Aufgaben zur Umsetzung der DS-GVO : 1 - 15
Laufende Tätigkeiten gemäß DS-GVO: 16 - 20

Kompakte Checkliste zur Umsetzung der Datenschutz-Grundverordnung

1. Die gesetzlichen Aufgaben des Datenschutzbeauftragten (DSB)

Der DSB überwacht die Einhaltung der DSGVO sowie weiterer anwendbarer Datenschutzvorschriften. Der DSB ist intern und extern erster Ansprechpartner in Fragen des Datenschutzes und berät u.a. bei Verfahrensverzeichnis und Datenschutz-Folgenabschätzung.

2. Verarbeitungstätigkeiten identifizieren

In einem ersten Schritt sollen zunächst alle Verarbeitungstätigkeiten identifiziert und zentrale Fragestellungen (Verantwortlicher, Datenarten, Datenherkunft, Datenübermittlung usw.) beantwortet werden. Anschließend können die Informationen zusammengeführt, Datenflussanalysen erstellt und die Ergebnisse ins Verfahrensverzeichnis überführt werden.

3. Verfahrensverzeichnis erstellen

Das Verfahrensverzeichnis ist ein Verzeichnis aller Verarbeitungstätigkeiten. Die Pflicht zur Führung eines Verfahrensverzeichnisses trifft den Verantwortlichen, wie auch – mit geringerem Umfang – den Auftragsverarbeiter. Die Führung des Verfahrensverzeichnisses hat schriftlich zu erfolgen, wobei ein elektronisches Format benutzt werden kann. Das Verfahrensverzeichnis ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen. Anhand des Verfahrensverzeichnisses ist es für die Aufsichtsbehörde möglich, die durchgeführten Verarbeitungstätigkeiten zu kontrollieren.

4. Datenschutz-Folgenabschätzung prüfen und ggf. durchführen,

Wenn aus Sicht der betroffenen Personen voraussichtlich ein hohes Risiko besteht, ist eine Datenschutz-Folgenabschätzung durchzuführen. Für bestimmte Verarbeitungstätigkeiten wird die Aufsichtsbehörde eine Liste führen, für die in jedem Fall eine Datenschutz-Folgenabschätzung notwendig sein wird. Daneben kann es auch eine Liste mit Ausnahmen geben.

5. Einhaltung der Datenschutz-Grundsätze sicherstellen

Für sämtliche Verarbeitungstätigkeiten ist die Einhaltung der Datenschutz-Grundsätze zu gewährleisten, z.B. durch das Stellen von Kontrollfragen:

a. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
b. Datenminimierung und Zweckbindung
c. Speicherbegrenzung
d. Richtigkeit, Integrität, Vertraulichkeit und Verfügbarkeit
e. Rechenschaftspflicht

6. Datensicherheitsmaßnahmen (TOMs) umsetzen - Beratung

Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen (TOMs) zu treffen, und zwar abhängig vom

a. Stand der Technik,
b. den Implementierungskosten,
c. dem Umfang, der Umstände und der Zwecke der Verarbeitung sowie
d. der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen.

Der Stand der Technik wird üblicherweise durch (inter-)national anerkannte Normen (z.B. ISO/IEC 27001:2013, BSI IT-Grundschutz usw.) repräsentiert. Diese Vorgaben sind auf die Gegebenheiten der eigenen Organisation anzupassen.

7. Rechte der betroffenen Personen wahren – Beratung

Neben den erweiterten Pflichten des Verantwortlichen gem. Art 12, 13 und 14 DSGVO (Transparenz und Information) hat der Verantwortliche umfangreiche Rechte der Betroffenen zu beachten und die fristgerechte Erfüllung bei Geltendmachung sicherzustellen.

a. Recht auf Auskunft (Art. 15 DSGVO)
b. Recht auf Berichtigung (Art. 16 DSGVO)
c. Recht auf Löschung bzw. Recht auf Vergessenwerden (Art. 17 DSGVO)
d. Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
e. Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
f. Recht auf Widerspruch (Art 21 DSGVO)

g. Festlegung und Dokumentation der Prozesse, insbesondere der Verantwortlichkeit

8. Einwilligungsprozess einführen - Beratung

Die Rechtmäßigkeit der Verarbeitung pb Daten kann, sofern diese nicht der Erfüllung eines Vertrages oder einer rechtlichen Verpflichtung dient, insbesondere durch die Einwilligung einer natürlichen Person sichergestellt werden. Dabei sind die Vorgaben der DSGVO im Detail zu beachten.

9. Informationspflichten einführen - Beratung

Um eine faire und transparente Verarbeitung pb Daten sicherzustellen, muss der Verantwortliche den betroffenen Personen alle Informationen zur Verfügung stellen, die Art, Zweck und Umfang der Verarbeitungstätigkeit beschreiben. Dabei wird unterschieden, ob die Daten direkt beim Betroffenen erhoben werden oder auf anderem Wege zum Verantwortlichen gelangten. Der Informationspflicht muss nicht nachgekommen werden, wenn der Betroffene bereits über alle Informationen die Verarbeitung seiner Daten betreffend verfügt.

10. Auftragsverarbeiter-Rahmenbedingungen sicherstellen

Auftragsverarbeiter ist jemand, der pb Daten im Auftrag eines Verantwortlichen verarbeitet (z.B. CloudDiensteanbieter, Hosting-Anbieter, Software-Provider, ausgelagerte Lohnverrechnung, Dienstleister innerhalb eines Konzerns usw.). Bei der Auswahl und Beauftragung des Auftragsverarbeiters sind bestimmte Rahmenbedingungen sicherzustellen und schriftlich zu vereinbaren.

11. Data Protection by Design / Data Protection by Default sicherstellen - Beratung

Data Protection by Design (Datenschutz durch Technikgestaltung) und Data Protection by Default (Datenschutz durch datenschutzfreundliche Voreinstellungen) sind zwei Anforderungen, um Datenschutzgrundsätze (z.B. Datenminimierung) zu implementieren – sowohl für technische (z.B. Software) als auch organisatorische (z.B. Organisationsprozesse) Aspekte. Data Protection by Design bedeutet, Datenschutz-Risiken schon bei der Entwicklung neuer Technologien festzustellen und zu prüfen, und den Datenschutz von Vornherein in die Gesamtkonzeption einzubeziehen. Data

Protection by Default bedeutet, dass Produkte oder Dienstleistungen standardmäßig datenschutzfreundlich konfiguriert sind. Im Sinne der Rechenschaftspflicht müssen die Überlegungen und Entscheidungen dokumentiert werden.

12. Datenpannen-Prozess einführen - Beratung

Es ist ein Prozess einzuführen, wie die fristgerechte Benachrichtigung bei Datenschutzverletzungen sowie die rechtzeitige Ergreifung geeigneter Gegenmaßnahmen erfolgen kann.

13. Datenschutz-Policy erstellen

Erstellung eines High-Level-Dokuments mit verbindlichen und zentralen Datenschutzvorgaben aus Organisationssicht, welches vom Top Management in Kraft zu setzen ist.

14. Mitarbeiter schulen

Schulung aller Mitarbeiter, die mit pb Daten zu tun haben, auf

a. die DSGVO und andere anwendbare Datenschutzvorschriften,
b. wichtige Bestimmungen in der Organisation (z.B. Datenschutz-Policy) sowie
c. die Konsequenzen bei Nichtbeachtung

15. Datenübermittlung (EU / international)

Pb Daten dürfen nur dann in Drittstaaten außerhalb der EU ohne angemessenes Schutzniveau übermittelt werden, wenn durch entsprechende Prozesse und Mechanismen sichergestellt ist, dass die Anforderungen der DSGVO eingehalten werden.

Laufende Tätigkeiten

16. Verfahrensverzeichnis aktualisieren

Das Verfahrensverzeichnis ist nach der erstmaligen Erstellung auf Basis einer umfassenden Datenerhebung laufend zu aktualisieren.

17. Audits durchführen

Ähnlich wie bei anderen Managementsystemen ist auch die Wirksamkeit und Effizienz eines DSMS regelmäßig zu prüfen. Das inkludiert die Durchführung regelmäßiger interner bzw. externer Audits zur Überwachung sowie die Ableitung entsprechender Maßnahmen zur kontinuierlichen Verbesserung des DSMS. Beispielsweise können auch bestehende Managementsysteme (z.B. ISMS nach ISO/IEC 27001) mit dem DSMS zusammengeführt werden.

18. Jahresbericht erstellen

Jährlich sollte ein Datenschutzbericht für die Geschäftsleitung erstellt werden

19. Kontakt mit Behörden und betroffenen Personen pflegen

Der Kontakt mit Behörden und betroffenen Personen sollte vorsorglich aufgebaut und gepflegt werden, um im Anlassfall entsprechende Kommunikationskanäle zur Verfügung zu haben.

20. KVP des Datenschutz-Managementsystems (DSMS) sicherstellen

Fortlaufende Verbesserung der Eignung, Angemessenheit und Wirksamkeit des DSMS sowie Miteinbeziehung von rechtlichen Änderungen (z.B. Urteile, Verordnungen usw.).