UNABHÄNGIGES DATENSCHUTZZENTRUM SAARLAND

Prüfung der Rechenschaftspflicht

nach Art. 5 Abs. 2 DSGVO

Verantwortlicher: <Verantwortlicher>

Datum: 04. Dezember 2018

Aktenzeichen: <Aktenzeichen>

Wir bitten um vollständige Beantwortung der folgenden Fragen und Zusendung der angeforderten Unterlagen auf Basis von Art. 58 DSGVO bis spätestens zum 31. Januar 2019.

Grundkonzept

1. Gibt es eine Datenschutzleitlinie im Unternehmen?
   - ☐ Ja. Bitte senden Sie uns eine Kopie der Leitlinie zu.
   - ☐ Nein.

2. Ist ein Datenschutzbeauftragter bestellt und der Aufsichtsbehörde gemeldet?
   - ☐ Ja.
     Meldedatum: _____
     Art der Meldung: ☐ Online ☐ Brief ☐E-Mail
   - ☐ Nein.

3. Welche Aufgaben hat Ihr Datenschutzbeauftragter in dieser Funktion (kurze Beschreibung)?

4. Nimmt der Datenschutzbeauftragte weitere Funktionen im oder für das Unternehmen wahr?
   - ☐ Ja. Bitte beschreiben Sie diese kurz.
   - ☐ Nein.

5. Sind, sofern mehrere Standorte oder Niederlassungen des Unternehmens vorhanden sind, diese in ein einheitliches Datenschutzkonzept eingebunden?
   - ☐ Ja. Bitte senden Sie uns eine Kopie des Datenschutzkonzepts zu.
   - ☐ Nein.

6. Entscheiden diese Standorte oder Niederlassungen eigenverantwortlich über Zwecke und Mittel bei der Verarbeitung personenbezogener Daten?
   - ☐ Ja.
   - ☐ Nein.

7. Sind interne Zuständigkeiten in Bezug auf datenschutzrelevante Vorgänge bzw. Abläufe (z.B. Schulung der Mitarbeiter, Meldung von Datenschutzverletzungen,…) personell festgelegt?
   - ☐ Ja. Bitte senden Sie uns eine Kopie der schriftlichen Festlegungen zu.
   - ☐ Nein.

8. Gibt es Regelungen für interne Kontrollen zur Einhaltung datenschutzrechtlicher Vorschriften?
   - ☐ Ja. Bitte senden Sie uns eine Kopie der Regelungen zu.
   - ☐ Nein.

9. Beschreiben Sie bitte kurz, wie mit den Berichten, Stellungnahmen o.ä. des Datenschutzbeauftragten im Unternehmen umgegangen wird.

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)

10. Ist ein vollständiges Verzeichnis von Verarbeitungstätigkeiten vorhanden?
    - ☐ Ja. Bitte nennen Sie die Anzahl der Verarbeitungstätigkeiten.
    - ☐ Nein. Bitte geben Sie den Grund an.

11. Beschreiben Sie bitte, nach welcher Methode (z.B. Zweck, Mittel, Prozess, IT-System,…) die einzelnen Verarbeitungstätigkeiten ermittelt werden.

12. Beschreiben Sie bitte die Regelungen, wie das Verzeichnis von Verarbeitungstätigkeiten verwaltet wird (z.B. Aktualisierungen oder hinsichtlich Änderungshistorie und –befugnisse etc.).

Einheitliches Risikomodell

13. Existiert ein Dokument zum unternehmensweiten Verständnis des Datenschutzrisikos?
    - ☐ Ja. Bitte senden Sie uns eine Kopie dieses Dokuments zu.
    - ☐ Nein.

14. Beschreiben Sie bitte, wie bei der Bewertung des Datenschutzrisikos nach Ihrer Auffassung der Schaden an den Rechten und Freiheiten natürlicher Personen zu verstehen ist.

15. Beschreiben Sie bitte, welche Skalen zur Modellierung der Eintrittswahrscheinlichkeit und Schwere eines Datenschutzrisikos im Unternehmen verwendet werden.

16. Beschreiben Sie bitte, wie Sie sicherstellen, dass alle relevanten Stellen den Unterschied zwischen dem Unternehmensrisiko (Fokus: Unternehmenswerte) und einem Datenschutzrisiko (Fokus: Rechte und Freiheiten natürlicher Personen) verstanden haben.

17. Ist das Risikomodell sowohl den Verantwortlichen für den Datenschutz als auch dem betrieblichen Datenschutzbeauftragten sowie dem Informationssicherheitsbeauftragten bekannt?
    - ☐ Ja.
    - ☐ Nein.

Datenschutzkonforme Verarbeitung

18. Ist für jede Verarbeitungstätigkeit nach Art. 30 DSGVO eine Legitimationsgrundlage für die Verarbeitung personenbezogener Daten (Einwilligung, Rechtsgrundlage) dokumentiert?
    - ☐ Ja.
    - ☐ Nein. Bitte geben Sie den Grund an.

19. Ist für die Verarbeitungen auf der Grundlage einer „Interessenabwägung“ nach Art. 6 Abs. 1 lit. f DSGVO eine Begründung dokumentiert?
    - ☐ Ja.
    - ☐ Nein. Bitte geben Sie den Grund an.

20. Sind Einwilligungen im Sinne des Art. 4 Nr. 11 DSGVO nach den Vorgaben des Art. 7 DSGVO ausgestaltet und können diese jederzeit widerrufen werden?
    - ☐ Ja.
    - ☐ Nein. Bitte geben Sie den Grund an.

21. Beschreiben Sie, in welchen Kontexten die Einwilligung der betroffenen Person eingeholt wird.

22. Übersenden Sie entsprechende Muster der von Ihnen verwendeten Einwilligungserklärungen.

23. Wurde für jede im Verzeichnis nach Art. 30 DSGVO dokumentierte Verarbeitung eine Schwellwertanalyse (d.h. Risikoüberprüfung) zur Vorbereitung der Frage, ob eine Datenschutzfolgenabschätzung durchgeführt werden muss, vorgenommen?
    - ☐ Ja.
    - ☐ Nein. Bitte geben Sie den Grund an.

24. Benennen Sie bitte die Verarbeitungstätigkeiten, für die Sie die Notwendigkeit der Durchführung einer Datenschutzfolgenabschätzung nach Art. 35 DSGVO ermittelt haben und stellen Sie uns die dokumentierten Ergebnisse der Datenschutzfolgeabschätzungen zur Verfügung.

25. Existiert ein Löschkonzept (z.B. nach DIN 66398), das auch den Umgang mit Archiven und Backups regelt?
    - ☐ Ja. Bitte senden Sie uns eine Kopie dieses Konzepts zu.
    - ☐ Nein. Bitte geben Sie den Grund an.

26. Werden geeignete Maßnahmen zur Sicherstellung der Verfügbarkeit, Vertraulichkeit und Integrität nach Art. 32 DSGVO getroffen?
    - ☐ Ja. Bitte senden Sie uns das Sicherheitskonzept zu.
    - ☐ Nein. Bitte geben Sie den Grund an.

27. Existiert ein Prozess (Plan-Do-Check-Act) zur Sicherstellung der Wirksamkeit der Maßnahmen nach Art. 32 DSGVO?
    - ☐ Ja. Bitte senden Sie uns eine Beschreibung dieses Prozesses zu.
    - ☐ Nein. Bitte geben Sie den Grund an.

28. Beschreiben Sie bitte, wie *Privacy by Design* nach Art. 25 Abs. 1 DSGVO unter besonderer Berücksichtigung der Grundsätze der Datensparsamkeit und der Einhaltung der Zweckbindung in den Verarbeitungstätigkeiten im Unternehmen konzeptionell umgesetzt wird.

29. Findet für Audits des Datenschutzbeauftragten eine einheitliche Prüfmethodik Anwendung?
    - ☐ Ja. Bitte senden Sie uns Kopien der letzten beiden Prüfberichte zu.
    - ☐ Nein. Bitte geben Sie den Grund an.

30. Beschreiben Sie bitte, wie sichergestellt ist, dass Auftragsverarbeiter nach Art. 28 DSGVO auf Basis eines geeigneten Risikomodells und darauf aufbauenden wirksamen technischen und organisatorischen Maßnahmen (entsprechend Art. 25 Abs. 1 DS-GVO) ausgewählt werden.

31. Beschreiben Sie bitte, wie sichergestellt ist, dass (bei Auftragsverarbeitungen) die Rechtsgrundlage der sog. zweiten Stufe bei Datentransfers in Drittstaaten korrekt ausgestaltet wird.

32. Existiert ein einheitliches Verschlüsselungskonzept?
    - ☐ Ja. Bitte senden Sie uns eine Kopie der schriftlichen Festlegungen zu.
    - ☐ Nein. Bitte geben Sie den Grund an.

33. Existiert ein einheitliches Pseudonymisierungskonzept?
    - ☐ Ja. Bitte senden Sie uns eine Kopie der schriftlichen Festlegungen zu.
    - ☐ Nein. Bitte geben Sie den Grund an.

34. Gibt es im Unternehmen Verarbeitungstätigkeiten, für die eine gemeinsame Verantwortlichkeit nach Art. 26 DSGVO gegeben ist?
    - ☐ Falls ja, beschreiben Sie bitte stichwortartig diese Verarbeitungen und legen Sie für zwei dieser Verarbeitungen die entsprechenden Vereinbarungen über die gemeinsame Verantwortlichkeit vor.
    - ☐ Nein.

Umgang mit Betroffenenrechten

35. Ist ein Prozess implementiert, wie mit Auskunftsansprüchen nach Art. 15 DSGVO umgegangen wird?
    - ☐ Ja. Bitte beschreiben Sie diesen Prozess.
    - ☐ Nein. Bitte geben Sie den Grund an.

36. Beschreiben Sie bitte, wie sichergestellt wird, dass die personenbezogenen Daten der Betroffenen aus allen vorhandenen Systemen und ggf. Zweigniederlassungen schnell und vollständig verfügbar sein können.

37. Werden betroffene Personen über alle im Verzeichnis nach Art. 30 DSGVO dokumentierten Verarbeitungstätigkeiten gemäß Art. 12 ff. und gegebenenfalls Art. 21 DSGVO transparent informiert?
    - ☐ Ja.
    - ☐ Nein. Bitte geben Sie den Grund an.

38. Wurde(n) die Webseite(n) seit dem 25. Mai 2018 derart überarbeitet, dass auf ihr/ihnen über die Datenverarbeitung (der Webseite) ausreichend gemäß Art. 13 DSGVO informiert wird?
    - ☐ Ja.
    - ☐ Nein. Bitte geben Sie den Grund an.

    Bitte senden Sie uns eine komplette Liste aller Domain-Namen Ihres Unternehmens zu.

39. Ist ein Verfahren implementiert, mit dem die Einhaltung der Fristen bezüglich der Betroffenenrechte gemäß Art. 14 - 22 DSGVO sichergestellt wird?
    - ☐ Ja. Bitte beschreiben Sie dieses Verfahren.
    - ☐ Nein. Bitte geben Sie den Grund an.

40. Ist ein Verfahren implementiert, mit dem auf Anfragen der Datenschutzaufsichtsbehörden bezüglich dort eingegangener Datenschutzbeschwerden reagiert wird?
    - ☐ Ja. Bitte beschreiben Sie dieses Verfahren.
    - ☐ Nein. Bitte geben Sie den Grund an.

41. Sind Schulungsunterlagen vorhanden, mit denen die Personen, die an den Prozessen zur Sicherstellung der Betroffenenrechte mitarbeiten, sachgerecht informiert werden?
    - ☐ Ja. Senden Sie uns bitte eine Kopie dieser Unterlagen zu.
    - ☐ Nein. Bitte geben Sie den Grund an.

42. Haben Sie Überlegungen dazu angestellt, wie Sie auf einen Antrag einer betroffenen Person auf Datenportabilität nach Art. 20 DSGVO reagieren? Beschreiben Sie bitte gegebenenfalls Ihre Überlegungen.

43. Wurde ein solcher Antrag bereits bei Ihnen gestellt?
    - ☐ Ja.
    - ☐ Nein.

Umgang mit Datenschutzverletzungen

44. Wie viele Datenschutzverletzungen nach Art. 33 DSGVO sind bei Ihnen seit dem 25. Mai 2018 bekannt geworden und wie viele davon der Aufsichtsbehörde gemeldet bzw. im Sinne des Art. 33 Abs. 5 DSGVO lediglich dokumentiert?

45. Beschreiben Sie bitte, wie Datenschutzverletzungen nach Art. 33/34 DSGVO im Unternehmen erkannt werden.

46. Beschreiben Sie bitte, wie Sie Datenschutzverletzungen, die bei Dienstleistern (auch in Drittstaaten) auftreten, erkennen, dokumentieren und aufarbeiten.

47. Findet das Risikomodell zur Einstufung des Datenschutzrisikos auch bei Datenschutzverletzungen nach Art.33/34 DSGVO Beachtung?
    - ☐ Ja.
    - ☐ Nein. Bitte geben Sie den Grund an.

48. Beschreiben Sie den Prozess für den Fall, dass bei Datenschutzverletzungen ein hohes Risiko für die Betroffenen festgestellt wird.

49. Beschreiben Sie, inwiefern gewährleistet ist, dass Datenschutzverletzungen innerhalb von 72 Stunden (auch an Wochenenden/Feiertagen) bei der zuständigen Aufsichtsbehörde gemeldet werden.

50. Ist geklärt und dokumentiert, bei welchen Stellen im Unternehmen die Meldefrist von 72 Stunden startet?
    - ☐ Ja. Bitte nennen Sie uns diese Stellen:_____
    - ☐ Nein. Bitte geben Sie den Grund an.