EU-Datenschutz-Grundverordnung (DSGVO): Ablaufplan Datenschutz-Folgenabschätzung

Checkliste - Prüfschritte

Stand: 21.06.2018

Hinweis:
Die Bestimmungen der DSGVO und des österreichischen Datenschutzgesetzes (DSG) in der Fassung des Datenschutz-Anpassungsgesetzes 2018 und des Datenschutz-Deregulierungs-Gesetzes 2018 gelten seit 25.5.2018. Alle Datenverarbeitungen müssen dieser Rechtslage entsprechen. (Siehe dazu „Überblick")

1. Prüfung, ob überhaupt die Voraussetzungen für die Durchführung einer verpflichtenden Datenschutz-Folgenabschätzung vorliegen:

Wird eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen (Profiling) durchgeführt, die in weiterer Folge als Grundlage für Entscheidungen herangezogen werden soll, die für natürliche Personen Rechtswirkungen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen könnte (z.B. zur Frage der Kreditvergabe)?

Werden in umfangreicher Art und Weise sensible Daten oder Daten über strafrechtliche Verurteilungen und Straftaten selbst verarbeitet?

Erfolgt bei der Datenverarbeitung eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche (z.B. Videoüberwachungen)?

Gibt es Listen der Datenschutzbehörde, die Fälle aufzählen, in denen eine Datenschutz-Folgenabschätzung zwingend durchzuführen ist bzw. nicht (verpflichtend) durchzuführen ist?

Hinweis: Derzeit hat die Datenschutzbehörde in Form einer Verordnung eine Liste von Verarbeitungstätigkeiten veröffentlicht, die keiner verpflichtend durchzuführenden Datenschutz-Folgenabschätzung zugeführt werden müssen („white list"-Verordnung).

Eine Liste über Verarbeitungsvorgänge, bei denen auf jeden Fall eine Datenschutz-Folgenabschätzung durchzuführen ist, besteht gegenwärtig noch nicht.

Wird bei der beabsichtigten Datenverarbeitung neue Technologie verwendet oder besteht aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen?

Prüfkriterien der Art 29-Gruppe zur Beurteilung, ob eine Datenverarbeitung wahrscheinlich ein hohes Risiko mit sich bringt (ist speziell beim letzten Aufzählungspunkt von besonderer Bedeutung):

> **Hinweis**:
> Werden zwei der Kriterien erfüllt, ist davon auszugehen, dass ein hohes Risiko mit der Datenverarbeitung einhergeht und eine Datenschutz-Folgenabschätzung durchzuführen ist.

- Bewirkt der Verarbeitungsvorgang ein (potentielles) Bewerten oder Einstufen betroffener Personen (etwa das Erstellen von Profilen und Prognosen), insbesondere auf Grundlage von Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen? Beispiel: Nutzer-Verhaltensprofile oder Marketingprofile durch Website-Analyse-Tools.
- Beinhaltet der Verarbeitungsvorgang eine automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung?
- Beinhaltet der Verarbeitungsvorgang möglicherweise eine systematische Überwachung, d.h. Vorgänge, die die Beobachtung, Überwachung oder Kontrolle betroffener Personen zum Ziel haben?
- Werden vertrauliche Daten oder höchst persönliche Daten verarbeitet? Beispiele: „Sensible Daten“, personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten; aber auch personenbezogene Daten, die mit häuslichen oder privaten Aktivitäten verknüpft sind (z.B. private elektronische Kommunikation), sich auf die Ausübung der Grundrechte auswirken (z.B. das Erfassen der Standortdaten, wodurch eine Verfolgung des Bewegungsverhaltens ermöglicht wird und den Schutz der Privatsphäre berühren kann) oder deren Nutzung möglicherweise ernsthafte Konsequenzen im Alltag der betroffenen Personen haben kann (z.B. Bankdaten, die für den Zahlungsbetrug missbraucht werden könnten)
- Erfolgt eine Datenverarbeitung in großem Umfang?
    - Zahl der betroffenen Personen (entweder konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe)
    - verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente
    - Dauer oder Dauerhaftigkeit der Datenverarbeitung
    - geografisches Ausmaß der Datenverarbeitung
- Beinhaltet die Datenverarbeitung ein (potentielles) Abgleichen oder Zusammenführen von Datensätzen? Beispiel: Zusammenführen von Datensätzen aus unterschiedlichen Anwendungszwecken und dieser Vorgang von den betroffenen Personen vernünftigerweise auch nicht erwartet werden konnte.
- Werden möglicherweise Daten schutzbedürftiger betroffener Personen verarbeitet? Beispiele: Kinder, Personen mit besonderem Schutzbedarf (Patienten, psychisch Kranke, Senioren, Asylbewerber), Arbeitnehmer.
- Beinhaltet der Verarbeitungsvorgang eine innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen? Beispiel: Kombination aus Fingerabdruck- und Gesichtserkennung zum Zweck einer verbesserten Zugangskontrolle.
- Kann die Datenverarbeitung die betroffenen Personen (potentiell) an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern? Beispiel: Durchsuchen von Bonitätsdatenbanken zum Zweck der Entscheidung, ob ein Kredit vergeben wird.

2. Erhebung der zu verarbeitenden personenbezogenen Datenarten (z.B. Namen, Adressen, Kontaktdaten, sensible Daten) und Feststellen der Rechtsgrundlage für die Datenverarbeitung:

Welche Datenarten werden verarbeitet?

Liegt eine Einwilligungserklärung des Betroffenen vor?

Ist die Datenverarbeitung für eine Vertragserfüllung oder die Durchführung vorvertraglicher Maßnahmen erforderlich?

Ist die Datenverarbeitung für die Erfüllung einer rechtlichen Verpflichtung, z.B. aus dem Arbeitsrecht, erforderlich?

Ist die Datenverarbeitung erforderlich, um lebenswichtige Interessen des Betroffenen oder einer anderen natürlichen Person zu schützen?

Ist die Datenverarbeitung für eine Aufgabenerfüllung erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde?

Besteht auf Seiten des Verantwortlichen oder eines Dritten ein berechtigtes Interesse an der Datenverarbeitung, und überwiegen nicht die Interessen oder Grundfreiheiten der betroffenen Person?

3. Werden die folgenden datenschutzrechtlichen Prinzipien eingehalten?

- Transparenz: Werden die Informationspflichten erfüllt?
- Zweckbindungsgrundsatz: Erfolgt die Datenverarbeitung für festgelegte, eindeutige und legitime Zwecke?
- Minimierungs- und Verhältnismäßigkeitsprinzip: Ist die Datenverarbeitung im Verhältnis zur Zweckerreichung angemessen? Beschränkt sich die Datenverarbeitung auf das notwendige Maß und ist sie für die Zweckerreichung erheblich (z.B. in Bezug auf die Datenarten, personellen Zugriff oder die Speicherungsdauer)?
- Wie wird sichergestellt, dass die Daten sachlich richtig und auf dem möglichst neuesten Stand sind?
- Verfügbarkeit, Integrität und Vertraulichkeitsgrundsatz: Welche Maßnahmen zur Datensicherheit wurden getroffen (etwa welchen Beschränkungen unterliegt die Offenbarung der Daten an Personen innerhalb und außerhalb der beteiligten Stellen)?

4. Beschreibung der geplanten Verarbeitungsvorgänge und Verarbeitungszwecke einschließlich der verfolgten berechtigten Interessen (bei der Datenverarbeitung auf Basis der Rechtsgrundlage „Interessenabwägung“) sowie der Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge

5. Welche möglichen Risiken bei der beabsichtigten Datenverarbeitung bestehen für folgende Schutzziele?

- **Datenverfügbarkeit**: Bestehen bei der beabsichtigten Datenverarbeitung Risiken in Bezug auf die Erfüllung der Betroffenenrechte (z.B. Auskunftsrecht, Widerrufsrecht, Widerspruchsrecht, Berichtigungsrecht, Löschungsrecht, Datenübertragbarkeitsrecht, Data breach notification oder bei der Einbindung von Auftragsverarbeitern die vertraglichen Verpflichtungen und die „Zuverlässigkeit“)?
- **Integrität und Vertraulichkeit**: Welche Risiken bestehen durch die beabsichtigte Datenverarbeitung in Bezug auf den Schutz der Privatsphäre des Betroffenen und das Datengeheimnis etwa in Form etwa unbefugter oder unrechtmäßiger Verarbeitung, (unbeabsichtigten) Verlust, (unbeabsichtigter) Zerstörung oder (unbeabsichtigter) Schädigung?
- **Zweckbindung:** Welche Risiken bestehen durch die beabsichtigte Datenverarbeitung in Bezug auf die Einhaltung des Zweckbindungsgrundsatzes? Besteht die Gefahr, dass im Zuge der Datenverarbeitung von der Einhaltung des einmal festgelegten eindeutigen Datenverarbeitungszweckes abgegangen wird?
- **Sonstige Datenschutzprinzipien**: Besteht bei der beabsichtigten Datenverarbeitung das Risiko, dass den sonstigen datenschutzrechtlichen Grundsätzen (z.B. Datenminimierung, Richtigkeit, Speicherbegrenzung, Rechtmäßigkeit, Transparenz) nicht nachgekommen werden kann? Besteht bei der beabsichtigten Datenverarbeitung das Risiko, dass den vorgeschriebenen Informationspflichten nicht nachgekommen werden kann.

6. Auf Basis der Identifizierung möglicher Risiken wird sodann eine Risikoanalyse durchgeführt: Zunächst werden die möglichen Bedrohungen für die Schutzziele festgehalten (Welches Risiko kann von wem ausgehen? Was könnten die Besonderheit und die Schwere der Risiken sein? Was könnten die Motive und Ursachen für die Bedrohung sein? Was könnte das mögliche Bedrohungsziel sein?). In weiterer Folge wird unter Berücksichtigung der Art, des Umfangs, der Umstände, der Zwecke der Verarbeitung und der Ursachen des Risikos die Eintrittswahrscheinlichkeit und die Schwere des Risikos zu beurteilen sein und die daraus folgenden möglichen Folgen einer Risikoverwirklichung für die Betroffenenrechte.

Diese möglichen Risikofolgen könnten beispielsweise sein:

- physischer, materieller und immaterieller Schaden beim Betroffenen
- Verlust der Kontrolle über die Daten
- Einschränkung bei der Erfüllung der Betroffenenrechte
- Diskriminierung
- Identitätsdiebstahl oder -betrug
- finanzielle Verluste
- unbefugte Aufhebung der Pseudonymisierung
- Rufschädigung
- Verlust der Vertraulichkeit (der Privatsphäre)
- erhebliche wirtschaftliche oder gesellschaftliche Nachteile

7. Festhalten der bisher getroffenen Abhilfemaßnahmen (status-quo-Erhebung): z.B. Anonymisierung- oder Pseudonymisierungsmaßnahmen, Einsatz von Verschlüsselungstechnologien etc.

8. Soll-Ist-Vergleich anstellen und Aufstellung eines Maßnahmenplanes zur Gewährleistung der Schutzziele (Datenverfügbarkeit, Integrität und Vertraulichkeit, Zweckbindung und die sonstigen Datenschutzprinzipien): Auf Basis der bisherigen Prüfschritte können allfällige „Lücken" bei der Risikominimierung oder –behebung festgestellt werden und sollte daraus ein entsprechender Maßnahmenplan abgeleitet werden. Dieser Maßnahmenplan könnte beispielsweise nachfolgende Bereiche umfassen:

- **personelle Maßnahmen**: z.B. PC-Benutzungsregelungen, Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten, Einschränkung von Schreib- und Änderungsrechten, dokumentierte Zuweisung von Berechtigungen und Rollen nach dem Erforderlichkeitsprinzip, Verpflichtungserklärungen der Mitarbeiter in Bezug auf die Einhaltung des Datengeheimnisses, Verfahren bei personellen Änderungen, Regelung bei Einsatz von Fremdpersonal, zur Wahrung des Datengeheimnisses, Schulungen, Abwehr von „social engineering-Angriffen" etc.
- **technisch-organisatorische Maßnahmen**: z.B. Änderung des internen Prozessablaufes zur Wahrung der Betroffenenrechte und datenschutzrechtliche Grundsätze (z.B. zur Vermeidung von „Zweck-Verkettungen" oder „Koppelungen" bei Einwilligungserklärungen), etwa durch betriebsinterne Richtlinien, Vertretungsregelungen für abwesende Mitarbeiter, Implementierung automatischer Sperr- und Löschmaßnahmen, Pseudonymisierungen und Anonymisierungen, geregelte Zweckänderungsverfahren, Protokollierung von Zugriffen und Änderungen, Nachweis der Quellen von Daten, Dokumentation von Verträgen (mit Auftragsverarbeitern, Übermittlungsempfängern, Mitarbeitern) etc.
- **Computersicherheit und Virenschutz**: z.B. Regelungen betreffend die Auswahl von Passwörtern, Umgang mit Wechselmedien, Einsatz von mobilen IT-Geräten
- **Netzwerksicherheit**: z.B. Firewalls, Sicherheit von Web-Browsern
- **Datensicherung und Notfallvorsorge**: z.B. die Erstellung eines Datensicherungskonzeptes, Regelung betreffend back-up-Datenträger, Reparatur- und Ausweichprozesse für Notfälle etc.
- **bauliche und infrastrukturelle Maßnahmen**: z.B. Zutrittskontrollen, Zugangsbeschränkungen etc.

Weitere Maßnahmemöglichkeiten, vor allem zum Schutz der Grundprinzipien, können auch dem Standard-

Datenschutzmodell entnommen werden, das von der Art 29-Gruppe ausdrücklich empfohlen wird: Website datenschutzzentrum.de

Bei der Entscheidung, welche konkreten Maßnahmen umgesetzt werden sollen/müssen, ist unter Berücksichtigung

- des Standes der Technik,
- der Implementierungskosten und
- der Art des Umfangs, der Umstände und der Datenverarbeitungszwecke sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Betroffenenrechte

darauf zu achten, dass ein jeweils angemessenes Schutzniveau gewährleistet wird. Es empfiehlt sich daher eine entsprechende Risikoauflistung (z.B. Risikomatrix) zu erstellen und danach Prioritäten bei der Maßnahmenumsetzung zu setzen.

Bleibt in einem Bereich ein hohes Risiko für die Betroffenenrechte bestehen, für das keine Minimierungsmaßnahmen gesetzt werden (können), ist die Datenschutzbehörde zu konsultieren.

9. Konsultation eines allenfalls bestellten betrieblichen Datenschutzbeauftragten

10. Muss der Standpunkt der Betroffenen oder ihrer Vertreter eingeholt werden?

- Gibt es Gründe, warum keine Einholung des Standpunkts der Betroffenen oder ihrer Vertreter erforderlich ist (etwa Unverhältnismäßigkeit, impraktikabel, Gefahr der Verletzung einer Geheimhaltungspflicht etwa bzgl. der Geschäftspläne des Unternehmens)? Wenn es Gründe für einen Verzicht gibt, ist eine Begründung zu dokumentieren.
- Bei Abweichen der endgültigen Entscheidung des Verantwortlichen vom Standpunkt der Betroffenen oder ihrer Vertreter muss eine Begründung dokumentiert werden.