Bayerisches Landesamt für
Datenschutzaufsicht

Prüfkatalog Rechenschaftspflicht

nach Art. 5 Abs. 2 DS-GVO bei (Groß-)Konzernen und Datengetriebenen Unternehmen

(Version 1.0)

MUSTER

Verantwortlicher: <Verantwortlicher>

Datum: <Datum>

Aktenzeichen: <Aktenzeichen>

Wir bitten um vollständige Beantwortung der in diesem Prüfkatalog gestellten Fragen und Zusendung der angeforderten Unterlagen auf Basis von Art. 58 DS-GVO bis spätestens zum <Rücksendedatum>.

A. Aufbauorganisation

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?
   - ☐ Beratung der Geschäftsführung
   - ☐ Beratung der Fachabteilungen
   - ☐ Sensibilisierung der Mitarbeiter
   - ☐ Durchführung interner Audits/Kontrollen
   - ☐ Beantwortung/Klärung von Datenschutzbeschwerden
   - ☐ Durchführung von Anfragen zu Betroffenenrechten
   - ☐ Aufgabenplanung der Fachabteilungen
   - ☐ Durchführung der Meldung von Datenschutzverletzungen (Art. 33/34 DS-GVO)
   - ☐ Sonstige: _____

4. Sind, sofern mehrere Standorte vorhanden sind, die anderen Niederlassungen in ein einheitliches Datenschutzkonzept eingebunden?
   - ☐ Ja. Bitte senden Sie uns eine Kopie des Datenschutzkonzepts (sofern vorhanden) zu bzw. beschreiben dieses kurz (ca. 1 Seite).
   - ☐ Nein

5. Gibt es ein Konzept im Unternehmen, wer bezogen auf den Datenschutz für was zuständig ist (z.B. Schulung der Mitarbeiter, Meldung von Datenschutzverletzungen,…)?
   - ☐ Ja. Bitte senden Sie uns eine Kopie des Konzepts (sofern vorhanden) zu bzw. beschreiben dieses kurz (ca. 1 Seite).
   - ☐ Nein

6. Gibt es Regelungen für interne Kontrollen zur Einhaltung datenschutzrechtlicher Vorschriften?
   - ☐ Ja. Bitte senden Sie uns eine Kopie der Regelungen(sofern vorhanden) zu bzw. beschreiben dieses kurz (Ca. 1 Seite).
   - ☐ Nein

7. Beschreiben Sie bitte kurz (ca. 1 Seite), wie mit den Berichten des Datenschutzbeauftragten im Unternehmen umgegangen wird?

8. Beschreiben Sie bitte kurz (ca. 1 Seite), wie überprüft wird, ob die Zusammenarbeit der verschiedenen Abteilungen in Datenschutzfragen funktioniert?

B.Basis-Anforderungen

Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO)

9. Ist ein vollständiges Verarbeitungsverzeichnis vorhanden?
   - ☐ Ja. Anzahl der Verarbeitungstätigkeiten:_____
   - ☐ Nein. Grund:_____

10. Beschreiben Sie bitte kurz (ca. 1 Seite), nach welcher Methode (z.B. Zweck, Mittel, Prozess, IT-System, Abstraktion, …) die einzelnen Verarbeitungstätigkeiten ermittelt werden.

11. Sind bei den Empfängern auch interne Stellen (z.B. Personal, Geschäftsleitung, Marketing,…) umfasst?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

12. Beschreiben Sie bitte kurz (ca. 1 Seite) die Regelungen, wie das Verarbeitungsverzeichnis verwaltet (z.B. aktualisiert) wird?

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 kurz (ca. 0,5 - 1 Seite), wie bei der Bewertung des Datenschutzrisikos der Schaden an den Rechten und Freiheiten verstanden wird

15. Beschreiben Sie bitte kurz (ca. 0,5 - 1 Seite), welche Skalen zur Modellierung der Eintrittswahrscheinlichkeit eines Datenschutzrisikos einheitlich im Unternehmen verwendet werden.

16. Beschreiben Sie bitte kurz (ca. 0,5 - 1 Seite), wie Sie sicherstellen, dass alle relevanten Stellen/Fachbereiche den Unterschied zwischen dem Unternehmensrisiko (Fokus: Unternehmenswerte) und einem Datenschutzrisiko (Fokus: Rechte und Freiheiten natürlicher Personen) verstanden haben?

17. Werden die in der DS-GVO vorkommenden Risikoklassen Kein/Geringes Risiko, Risiko, Hohes Risiko einheitlich im Unternehmen verwendet?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

18. Ist das Risikomodell sowohl den Verantwortlichen für Datenschutz als auch dem betrieblichen Datenschutzbeauftragten sowie dem Informationssicherheitsbeauftragten bekannt und wurde von diesen verstanden?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

C. Datenschutzkonforme Verarbeitung

19. Ist für jede Verarbeitungstätigkeit nach Art. 30 DS-GVO eine Rechtsgrundlage vorhanden?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

20. Ist für die Verarbeitungen auf der Rechtsgrundlage „Interessenabwägung" nach Art. 6 Abs. 1 lit. f DS-GVO eine dokumentierte Begründung vorhanden?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

21. Sind Einwilligungen nach den Formalien des Art. 7 DS-GVO ausgestaltet und können diese jederzeit widerrufen werden?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

22. Wurde für jede im Verzeichnis nach Art. 30 DS-GVO dokumentierte Verarbeitung eine Schwellwertanalyse (d.h. Risikoüberprüfung) zur Vorbereitung der Frage, ob eine Datenschutzfolgenabschätzung durchgeführt werden muss, vorgenommen?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

    Bezeichnen Sie bitte stichwortartig die Verarbeitungstätigkeiten, für die Sie die Notwendigkeit der Durchführung einer Datenschutzfolgenabschätzung nach Art. 35 DS-GVO ermittelt haben:_____

23. 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. Grund:_____

24. Werden geeignete Security-Maßnahmen zur Sicherstellung der Verfügbarkeit, Vertraulichkeit und Integrität nach Art. 32 DS-GVO getroffen?
    - ☐ Ja. Bitte senden Sie uns bitte das IT-Sicherheitskonzept bzw. eine Zusammenfassung davon zu.
    - ☐ Nein. Grund:_____

25. Existiert ein Prozess (Plan-Do-Check-Act) zur Sicherstellung der Wirksamkeit der Security- Maßnahmen nach Art. 32 DS-GVO?
    - ☐ Ja. Bitte senden Sie uns bitte eine kurze Beschreibung dieses Prozesses zu
    - ☐ Nein. Grund:_____

26. Beschreiben Sie uns bitte konzeptionell (ca. 1 Seite), wie Datenschutz durch Technikgestaltung nach Art. 25 Abs. 1 DS-GVO bei Ihnen unter besonderer Berücksichtigung der Grundsätze der Datensparsamkeit und der Einhaltung der Zweckbindung in den Verarbeitungstätigkeiten umgesetzt wird.

27. Sind die letzten (zwei) Audits des Datenschutzbeauftragten vorhanden und besitzen diese eine einheitliche Prüfmethodik?
    - ☐ Ja. Bitte senden Sie uns Kopien der Prüfberichte zu.
    - ☐ Nein. Grund:_____

28. Beschreiben Sie bitte kurz (ca. 1 Seite), wie Sie sicherstellen, dass Auftragsverarbeiter nach Art. 28 DS-GVO auf Basis eines geeigneten Risikomodells und darauf aufbauenden wirksamen technischen und organisatorischen Maßnahmen (entsprechend Art. 25 Abs. 1 DS-GVO) ausgewählt werden?

29. Beschreiben Sie bitte kurz (ca. 1 Seite), wie Sie sicherstellen, dass (bei Auftragsverarbeitungen) die Rechtsgrundlage der sog. zweiten Stufe bei Datentransfers in Drittstatten korrekt ausgestaltet wird.

30. Existiert ein einheitliches Kryptokonzept?
    - ☐ Ja. Bitte senden Sie uns bitte eine Kopie des Konzepts zu.
    - ☐ Nein. Grund:_____

31. Existiert ein einheitliches Pseudonymisierungskonzept?
    - ☐ Ja. Bitte senden Sie uns bitte eine Kopie des Konzepts zu.
    - ☐ Nein. Grund:_____

32. Gibt es bei Ihnen Verarbeitungstätigkeiten, für die eine gemeinsame Verantwortlichkeit nach Art. 26 DS-GVO gegeben ist?
    - ☐ Falls ja, beschreiben Sie bitte stichwortartig diese Verarbeitungen und legen uns für eine dieser Verarbeitungen den entsprechenden Vertrag über die gemeinsame Verantwortlichkeit vor.
    - ☐ Nein.

D. Umgang mit Betroffenenrechten

33. Ist ein dokumentierter Prozess vorhanden, wie mit Auskunftsansprüchen nach Art. 15 DS-GVO umgegangen wird?
    - ☐ Ja. Bitte beschreiben Sie diesen Prozess kurz (ca. 1 Seite)
    - ☐ Nein. Grund:_____

34. Beschreiben Sie bitte kurz (ca. 1 Seite), wie sichergestellt wird, dass die personenbezogenen Daten der Betroffenen aus allen vorhandenen Systemen und ggf. Zweigniederlassungen schnell und vollständig verfügbar sein können?

35. Sind für alle im Verzeichnis nach Art. 30 DS-GVO dokumentierten Verarbeitungstätigkeiten geeignete (ggf. gemeinsame) Informationen gemäß Art. 13, 14 DS-GVO vorhanden?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

36. Wurden die Webseite(n) seit dem 25.Mai 2018 derart überarbeitet, dass auf ihnen über die Datenverarbeitung (der Webseite) ausreichend gemäß Art. 13 DS-GVO informiert wird?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

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

37. Ist ein Verfahren vorhanden, mit dem die Antwortzeiten auf Fristeinhaltung bezüglich der Betroffenenrechte gemäß Art. 14 - 22 sicherstellt werden.
    - ☐ Ja. Bitte beschreiben Sie dieses Verfahren kurz (ca. 1 Seite)
    - ☐ Nein. Grund:_____

38. Ist ein Verfahren vorhanden, mit dem auf Anfragen der Datenschutzaufsichtsbehörden bezüglich dort eingegangener Datenschutzbeschwerden reagiert wird.
    - ☐ Ja. Bitte beschreiben Sie dieses Verfahren kurz (ca. 1 Seite)
    - ☐ Nein. Grund:_____

39. Sind Schulungsunterlagen vorhanden, mit denen die Personen, die an den Prozessen zur Sicherstellung der Betroffenen mitarbeiten, sachgerecht informiert werden.
    - ☐ Ja. Senden Sie uns bitte eine Kopie dieser Unterlagen zu.
    - ☐ Nein. Grund:_____

40. Ist ein Software-Tool vorhanden, mit dem Anfragen von Betroffenen verwaltet werden? Mit welchen Rollen-/Rechtekonzepten wird dieses Tool konfiguriert?
    - ☐ Ja. Name der Software:_____
    - ☐ Nein. Grund:_____

41. Welche Überlegungen haben Sie angestellt, um auf einen Antrag einer betroffenen Person auf Datenportabilität nach Art. 20 DS-GVO zu reagieren?
    - ☐ Beschreiben Sie bitte kurz dieses Verfahren:_____
    - ☐ Bisher keine Überlegungen angestellt.

E. Umgang mit Datenschutzverletzungen

42. Wie viele Datenschutzverletzungen nach Art. 33 DS-GVO sind bei Ihnen bekannt geworden?
    - ☐ Anzahl seit 25.05.2018:_____
    - ☐ Keine

43. Beschreiben Sie bitte kurz (ca. 1 Seite), wie Datenschutzverletzungen nach Art. 33/34 DS-GVO im Unternehmen erkannt werden.

44. Beschreiben Sie bitte kurz (ca. 1 Seite), wie Sie Datenschutzverletzungen, die bei Dienstleistern (auch in Drittstaaten) auftreten, erkennen, dokumentieren und aufarbeiten?

45. Beschreiben Sie bitte kurz (ca. 1 Seite), ob, und wenn ja, wie Sie nur Dienstleister auswählen, die ein überzeugendes Konzept zur Erkennung von Datenschutzverletzungen bei sich umgesetzt haben?

46. Wird das Risikomodell zur Einstufung des Datenschutzrisikos auch bei Datenschutzverletzungen nach Art.33/34 DS-GVO eingesetzt?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

47. Beschreiben Sie uns bitte kurz(ca. 0,5-1 Seite) Ihren Prozess, wie Sie bei Datenschutzverletzungen feststellen, dass ein hohes Risiko für die Betroffenen vorliegt und wie Sie diese zu informieren beabsichtigen.

48. Ist der Meldeweg zur zuständigen Aufsichtsbehörde für alle beteiligten Stellen zur Aufarbeitung der Datenschutzverletzungen bekannt?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

49. Gibt es einen (dokumentierten) Prozess, um Datenschutzverletzungen innerhalb 72 Stunden (auch an Wochenenden/Feiertagen) bei der zuständigen Aufsichtsbehörde zu melden?
    - ☐ Ja.
    - ☐ Nein. Grund:_____

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