Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

# Typische Fehler bei Datenschutzerklärungen

In unserer Beratungs- und Prüfungspraxis sind immer wieder ähnliche Verstöße gegen die Informationspflichten nach Art. 13 und 14 der Datenschutz-Grundverordnung (DSGVO) festzustellen. Die Mängel in Datenschutzerklärungen, die bereits einzeln den Sanktionstatbestand von Art. 83 Abs. 5 lit. b DSGVO erfüllen und mit Geldbußen von bis zu 20 Millionen Euro oder von bis zu vier Prozent des weltweiten Konzernvorjahresumsatzes belegt werden können, werden im Folgenden aufgelistet und erklärt.

## 1. Kontaktdaten der Datenschutzbeauftragten

**Art. 13 Abs. 1 lit. b, Art. 14 Abs. 1 lit. b DSGVO**

Typische Fehler: Die Kontaktdaten der Datenschutzbeauftragten und der Verantwortlichen sind gleich. Die Kontaktdaten sind unvollständig.

Die Kontaktdaten der Datenschutzbeauftragten können nicht dieselben sein wie die der Verantwortlichen selbst. Denn nach Art. 38 Abs. 5 DSGVO sind Datenschutzbeauftragte auch gegenüber den Verantwortlichen zur Verschwiegenheit verpflichtet. Öffnet aber beispielsweise die Poststelle eines Verantwortlichen die Post an die bzw. den Datenschutzbeauftragte:n oder wird ein gemeinsames Postfach verwendet (oder auch ein gemeinsames Kontaktformular), gelangt die Kommunikation mit den Datenschutzbeauftragten rechtswidrig den Verantwortlichen zur Kenntnis.

Datenschutzbeauftragte müssen für betroffene Personen direkt erreichbar sein. An sie adressierte Post muss ungeöffnet weitergeleitet werden. Es muss ein gesonderter E-Mail-Account bestehen, auf den nur die Datenschutzbeauftragten selbst oder ihre hiermit beauftragten Mitarbeiter:innen Zugriff haben. Für elektronische Kommunikation ist ein sicheres Verfahren bereitzustellen, etwa ein verschlüsseltes Kontaktformular oder eine OpenPGP-Verschlüsselung. Je nach Tätigkeit der Verantwortlichen müssen betroffene Personen ggf.

**Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI)**
Alt-Moabit 59-61, 10555 Berlin
Eingang: Alt-Moabit 60

**Telefon:** 030 13889-0
**Telefax:** 030 215 50 50
**Sprechzeiten:** Mo.-Fr. 10-15 Uhr,
Do. 10-18 Uhr, oder nach Vereinbarung

**E-Mail:** mailbox@datenschutz-berlin.de
**Website:** www.datenschutz-berlin.de

auch die Möglichkeit haben, sich telefonisch an die Datenschutzbeauftragten zu wenden, etwa wenn die Kommunikation mit den Kund:innen auch sonst vor allem telefonisch erfolgt. Wenn keine Durchwahl angegeben ist, darf die Telefonzentrale dabei nicht die Angabe von Namen oder Details zum Anliegen verlangen. Sind Datenschutzbeauftragte telefonisch tatsächlich regelmäßig erreichbar, kann je nach Tätigkeit der Verantwortlichen unter Umständen die Angabe eines E-Mail-Kontakts entbehrlich sein.

Zu veröffentlichen sind die Kontaktdaten der bzw. des benannten Datenschutzbeauftragten. Hierzu gehört nicht zwingend der Name; dennoch empfehlen wir, als vertrauensbildende Maßnahme auch den Namen zu veröffentlichen.

## 2. Angaben zur Verarbeitung

**Art. 13 Abs. 1 lit. c bis e, Art. 14 Abs. 1 lit. c bis e, Abs. 2 lit. f DSGVO**

Typische Fehler: Datenverarbeitungen werden nicht vollständig beschrieben, sondern nur beispielhaft.

Jede Verarbeitung personenbezogener Daten muss vollständig beschrieben werden. Beispiele sind nur zur reinen Erläuterung von Oberbegriffen zulässig; der Oberbegriff selbst muss alle Verarbeitungen abdecken.

## 3. Zwecke und Rechtsgrundlage der Verarbeitung

**Art. 13 Abs. 1 lit. c, Art. 14 Abs. 1 lit. c DSGVO**

Typische Fehler: Zwecke werden unvollständig angegeben und/oder nicht konkreten Datenverarbeitungen zugeordnet. Rechtsgrundlagen werden nur allgemein beschrieben, aber nicht zugeordnet. Rechtsgrundlagen werden unvollständig angegeben, insbesondere ohne die Verpflichtungsnorm, die die Verarbeitung vorschreibt.

Es sind sämtliche Zwecke anzugeben, für die die personenbezogenen Daten verarbeitet werden. Ebenso müssen sämtliche Rechtsgrundlagen angegeben werden, auf die sich die Verantwortlichen stützen. Es ist zulässig – und aus Sicht der Verantwortlichen auch sinnvoll – alle einschlägigen Rechtsgrundlagen anzugeben, etwa für den Fall, dass eine Rechtsgrundlage entgegen der Annahme der Verantwortlichen doch nicht tragfähig ist. Ein nachträglicher Austausch der Rechtsgrundlage ist in aller Regel nicht möglich.

Wenn unterschiedliche Datenkategorien zu unterschiedlichen Zwecken und auf unterschiedlichen Rechtsgrundlagen verarbeitet werden, muss differenziert werden. Es muss genau ersichtlich sein, welche Datenkategorien zu welchem Zweck auf welcher Rechtsgrundlage verarbeitet werden. Hierzu können Tabellen hilfreich sein. Möglich ist aber auch eine klare Differenzierung im Fließtext.

Nicht ausreichend ist es, nur im Sinne einer Darstellung der Rechtsgrundlagen abstrakt aufzuführen, welche Rechtsgrundlagen das Gesetz kennt. Die Verantwortlichen müssen jeder Verarbeitung die konkrete Rechtsgrundlage zuordnen. Dies sollte auch durch Angabe der konkreten Rechtsnorm (z. B. „Art. 6 Abs. 1 Uabs. 1 lit. b DSGVO“) erfolgen. Ist die Rechtsgrundlage Art. 6 Abs. 1 Uabs. 1 lit. c oder e DSGVO, muss zusätzlich auch die konkrete Verpflichtungsnorm (im Fall einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 Uabs. 1 lit. c DSGVO) bzw. Aufgabennorm (im Fall der Aufgabenübertragung nach Art. 6 Abs. 1 Uabs. 1 lit. e DSGVO) angegeben werden.

Beispiel: „Rechtsgrundlage für die steuerrechtliche Aufbewahrung ist Art. 6 Abs. 1 Uabs. 1 lit. c DSGVO i. V. m. §§ 147 AO, 257 HGB.“ oder „Rechtsgrundlage für die Speicherung Ihrer Einwilligung sind Art. 6 Abs. 1 Uabs. 1 lit. c i. V. m. Art. 5 Abs. 2 DSGVO, Art. 7 Abs. 1 DSGVO und Art. 24 Abs. 1 DSGVO sowie Art. 6 Abs. 1 Uabs. 1 lit. f DSGVO.“

## 4. Berechtigte Interessen

**Art. 13 Abs. 1 lit. d, Art. 14 Abs. 2 lit. b DSGVO**

Typische Fehler: Berechtigte Interessen werden gar nicht, unvollständig oder nur ganz allgemein angegeben und/oder nicht der konkreten Verarbeitung zugeordnet.

Wenn die Rechtsgrundlage eine Interessenabwägung nach Art. 6 Abs. 1 Uabs. 1 lit. f DSGVO ist, müssen für jede einzelne Verarbeitung sämtliche berechtigten Interessen angegeben werden, auf die sich die Verantwortlichen stützen wollen. Nur die angegebenen Interessen können bei der Interessenabwägung berücksichtigt werden. Eine allgemeine Angabe „Berechtigtes Interesse ist das Wohlergehen unserer Mitarbeiter:innen und Anteilseigner:innen“ ist zwar zur Erfüllung des Wortlauts von Art. 13 Abs. 1 lit. d und Art. 14 Abs. 1 lit. e DSGVO ausreichend, führt aber zwangsläufig zur Rechtswidrigkeit der Datenverarbeitung, weil die Erforderlichkeit gerade der konkreten Verarbeitung nicht nachgewiesen werden kann.

Beispiel: „Berechtigtes Interesse an der Speicherung Ihrer Einwilligung auf der Basis von Art. 6 Abs. 1 Uabs. 1 lit. f DSGVO ist der Nachweis Ihrer Einwilligung, d. h. die Verteidigung gegen Rechtsansprüche."

## 5. Empfänger bzw. Kategorien von Empfängern

**Art. 13 Abs. 1 lit. e, Art. 14 Abs. 1 lit. e DSGVO**

Typische Fehler: Interne Empfänger und Auftragsverarbeiter werden nicht angegeben. Obwohl bereits konkret bekannt, werden Empfänger nur als Kategorien angegeben. Es werden nur die Auftragsverarbeiter auf der ersten Stufe angegeben, nicht die Unterauftragsverarbeiter.

Anzugeben sind die konkreten Empfänger, soweit diese bereits feststehen. Beispiel: Ein Webshop macht bei Kauf auf Rechnung Bonitätsanfragen bei einer Auskunftei. Diese Auskunftei steht bereits vorab fest, sodass sie als Empfänger namentlich zu benennen ist. Kategorien von Empfängern dürfen nur dann angegeben werden, wenn die einzelnen Empfänger noch nicht feststehen. (Bitte beachten Sie, dass die Empfänger, die personenbezogene Daten einer betroffenen Person erhalten haben, in jedem Fall nach Art. 15 Abs. 1 lit. c und Art. 19 Satz 2 DSGVO konkret benannt und hierfür gespeichert werden müssen.)

Empfänger sind nach der Definition in Art. 4 Nr. 9 DSGVO nicht nur Dritte, sondern auch Auftragsverarbeiter und interne Empfänger bei den Verantwortlichen, denen personenbezogene Daten offengelegt werden; Offenlegung umfasst nach Art. 4 Nr. 2 DSGVO jede Art der Bereitstellung, sodass auch das Einräumen einer Zugriffsmöglichkeit genügt. Interne Empfänger sind nicht mit ihrem bürgerlichen Namen zu benennen, sondern die internen Stellen, d. h. in der Regel als Abteilung.

Auch Unterauftragsverarbeiter sind Empfänger, sodass sämtliche Empfänger über die gesamte Kette an Unterauftragsverarbeitern anzugeben sind. Nicht angegeben werden müssen dagegen diejenigen Empfänger, an die ein Empfänger, dem die Daten in eigener Verantwortlichkeit offengelegt werden, wiederum die Daten offenlegt. Insoweit ist der Empfänger selbst in der Verpflichtung, nach Art. 14 DSGVO zu informieren.

Es ist klarzustellen – etwa durch eine Zwischenüberschrift, eine Einleitung oder eine andere geeignete Formulierung –, dass die genannten Stellen Empfänger sind. Der Begriff Empfänger muss nicht ausdrücklich verwendet werden.

Beispiel: „Zugriff auf Ihre Daten haben unsere Personalabteilung und die Buchhaltung. Unsere Administrator:innen haben technisch notwendig die Möglichkeit, auf sämtliche mittels IT verarbeitete Daten zuzugreifen. Für das Webhosting setzen wir die XYZ GmbH, ABC-Straße 1, 01234 MNO-Stadt, als Auftragsverarbeiter ein."

## 6. Datenexporte

**Art. 13 Abs. 1 lit. f, Art. 14 Abs. 1 lit. f DSGVO**

Typische Fehler: Datenexporte werden überhaupt nicht angegeben, insbesondere bei Nutzung von Cloud- oder US-Dienstleistern. Wenn Datenexporte angegeben werden, werden nur die USA angegeben. Datenexporte durch Unterauftragsverarbeiter werden nicht angegeben. Garantien für den Datenexport werden nicht angegeben.

Zu beachten ist, dass bereits ein Fernzugriff und die technisch eingeräumte Möglichkeit zum Fernzugriff aus einem Drittland einen Datenexport darstellt, etwa die Anzeige am Bildschirm zu Support- oder Administrationszwecken.

Datenexporte sind auch dann anzugeben, wenn sie erst auf einer späteren Stufe in der Auftragsverarbeiterkette erfolgen. Dies kann etwa der Fall sein, wenn der Auftragsverarbeiter die Daten in die USA an einen Unterauftragsverarbeiter übermittelt und dieser wiederum im Rahmen eines 24/7-Follow-the-Sun-Supports je nach Tageszeit weiteren Unterauftragsverarbeitern in anderen Drittländern Zugriff zu Supportzwecken ermöglicht.

Wenn kein Angemessenheitsbeschluss nach Art. 45 DSGVO vorliegt, kommen als Garantien für den Datenexport meist Standardvertragsklauseln zum Einsatz. Die EU-Kommission hat ein Set von Standardvertragsklauseln für Auftragsverarbeitungsverträge und ein Set für Datenexporte beschlossen, sodass für Datenexporte auf das richtige Set zu verweisen ist. Dieses wiederum enthält verschiedene Module und Optionen. Da Art. 13 Abs. 1 lit. f und Art. 14 Abs. 1 lit. f DSGVO (anders als Art. 15 Abs. 2 DSGVO) nur „einen Verweis" auf die Garantien verlangen, genügt es, das Set und das gewählte Modul zu benennen. Alle weiteren Details kann die betroffene Person erfahren, indem sie eine Kopie der ausgefüllten Standardvertragsklauseln und weiteren Bestandteile der Garantien wie ergänzende Schutzmaßnahmen anfordert. Hierfür ist in den Informationen nach Art. 13 und 14 DSGVO anzugeben, wie eine Kopie von den Garantien zu erhalten ist oder wo diese verfügbar sind. Ein reiner Verweis auf die Verfügbarkeit der nicht ausgefüllten Standardvertragsklauseln genügt allerdings nicht, weil diese nicht die (gesamten) Garantien darstellen.

In jedem Fall sind die im Einzelfall konkret verwendeten Garantien anzugeben, bei unterschiedlichen Garantien für unterschiedliche Datenexporte ist zu differenzieren.

## 7. Speicherdauer

**Art. 13 Abs. 2 lit. a, Art. 14 Abs. 2 lit. a DSGVO**

Typischer Fehler: Anstatt die Löschfristen anzugeben, wird allgemein auf nicht näher benannte gesetzliche Vorschriften verwiesen, die teilweise Aufbewahrungspflichten vorsehen.

Die Aufbewahrungsdauer bzw. Löschfrist ist konkret zu benennen, und zwar sowohl die Frist als auch der Fristbeginn. Da sich die Aufbewahrungs- und Löschfristen für die verschiedenen Daten und ggf. auch Zwecke unterscheiden, ist zu differenzieren. Ist noch nicht absehbar, wie lange eine bestimmte Kategorie personenbezogener Daten erforderlich ist, müssen konkrete Fristen für eine erneute Überprüfung der fortgesetzten Speicherung angegeben werden. Werden keine konkreten Löschfristen angegeben, lässt das die Vermutung zu, dass rechtswidrig überhaupt keine Löschfristen definiert sind und bei den Verantwortlichen ein größeres datenschutzrechtliches Problem besteht.

Es kann im Einzelfall vorkommen, dass personenbezogene Daten über den üblichen Zeitraum hinaus aufbewahrt werden müssen, etwa wenn ein Besteuerungsverfahren beim Ablauf der Fristen nach § 147 AO noch nicht abgeschlossen ist. Es wird – jedenfalls derzeit – nicht beanstandet, wenn diese Sonderfälle nicht ausdrücklich aufgeführt sind, sondern die Löschfristen im Sinne von Regelfristen angegeben sind.

Beispiel: „Geschäfts- und Handelsbriefe und andere steuerrelevante Unterlagen löschen wir in der Regel bis zum 31. März des siebten Kalenderjahrs nach Entstehen, bei Buchungsbelegen des elften Kalenderjahrs nach Entstehen.“ oder „Ist Ihre Bewerbung nicht erfolgreich, verarbeiten wir Ihre Daten noch bis zu sechs Monate nach Versand der Absage (um uns gegen eventuelle Rechtsansprüche zu verteidigen, insbesondere wegen einer angeblichen Benachteiligung im Bewerbungsverfahren).“ oder „Ob Fotos von unseren Veranstaltungen dauerhaft für die Dokumentation unserer Arbeit erforderlich sind, wird innerhalb von drei Monaten nach Ende der Veranstaltung geprüft; nicht relevante Fotos werden sofort nach der Prüfung gelöscht. Alle fünf Jahre wird überprüft, ob die Fotos weiterhin benötigt werden, und nicht mehr benötigte Fotos werden sofort nach der Prüfung gelöscht.“

## 8. Recht zur Beschwerde bei einer Aufsichtsbehörde

**Art. 13 Abs. 2 lit. d, Art. 14 Abs. 2 lit. e DSGVO**

Typische Fehler: Es wird nur davon gesprochen, dass sich betroffene Personen bei der für die Verantwortlichen zuständigen Aufsichtsbehörde beschweren können.

Tatsächlich haben betroffene Personen das Recht, sich bei einer Aufsichtsbehörde ihrer Wahl zu beschweren. Es ist eine freundliche Geste, die für die Verantwortlichen zuständige Aufsichtsbehörde konkret mit Anschrift und Website zu benennen, aber dies darf nur beispielhaft geschehen.

## 9. Freiwilligkeit der Angabe, Folgen bei Verweigerung

**Art. 13 Abs. 2 lit. e DSGVO**

Typische Fehler: Es fehlen Angaben zur Freiwilligkeit der Angabe und/oder ob und welche Nachteile bei Verweigerung entstehen.

## 10. Sprache der Datenschutzerklärung

**Art. 12 DSGVO**

Typische Fehler: Die Datenschutzerklärung ist voller orthographischer, grammatikalischer und begrifflicher Fehler. Die Sprache ist unnötig kompliziert. Die Datenschutzerklärung liegt nicht auf Deutsch vor.

Rechtliche Präzision und einfache Sprache stehen in einem Konflikt. Jedenfalls sollten Fehler vermieden werden, die die Datenschutzerklärung schwer verständlich machen, etwa durch automatische oder schlechte Übersetzungen. Die Informationen müssen in einer Sprache gegeben werden, die die betroffenen Personen verstehen, üblicherweise auf Deutsch. Selbst wenn die Arbeitssprache im Unternehmen Englisch ist, genügt eine englische Datenschutzerklärung für Beschäftigte nur dann, wenn diese ausreichende Sprachkenntnisse haben, auch solche Texte mit juristischen Fachbegriffen zu verstehen oder die Datenschutzerklärung ausreichend einfach geschrieben ist. Die Informationen können grundsätzlich in einem Mehrebenensystem in unterschiedlichen Detailgraden gegeben

werden, wobei alle wesentlichen Informationen auf der ersten Ebene gegeben werden müssen. In jedem Fall muss aber ein vollständiger Ausdruck ohne größeren Aufwand möglich sein – dies ist nicht der Fall, wenn erst einmal alle Ebenen einzeln aufgerufen werden müssen.

## 11. Versteckte Einwilligungen

Typische Fehler: In der Datenschutzerklärung finden sich versteckte Einwilligungen nach dem Muster „Wenn Sie X machen, willigen Sie ein, dass wir Y mit Ihren Daten machen“.

Eine Datenschutzerklärung ist eine Information an die betroffenen Personen und damit bereits im Ansatz der falsche Ort für eine Einwilligungserklärung. Außerdem muss jede Einwilligung freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegeben werden, und zwar in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (Art. 4 Nr. 11 DSGVO). In einer Datenschutzerklärung enthaltene Einwilligungen werden von den betroffenen Personen üblicherweise nicht einmal wahrgenommen, geschweige denn, dass sie irgendeiner Datenverarbeitung zustimmen wollen. Einwilligungserklärungen müssen daher an anderer Stelle eingeholt werden. Auf die zusätzlichen Anforderungen von Art. 7 DSGVO wird verwiesen.