zu ermitteln sind oder (vi) bei denen es sich um Softwarecode entweder in Form von Objektcode oder Quellcode gemäß einer Open-Source-Lizenz handelt. Dem EMPFÄNGER steht es zu, einer gesetzlich vorgeschriebenen Offenlegung nachzukommen, sofern sie die OFFEN LEGENDE PARTEI im Voraus über die Offenlegungspflicht informiert und dies unter vertretbaren Umständen möglich ist, ohne gegen gesetzliche oder behördliche Vorschriften zu verstoßen

10. Zusicherungen und Gewährleistungen

10.1 Allgemeine Zusicherungen und Gewährleistungen. Red Hat erklärt und gewährleistet, dass (a) die SERVICES mit hinreichender Sachkenntnis und Sorgfalt bereitgestellt werden, (b) die SERVICES von qualifiziertem Personal professionell und fachgerecht durchgeführt werden, (c) Red Hat zum Abschluss des vorliegenden VERTRAGES bevollmächtigt ist und (d) die mit dem Warenzeichen von Red Hat gekennzeichnete SOFTWARE nach Kenntnis von Red Hat zum Zeitpunkt der Bereitstellung an den KUNDEN keine bösartigen oder versteckten Mechanismen oder Codes enthält, die die SOFTWARE beschädigen könnten.

10.2 Disclaimer of Warranty. EXCEPT AS EXPRESSLY PROVIDED IN SECTION 10.1 OR BY A THIRD PARTY VENDOR DIRECTLY TO CLIENT UNDER A SEPARATE AGREEMENT, THE SERVICES, SOFTWARE AND ANY HARDWARE ARE PROVIDED BY RED HAT "AS IS" AND WITHOUT WARRANTIES, REPRESENTATIONS, CONDITIONS OR OTHER TERMS OF ANY KIND AND RED HAT EXCLUDES ALL IMPLIED WARRANTIES TO THE EXTENT PERMISSIBLE BY LAW (INCLUDING, WITHOUT LIMITATION,THOSE OF MERCHANTABILITY, SALE BY DESCRIPTION, SALE BY SAMPLE, SATISFACTORY QUALITY, NON-INFRINGEMENT AND FITNESS FOR A PARTICULAR PURPOSE). FOR THE AVOIDANCE OF DOUBT AND TO THE EXTENT PERMITTED BY LAW, SECTION 39 OF THE SALE OF GOODS AND SUPPLY OF SERVICES ACT 1980 IS EXCLUDED AND THE CLIENT AGREES THAT THIS EXCLUSION IS FAIR AND REASONABLE.

10.2 Ausschluss der Gewährleistung. SOFERN IN ABSATZ 10.1 ODER IN EINER ZWISCHEN EINEM DRITTANBIETER UND DEM KUNDEN SEPARAT GETROFFENEN VEREINBARUNG NICHT AUSDRÜCKLICH ETWAS ANDERES VEREINBART WURDE, STELLT RED HAT DIE SERVICELEISTUNGEN, SOFTWAREPROGRAMME UND SÄMTLICHE HARDWARE SO WIE SIE „GEHT UND STEHT" OHNE JEDWEDE ZUSICHERUNGEN, GEWÄHRLEISTUNGEN ODER SONSTIGE BEDINGUNGEN ZUR VERFÜGUNG, UND SÄMTLICHE STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN WERDEN VON RED HAT IM RECHTLICH ZULÄSSIGEN UMFANG AUSGESCHLOSSEN (INSBESONDERE GEWÄHRLEISTUNGEN IN BEZUG AUF MARKTGÄNGIGE QUALITÄT, VERKAUF NACH WARENBESCHREIBUNG, VERKAUF NACH MUSTER, ZUFRIEDEN STELLENDE QUALITÄT, NICHTVERLETZUNG VON SCHUTZRECHTEN DRITTER ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK). ES WIRD VORSORGLICH DARAUF HINGEWIESEN, DASS § 39 DES GESETZES BETREFFEND DEN VERKAUF VON WAREN UND DIENSTLEISTUNGEN VON 1980 KEINE ANWENDUNG FINDET, UND DER KUNDE ERKLÄRT SEIN EINVERSTÄNDNIS, DASS DIESER AUSSCHLUSS BILLIG UND ANGEMESSEN IST.

RED HAT DOES NOT GUARANTEE OR WARRANT THAT THE USE OF THE SERVICES, SOFTWARE OR HARDWARE WILL BE UNINTERRUPTED, COMPLY WITH REGULATORY REQUIREMENTS, BE ERROR FREE OR THAT RED HAT WILL CORRECT ALL SOFTWARE ERRORS. FOR THE BREACH OF THE WARRANTIES SET FORTH IN SECTION 10.1, CLIENT'S EXCLUSIVE REMEDY, AND RED HAT'S ENTIRE LIABILITY, WILL BE THE REPERFORMANCE OF DEFICIENT SERVICES, OR IF RED HAT CANNOT SUBSTANTIALLY CORRECT A BREACH IN A COMMERCIALLY REASONABLE MANNER, CLIENT MAY TERMINATE THE RELEVANT SERVICES AND RECEIVE A PRO RATA REFUND OF THE FEES PAID FOR THE DEFICIENT SERVICES AS OF THE EFFECTIVE DATE OF TERMINATION.

RED HAT ÜBERNIMMT KEINE GARANTIE ODER GEWÄHRLEISTUNG, DASS DIE INANSPRUCHNAHME DER SERVICELEISTUNGEN SOWIE DIE NUTZUNG DER SOFT- UND HARDWARE KEINEN UNTERBRECHUNGEN UNTERLIEGT, DEN GESETZLICHEN ANFORDERUNGEN ENTSPRICHT, FEHLERFREI IST ODER DASS SÄMTLICHE SOFTWAREFEHLER VON RED HAT BEHOBEN WERDEN. IM FALLE EINES VERSTOßES GEGEN DIE IN ABSATZ 10.1 ANGEGEBENEN GEWÄHRLEISTUNGEN BESTEHT DAS AUSSCHLIEßLICHE RECHTSMITTEL DES KUNDEN UND DIE GESAMTE VERPFLICHTUNG VON RED HAT IN DER NACHBESSERUNG FEHLERHAFTER SERVICELEISTUNGEN. FALLS RED HAT EINEN VERSTOß NICHT IN WIRTSCHAFTLICH ANGEMESSENER WEISE IM WESENTLICHEN BEHEBEN KANN, IST DER KUNDE BERECHTIGT, DIE JEWEILIGEN SERVICELEISTUNGEN ZU KÜNDIGEN UND KANN MIT WIRKSAMKEIT DER KÜNDIGUNG EINE ANTEILIGE ERSTATTUNG DER FÜR DIE FEHLERHAFTEN SERVICELEISTUNGEN GEZAHLTEN GEBÜHREN VERLANGEN.

Without limiting the generality of the foregoing disclaimer, the Software, Services and any hardware provided are not specifically designed, manufactured or intended for use in (a) the planning, construction, maintenance, control, or direct operation of nuclear facilities, (b) aircraft navigation, control or communication systems, weapons systems, or (c) direct life support systems. Client agrees that it is solely responsible for the results obtained from the use of the Software and Services in such areas.

Unbeschadet der Allgemeingültigkeit des vorgenannten Haftungsausschlusses wurden die bereitgestellten Serviceleistungen, SOFTWARE sowie die Hardware nicht speziell zur Anwendung in folgenden Bereichen konzipiert und hergestellt und sind nicht für die Anwendung in folgenden Bereichen bestimmt: (a) Planung, Konstruktion, Instandhaltung, Kontrolle und direkter Betrieb von Kernenergieanlagen, (b) Flugzeugnavigation, Kontroll- oder Kommunikationssysteme, Waffensysteme oder (c) Lebensrettungssysteme. Der KUNDE bestätigt, dass er für die Folgen einer Nutzung der SOFTWARE und SERVICES in den genannten Bereichen allein verantwortlich ist.

11. Open Source Assurance Program

For Software that is Red Hat branded, purchases under this Agreement may entitle Client to participate in Red Hat's Open Source Assurance Program which is described at http://www.redhat.com/rhel/details/assurance/. The terms for this optional program are subject to a separate agreement which can be viewed at http://www.redhat.com/legal/open_source_assurance_agreement.html.

12. Governing Law/Consent to Jurisdiction

This Agreement (and all Order Forms) and any dispute or claim arising out of or in relation to or in connection with it is governed by, and will be construed in accordance with, Irish law, without giving effect to the United Nations Convention on Contracts for the International Sale of Goods. Each party irrevocably agrees that the Irish courts will have exclusive jurisdiction to settle any dispute or claim that arises from or in connection with this Agreement (and all Order Forms).

13. Miscellaneous

13.1 Notices. Notices must be in English and German, in writing, and will be deemed given when delivered by hand or five (5) days after being sent using a method that provides for positive confirmation of delivery to the respective addresses or facsimile numbers indicated in an Order Form; provided that any notice from Client to Red Hat includes a copy sent to: Red Hat, Inc., Attention: General Counsel, 100 East Davie Street, Raleigh, North Carolina 27601; Facsimile: +1-919-754 3704.

13.2 Assignment. This Agreement is assignable by either party only with the other party's prior written consent, which will not be unreasonably withheld, conditioned or delayed; provided, however, either party may, upon written notice and without the prior approval of the other party, (a) assign this Agreement to an Affiliate as long as the Affiliate has sufficient credit to satisfy its obligations under this Agreement and the scope of Service is not affected; and (b) assign this Agreement pursuant to a merger or a sale of all or substantially all of such party's assets or stock.

13.3 Independent Contractor. Red Hat is an independent contractor and nothing in this Agreement or related to Red Hat's performance of any Order Form will be construed to create an employment or agency relationship between Client (or any Client personnel) and Red Hat (or any Red Hat personnel). Each party will be solely responsible for supervision, direction, control and payment of its personnel, including applicable taxes, deductions, other payments and benefits. Red Hat may subcontract Services under an Order Form to third parties or Affiliates without the approval of Client; provided, however, that (a)

11. Open Source Schutzprogramm

Falls der KUNDE gemäß vorliegendem VERTRAG Red Hat SOFTWARE erwirbt, ist er zur Teilnahme am "Red Hat Open Source Assurance Program" berechtigt. Nähere Angaben hierzu können unter http://www.redhat.com/rhel/details/assurance/ abgerufen werden. Die Bedingungen für dieses optionale Programm unterliegen einer gesonderten Vereinbarung und können unter http://www.redhat.com/legal/open_source_assurance_agreement.html eingesehen werden.

12. Geltendes Recht /Anerkennung des Gerichtstandes

Der vorliegende VERTRAG, einschließlich sämtlicher ORDER FORMS, deren Auslegung sowie sämtliche Streitigkeiten oder Forderungen, die auf Grund oder in Verbindung mit diesem VERTRAG oder den ORDER FORMS entstehen, unterliegen dem irischen Recht, wobei das Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenverkauf keine Anwendung findet. Die Parteien erkennen unwiderruflich an, dass ausschließlich die irischen Gerichte für die Beilegung von Streitigkeiten oder Forderungen aus oder in Verbindung mit diesem VERTRAG und sämtlichen ORDER FORMS zuständig sind.

13. Sonstige Bestimmungen

13.1 Mitteilungen. Mitteilungen bedürfen der Schriftform und sind in englischer und deutscher Sprache zu verfassen. Sie gelten als zugestellt, wenn sie per Boten oder fünf (5) Tage nach Versand unter Verwendung einer Versandmethode mit positiver Zustellungsbestätigung an die jeweils in der ORDER FORM angegebenen Adressen oder Faxnummern zugestellt wurden. Mitteilungen des KUNDEN an Red Hat sind darüber hinaus in Kopie an folgende Adresse zu senden: Red Hat, Inc., Attention: General Counsel, 100 East Davie Street, Raleigh, North Carolina 27601; Fax: +1-919-754 3704.

13.2 Abtretung. Die Parteien dürfen den vorliegenden VERTRAG nur mit der vorherigen schriftlichen Zustimmung der jeweils anderen Partei abtreten, welche nicht ohne triftigen Grund verweigert, an Bedingungen geknüpft oder verzögert werden darf. Die Parteien sind jedoch nach schriftlicher Mitteilung und ohne die vorherige Zustimmung der jeweils anderen Partei berechtigt, (a) diesen VERTRAG an ein VERBUNDENES UNTERNEHMEN abzutreten, solange dieses Unternehmen über eine ausreichende Kreditwürdigkeit zur Erfüllung seiner Verpflichtungen aus vorliegendem VERTRAG verfügt und der Umfang der SERVICES nicht beeinträchtigt wird, und (b) diesen VERTRAG im Zuge eines Unternehmenszusammenschlusses oder der Veräußerung sämtlicher oder wesentlicher Vermögenswerte oder Geschäftsanteile abzutreten.

13.3 Selbständiger Unternehmer. Red Hat ist ein selbständiges Unternehmen, und der vorliegende VERTRAG oder die Erfüllung einer ORDER FORM ist nicht dahingehend auszulegen, dass damit zwischen dem KUNDEN (oder den Mitarbeitern des KUNDEN) und Red Hat (oder den Mitarbeitern von Red Hat) ein Anstellungs- oder Vertretungsverhältnis geschaffen wird. Die Parteien sind jeweils allein für die Überwachung, Leitung, Kontrolle und Vergütung ihrer Mitarbeiter verantwortlich, einschließlich der Entrichtung von einschlägigen Steuern, Abzügen und sonstigen Zahlungen und Leistungen. Red Hat ist berechtigt, SERVICES aus einer ORDER

subcontractors agree to protect Client Confidential Information, and (b) Red Hat remains responsible to Client for performance of its obligations hereunder.

FORM ohne Zustimmung des KUNDEN im Subunternehmervertrag an Dritte oder VERBUNDENE UNTERNEHMEN weiterzugeben. Dies setzt jedoch voraus, dass (a) sich die Unterauftragnehmer zur Geheimhaltung der VERTRAULICHEN INFORMATIONEN des KUNDEN verpflichten, und (b) Red Hat gegenüber dem KUNDEN weiterhin für die Erfüllung seiner Verpflichtungen aus vorliegendem VERTRAG haftet.

13.4 Force Majeure. Neither party will be liable for any failure to perform its obligations or delays in performance (except of obligations to pay money) caused by acts of God, wars, riots, governmental acts, strikes, fires, floods, hurricanes, earthquakes, government restrictions, terrorist acts or other causes beyond its reasonable control.

13.4 Höhere Gewalt. Keine der Parteien haftet für die Nichterfüllung ihrer Pflichten oder für Leistungsverzug (mit Ausnahme der Zahlungsverpflichtung) auf Grund von höherer Gewalt, Krieg, Ausschreitung, Verwaltungsakten, Streik, Feuer, Überschwemmung, Orkan, Erdbeben, staatliche Beschränkungen, Terrorakte oder auf Grund anderer von den Parteien nicht zu vertretenden Umständen.

13.5 Non-solicitation. Client agrees not to solicit or hire any personnel of Red Hat involved with the delivery of Services in connection with any Order Form during the term of and for twelve (12) months after termination or expiration of such Order Form; provided that Client may hire an individual employed by Red Hat who, without other solicitation, responds to advertisements or solicitations aimed at the general public.

13.5 Keine Abwerbung. Der KUNDE verpflichtet sich für die Laufzeit einer ORDER FORM und darüber hinaus für zwölf (12) Monate nach Kündigung oder Ablauf der ORDER FORM, keine Mitarbeiter von Red Hat abzuwerben oder einzustellen, die an der Bereitstellung der SERVICES in Verbindung mit den ORDER FORMS beteiligt sind. Der KUNDE ist jedoch berechtigt, einen Angestellten von Red Hat einzustellen, der sich ohne anderweitige Abwerbung auf Stellenangebote meldet, die an die Allgemeinheit gerichtet sind.

13.6 Export. Red Hat may supply Client with technical data that is subject to export control restrictions. Red Hat will not be responsible for compliance by Client with applicable export obligations or requirements for this technical data. Client agrees to comply with all applicable export control restrictions. If Client breaches this Section 13.6 or the export provisions of an applicable end user license agreement for the Software, or any provision referencing these sections, Red Hat may terminate this Agreement and/or the applicable Order Form and its obligations thereunder without liability to Client.

13.6 Export. Red Hat stellt dem KUNDEN ggf. technische Daten zur Verfügung, die Exportbeschränkungen unterliegen. Red Hat haftet im Hinblick auf diese technischen Daten nicht für die Einhaltung geltender Exportverpflichtungen oder -anforderungen durch den KUNDEN. Der KUNDE verpflichtet sich zur Einhaltung sämtlicher Exportbeschränkungen. Falls der KUNDE gegen den vorliegenden Absatz 13.6 oder eine für die SOFTWARE geltende Endbenutzer-Lizenzvereinbarung oder gegen eine diesbezügliche Bestimmung verstößt, so kann Red Hat den vorliegenden VERTRAG und/oder die jeweilige ORDER FORM sowie seine damit verbundenen Verpflichtungen ohne Entstehung einer Haftung aufkündigen.

13.7 Privacy. Red Hat manages and stores Client Information in a centralised database which is accessible to Red Hat's Affiliates. In order to provide the Services, it may further be necessary for Client Information to be transferred between Red Hat, its Affiliates, Business Partners and/or subcontractors. Red Hat's Affiliates, its Business Partners and/or subcontractors may have their place of business in a country outside of the European Union, which, like the United States, may not provide an adequate level of data protection in terms of European data protection regulations. Red Hat will ensure that transfer of personal data to recipients in such countries is based on legal provisions or that an adequate level of data protection is ensured in accordance with European data protection regulations. **Client acknowledges and agrees that Red Hat may process Client Information for the purposes and in the scope set out in this section. Client further acknowledges and agrees that Red Hat and its Affiliates may process and use the Client Information for the purposes of marketing their own products and/or services. Client may revoke its consent for the use of personal data for marketing purposes at any time with future effect by giving notice to Red Hat under https://www.redhat.com/apps/response/feedback.html.**

13.7 Datenschutz. Die KUNDENINFORMATIONEN werden von Red Hat in einer zentralen Datenbank verwaltet und gespeichert, auf die VERBUNDENE UNTERNEHMEN von Red Hat zugreifen können. Um den KUNDEN die SERVICES zur Verfügung stellen zu können, ist es unter Umständen zudem erforderlich, dass Red Hat KUNDENINFORMATIONEN ihren VERBUNDENEN UNTERNEHMEN, GESCHÄFTSPARTNERN und/oder Unterauftragnehmern übermittelt. Die mit Red Hat VERBUNDENEN UNTERNEHMEN, ihre GESCHÄFTSPARTNER und/oder Unterauftragnehmer können ihren Geschäftssitz in einem Land außerhalb der Europäischen Union haben, dass, wie z.B. die Vereinigten Staaten, kein angemessenes Datenschutzniveau im Sinne der europäischen Datenschutzvorschriften aufweist. Red Hat wird dafür Sorge tragen, dass eine Übermittlung an Empfänger in solche Länder auf Grundlage einer gesetzlichen Vorschrift erfolgt oder auf sonstige Weise ein angemessenes Datenschutzniveau im Sinne der europäischen Datenschutzvorschriften hergestellt wird. **Der KUNDE willigt ein, dass Red Hat die KUNDENINFORMATIONEN zu den in dieser Ziffer genannten Zwecken und im in dieser Ziffer beschriebenen Umfang verarbeiten darf. Desweiteren willigt der KUNDE ein, dass Red Hat sowie die mit ihr VERBUNDENEN UNTERNEHMEN die KUNDENINFORMATIONEN zur Bewerbung ihrer Produkte und Services verarbeiten dürfen. Der KUNDE kann die Einwilligung zur Nutzung seiner personenbezogenen Daten zu Werbezwecken jederzeit mit Wirkung für die Zukunft durch Mitteilung an Red Hat widerrufen: https://www.redhat.com/apps/response/feedback.html.**

13.8 **Dispute Resolution.** Each party agrees to give the other a written description of any problem(s) that may arise and to make a good faith effort to amicably resolve any such problem before commencing any proceeding. Notwithstanding the foregoing, either party may take any action reasonably required to protect such party's rights. No claim or action, regardless of form, arising out of this Agreement or an Order Form may be brought by either party more than one (1) year after the cause of action has accrued.

13.8 **Beilegung von Streitfällen.** Die Parteien verpflichten sich, sämtliche ggf. entstehenden Problemfälle der jeweils anderen Partei schriftlich darzulegen und sich nach Treu und Glauben um eine gütliche Lösung des Problems zu bemühen, bevor weitere Maßnahmen eingeleitet werden. Die Parteien können unbeschadet des Vorangehenden angemessene Maßnahmen ergreifen, die zum Schutz ihrer jeweiligen Rechte erforderlich sind. Nach mehr als einem (1) Jahr nach Eintreten eines Klagegrundes auf Grund dieses VERTRAGES oder einer ORDER FORM sind die Parteien nicht mehr berechtigt, Forderungen oder Klagen in jedweder Form vorzubringen.

13.9 **Headings.** All headings contained in this Agreement are inserted for identification and convenience and will not be deemed part of this Agreement for purposes of interpretation.

13.9 **Überschriften.** Sämtliche Überschriften in vorliegendem VERTRAG dienen lediglich der Gliederung und Übersicht und gelten nicht als Bestandteil dieses VERTRAGES zum Zwecke der Auslegung..

13.10 **Severability.** If any provision of this Agreement is held invalid or unenforceable for any reason but would be valid and enforceable if appropriately modified, then such provision will apply with the modification necessary to make it valid and enforceable. If such provision cannot be so modified, the parties agree that such invalidity will not affect the validity of the remaining provisions of the Agreement.

13.10 **Teilnichtigkeit.** Sollten einzelne Bestimmungen dieses VERTRAGES gleich aus welchem Rechtsgrund ungültig oder nicht durchsetzbar sein, die jedoch im Falle einer entsprechenden Änderung gültig oder durchsetzbar wären, so ist die jeweilige Bestimmung zum Zwecke ihrer Gültigkeit und Durchsetzbarkeit mit der erforderlichen Änderung anzuwenden. Sollte eine derartige Änderung dieser Bestimmung nicht möglich sein, wird zwischen den Parteien vereinbart, dass die Gültigkeit der übrigen Bestimmungen des VERTRAGES durch die Ungültigkeit dieser Bestimmung nicht berührt wird.

13.11 **Waiver.** The delay or failure of either party to exercise any rights under this Agreement will not constitute or be deemed a waiver or forfeiture of such rights. No waiver will be valid unless in writing and signed by an authorized representative of the party against whom such waiver is sought to be enforced..

13.11 **Verzicht.** Ein Verzug oder Versäumnis seitens der Parteien, jedwede Rechte aus vorliegendem VERTRAG geltend zu machen, stellt keinen Verzicht oder Verfall eines solchen Rechts dar. Eine Verzichtserklärung bedarf zu ihrer Gültigkeit der Schriftform und ist von einem bevollmächtigten Vertreter derjenigen Partei zu unterzeichnen, von der ein solcher Verzicht eingegangen wird.

13.12 **Complete Agreement.** Each Order Form (a) is a separate agreement and is deemed to incorporate this Agreement, unless otherwise expressly provided in that Order Form; (b) constitutes the exclusive terms and conditions with respect to the subject matter of that Order Form, notwithstanding any different or additional terms that may be contained in the form of purchase order or other document used by Client to place orders or otherwise effect transactions under this Agreement; and (c) represents the final, complete and exclusive statement of the agreement between the parties with respect thereto, notwithstanding any prior written agreements or prior and contemporaneous oral agreements with respect to the subject matter of the Order Form. In the event of any conflict between this Agreement, any Order Form and any end user license agreement for Software, this Agreement will take precedence unless otherwise expressly provided in the Order Form. Notwithstanding any provision to the contrary in this Agreement, any applicable end user licence agreement will be governed by the laws of the State of New York and of the United States, without regard to any conflict of laws provisions. The parties have not relied upon, and will have no remedy in respect of, any warranty, statement, representation or understanding made by any party (whether or not that party is a party to this Agreement) unless it is expressly set out in this Agreement. Nothing in this Agreement will restrict either party's liability for fraudulent misrepresentation.

13.12 **Gesamter Vertrag.** Jede ORDER FORM (a) stellt eine gesonderte Vereinbarung dar und ist Bestandteil des vorliegenden VERTRAGES, sofern in der jeweiligen ORDER FORM nicht ausdrücklich etwas anderes bestimmt ist; (b) beinhaltet die ausschließlichen Bedingungen in Bezug auf den Gegenstand der ORDER FORM, und zwar ungeachtet abweichender oder zusätzlicher Bedingungen in den Bestellaufträgen oder sonstigen Dokumenten des KUNDEN, die von ihm zur Erteilung von Aufträgen oder zur Durchführung von Geschäften gemäß vorliegendem VERTRAG verwendet werden; (c) stellt ungeachtet jedweder vorhergehenden schriftlichen oder gleichzeitig mündlichen Vereinbarungen im Hinblick auf den Gegenstand der ORDER FORM den diesbezüglich endgültigen, vollständigen und ausschließlichen Vertragsinhalt zwischen den Parteien dar. Sollte sich zwischen dem vorliegenden VERTRAG, einer ORDER FORM und einem SOFTWARE Endbenutzer-Lizenzvertrag ein Widerspruch ergeben, so hat dieser VERTRAG Vorrang, es sei denn, in der ORDER FORM ist ausdrücklich etwas anderes bestimmt. Ungeachtet gegenteiliger Bestimmungen in vorliegendem VERTRAG unterliegt jeder gültige Endbenutzer-Lizenzvertrag dem Recht des US-Bundesstaates New York und der Vereinigten Staaten, und zwar ohne Anwendung der Bestimmungen des Internationalen Privatrechts. Die Parteien haben sich nicht auf eine Gewährleistung, Erklärung, Zusicherung oder Abrede seitens einer Partei berufen (unabhängig davon, ob es sich um eine am vorliegenden VERTRAG beteiligte Partei handelt) und können diesbezüglich keine Rechtsmittel geltend machen. Die Bestimmungen in vorliegendem VERTRAG stellen keine

Haftungsbeschränkung der Parteien in Bezug auf arglistige Täuschung dar.

13.13 Amendment. Neither this Agreement nor any Order Form may be amended or modified except in a writing signed by the parties, which writing makes specific reference to this Agreement or the applicable Order Form.

13.13 Änderungen. Eine Änderung oder Ergänzung des vorliegenden VERTRAGES oder einer ORDER FORM bedarf der Schriftform und ist von den Parteien zu unterzeichnen, wobei in der schriftlichen Ergänzung speziell auf den vorliegenden VERTRAG oder die entsprechende ORDER FORM zu verweisen ist.

13.14 Counterparts and Facsimile Signature. In the event this Agreement is executed with signatures, this Agreement may be executed in counterparts, each of which will be deemed an original and all of which will constitute one and the same document. The parties may exchange signature pages by facsimile and such signatures will be effective to bind the parties to all the terms contained in this Agreement.

13.14 Zweitausfertigungen und Faksimileunterschrift. Falls der vorliegende VERTRAG durch Unterzeichnung ausgefertigt wird, kann dies in mehreren Ausfertigungen erfolgen. Jede Ausfertigung gilt als Original und stellt ein und dasselbe Dokument dar. Die Parteien können die Unterschriftenseiten per Fax übersenden, und durch ihre Unterschriften sind die Parteien an alle in vorliegendem VERTRAG enthaltenen Bestimmungen gebunden.

13.15 Further Assurance. Client will, at the request and cost of Red Hat, use all reasonable endeavours to do or procure the doing of all such further acts and execute or procure the valid execution of all such documents, as may from time to time be necessary in Red Hat's reasonable opinion to give full effect to this Agreement and to vest in Red Hat the full benefit of the rights and benefits to be transferred to it under this Agreement.

13.15 Sonstige Zusicherung. Der KUNDE unternimmt auf Wunsch und Kosten von Red Hat alle angemessenen Anstrengungen, um sämtliche weiteren Handlungen durchzuführen oder zu veranlassen und fertigt darüber hinaus sämtliche Dokumente aus oder veranlasst deren rechtsgültige Ausfertigung, wie es jeweils im vertretbaren Ermessen von Red Hat für die Durchführung dieses VERTRAGES und für die Übertragung der notwendigen Rechte und Vorteile auf Red Hat gemäß vorliegendem VERTRAG erforderlich ist.

13.16 English Language. This Agreement has been negotiated by the parties in English. The parties confirm that it is their wish that this Agreement, as well as all other documents relating thereto, have been and shall be drawn up in the English language. The English language version of this Agreement will prevail in all respects over any translation, and all other versions are for convenience only and are not binding.

13.16 Englische Sprachversion. Der vorliegende VERTRAG wurde zwischen den Parteien in englischer Sprache verhandelt. Die Parteien bestätigen, dass es ihr Wunsch ist, diesen VERTRAG sowie sämtliche damit verbundenen Dokumente in englischer Sprache zu verfassen. Die englische Fassung dieses VERTRAGES hat in jeder Hinsicht Vorrang vor sämtlichen Übersetzungen, und alle anderen Fassungen werden lediglich gefälligkeitshalber zur Verfügung gestellt und sind nicht verbindlich.

APPENDIX 1
SUBSCRIPTION SERVICES

ANHANG 1
SUBSCRIPTION SERVICES

Red Hat sells subscriptions that entitle you to receive Red Hat services and/or Software during the period of the subscription (generally, one or three years). This Appendix to the Order Form describes the **"Subscription Services"** that Red Hat provides for:

- Software product offerings (these subscriptions are called **"Software Subscriptions"**);
- Support and maintenance services offerings (these subscriptions are called **"Support Subscriptions"**); and
- Software delivery and management services offerings (these subscriptions are called **"Management Subscriptions"**).

The Exhibits to this Appendix provide additional terms concerning the Subscription Services. Whether you purchase Subscription Services from us or though one of our authorized Business Partners, we agree to provide you with the Subscription Services on the terms described in this Appendix, which includes the Exhibits and documents referred to in this Appendix (together, the **"Appendix"**). In exchange, you agree to comply with the terms of the Agreement, including this Appendix.

When we use a capitalized term in this Appendix without defining it, the term has the meaning defined in the Agreement to which this Appendix applies, such as the Red Hat Enterprise Agreement. In the event of a conflict, inconsistency or difference between this Appendix and an Exhibit to this Appendix, the terms of the Exhibit control.

1. Subscription Services – An Overview

1.1 Subscription Units: We charge you a fee for our Subscription Services based on the total number of Units of Software or other Red Hat Products that you deploy, install, use or execute (as described more fully in Tables 1.4, 1.5 and 1.6 below and elsewhere in the Appendix). For example, Software Subscriptions for Red Hat Enterprise Linux Server are priced based on the number and other characteristics of Systems, Virtual Nodes or Physical Nodes (e.g. Socket-pairs, Virtual Guests, etc.) on which you install or use the Software, while Software Subscriptions for Red Hat JBoss Enterprise Application Platform are priced based on the number of Cores running that Software, in a range called a Core Band. **"Red Hat Products"** refers collectively to the Software Subscriptions, Support Subscriptions and Management Subscriptions listed in Tables 1.4, 1.5 and 1.6. Note that Red Hat Products do not include generally available open source projects such as www.wildfly.org, www.jboss.org, www.fedoraproject.org, www.openstack.redhat.com, www.gluster.org, www.centos.org and/or other community projects.

Red Hat verkauft Subscriptions, die Sie zum Erhalt von Services und/oder Software von Red Hat während der Laufzeit der Subscription berechtigen (im Allgemeinen ein Jahr oder drei Jahre). In diesem Anhang des Bestellformulars werden die von Red Hat geleisteten **"SUBSCRIPTION SERVICES"** beschrieben:

- Bereitstellung von Software-Produkten (diese Subscriptions werden **„Software Subscriptions"** genannt);
- Support-Dienstleistungsangebote (diese Subscriptions werden **„SUPPORT SUBSCRIPTIONS"** genannt); und
- Angebote für Softwarebereitstellungs- und Management-Dienstleistungen (diese Subscriptions werden **„MANAGEMENT SUBSCRIPTIONS"** genannt).

Die diesem ANHANG beigefügten Exhibits enthalten zusätzliche Bedingungen, die die SUBSCRIPTION SERVICES betreffen. Wir verpflichten uns zur Erbringung der SUBSCRIPTION SERVICES zu den Bedingungen zu erbringen, die in diesem Anhang und in den in diesem Anhang referenzierten Exhibits und Dokumenten enthalten sind (zusammen der **„ANHANG"**), unabhängig davon ob Sie Subscription Services direkt von uns oder von einem unserer autorisierten Geschäftspartner erwerben. Im Gegenzug verpflichten Sie sich zur Einhaltung der in diesem VERTRAG, einschließlich des ANHANGS, aufgeführten Geschäftsbedingungen.

Mit Großbuchstaben geschriebene und in diesem Anhang nicht definierte Begriffe haben die ihnen in dem VERTRAG, zu dem dieser ANHANG gehört, wie etwa das Red Hat Enterprise Agreement, zugeordnete Bedeutung. Im Falle eines Widerspruchs, einer Unvereinbarkeit oder eines Unterschieds zwischen diesem Anhang und einem Exhibit dieses Anhangs sind die Bestimmungen des Exhibits ausschlaggebend.

1. SUBSCRIPTION SERVICES im Überblick

1.1 Einheiten einer Subscription: Wir erheben eine Gebühr für unsere SUBSCRIPTION SERVICES, die von der Gesamtanzahl der SOFTWAREEINHEITEN oder anderer RED HAT PRODUKTE abhängig ist, die Sie einsetzen, installieren, verwenden oder ausführen (wie es in den Tabellen 1,4, 1,5 und 1,6 unten und an anderen Stellen im ANHANG ausführlich beschrieben wird). Zum Beispiel werden SOFTWARE SUBSCRIPTIONS für Red Hat Enterprise Linux Server im Allgemeinen nach der Anzahl und anderen Charakteristika von SYSTEMEN, VIRTUAL NODES oder PHYSICAL NODES (z. B. Socket Pairs, VIRTUELLE GÄSTE, etc.) berechnet, auf denen Sie die SOFTWARE installieren oder benutzen, während SOFTWARE SUBSCRIPTIONS für Red Hat JBoss Enterprise Application Platform nach der Anzahl der CORES berechnet werden, auf denen die SOFTWARE läuft, wobei ein als CORE-BAND bezeichneter Rahmen maßgeblich ist. **"Red Hat Produkte"** bezeichnen gesammelt die Software Subscriptions, Support Subscriptions und Management Subscriptions, wie in Tabelle 1.4, 1.5 and 1.6 genannt. Bitte beachten Sie, dass Red Hat Produkte keine allgemein verfügbaren Open-Source-Projekte wie www.wildfly.org, www.jboss.org, www.fedoraproject.org, www.openstack.redhat.com, www.gluster.org, www.centos.org und andere Gemeinschaftsprojekte beinhalten.

1.2 **Use of Software and Subscription Services:** While you have subscriptions entitling you to receive Subscription Services for a Red Hat Product, you are required to purchase Subscription Services in a quantity equal to the total number of Units of that Red Hat Product (including variants or components thereof). In addition, if you are using Subscription Services to support or maintain a Red Hat Product and/or non-Red Hat Product, then you are required to purchase Subscription Services for each instance of such Red Hat Product and/or non-Red Hat Product for which you use Subscription Services. The Agreement (including pricing) is premised on our understanding that you will use the Subscription Services and Software only for your internal use (which includes Affiliates). You agree not to use Software Subscriptions with higher support service levels (e.g. Standard and/or Premium) to provide such higher support levels to Units with Subscriptions that include lower support levels (e.g. Self-support and/or Standard), unless you report and pay for the higher support service levels on such Units. You may migrate from one Unit of a given Software Subscription to another Unit with the same Subscription Services characteristics (such as from one on-premise System or Physical Node to another on-premise System or Physical Node) without the purchase of additional Software Subscriptions, provided that you do not increase the quantity of Units or other Software Subscription characteristics (such as the number of Socket-pairs, Virtual Guests or vCPUs). Distributing the Software or any portion of the Subscription Services to a third party or using any of the Subscription Services for the benefit of a third party is a material breach of the Agreement even though the open source licenses applicable to individual software packages may give you the right to distribute those packages (and this Appendix is not intended to interfere with your rights under those individual licenses). The foregoing sentence is not intended to limit your internal use of the Software to run a web site and/or to offer your own software as a service, provided such a web site or service (a) does not include a distribution of the Software or Subscription Services and (b) provides a material value added application or service other than the Software and/or Subscription Services. The Subscription Services may be used under the terms of this Appendix by third parties acting on your behalf, such as contractors, subcontractors or outsourcing vendors provided (i) you remain responsible for all of your obligations under the Agreement and this Appendix and for the activities and omissions of the third parties and (ii) you obtain Red Hat's written consent before you migrate your Software Subscriptions off of your premises and, in the case of a migration to a third party cloud or hosting provider, you are qualified for the Red Hat Cloud Access program and agree to the terms of Red Hat's Cloud Access program as set forth in Exhibit 1.J. Any unauthorized use of the Subscription Services is a material breach of the Agreement, such as (a) only purchasing or renewing Subscription Services based on some, but not all, of the total number of Units of Software or other Red Hat Products, (b) providing Software Access or Software Maintenance (each defined below) to third parties, (c) using Software Access, Software Maintenance, Production Support and/or Development Support (each defined below) to provide support to third parties, (d) using Subscription Services in connection with any redistribution of Software and/or (e) using Subscription Services to support or maintain any non-Red Hat Software products without purchasing Subscription Services for each instance of such non-Red Hat Product for which you use Subscription Services. For the purposes of this paragraph (for example, in calculating the total number of Units of Software), Software

1.2 **Nutzung von Software und Subscription Services:** Solange Sie Subscriptions haben, die Sie berechtigen, SUBSCRIPTION SERVICES für ein Red Hat Produkt zu erhalten, müssen Sie die Anzahl der SUBSCRIPTION SERVICES erwerben, die der Gesamtzahl der Einheiten des entsprechenden Red Hat Produktes (bzw. Abwandlungen oder Bestandteilen davon) entspricht. Wenn Sie SUBSCRIPTION SERVICES für den Support oder die Wartung eines Red Hat Produktes und/oder Fremdproduktes benutzen, müssen Sie außerdem SUBSCRIPTION SERVICES für jede Instanz eines derartigen Red Hat Produktes und/oder Fremdproduktes erwerben, für die Sie SUBSCRIPTION SERVICES verwenden. Der VERTRAG (einschließlich der Preisangaben) setzt Ihr Einverständnis voraus, dass Sie die SUBSCRIPTION SERVICES und SOFTWARE nur für Ihren internen Bedarf (dies schließt Ihre VERBUNDENEN UNTERNEHMEN ein) verwenden. Sie sind damit einverstanden, SOFTWARE SUBSCRIPTIONS nicht mit höheren Support Service Levels (z.B. Standard oder Premium) zu nutzen und diese höheren Support Service Levels nicht für EINHEITEN mit niedrigeren Support Levels (z.B.Self-Support und/oder Standard) einzusetzen, es sei denn, Sie reporten und bezahlen die höheren Support Service Levels für diese Units. Sie sind berechtigt, SOFTWARE SUBSCRIPTIONS von einer Einheit auf eine andere zu verschieben und die gleichen Merkmale weiterhin zu nutzen (wie von einem Vor-Ort-System oder Physical Node" auf ein anderes oder einen anderen „Physical Node") ohne zusätzliche SOFTWARE SUBSCRIPTIONS erwerben zu müssen, vorausgesetzt, dass Sie die Menge der Einheiten oder andere SOFTWARE SUBSCRIPTION-Merkmale (wie die Anzahl der Socket Pairs, virtuelle Gäste oder vCPUs) nicht erhöhen. Die Weitergabe der SOFTWARE oder irgendeines Teils der SUBSCRIPTION SERVICES an eine Drittpartei oder Verwendung eines Teils der SUBSCRIPTIONS SERVICES zu Nutzen einer Drittpartei ist ein erheblicher Vertragsbruch, trotz des Umstandes, dass die auf einzelne Software-Pakete zutreffenden quelloffenen Lizenzen Ihnen möglicherweise das Recht geben, diese Pakete weiter zu geben (und dieser ANHANG soll Ihre Rechte unter diesen individuellen Lizenzen nicht beeinflussen). Mit dem vorstehenden Satz wird nicht bezweckt, Ihre interne Nutzung der Software zu begrenzen, wenn Sie eine Website betreiben und/oder Ihrer eigene Software als Service anbieten, vorausgesetzt, dass eine solche Website oder ein solcher Service a) nicht die Verbreitung der SOFTWARE oder SUBSCRIPTIONS SERVICES einschließt und b) eine Anwendung oder Dienstleistung mit einem materiellen Mehrwert anbietet, die sich von der SOFTWARE und/oder den SUBSCRIPTION SERVICES unterscheidet. Die SUBSCRIPTION SERVICES können gemäß den Bedingungen in diesem ANHANG von einer in Ihrem Auftrag handelnden Drittpartei wie Auftragnehmer und Subunternehmer oder Outsourcing-Anbieter genutzt werden, vorausgesetzt dass Sie (i) für all Ihre eigenen Verpflichtungen gemäß dem VERTRAG und diesem ANHANG und die Handlungen oder Unterlassungen von diesen Drittparteien verantwortlich bleiben und (ii) eine schriftliche Einverständniserklärung von Red Hat dazu erhalten, dass Sie Ihre SOFTWARE SUBSCRIPTIONS außerhalb Ihres Standorts verlegen dürfen und, im Falle einer Migration zu einer externen Cloud oder einem externen Hosting-Anbieter, für das Red Hat Cloud Access Programm autorisiert sind und mit diesem Programm und den zugehörigen Bedingungen einverstanden sind, wie in EXHIBIT 1.J. dargelegt. Jeder unbefugte Gebrauch von SUBSCRIPTION SERVICES ist ein erheblicher

would include versions or copies that have the Red Hat trademark(s) and/or logo file(s) removed. The licenses that are applicable to the individual open source software packages are perpetual (subject to your compliance with their terms), but the other benefits of a Software Subscription will expire if not renewed.

Vertragsbruch, so zum Beispiel (a) der Ankauf oder die Verlängerung von SUBSCRIPTION SERVICES nur für einige, nicht aber für die Gesamtzahl der EINHEITEN an SOFTWARE oder anderer Red Hat PRODUKTE, (b) Bereitstellung von SOFTWAREZUGANG oder SOFTWAREWARTUNG (jeweils im Folgenden definiert) an Drittparteien, (c) Gebrauch von SOFTWAREZUGANG, SOFTWAREWARTUNG, PRODUCTION SUPPORT und/oder ENTWICKLUNGS-SUPPORT (jeweils im Folgenden definiert) zur Bereitstellung von Support für Drittparteien, (d) Gebrauch von SUBSCRIPTION SERVICES in Verbindung mit einer Neudistribution von Software, und/oder (e) Gebrauch von SUBSCRIPTION SERVICES für Support oder Wartung von Red Hat-fremden Software Produkten ohne den Erwerb von SUBSCRIPTION SERVICES für jegliche Red Hat-fremde Produkte, für die Sie die SUBSCRIPTION SERVICES nutzen. Im Sinne dieses Abschnitts (z. B. zur Berechnung der Gesamtzahl der SOFTWARE-EINHEITEN) gelten auch Versionen oder Kopien als SOFTWARE, von denen das/die Red Hat-Markenzeichen und/oder -Logo(s) entfernt wurden. Die für die einzelnen quelloffenen Software-Pakete geltenden Lizenzen gelten unbefristet (unter der Bedingung, dass Sie deren Bedingungen zustimmen), die anderen Leistungen der SOFTWARE SUBSCRIPTION verfallen jedoch bei Nichtverlängerung.

1.3 **Subscription Start Date:** Unless otherwise agreed in an Order Form, the Subscription Services will begin on the date you purchase the Subscription Services (please note that the foregoing does not limit your obligation to pay for Subscription Services that you previously used but for which you have not paid).

1.3 **Anfangsdatum der SUBSCRIPTION:** Die SUBSCRIPTION SERVICES beginnen am Tag; an dem Sie diese erwerben, es sei denn im Bestellformular wurden andere Vereinbarungen getroffen (bitte beachten Sie, dass das Vorstehende Ihre Verpflichtung zur Zahlung für SUBSCRIPTION SERVICES, die Sie zuvor genutzt, für die Sie aber nicht bezahlt haben, in keiner Weise einschränkt).

1.4 Software Subscriptions

Benefits of a Software Subscription: For each Software Subscription that you purchase, Red Hat provides you one or more of the following benefits:

- **Software Access:** Access to the Software.
- **Software Maintenance:** Access to updates, upgrades, corrections, security advisories and bug fixes for the Software, if and when available.
- **Support:** Access to Red Hat support for issues relating to Software used for Development Purposes and/or Production Purposes (each of which is defined below).
- **Open Source Assurance:** Purchases under this Appendix for Software Subscriptions may entitle you to participate in Red Hat's Open Source Assurance Program subject to a separate agreement, which can be viewed at www.redhat.com/legal/open_source_assurance_agreement.html.

1.4 SOFTWARE SUBSCRIPTIONS

Leistungen bei einer SOFTWARE SUBSCRIPTION: Für jede von Ihnen erworbene SOFTWARE SUBSCRIPTION stellt Ihnen Red Hat eine oder mehrere der folgenden Leistungen zur Verfügung:

- **SOFTWAREZUGANG:** ZUGANG zur SOFTWARE.
- **SOFTWAREWARTUNG:** Zugriff auf Updates, Upgrades, Korrekturen, Sicherheitshinweise und Fehlerbehebungen für die SOFTWARE, sobald und soweit diese verfügbar sind.
- **SUPPORT:** Zugang zum Red Hat Support für Probleme, die mit SOFTWARE zu tun haben, die zu ENTWICKLUNGS- und/oder PRODUKTIONSZWECKEN (jeweils im Folgenden definiert) verwendet wird.
- **Open Source Assurance:** Der Erwerb von Red Hat SUBSCRIPTIONS kann Sie zur Teilnahme an Red Hat's Open Source Assurance Program berechtigen, das einem separatem Vertrag unterliegt, der unter www.redhat.com/legal/open_source_assurance_agreement.html eingesehen werden kann.

Descriptions of Red Hat Software Subscriptions: Table 1.4 below lists the Software Subscriptions offered by Red Hat, the Unit descriptions that are used to measure your use of each Software Subscription. The End User License Agreement(s) that governs your use of the Software is/are located at www.redhat.com/licenses/EULAs (note that for certain Red Hat Products multiple EULAs will apply). The Exhibits listed in Table 1.4 contain additional information concerning the scope of the Software Subscriptions and how Red Hat provides Subscription Services to you.

Beschreibung von Red Hat SOFTWARE SUBSCRIPTIONS: Tabelle 1.4 führt die von Red Hat angebotenen SOFTWARE SUBSCRIPTIONS auf und beschreibt die zur Berechnung Ihrer Nutzung der SOFTWARE SUBSCRIPTIONS verwendeten EINHEITEN. Das/Die End User License Agreement(s), welche(s) Ihre Nutzung der Software regelt/regeln, findet sich unter www.redhat.com/licenses/EULAs (beachten Sie, dass bei bestimmten Red Hat Produkten mehrere EULAs gelten). Die Exhibits in Tabelle 1.4 enthalten zusätzliche Informationen über den Umfang der SOFTWARE SUBSCRIPTIONS und die Art und Weise,

wie Red Hat Ihnen SUBSCRIPTION SERVICES liefert.

Table 1.4

Software Subscription	Unit Description (used to measure your use of Software Subscriptions)	Exhibit Containing Additional Terms
Red Hat Enterprise Linux Server (Physical or Virtual Nodes) Red Hat Enterprise Linux for SAP HANA	**Physical Node:** a physical system on which you install or execute all or a portion of the Software including, without limitation, a server, work station, laptop, blade or other physical system, as applicable: OR **Virtual Node:** an instance of the Software executed, in whole or in part, on a virtual machine.	1.A
Red Hat Enterprise Linux for Virtual Datacenters	**Physical Node:** a physical system on which you install or execute all or a portion of the Software including, without limitation, a server, work station, laptop, blade or other physical system, as applicable.	1.A
Red Hat Enterprise Linux Server Entry Level	**Physical Node:** a physical system on which you install or execute all or a portion of the Software including, without limitation, a server, work station, laptop, blade or other physical system, as applicable.	1.A
Red Hat Enterprise Linux Server Red Hat Enterprise Linux for HPC Compute Nodes Red Hat Enterprise Linux for HPC Head Nodes Red Hat Enterprise Linux for Grid Node Red Hat Enterprise Linux for IBM POWER Red Hat Enterprise Linux for PRIMEQUEST Red Hat Enterprise Linux for SAP Applications Red Hat Enterprise Linux Server Add-Ons: High Availability Load Balancer Resilient Storage Scalable File System Smart Management Extended Update Support Extended Life Cycle Support High Performance Network	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable; or **vCPU:** a a physical CPU, in whole or in part, which is assigned to a virtual machine on which you install or execute all or a portion of the Software. **Note:** Additional terms regarding virtualization, disaster recovery, academic offerings and supported use cases, which may affect the types or quantities of Software Subscription you purchase, are contained in Exhibit 1.A.	1.A
Red Hat MRG Real-time Red Hat Enterprise Linux Desktop Red Hat Enterprise Linux Workstation	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	1.A
Red Hat Enterprise Linux for IBM System z	**IFL:** an IFL, or an Integrated Facility for Linux, is a mainframe CPU dedicated to Linux workloads.	1.A
Red Hat Enterprise Virtualization	**Physical Node:** a physical system on which you install or execute all or a portion of the Software including, without limitation, a server, work station, laptop, blade or other physical system, as applicable.	1.A
Red Hat Enterprise Linux with Smart Virtualization	**Physical Node:** a physical system on which you install or execute all or a portion of the Software, including, without limitation, a server, work station, laptop, blade, or other physical system, as applicable.	1.A

Software Subscription	Unit Description (used to measure your use of Software Subscriptions)	Exhibit Containing Additional Terms
Red Hat Enterprise Linux Academic Server Red Hat Enterprise Linux Academic Desktop Red Hat Enterprise Linux Academic Workstation	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	1.A
Red Hat Enterprise Linux Academic Site Subscription	**Full Time Equivalent or FTE:** the total number of (a) full time faculty, (b) one third of the part time faculty, (c) the full time staff and (d) one half of the part time staff.	1.A
Red Hat Infrastructure for Academic Institutions - Site Subscription	**Full Time Equivalent or FTE:** the total number of (a) full time faculty, (b) one third of the part time faculty, (c) the full time staff and (d) one half of the part time staff.	1.A
Red Hat Enterprise Linux Developer Suite	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	1.C
Red Hat JBoss Enterprise Application Platform Red Hat JBoss Web Server Red Hat JBoss Web Server Plus Red Hat JBoss Fuse Service Works Red Hat JBoss Data Virtualization Red Hat JBoss Fuse Red Hat JBoss A-MQ Red Hat JBoss Portal Red Hat JBoss BPM Suite Red Hat JBoss BRMS plus BPM Suite Red Hat JBoss BRMS Red Hat JBoss Data Grid Red Hat JBoss Middleware add-on option: Management Extended Life Cycle Support	**Core Band:** a group of processing cores (16 or 64), where a single "**Core**" is (a) a physical processing core located in a CPU or (b) a virtual processing core within a virtual machine, in each case, that contains or executes the Software running for Production Purposes.	1.B
Red Hat JBoss Developer Studio	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	1.C
Red Hat Storage Server for On-premise	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	1.D
Red Hat Storage Server for Public Cloud	**Virtual Guest:** an instance of the Software that is executed, in whole or in part, on a virtual machine.	1.D, 1.J

Software Subscription	Unit Description (used to measure your use of Software Subscriptions)	Exhibit Containing Additional Terms
Red Hat Storage Server for Hybrid Cloud	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable; and **Virtual Guest:** an instance of the Software that is executed, in whole or in part, on a virtual machine.	1.D, 1.J
Red Hat Storage for Red Hat Enterprise Linux OpenStack Platform	**Physical Node:** a physical system on which you install or execute all or a portion of the Software, including, without limitation, a server, work station, laptop, blade, or other physical system, as applicable.	1.A, 1.D
OpenShift Enterprise OpenShift Enterprise Broker Infrastructure Red Hat JBoss Middleware for OpenShift Enterprise	**Physical Node:** a physical system on which you install or execute all or a portion of the Software including, without limitation, a server, work station, laptop, blade or other physical system, as applicable. **Virtual Guest:** an instance of the Software that is executed, in whole or in part, on a virtual machine.	1.B, 1.K
Red Hat Cloud Infrastructure	**Physical Node:** a physical system on which you install or execute all or a portion of the Software including, without limitation, a server, work station, laptop, blade or other physical system, as applicable.	1.E, 1.I
Red Hat Enterprise Linux OpenStack Platform	**Physical Node:** a physical system on which you install or execute all or a portion of the Software, including, without limitation, a server, work station, laptop, blade, or other physical system, as applicable.	1.A, 1.F

Tabelle 1.4

SOFTWARE SUBSCRIPTIONS	Beschreibung der EINHEITEN (verwendet zur Berechnung Ihrer Nutzung der SOFTWARE SUBSCRIPTIONS)	Exhibit mit zusätzlichen Bedingungen
Red Hat Enterprise Linux Server (PHYSICAL oder VIRTUAL NODES) Red Hat Enterprise Linux for SAP HANA	**Physical Node:** ein physikalisches System, auf dem man die gesamte oder einen Teil der Software installiert oder einsetzt, einschließlich unter anderem ein Server,eine Workstation, ein Laptop, ein Blade oder ein sonstiges physikalisches System: ODER **Virtual Node:** eine Instanz der SOFTWARE die ganz oder teilweise auf einer virtuellen Maschine ausgeführt wird.	1.A
Red Hat Enterprise Linux für virtuelle Datenzentren	**Physical Node:** ein physikalisches System, auf dem man die gesamte oder einen Teil der Software installiert oder einsetzt, einschließlich unter anderem ein Server, eine Workstation, ein Laptop, ein Blade oder ein sonstiges physikalisches System.	1.A
Red Hat Enterprise Linux Server Entry Level	**Physical Node:** ein physikalisches System, auf dem man die gesamte oder einen Teil der Software installiert oder einsetzt, einschließlich unter anderem ein Server, eine Workstation, ein Laptop, ein Blade oder ein sonstiges physikalisches System.	1.A
Red Hat Enterprise Linux Server Red Hat Enterprise Linux für HPC Netzwerkelemente Red Hat Enterprise Linux für HPC Head Netzwerkelemente Red Hat Enterprise Linux für Grid Node Red Hat Enterprise Linux für IBM POWER Red Hat Enterprise Linux for PRIMEQUEST Red Hat Enterprise Linux für SAP	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird oder **vCPU:** eine physikalische CPU, ganz oder teilweise, die einer virtuellen Maschine zugewiesen ist, auf der Sie alle oder einen Teil der Software installieren oder einsetzen. **Modul:** eine Berechtigung für Smart Management, ein System, Virtual Node oder Physical Node zu managen.	1.A

SOFTWARE SUBSCRIPTIONS	Beschreibung der EINHEITEN (verwendet zur Berechnung Ihrer Nutzung der SOFTWARE SUBSCRIPTIONS)	Exhibit mit zusätzlichen Bedingungen
Applications Red Hat Enterprise Linux Server Add-Ons: Hohe Verfügbarkeit Lastverteiler Ausfallsicherer Speicher Skalierbares Dateisystem Smart Management Extended Update Support Extended Life Cycle Support Hochleistungsnetzwerk	**Hinweis:** Weitere Begriffe, wie Virtualisierung, Disaster Recovery, akademische Angebote und unterstützte Anwendungsfälle, die die Art oder Menge der von Ihnen erworbenen Software Subscription betreffen, sind Exhibit 1.A zu entnehmen.	
Red Hat MRG Real-time Red Hat Enterprise Linux Desktop Red Hat Enterprise Linux Workstation	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.A
Red Hat Enterprise Linux für IBM System z	**IFL:** Eine IFL, oder Integrated Facility for Linux, ist eine für Linux-Arbeitsprozesse bestimmte Mainframe-CPU.	1.A
Red Hat Enterprise Virtualisierung	**Physical Node:** ein physikalisches System, auf dem man die gesamte oder einen Teil der Software installiert oder einsetzt, einschließlich unter anderem Server, Workstation, Laptop, Blade oder ein sonstiges physikalisches System.	1.A
Red Hat Enterprise Linux with Smart Virtualization	**Physical Node:** ein physikalisches System, auf dem man die gesamte oder einen Teil der Software installiert oder einsetzt, einschließlich unter anderem Server, Workstation, Laptop, Blade oder ein sonstiges physikalisches System.	1.A
Red Hat Enterprise Linux Academic Server Red Hat Enterprise Linux Academic Desktop Red Hat Enterprise Linux Academic Workstation	**System:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.A
Red Hat Enterprise Linux Academic Site Subscription	**Full Time Equivalent oder FTE:** die vollständige Anzahl (a) der Vollzeit Fakultät, (b) von einem Drittel der Teilzeit Fakultät, (c) der Vollzeit-mitarbeiter und (d) von einem Drittel der Teilzeitmitarbeiter.	1.A
Red Hat Infrastructure for Academic Institutions - Site Subscription	**Full Time Equivalent oder FTE:** die vollständige Anzahl (a) der Vollzeit Fakultät, (b) von einem Drittel der Teilzeit Fakultät, (c) der Vollzeit-mitarbeiter und (d) von einem Drittel der Teilzeitmitarbeiter.	1.A
Red Hat Enterprise Linux Developer Suite	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.C

SOFTWARE SUBSCRIPTIONS	Beschreibung der EINHEITEN (verwendet zur Berechnung Ihrer Nutzung der SOFTWARE SUBSCRIPTIONS)	Exhibit mit zusätzlichen Bedingungen
Red Hat JBoss Application Platform Red Hat JBoss Web Server Red Hat JBoss Web Server Plus Red Hat JBoss Fuse Service Works Red Hat JBoss Datenvirtualisierung Red Hat JBoss Fuse Red Hat JBoss A-MQ Red Hat JBoss Portal Red Hat JBoss BPM Suite Red Hat JBoss BRMS plus BPM Suite Red Hat JBoss BRMS Red Hat JBoss Data Grid Red Hat JBoss Middleware Add-on Option: Management Extended Life Cycle Support	**CORE-Band:** eine Gruppe von Prozessorkernen (16 oder 64), bei denen ein einzelner „**Core**" (a) ein physikalischer Prozessorkern ist, der sich in einer CPU befindet, bzw. (b) ein virtueller Prozessorkern in einer virtuellen Maschine ist, und der in beiden Fällen die für die PRODUKTIONSZWECKE eingesetzte SOFTWARE enthält oder ausführt.	1.B
Red Hat JBoss Developer Studio	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.C
Red Hat Storage Server für den Einsatz am Standort	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.D
Red Hat Storage Server für Public Cloud	**Virtual Guest:** eine Instanz der SOFTWARE, die ganz oder teilweise auf einer virtuellen Maschine ausgeführt wird.	1.D, 1.J
Red Hat Storage für eine Hybrid Cloud	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird; und **Virtual Guest:** eine Instanz der SOFTWARE, die ganz oder teilweise auf einer virtuellen Maschine ausgeführt wird.	1.D, 1.J
Red Hat Storage for Red Hat Enterprise Linux OpenStack Platform	**Physical Node:** ein physikalisches System, auf dem man die gesamte oder einen Teil der Software installiert oder einsetzt, einschließlich unter anderem ein Server, eine Workstation, ein Laptop, ein Blade oder ein	1.A, 1.D

SOFTWARE SUBSCRIPTIONS	Beschreibung der EINHEITEN (verwendet zur Berechnung Ihrer Nutzung der SOFTWARE SUBSCRIPTIONS)	Exhibit mit zusätzlichen Bedingungen
	sonstiges physikalisches System.	
OpenShift Enterprise OpenShift Enterprise Broker Infrastructure Red Hat JBoss Middleware für OpenShift Enterprise	**Physical Node:** ein physikalisches System, auf dem man die gesamte oder einen Teil der Software installiert oder einsetzt, einschließlich unter anderem Server, Workstation, Laptop, Blade oder ein sonstiges physikalisches System. **Virtual Guest:** eine Instanz der SOFTWARE, die ganz oder teilweise auf einer virtuellen Maschine ausgeführt wird.	1.B, 1.K
Red Hat Cloud Infrastructure	**Physical Node:** ein physikalisches System, auf dem man die gesamte oder einen Teil der Software installiert oder einsetzt, einschließlich unter anderem Server, Workstation, Laptop, Blade oder ein sonstiges physikalisches System.	1.E, 1.I
Red Hat Enterprise Linux OpenStack Platform	**Physikalischer Knoten:** ein physikalisches System, auf dem man die gesamte oder einen Teil der Software installiert oder einsetzt, einschließlich unter anderem Server, Workstation, Laptop, Blade oder ein sonstiges physikalisches System.	1.A, 1.F

1.5 Support Subscriptions. Table 1.5 below lists the Support Subscriptions offered by Red Hat and the Unit description that is used to measure your use of the Support Subscription(s). The End User License Agreement that governs your use of the Software is located at www.redhat.com/licenses/EULAs. The Exhibits listed in Table 1.5 contain additional information concerning the scope of the Support Subscriptions and how Red Hat provides Subscription Services to you.

1.5 SUPPORT SUBSCRIPTIONS. In Tabelle 1.5 unten werden die SUPPORT SUBSCRIPTIONS, die von Red Hat angeboten werden, sowie eine Beschreibung der EINHEIT aufgelistet, die verwendet wird, um Ihre Nutzung der SUPPORT SUBSCRIPTION(S) zu messen. Das End User License Agreement, in dem der Gebrauch der Software geregelt wird, befindet sich unter www.redhat.com/licenses/EULAs. Die Exhibits in Tabelle 1.5 enthalten zusätzliche Informationen über den Umfang der SUPPORT SUBSCRIPTIONS und die Art und Weise wie Red Hat Ihnen SUBSCRIPTION SERVICES liefert.

Table 1.5

Support Subscription	Unit Description (used to measure your use of Support Subscriptions)	Exhibit Containing Additional Terms
Technical Account Management ("TAM") Service TAM Extension	**Point of Contact:** a Red Hat associate whom you are authorized to contact to request support for a particular team, geography or Red Hat product line.	1.G
Extended Update Support	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	1.G
Red Hat Enterprise Linux Extended Life Cycle Support	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	1.G
Red Hat JBoss Middleware Extended Life Cycle Support	**Core Band:** a group of processing cores (16 or 64), where a single "**Core**" is (a) a physical processing core located in a CPU or (b) a virtual processing core within a virtual machine, in each case, that contains or executes the Software running for Production Purposes.	1.G
Red Hat Enterprise Linux Developer Workstation	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	1.G
Red Hat Enterprise Linux Developer	**System:** a system on which you install or execute all or a portion of the	1.G

Support Subscription	Unit Description (used to measure your use of Support Subscriptions)	Exhibit Containing Additional Terms
Support	Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	

Tabelle 1.6

SUPPORT SUBSCRIPTIONS	Beschreibung der EINHEITEN (verwendet zur Berechnung Ihrer Nutzung der SUPPORT SUBSCRIPTIONS)	Exhibit mit zusätzlichen Bedingungen
Technical Account Management ("**TAM**") Service TAM Erweiterung	**KONTAKTPUNKT:** ein(e) Red Hat Mitarbeiter(in), den (die) Sie bei Supportanfragen für ein bestimmtes Team, einen geografischen Bereich oder eine Produktlinie von Red Hat kontaktieren können.	1.G
Extended Update Support	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.G
Red Hat Enterprise Linux Extended Life Cycle Support	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.G
Red Hat JBoss Middleware Extended Life Cycle Support	**CORE-Band:** eine Gruppe von Prozessorkernen (16 oder 64), bei denen ein einzelner „**Core**" (a) ein physikalischer Prozessorkern ist, der sich in einer CPU befindet, bzw. (b) ein virtueller Prozessorkern in einer virtuellen Maschine ist, und der in beiden Fällen die für die PRODUKTIONSZWECKE eingesetzte SOFTWARE enthält oder ausführt.	1.G
Red Hat Enterprise Linux Workstation	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.G
Red Hat Enterprise Linux Developer Support	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.G

1.6 **Management Subscriptions.** Table 1.6 below lists the Management Subscriptions offered by Red Hat and the Unit description that is used to measure your use of the Management Subscription(s). The End User License Agreement that governs your use of the Software is located at www.redhat.com/licenses/EULAs. The Exhibits listed in Table 1.6 contain additional information concerning the scope of the Management Subscriptions and how Red Hat provides Subscription Services to you.

1.6 **Management Subscriptions.** Tabelle 1.6 führt die von Red Hat angebotenen MANAGEMENT SUBSCRIPTIONS auf und beschreibt die zur Berechnung Ihrer Nutzung der MANAGEMENT SUBSCRIPTION(S) verwendeten EINHEITEN. Das End User License Agreement, in dem der Gebrauch der Software geregelt wird, befindet sich unter www.redhat.com/licenses/EULAs. Zum Verständnis Ihrer Rechte und Verpflichtungen ist es wichtig, dass Sie die Informationen in den Links in Tabelle 1.6 eingehend studieren. Die Exhibits in Tabelle 1.6 enthalten zusätzliche Informationen über den Umfang der MANAGEMENT SUBSCRIPTIONS und die Art und Weise, wie Red Hat Ihnen SUBSCRIPTION SERVICES liefert.

Table 1.6

Management Subscription	Unit Description (used to measure your use of Management Subscriptions) and End User License Terms	Exhibit Containing Additional Terms
Red Hat Satellite Server Red Hat Satellite Server Starter Pack	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable. If you install or use the optional embedded database, then you agree to comply with the terms located at www.redhat.com/licenses/satellite_embedded.html for the embedded database.	1.H
Red Hat Satellite Proxy	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	1.H
Red Hat Smart Management	**Module:** an entitlement to monitor one System, Virtual Node or Physical Node.	1.H
Red Hat Monitoring Module	**Module:** an entitlement to monitor one System, Virtual Node or Physical Node.	1.H
Red Hat JBoss Operations Network	**Core Band:** a group of processing cores (16 or 64), where a single "**Core**" is (a) a physical processing core located in a CPU or (b) a virtual processing core within a virtual machine, in each case, that contains or executes the Software running for Production Purposes.	1.H
Red Hat Directory Server	**System:** a system on which you install or execute all or a portion of the Software. A System includes each instance of the Software installed or executed on, without limitation, a server, work station, laptop, virtual machine, blade, node, partition, appliance or engine, as applicable.	1.H
Red Hat CloudForms (and its predecessor ManageIQ EVM Suite)	**Managed Node:** a server, blade or node managed by the Software.	1.I
Red Hat CloudForms for Public Cloud (and its predecessor ManageIQ EVM for Public Cloud)	**Managed VM:** a virtual machine on a public cloud managed by the Software.	1.I

Tabelle 1.6

MANAGEMENT SUBSCRIPTION	Beschreibung der EINHEITEN (verwendet zur Berechnung Ihrer Nutzung der MANAGEMENT SUBSCRIPTION) und End User License Bedingungen	Exhibit mit zusätzlichen Bedingungen
Red Hat Satellite Server Red Hat Satellite Server Starter Pack	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird. Wenn Sie die optional eingebettete Datenbank installieren oder nutzen, verpflichten Sie sich zur Einhaltung der Bedingungen für die eingebettete Datenbank, die unter www.redhat.com/licenses/satellite_embedded.html einsehbar sind.	1.H

MANAGEMENT SUBSCRIPTION	Beschreibung der EINHEITEN (verwendet zur Berechnung Ihrer Nutzung der MANAGEMENT SUBSCRIPTION) und End User License Bedingungen	Exhibit mit zusätzlichen Bedingungen
Red Hat Satellite Proxy	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.H
Red Hat Smart Management	**Modul:** eine Berechtigung zur Überwachung eines SYSTEMS, eines virtual Nodes oder eines physcal Nodes.	1.H
Red Hat Monitoring Module	**Modul:** eine Berechtigung zur Überwachung eines SYSTEMS, eines virtual Nodes oder eines physcal Nodes..	1.H
Red Hat JBoss Operations Network	**CORE-Band:** eine Gruppe von Prozessorkernen (16 oder 64), bei denen ein einzelner „**Core**"(a) ein physikalischer Prozessorkern ist, der sich in einer CPU befindet, bzw. (b) ein virtueller Prozessorkern in einer virtuellen Maschine ist, und der in beiden Fällen die für die PRODUKTIONSZWECKE eingesetzte SOFTWARE enthält oder ausführt.	1.H
Red Hat Directory Server	**SYSTEM:** ein SYSTEM, auf dem Sie die SOFTWARE teilweise oder insgesamt installieren oder einsetzen. Ein SYSTEM beinhaltet uneingeschränkt jede Instanz der SOFTWARE, die auf einem Server, einer Workstation, einem Laptop, einer virtuellen Maschine, Blade, Netzwerkelement, Partition, Gerät oder Maschine installiert oder eingesetzt wird.	1.H
Red Hat CloudForms (und sein Vorgänger ManageIQ EVM Suite)	**Managed Node:** Server, Blade oder Node, der von der Software verwaltet wird.	1.I
Red Hat CloudForms für Public Cloud (und sein Vorgänger ManageIQ EVM für Public Cloud)	**Verwaltete VM:** eine virtuelle Maschine auf einer öffentlichen Cloud, die von der Software verwaltet wird.	1.I

1.7 **Software Subscription Lifecycle.** During the life cycle of Red Hat Software, the scope of Software Maintenance and Support evolves and, after a number of years, we discontinue Software Maintenance and Support for older versions of Software. The details of the Software Maintenance and Production Support life cycle are set forth at https://access.redhat.com/support/policy/update_policies.html. If available, you may purchase Extended Update Support and/or Extended Life Cycle Support, as described in Exhibit 1.G, to extend your Subscription Services for certain versions of Software.

1.7 **Software Subscription Lifecycle.** Im Laufe des Lebenszyklus von Red Hat SOFTWARE verändert sich der Umfang der/des von uns geleisteten SOFTWAREWARTUNG und SUPPORTS, und nach einigen Jahren stellen wir die SOFTWAREWARTUNG und den SUPPORT für ältere Versionen der SOFTWARE ein. Die Einzelheiten für den Lebenszyklus von Software-Wartung und Production Support sind unter https://access.redhat.com/support/policy/update_policies.html zu finden. Falls verfügbar, können Sie einen Extended Update Support und/oder Extended Life Cycle Support erwerben, wie sie in Exhibit 1.G beschrieben sind, um Ihre SUBSCRIPTION SERVICES für bestimmte Softwareversionen zu verlängern.

2. Production Support and Development Support Terms

2.1 Definitions. **"Development Purposes"** means using the Software for the specific purpose of (a) developing, (b) single-user prototyping, quality assurance or testing and/or (c) demonstrating software or hardware that runs with or on the Software. **"Production Purposes"** means using the Software (a) in a production environment, (b) generally using live data and/or applications for a purpose other than Development Purposes, (c) for multi-user prototyping, quality assurance and testing and/or (d) for backup instances. **"Supported Hardware"** means the hardware and platforms that are listed at (i) https://hardware.redhat.com and http://www.redhat.com/resourcelibrary/articles/enterprise-linux-virtualization-support for Red Hat Enterprise Linux and Red Hat Enterprise Virtualization subscriptions, (ii) http://www.jboss.com/products/platforms/application/supportedconfigurations/ for Red Hat JBoss Middleware subscriptions, and (iii) https://access.redhat.com/knowledge/articles/66206 for Red Hat Storage Server. **"Evaluation Subscriptions"** are Subscription Services provided for the sole purpose of evaluating the suitability of the Subscription Services for your future purchase from Red Hat or through one of our authorized Business Partners, and not for Production Purposes, Development Purposes or any other purpose (**"Evaluation Purposes"**). **"Support Contact(s)"** is a person authorized by you to open support requests and/or contact Red Hat support personnel.

2.2 Use Cases. Subscription Services are provided for Software only when used for its supported purpose (**"Use Case"**). The Use Case determines which Subscription is required and what fees are charged. If you use or deploy the Software in a manner contrary to a supported Use Case, you are responsible for purchasing the appropriate Subscription(s) to cover such usage. For example, if you are using a Red Hat Enterprise Linux Desktop Subscription as a server, you are obligated to purchase a Red Hat Enterprise Linux Server Subscription.

2.3 Evaluations. By requesting an Evaluation Subscription, you represent that you will be using the Subscription Services for Evaluation Purposes only and you understand that Red Hat is relying on the accuracy of your representation in providing you with access to the Evaluation Subscription(s). If you use the Red Hat Evaluation Subscription(s) for any other purposes, you are in violation of this Agreement and are required to pay the applicable subscription fees in accordance with Sections 1.1 and 1.2 above, in addition to any and all other remedies available to Red Hat under applicable law. Examples of such violations include, but are not limited to, using the Subscription Services provided under an Evaluation Subscription for Production Purposes, offering support services to third parties, or complementing or supplementing third party support services with Subscription Services received through an Evaluation Subscription.

2. PRODUKTIONSSUPPORT und ENTWICKLUNGS-SUPPORT Bedingungen

2.1 Definitionen. **"ENTWICKLUNGSZWECKE"** bedeutet die Anwendung der SOFTWARE für den bestimmten Zweck (a) der Entwicklung, b) der Erstellung von Einzelbenutzer-Prototypen, der Qualitätssicherung oder der Prüfung und c) der Vorstellung von Software oder Hardware, die mit oder auf der SOFTWARE ausgeführt wird. **"PRODUKTIONSZWECKE"** bedeutet die Anwendung der SOFTWARE (a) in einer Produktionsumgebung, (b) unter dem generellen Einsatz von Livedaten und/oder Anwendungen zu anderen als Entwicklungszwecken, (c) für die Erstellung von Mehrbenutzer-Prototypen, der Qualitätssicherung oder Prüfung und/oder (d) für Backup-Instanzen. **"UNTERSTÜTZTE HARDWARE"** bedeutet die Hardware und Plattformen, aufgelistet auf (i) https://hardware.redhat.com und http://www.redhat.com/resourcelibrary/articles/enterprise-linux-virtualization-support für Red Hat Enterprise Linux und Red Hat Enterprise Virtualization Subscriptions, (ii) http://www.jboss.com/products/platforms/application/supportedconfigurations/ für Red Hat JBoss Middleware Subscriptions, und (iii) https://access.redhat.com/knowledge/articles/66206 für Red Hat Storage Server. **"EVALUATION SUBSCRIPTIONS"** sind SUBSCRIPTION SERVICES, deren alleiniger Zweck die Eignungsbewertung der SUBSCRIPTION SERVICES für Ihren zukünftigen Einkauf bei Red Hat oder bei einem unserer autorisierten Business Partner ist und die keinen PRODUKTIONS- oder ENTWICKLUNGSZWECKEN oder anderen Zwecken dient (**"EVALUIERUNGSZWECKE"**). **"SUPPORT-KONTAKT(E)"** ist eine Person, die von Ihnen ermächtigt wurde, für Sie Support-Anfragen zu stellen und/oder das Support-Personal von Red Hat zu kontaktieren.

2.2 ANWENDUNGSFÄLLE SUBSCRIPTION SERVICES werden nur für SOFTWARE geleistet, die für ihren unterstützten Anwendungszweck eingesetzt wird. (**"ANWENDUNGSFÄLLE"**). Der ANWENDUNGSFALL legt fest, welche SUBSCRIPTION erforderlich ist und welche Gebühren erhoben werden. Wenn Sie die SOFTWARE auf eine Weise verwenden, die nicht dem unterstützten ANWENDUNGSFALL entspricht, sind Sie dafür verantwortlich, die entsprechenden SUBSCRIPTION(S) zu erwerben, die eine solche Anwendung abdecken. Wenn Sie zum Beispiel eine Red Hat Enterprise Linux Desktop SUBSCRIPTION als Server verwenden, müssen Sie eine Red Hat Enterprise Linux Server SUBSCRIPTION dazu erwerben.

2.3 EVALUIERUNGEN. Wenn Sie eine EVALUATION SUBSCRIPTION anfordern, erklären Sie, dass Sie die SUBSCRIPTION SERVICES ausschließlich für EVALUIERUNGSZWECKE benutzen, und Sie verstehen, dass Red Hat sich auf die Genauigkeit Ihrer Darstellung verläßt, wenn es Ihnen den Zugang zu der (den) EVALUATION SUBSCRIPTION(S) gibt. Wenn Sie Red Hat EVALUATION SUBSCRITION(S(zu anderen Zwecken verwenden, verletzen Sie diesen VERTRAG und müssen die gültigen Subskriptionsgebühren gemäß Abschnitten 1.1. und 1.2. oben entrichten, und zwar unbeschadet aller übrigen Rechte , die Red Hat nach geltendem Recht zustehen. Beispiele solcher Verletzungen sind u.a. die Verwendung von als EVALUATION SUBSCRITION gewährten SUBSCRIPTION SERVICES zu PRODUKTIONSZWECKEN, das Anbieten von Supportdiensten an Dritte oder Ergänzungen oder Erweiterungen von Supportdiensten an Dritte durch SUBSCRIPTION SERVICES, die als

EVALUATION SERVICES gewährt werden.

2.4 **Support from Business Partner.** Some clients obtain support for their Software Subscriptions from an authorized Red Hat Business Partner, in which case the Business Partner provides the support to the client rather than Red Hat. Sections - 2.8 apply to you only if you have purchased Subscription Services with Production Support provided by Red Hat. If you have purchased Subscription Services with support provided by a Business Partner, Sections 2.5 – 2.8 do not apply to you and you should work with your Business Partner to obtain support services.

2.4 **Support von GESCHÄFTSPARTNERN.** Einige Kunden erhalten für ihre SOFTWARE SUBSCRIPTIONS Support von einem autorisierten GESCHÄFTSPARTNER von Red Hat. In diesem Fall ist nicht Red Hat, sondern der Geschäftspartner für den Support zuständig. Abschnitte 2.5 bis 2.8 sind für Sie nur relevant, wenn Sie die SUBSCRIPTION SERVICES mit PRODUCTION SUPPORT von Red Hat erworben haben. Falls Sie SUBSCRIPTION SERVICES erworben haben und SUPPORT von einem GESCHÄFTSPARTNER geleistet wird, sind Abschnitte 2.5 bis 2.8 für Sie nicht relevant und Sie sollten sich für SUPPORT SERVICES an den GESCHÄFTSPARTNER wenden.

2.5 **Support from Red Hat. "Development Support"** consists of assistance with installation, usage, problem diagnosis and bug fixes for the applicable Software used for Development Purposes during specific Red Hat life cycle phases (as referenced in Section 1.7 above). Development Support also consists of advice on architecture, design, development and prototyping. Requests for deployment and maintenance assistance and/or assistance for Production Purposes are not included within the scope of Development Support, but rather are available on a consulting basis under the terms of a separate agreement.

2.5 **Support von Red Hat. "ENTWICKLUNGSSUPPORT"** beinhaltet Hilfe bei Installation, Gebrauch, Problemdiagnosen und Fehlerbehebungen für die entsprechende für Entwicklungszwecke verwendete SOFTWARE während spezifischer Phasen im Red Hat-Lebenszyklus (wie in Abschnitt 1.7 oben referenziert). ENTWICKLUNGSSUPPORT beinhaltet auch Beratung zu Architektur, Design, Entwicklung und Erstellung von Prototypen. Anfragen bezüglich Architektur, Design, Entwicklung, Erstellung von Prototypen, installierten EINHEITEN und Wartung und/oder Produktionszwecken gehören nicht zum Aufgabenbereich des ENTWICKLUNGSSUPPORTS, sondern sind stattdessen auf der Basis von Consultingleistungen gemäß den Bedingungen eines separaten Vertrags erhältlich.

"Production Support" consists of assistance with installation, application testing, usage, problem diagnosis and bug fixes for the Software used for Production Purposes during specific Red Hat life cycle phases (as referenced in Section 1.7 above). Production Support does not include assistance with code development, system design, network design, architectural design, optimizations, tuning recommendations, development or implementation of security rules or policies, third party software made available with Red Hat Software (listed at www.redhat.com/licenses/thirdparty/eula.html), supplementary RHN channels and/or preview technologies.

"PRODUKTIONSSUPPORT" beinhaltet Hilfe bei Installation, Anwendungstests, Nutzung, Problemdiagnosen und Fehlerbehebungen für die zu Produktionszwecken verwendete SOFTWARE während spezifischer Phasen im Red Hat-Lebenszyklus (wie in Abschnitt 1.7 oben referenziert). PRODUKTIONSSUPPORT bietet keine Hilfe bei Code-Entwicklung, System-, Netzwerk- oder Architektur-Design, Optimierungen, Empfehlungen für Tuning, Entwicklung oder Implementierung von Sicherheitsregeln oder -richtlinien, Drittparteiensoftware, die zusammen mit Red Hat SOFTWARE (aufgeführt bei www.redhat.com/licenses/thirdparty/eula.html), oder mit zusätzlichen RHN-Kanälen und/oder Vorschautechnologien zur Verfügung gestellt werden.

To access and use Support, you must provide Red Hat with sufficient information to validate your entitlement to the relevant Support. The scope of the Support is based on the level (for example, Self-support, Standard or Premium) and type of Subscription Services you purchased. Certain Support is provided only during Red Hat's local standard business hours.

Für den Zugriff auf und die Nutzung des SUPPORTS müssen Sie Red Hat ausreichende Informationen liefern, um ihre Berechtigung für den entsprechenden Support zu validieren. Der Umfang des SUPPORTS hängt von dem Level (z. B. Self-Support, Standard oder Premium) und der Art der von Ihnen erworbenen Subscription Services ab. Bestimmte Arten von Support sind nur während der normalen lokalen Geschäftszeiten von Red Hat verfügbar.

2.6 **Support Coverage.** We do not provide Production or Development Support for Software that (a) you (or a third party) have modified or recompiled, (b) is running on hardware or hypervisor that is not Supported Hardware or (c) is running in an unsupported Use Case as described in an Exhibit. You are responsible for testing the Software before deploying it in your environment. You should also backup your systems on a regular basis and have those backups available if needed for support purposes.

2.6 **SUPPORT-ABDECKUNG.** Wir leisten keinen PRODUKTIONS- oder ENTWICKLUNGS-SUPPORT bei SOFTWARE die (a) von Ihnen (oder einer Drittpartei) modifiziert wurde, (b) auf nicht UNTERSTÜTZTER HARDWARE oder auf einem HYPERVISOR ausgeführt wird, oder (c) in einem nicht unterstützten ANWENDUNGSFALL ausgeführt wird, der in einem Exhibit beschrieben ist. Sie sind für den Test der SOFTWARE vor dem Einsatz in Ihrer Umgebung verantwortlich. Sie sollten auch regelmäßig Backups Ihrer Systeme erstellen und diese Backups für

Supportzwecke verfügbar halten.

Red Hat will use commercially reasonable efforts to provide Support in accordance with the guidelines shown in Table 2.7 below. Support is provided in the English language and may be available in other languages based on available resources. Red Hat's Support telephone numbers and local standard business hours (**"Standard Business Hours"**) are listed at https://access.redhat.com/support/contact/technicalSupport.html.

Red Hat wird wirtschaftlich angemessene Anstrengungen unternehmen, um den SUPPORT gemäß den in Tabelle 2,7 niedergelegten Richtlinien zu erbringen. Der Support wird in englischer Sprache geleistet und kann je nach verfügbaren Ressourcen in anderen Sprachen erhältlich sein. Die Telefonnummern und normalen regionalen Geschäftszeiten (**"NORMALE GESCHÄFTSZEITEN"**) des Technischen Supports von Red Hat sind aufgeführt unter https://access.redhat.com/support/contact/technicalSupport.html.

2.7 **Service Level Guidelines.** Support is available in one or more of the following support levels, depending on the Red Hat Product: Self-support, Standard or Premium, as shown in the table below. Software Access and Software Maintenance are generally provided to you through a Red Hat-hosted delivery portal, such as Red Hat Customer Portal, Red Hat Update Infrastructure (**"RHUI"**), and/or Red Hat Network (**"RHN"**) (collectively, **"Red Hat Portal"**). After the Initial Response, Red Hat will provide status updates on the issue until (i) the issue is resolved; (ii) the issue is downgraded to a lower Severity Level (in which case status updates will be provided in accordance with the update guidelines applicable the new Severity Level); or (iii) the parties agree on an alternative update schedule.

2.7 **Service Level Guidelines.** Der Support ist in einem der folgenden Supportlevel verfügbar, abhängig vom Red Hat Produkt: Self-Support, Standard oder Premium, wie in der folgenden Tabelle dargestellt. SOFTWARE-ZUGANG und SOFTWAREWARTUNG werden im Allgemeinen durch ein von Red Hat gehostetes Delivery Portal bereitgestellt, d. h. entweder durch das Red Hat Customer Portal, das Red Hat Update Infrastructure (**„RHUI"**) und/oder Red Hat Network (**„RHN"**) (zusammenfassend als **„Red Hat Portal"** bezeichnet). Nach einer ersten Reaktion liefert Red Hat regelmäßige Statusberichte (i) bis zur abschließenden Problembehebung, (ii) bis das Problem auf eine niedrigere Priorität abgestuft ist (in diesem Fall werden die Statusberichte entsprechend den Aktualisierungsrichtlinien für die neue Prioritätsstufe ausgegeben), oder (iii) die Parteien einen neuen Aktualisierungszeitplan vereinbaren.

Table 2.7

	Self-support	Standard	Premium	
Hours of Coverage	none	Standard Business Hours	Standard Business Hours 24x7 for Severity 1 and 2	
Support Channel	none	Web and Phone	Web and Phone	
Number of Cases	none	Unlimited	Unlimited	
Software Maintenance	via Red Hat Portal	via Red Hat Portal	via Red Hat Portal	
Response Guidelines	N/A	Initial and Ongoing Response	Initial Response	Ongoing Response
Severity 1 (Urgent): A problem that severely impacts your use of the Software in a production environment (such as the loss of production data or production systems not functioning). The situation halts your business operations and no procedural work around exists.	N/A	1 Business Hour	1 hour	1 hour
Severity 2 (High): A problem where the Software is functioning but your use in a production environment is severely reduced. The situation is causing a high impact to portions of your business operations and no procedural work around exists.	N/A	4 Business Hours	2 hours	4 hours
Severity 3 (Medium): A problem that involves partial, non-critical loss of use of the Software in a production environment or development environment. For production environments, there is a medium-to-low impact on your business, but your business continues to function, including by using a procedural work around. For development environments, the situation is causing your project to no longer continue or migrate into production.	N/A	1 Business Day	4 Business Hours	8 Business Hours
Severity 4 (Low): A general usage question, reporting of a documentation error or recommendation for a future product enhancement	N/A	2 Business Days	8 Business Hours	2 Business Days

	Self-support	Standard	Premium	
or modification: For production environments, there is low-to-no impact on your business or the performance or functionality of your system. For development environments, there is a medium-to-low impact on your business, but your business continues to function, including by using a procedural work around.				

Note: The guidelines set forth in Table 2.7 do not apply to the Developer Subscriptions described in Exhibit 1.C or to the Red Hat Enterprise Linux Developer Workstation and Red Hat Enterprise Linux Developer Support Subscriptions described in Exhibit 1.G.

Tabelle 2.7

	Self-Support	Standard	Premium	
Abgedeckte Stunden	Keine	Normale Geschäftszeiten	NORMALE GESCHÄFTSZEITEN 24x7 bei Priorität 1 und 2	
Kommunikationskanal für Support	Keine	Web und Telefon	Web und Telefon	
Anzahl der Fälle	Keine	Unbegrenzt	Unbegrenzt	
Softwarewartung	via Red Hat Portal	via Red Hat Portal	via Red Hat Portal	
Reaktionsrichtlinien	k. A.	Erstreaktion und anhaltende Reaktion	Erstreaktion	Anhaltende Reaktion
Priorität 1 (Dringlich): Ein Problem, das die Verwendung der SOFTWARE in einer Produktionsumgebung erheblich einschränkt (wie Verlust von Produktionsdaten oder bei dem Ihr Produktionssystem nicht funktioniert). Die Situation bringt Ihre Geschäftsvorgänge zum Stillstand und es gibt kein Abhilfeverfahren.	k. A.	1 Geschäftsstunde	1 Stunde	1 Stunde
Priorität 2 (Hoch): Ein Problem, bei dem die SOFTWARE zwar noch funktioniert, aber die Verwendung in einer Produktionsumgebung erheblich eingeschränkt ist. Das Problem beeinträchtigt einen Teil Ihrer Geschäftsvorgänge in starkem Umfang und es gibt kein Abhilfeverfahren.	k. A.	4 GESCHÄFTSSTUNDEN	2 Stunden	4 Stunden
Priorität 3 (Mittel): Ein Problem, das eine partielle, nicht kritische Einschränkung der Verwendbarkeit der SOFTWARE in einer Produktions- oder Entwicklungsumgebung verursacht. Es besteht eine mittlere bis niedrige Beeinträchtigung Ihrer Arbeitsvorgänge in einer Produktionsumgebung, ihr Geschäft funktioniert jedoch weiter, u. a. durch Anwendung von Abhilfeverfahren. Für Entwicklungsumgebungen, bei denen das Problem Ihr Projekt zum Abbruch zwingt oder zur Migration in die Produktion.	k. A.	1 WERKTAG	4 GESCHÄFTS STUNDEN	8 GESCHÄFTS STUNDEN
Priorität 4 (Niedrig): Eine generelle Frage zur Anwendung, Meldung eines Dokumentationsfehlers oder Empfehlung für eine künftige Produktverbesserung- oder Modifikation. Für eine Produktionsumgebung ist dies keine oder nur geringe Beeinträchtigung Ihres Geschäfts oder der Leistung bzw. Funktionalität Ihres Systems. Es besteht eine mittlere bis niedrige Beeinträchtigung Ihrer Entwicklungsumgebung, Ihr Geschäft funktioniert jedoch weiter, u. a. durch Anwendung von Abhilfeverfahren.	k. A.	2 WERKTAGE	8 GESCHÄFTS STUNDEN	2 WERKTAGE

Anm.: Die in Tabelle 2.7 beschriebenen Richtlinien gelten weder für die in Exhibit 1.C genannten DEVELOPER SUPPORT SUBSCRIPTIONS noch für die in Exhibit 1.G genannten Red Hat Enterprise Linux Developer Workstation und Red Hat Enterprise Linux Developer Support Subscriptions.

2.8 Support Contacts

For the Software Subscriptions, you may contact Red Hat through your designated Support Contacts. You may designate up to the number of contacts described in Table 2.8 below based on the number of Standard and Premium Software Subscriptions you have purchased (other than for Academic Edition Customers with Campus Wide Subscriptions*). We will provide Subscription Services to you solely by communicating during the Hours of Coverage with the individual Support Contact(s) you appoint. For Premium Support, in order to receive 24x7 coverage for Severity 1 and 2 issues, you must provide a dedicated point of contact who will be available until the issue is resolved. You may change your designated Support Contacts by notifying us in writing and giving us five business days to process the change. The Support Contacts should have "read and write" access to the necessary files, English language communication skills and relevant technical knowledge.

2.8 Support-Kontakte

Für die Software Subscriptions können Sie Red Hat über Ihre benannten Support-Kontakte kontaktieren. Sie können bis zu der in nachstehender Tabelle 2.8 angegebenen Anzahl an Kontakten benennen, je nach der Anzahl der Standard und Premium Software Subscriptions, die Sie erworben haben (mit Ausnahme von Academic Edition Kunden mit Campus Wide Subscriptions*). Wir werden Ihnen Subscription Services ausschließlich durch Kommunikation mit der/den von Ihnen ernannten Support-Kontaktperson(en) während der abgedeckten Stunden bereitstellen. Um rund um die Uhr Premium Support bei Fragen der Prioritätsstufen 1 und 2 zu erhalten, müssen Sie eine Kontaktperson benennen, die verfügbar ist, bis die Frage gelöst ist. Sie können Ihre benannten Support-Kontakte ändern, indem Sie uns schriftlich darüber unterrichten und uns fünf Geschäftstage Zeit geben, diese Änderung zu bearbeiten. Die Support-Kontakte sollten eine Lese- und Schreibberechtigung für die notwendigen Dateien sowie englische Sprachkenntnisse und die entsprechenden technischen Kenntnisse haben.

Table 2.8

Number of Standard and Premium Software Subscriptions (excluding Red Hat JBoss Subscriptions)	Number of Cores Included in Red Hat JBoss Software Subscriptions	Support Contacts
1 to 50	1 to 32	2
51 to 100	33 to 64	4
101 to 250	65 to 96	6
251 to 500	97 to 128	8
501 to 1000	129 to 160	10
1001 and over	161 to 192	12

*For Academic Edition Customers with Campus Wide Subscriptions, you may have three (3) Support Contacts for every one thousand (1,000) FTE's.

Tabelle 2.8

Anzahl der Standard und Premium Software Subscriptions (ohne Red Hat JBoss Subscriptions)	Anzahl der in den Red Hat JBoss Software Subscriptions enthaltenen Cores	Support-Kontakte
1 bis 50	1 bis 32	2
51 bis 100	33 bis 64	4
101 bis 250	65 bis 96	6
251 bis 500	97 bis 128	8
501 bis 1000	129 bis 160	10
1001 oder mehr	161 bis 192	12

*Academic Edition Kunden mit Campus Wide Subscriptions können drei (3) Support-Kontakte für alle tausend (1.000) FTE's haben.

EXHIBIT 1.A
RED HAT ENTERPRISE LINUX AND RELATED SOFTWARE SUBSCRIPTIONS

EXHIBIT 1.A
RED HAT ENTERPRISE LINUX UND VERBUNDENE SOFTWARE SUBSCRIPTIONS

redhat.

1. Unit of Measure and Purchasing Requirements for Red Hat Enterprise Linux Server

You must purchase the appropriate number and type of Software Subscription(s) for each Unit of Red Hat Enterprise Linux Server including variants such as Red Hat Enterprise Linux Server for HPC Compute Nodes, Red Hat Enterprise Linux for IBM POWER and Red Hat Enterprise Linux for SAP Applications, based on the capacity of such Unit as described in Table 1 below. Multiple Software Subscriptions may be "stacked" to account for the capacity of a given Unit. "Stacking" (or "Stackable") means the application of more than one of the same Subscription to account for additional capacity.

1. MASSEINHEIT und ERWERBSVORAUSSETZUNGEN für Red Hat Enterprise Linux Server

Sie müssen die entsprechende Anzahl und Art von SOFTWARE SUBSCRIPTION(S) für jede Einheit von Red Hat Enterprise Linux Server erwerben, einschließlich Varianten wie Red Hat Enterprise Linux Server for HPC Netzwerkelemente, Red Hat Enterprise Linux für IBM POWER und Red Hat Enterprise Linux für SAP Applications, ausgehend von der Kapazität einer solchen Einheit gemäß der nachstehenden Tabelle 1. Mehrere Software Subscriptions können "gestapelt" werden, um sie an die Kapazität einer bestimmten Einheit anzupassen. "Stapeln" (oder "stapelbar") bedeutet den Einsatz mehrerer gleicher Subscriptions in Anpassung an die zusätzliche Kapazität..

Table 1

Software Subscription	Support Level	Unit of Measure	Capacity		Stackable
			Socket(s)	Virtual Nodes	
Red Hat Enterprise Linux Server (Physical or Virtual Nodes) Red Hat Enterprise Linux for SAP HANA	Standard or Premium	Physical Node OR Virtual Node	Socket-pair for each Physical Node OR 2 Virtual Nodes		Physical Node: Yes Virtual Node: Yes, up to a maximum of 4 virtual instances[2] per Physical Node
Red Hat Enterprise Linux for Virtual Datacenters[1]	Standard or Premium	Physical Node	Socket-pair	Unlimited Virtual Nodes running on a Socket-pair	Physical Node: Yes Virtual Node: Yes
Red Hat Enterprise Linux Server Entry Level	Self-support	Physical Node	Socket-pair	None	Physical Node: No Virtual Node: Yes, up to a maximum of 4 virtual instances[2] per Physical Node
Red Hat Enterprise Linux OpenStack Platform	Standard or Premium	Physical Node	Socket-pair	Unlimited Virtual Nodes running on a Socket-pair	Physical Node: Yes Virtual Node: Yes
Red Hat Enterprise Linux with Smart Virtualization	Standard or Premium	Physical Node	Socket-pair	Unlimited Virtual Nodes running on a Socket-pair	Physical Node: Yes Virtual Node: Yes
Red Hat Enterprise Linux Server	Standard or Premium	System	1-2 Sockets, 4 Sockets, or 8 Sockets	1 Virtual Guest, 4 Virtual Guests, or Unlimited Virtual Guests	Sockets: No Virtual Guest: Yes
Red Hat Enterprise Linux Server	Self-support	System	1-2 Sockets	1 Virtual Guest	Sockets: No Virtual Guest: No
Red Hat Enterprise Linux for PRIMEQUEST	Premium	System	1-2 Sockets, 4 Sockets, 6 Sockets or 8 Sockets	1 Virtual Guest,4 Virtual Guests, or Unlimited Virtual Guests	Sockets: No Virtual Guest: Yes

Tabelle 1

Software Subscription	Support Level	Maßeinheit	Kapazität		Stapelbar
			Socket	Virtual Node	
Red Hat Enterprise Linux Server (physikalische oder virtual Nodes) Red Hat Enterprise Linux for SAP HANA	Standard oder Premium	Physikalischer ODER Virtual Node	Socket Pair für jeden Physical Node ODER 2 Virtual Nodes		Physical Nodes: Ja Virtual Nodes: Ja, bis zu 4 virtuellen Instanzen[2] pro Physical Node
Red Hat Enterprise Linux für virtuelle Datenzentren[1]	Standard oder Premium	Physical Node	Socket Pair	Unbegrenzte Virtual Nodes auf einem Socket Pair	Physical Node: Ja Virtual Node: Ja
Red Hat Enterprise Linux Server Entry Level	Self-Support	Physical Node	Socket Pair	Keine	Physical Node: Nein Virtual Nodes: Ja, bis zu 4 virtuelle Instanzen[2] pro Physical Node
Red Hat Enterprise Linux OpenStack Platform	Standard oder Premium	Physical Node	Socket Pair	Unbegrenzte Virtual Nodes auf einem Socket Pair	Physical Nodes: Ja Virtual Nodes: Ja
Red Hat Enterprise Linux with Smart Virtualization	Standard oder Premium	Physical Node	Socket Pair	Unbegrenzte Virtual Nodes auf einem Socket Pair	Physical Nodes: Ja Virtual Nodes: Ja
Red Hat Enterprise Linux Server	Standard oder Premium	System	1-2 Sockets, 4 Sockets oder 8 Sockets	1 Virtual Guest, 4 Virtual Guests oder unbegrenzte Virtual Guests	Socket: Nein Virtual Guest: Ja
Red Hat Enterprise Linux Server	Self-Support	System	1-2 Socket	1 Virtual Guest	: Nein Virtual Guest: Nein
Red Hat Enterprise Linux für PRIMEQUEST	Premium	System	1-2 Sockets, 4 Sockets, 6 Sockets oder 8 Sockets	1 Virtual Guest,4 Virtual Guests, oder Unlimited Virtual Guests	Sockets: Nein Virtual Guest: Ja

A "Socket" is a socket occupied by a CPU on a System or Physical Node. A **"Socket-pair"** is up to two sockets each occupied by a CPU on a System or Physical Node. A **"Virtual Guest"** is an instance of the Software that is executed, in whole or in part, on a System that is a virtual machine. When you deploy a guest operating system in a virtualized environment, you are responsible for securing the required license rights for any third party operating systems or other software that you use.

[1]Please note that Red Hat Enterprise Linux for Virtual Datacenters Subscriptions do not include an entitlement for the host operating system.
[2]The maximum number of four (4) virtual instances may consist of Red Hat Enterprise Linux Virtual Nodes, Virtual Guests or any other guest operating system.

2. Red Hat Enterprise Linux Server Add-Ons

Red Hat Enterprise Linux Server Subscriptions may be purchased with one or more add-on options (**"Add-On(s)"**). Add-Ons require a separate paid and active Software Subscription for each Unit that deploys, installs, uses or executes such Add-On. Each Unit of Add-

Ein "SOCKET" ist ein Socket, der von einer CPU auf einem System oder Physical Nodes benutzt wird. Ein **„SOCKET-PAIR"** besteht aus bis zu zwei Sockets, die von je einer CPU auf einem SYSTEM oder "Physical Node" benutzt werden. Ein **„VIRTUAL GUEST "** ist eine Instanz der SOFTWARE, die auf einem System installiert oder ausgeführt wird, das eine virtuelle Maschine ist. Wenn Sie in einer virtualisierten Umgebung ein Gast-Betriebssystem zum Einsatz bringen, sind Sie für die Erlangung der erforderlichen Lizenzrechte für Betriebssysteme von Drittparteien und für von Ihnen benutzte Software verantwortlich.

[1]Bitte beachten Sie, dass Red Hat Enterprise Linux für Virtual DatacentersSubscriptions keine Berechtigung für das Host-Betriebssystem enthalten.
[2]Die Höchstanzahl von vier (4) virtuellen Instanzen kann aus Red Hat Enterprise Linux Virtual Nodes, Virtual Guests oder anderen Gastbetriebssystemen bestehen.

2. Red Hat Enterprise Linux Server Add-Ons

Red Hat Enterprise Linux Server Subscriptions können mit einer oder mehreren Add-On-Optionen (**„ADD-ON(S)"**) erworben werden. Für ADD-ONs ist eine gesondert bezahlte aktive SOFTWARE SUBSCRIPTION für jede EINHEIT erforderlich, die solche ADD-

Ons must match the Support Level (Standard and/or Premium), Unit of Measure and capacity as the underlying Red Hat Enterprise Linux Unit. Add-Ons are not supported on Red Hat Enterprise Linux Subscriptions with a Self-support service level except Smart Management Add-Ons. The Add-Ons include: High Availability, Load Balancer, Resilient Storage, Scalable File System, Smart Management, Extended Update Support, Extended Life Cycle Support and High Performance Network.

ONs einsetzt, installiert, verwendet oder ausführt. Jede Add-On-Einheit muss dem Support Level (Standard und/oder Premium), der Maßeinheit und der Kapazität der zugrunde liegenden Red Hat Enterprise Linux Einheit entsprechen. Add-Ons werden auf Red Hat Enterprise Linux Subscriptions mit Self-Support Service Level nicht unterstützt, außer Smart Management Add-Ons. Die ADD-ONS beinhalten: Hohe Verfügbarkeit, Lastverteiler, ausfallsicherer Speicher, skalierbares Dateisystem, Smart Management, Extended Update Support, Extended Life Cycle Support und Hochleistungsnetzwerk.

3. Red Hat Enterprise Linux Server Support Options

Red Hat Enterprise Linux Server Subscriptions may be purchased with various levels of Production Support including Self-support, Standard and Premium Support Levels. Note that not all Production Support options are available for all Red Hat Enterprise Linux Server Subscriptions, configurations or customers. For example, Self-support is available only for (a) Systems without Add-Ons (except Smart Management); and (b) customers who do not have a Red Hat Technical Account Manager.

3. Red Hat Enterprise Linux Server Support Optionen

Red Hat Enterprise Linux Server SUBSCRIPTIONS können mit verschiedenen Leveln an PRODUKTIONSSUPPORT, einschließlich SELF-SUPPORT, STANDARD und PREMIUM SUPPORT LEVEL erworben werden. Bitte beachten Sie, dass nicht alle PRODUKTIONSSUPPORT Optionen für alle Red Hat Enterprise Linux Server SUBSCRIPTIONS, Konfigurationen oder Kunden erhältlich sind. Zum Beispiel ist SELF-SUPPORT nur verfügbar für (a) SYSTEME ohne ADD-ONS (außer Smart Management); und (b) Kunden, die keinen Technical Account Manager von Red Hat haben.

4. Red Hat Enterprise Linux Server Use Cases

Subscription Services are provided for Software only when used for its supported purpose (**"Use Case"**) in accordance with the terms of this Exhibit and Table 4 below.

4. Red Hat Enterprise Linux Server Anwendungsfälle

SUBSCRIPTION SERVICES werden für SOFTWARE nur geleistet, wenn diese für ihre unterstützten Zwecke (**"ANWENDUNGSFALL"**) gemäß den Bedingungen dieses Exhibits und der unten stehenden Tabelle 4 benutzt werden.

Table 4

Software	Use Case
Red Hat Enterprise Linux Server Red Hat Enterprise Linux Server for Mainframe	Server computing, including delivery of services to other logical or physical client or server systems and the execution of multi-user applications. You may not split or apply one Red Hat Enterprise Linux Software Subscription to two or more Units.
Red Hat Enterprise Linux for IBM POWER	Supports up to 15 logical partitions per System.
Red Hat Enterprise Linux for PRIMEQUEST	Subscription Services are provided only on Fujitsu PRIMEQUEST systems. You may not split or apply one Red Hat Enterprise Linux for PRIMEQUEST Software Subscription to two or more Units or any other systems.
Red Hat Enterprise Linux for SAP HANA	Subscription Services are provided only on systems certified to run SAP's HANA platform.
Red Hat Enterprise Linux for HPC Compute Nodes Red Hat Enterprise Linux for HPC Head Nodes	High performance computing (**"HPC"**) that consists of a minimum set of four Systems that are networked and managed to perform compute-intensive workloads (**"cluster"**) with all of the following characteristics: (a) the cluster is used for compute-intensive distributed tasks sent to individual compute nodes within the cluster, (b) the cluster works as a single entity or system on specific tasks by performing compute-intensive operations on sets of data (Systems running a database, web application, load balancing or file serving clusters are not considered HPC nodes), (c) the number of management or head nodes does not exceed one quarter of the total number of nodes in the cluster and (d) all compute nodes in the cluster have the same Red Hat Enterprise Linux configuration. When Red Hat Enterprise Linux for HPC Head Nodes (an optional Software Subscription for management of compute nodes) is combined with Red Hat Enterprise Linux for HPC Compute Nodes Software Subscriptions for the compute nodes in the same cluster, the compute nodes assume the Service Level Agreement (**"SLA"**) of the Head Node.
Red Hat Enterprise Linux for Grid Nodes	A compute **"Grid"** means a minimum of fifty (50) Socket-pairs that are networked and managed to solve workloads with the following characteristics: (a) all the nodes in the group of systems have the same Red Hat Enterprise Linux configuration, (b) the group of systems is running a single application or is controlled by a single job scheduler, (c) the workloads are sent to the group of systems by a job scheduler, (d) the workloads are maintained in a single distributed application across the nodes in the group of systems, (e) the workloads are non-interactive, and (f) the production outage of the complete group of systems is defined as 30% of the nodes in the group of systems being unable to run the workload. The nodes in Grid are not running databases, web applications, load balancing, or file services.

Software	Use Case
Red Hat Enterprise Linux with Smart Virtualization	Supported on physical hardware solely to support virtual guests. Red Hat Enterprise Linux with Smart Virtualization is designed to run and manage virtual instances. The included Red Hat Enterprise Linux is supported solely when used as the host operating system with the Red Hat Enterprise Virtualization Hypervisor or when used as the guest operating system with virtual machines.
Add-Ons: High Availability, Load Balancer, Resilient Storage, Scalable File System, Extended Update Support, Extended Life Cycle Support and High Performance Network	Only supported on active Standard and Premium level Red Hat Enterprise Linux Server Software Subscriptions.
Red Hat Enterprise Linux Server used as a Virtual Guest	Virtual Guests may be pooled or shared on any other System that has a Software Subscription with the same (a) support level (Standard or Premium) and (b) number of Virtual Guests (1, 4 or unlimited Virtual Guests), provided that you do not exceed the total number of Virtual Guests associated with the underlying Software Subscriptions. **Note:** When you use Red Hat Enterprise Virtualization or third party software as a host operating system or hypervisor, you must purchase separate Software Subscriptions for each host System running the Virtual Guest.
Red Hat Enterprise Linux for Disaster Recovery	Systems or Physical Nodes used intermittently for disaster recovery purposes such as systems receiving periodic backups of data from production servers, provided those disaster recovery systems have the same Service Levels (as set forth in Appendix 1, Section 2.7) and configurations (e.g. Socket-pairs, Virtual Guests, Cores).
Red Hat Enterprise Linux for Retail	Systems used at retail store locations with the same application stack excluding any data center deployments.

Tabelle 4

Software	Anwendungsfall
Red Hat Enterprise Linux Server Red Hat Enterprise Linux Server für Mainframe	Server Computing, einschließlich Service an andere logische oder physische Klienten oder Serversysteme, und Ausführung von Mehrbenutzer-Applikationen. Sie können keine Red Hat Enterprise Linux SOFTWARE SUBSCRIPTION splitten oder auf mehr als eine EINHEIT anwenden.
Red Hat Enterprise Linux für IBM POWER	Unterstützt bis zu 15 logische Partitionen pro SYSTEM.
Red Hat Enterprise Linux für PRIMEQUEST	Subscription Services werden nur auf Fujitsu PRIMEQUEST Systemen erbracht. Sie dürfen Red Hat Enterprise Linux für PRIMEQUEST Software Subscriptions nicht auf zwei oder mehr Einheiten oder auf andere Systeme verteilen oder einsetzen.
Red Hat Enterprise Linux for SAP HANA	Subscription Services werden nur auf Systemen erbracht die für SAP HANA zertifiziert sind.
Red Hat Enterprise Linux für HPC Netzwerkelemente Red Hat Enterprise Linux für HPC Head Netzwerkelemente	Hochleistungsrechnen („**HPC**"), das mindestens eine Gruppe von vier SYSTEMEN in einem Netzwerk involviert, die zur Durchführung von rechnerintensiver Arbeitsaufgaben („**Cluster**") eingesetzt werden, mit allen der folgenden Merkmale: (a) der Cluster wird für rechnerintensive verteilte Aufgaben benutzt, die an einzelne Netzwerkelemente innerhalb des Clusters gesandt werden, (b) der Cluster arbeitet mit spezifischen Aufgaben durch rechnerintensive Operationen an Datensätzen als integriertes System (Systeme für Datenbanken, Web-Applikationen, Lastverteilung oder als Dateiserver eingesetzte Cluster werden nicht als HPC-Netzwerkelemente angesehen), (c) die Anzahl der Management oder Head Netzwerkelemente überschreitet nicht ein Viertel der Gesamtzahl der Netzwerkelemente im Cluster und (d) sämtliche Netzwerkelemente im Cluster haben die gleiche Red Hat Enterprise Linux Konfiguration. Wenn Red Hat Enterprise Linux für HPC Head Nodes (optionale Software Subscription zur Verwaltung von Netzwerkelementen) mit Red Hat Enterprise Linux für HPC Compute Nodes Software Subscriptions für die Netzwerkelemente im selben Cluster kombiniert wird, setzen die Netzwerkelemente die Service Level Agreement („**SLA**") des Netzwerkelements voraus.
Red Hat Enterprise Linux für Grid Nodes	Ein Computer-„**Grid**" bezeichnet ein Minimum aus fünfzig (50) Socket Pairs, die zur Lösung von Workloads mit folgenden Eigenschaften vernetzt und verwaltet werden: (a) sämtliche Netzwerkelemente in der Systemgruppe haben die gleiche Red Hat Enterprise Linux Konfiguration, (b) die Systemgruppe betreibt eine einzelne Applikation oder wird von einem einzigen Auftragsplaner kontrolliert, (c) die Workloads werden durch den Auftragsplaner an die Systemgruppe gesendet, (d) die Workloads werden in einer einheitlichen verteilten Anwendung in den Nodes der Systemgruppe gepflegt, (e) die Workloads sind nicht interaktiv und (f) als Produktionsausfall der kompletten Systemgruppe ist definiert, wenn 30 Prozent der Nodes einer Systemgruppe eine

Software	Anwendungsfall
	Workload nicht ausführen können. Die Nodes im Grid führen keine Datenbanken, Webapplikationen, Load Balancing oder File Services aus.
Red Hat Enterprise Linux with Smart Virtualization	Unterstützt auf physikalischer Hardware nur, um Virtuelle Gäste zu unterstützen. Red Hat Enterprise Linux with Smart Virtualization ist entwickelt, um gemanagte Virtuelle Instanzen zu betreiben. Das enthaltene Red Hat Enterprise Linux wird nur als Host-Betriebssystem mit dem Red Hat Enterprise Virtualisierungs Hypervisor unterstützt oder wenn es als Gast-Betriebssystem mit Virtuellen Maschinen betrieben wird.
Add-Ons: Hohe Verfügbarkeit, Lastverteiler, ausfallsicherer Speicher, skalierbares Dateisystem, Extended Update Support, Extended Life Cycle Support und Hochleistungsnetzwerk	Nur unterstützt mit aktiven STANDARD und PREMIUM Level Red Hat Enterprise Linux Server SOFTWARE SUBSCRIPTIONS.
Red Hat Enterprise Linux Server, als VIRTUELLER GAST verwendet	VIRTUELLE GÄSTE können auf jedem anderen SYSTEM mit einer SOFTWARE SUBSCRIPTION mit (a) den gleichen Support-Levels (STANDARD OR PREMIUM) und (b) der gleichen Anzahl von VIRTUELLEN GÄSTEN (1, 4 oder unbegrenzte Anzahl VIRTUELLER GÄSTE) zu Pools zusammengelegt oder geteilt werden, vorausgesetzt, dass Sie nicht die Gesamtzahl der VIRTUELLEN GÄSTE überschreiten, die mit den zugrundeliegenden SOFTWARE SUBSCRIPTIONS verbunden sind. **Anm.:**Wenn Sie Red Hat Enterprise Virtualization oder Software von Drittanbietern als Host-Betriebssystem oder Hypervisor nutzen, müssen Sie für jedes Gast-SYSTEM, auf dem VIRTUELLE GÄSTE ausgeführt werden, eine separate SOFTWARE SUBSCRIPTION erwerben.
Red Hat Enterprise Linux für Disaster Recovery	Systeme oder physical Nodes, die zwischenzeitlich für Disaster-Recovery-Zwecke genutzt werden, wie Systeme, die regelmäßige Daten-Backups von Produktionsservern erhalten, vorausgesetzt, diese Disaster-Recovery-Systeme haben dieselben Service Levels (wie in Appendix 1, Abschnitt 2,7 beschrieben) und Konfigurationen (z.B. SOCKET PAIRS, VIRTUAL PAIRS, Cores).
Red Hat Enterprise Linux für den Handel	Systeme, die in Handelsbetrieben mit demselben Anwendungs-Stack ohne Datenzentrums-Anwendung eingesetzt werden.

5. Red Hat Enterprise Virtualization Use Cases

You must purchase the appropriate number and type of Software Subscription(s) for each Physical Node that deploys, installs, uses or executes Red Hat Enterprise Virtualization based on the number of Socket-pairs. Subscription Services are provided for Red Hat Enterprise Virtualization only when used for its supported Use Case in accordance with the terms of this Exhibit and Table 5 below. A Red Hat Enterprise Virtualization Subscription comes with RHEV-Manager, which requires the purchase of an underlying Red Hat Enterprise Linux Subscription for each Unit (i.e., Physical Node or Virtual Node) running RHEV-Manager.

5. Red Hat Enterprise Virtualization - Anwendungsfälle

Sie müssen eine ausreichende Anzahl und Typ Software Subscription(s) für jeden physical Node, der Red Hat Enterprise Virtualization auf der Basis der Anzahl der Socket Pairs einsetzt, installiert, verwendet oder ausführt, erwerben. SUBSCRIPTION SERVICES werden für Red Hat Enterprise Virtualization nur geleistet, wenn diese für den im Folgenden genannten unterstützten ANWENDUNGSFALL und gemäß den Bedingungen dieses Exhibits und der unten stehenden Tabelle 5 benutzt werden. Eine Red Hat Enterprise Virtualization Subscription wird mit einem RHEV-Manager geliefert, der den Erwerb einer Red Hat Enterprise Linux Subscription für jedes System (d.h. physical Node oder virtual Node) erfordert, auf dem ein RHEV-Manager läuft.

Table 5

Software	Use Case
Red Hat Enterprise Virtualization	Supported on physical hardware solely to support virtual guests. Red Hat Enterprise Virtualization is designed to run and manage virtual instances and does not support user-space applications. Red Hat Enterprise Virtualization may be used as a virtual desktop infrastructure solution, however, the Subscription does not come with software or support for the desktop operating system. You must purchase the operating system for each instance of a desktop or server separately.

Tabelle 5

Software	Anwendungsfall
Red Hat Enterprise Virtualization	Auf physikalischer Hardware nur für den Support VIRTUELLE GÄSTE unterstützt. Red Hat Enterprise Virtualization wurde entwickelt, um VIRTUELLE INSTANZEN auszuführen und zu verwalten, und unterstützt keine Anwendungen im Benutzerkontext. Red Hat Enterprise Virtualization kann als virtuelle Desktop-Infrastrukturlösung