Stand: Dezember 2017

Newsletter EU-Datenschutz-Grundverordnung – Nr. 14

Datenschutz-Folgenabschätzung

Vorbemerkung:
Die Datenschutz-Grundverordnung (DSGVO) regelt die Rahmenbedingungen für Datenschutz und Datensicherheit. Hierbei führt sie für die Verarbeitung von personenbezogenen Daten einen risikobasierten Ansatz ein. Dies bedeutet: Je risikoreicher und schadensgeneigter eine Verarbeitung von Daten für Betroffene sein kann, umso höhere Anforderungen stellt die DSGVO an die Anwendung, Art. 24, 32 DSGVO. Immer dann, wenn eine Datenverarbeitung für die Rechte und Freiheiten einer Person ein hohes oder ein sehr hohes Risiko zur Folge hat, hat der Verantwortliche vor deren Einführung eine sog. Datenschutz-Folgenabschätzung (DSFA) vorzunehmen und zu ermitteln, welche Folgen eine geplante Verarbeitung für den Schutz der Daten Betroffener hätte. Über das Instrumentarium der DSFA sollen Risiken beschrieben, bewertet und reduziert werden.

Lässt sich ein (sehr) hohes Risiko nicht durch angemessene technische und/oder organisatorische Maßnahmen reduzieren, ist für den Einsatz der Anwendung vorab eine Genehmigung der zuständigen Datenschutzaufsichtsbehörde einzuholen.

Eine DSFA ist zu überprüfen und anzupassen, sollten neue Risiken hinzukommen, die bereits behandelte Risiken ändern oder wesentlich erschweren. Über Prüfroutinen kann sichergestellt werden, dass eine DSFA noch aktuell ist.

<u>Behandlung bereits vorhandener Datenverarbeitungen</u>
Für diese gibt es keinen Bestandsschutz, d. h. eine DSFA ist durchzuführen, wenn die Voraussetzungen hierfür vorliegen oder neue Risiken zu einer entsprechenden Wertung führen. Gestützt auf Erwägungsgrund 171 der DS-GVO sehen die Leitlinien zu DSFA der Art.-29-Datenschutzgruppe (Stand: 04.10.2017)* vor, dass eine DSFA nicht durchzuführen ist, wenn eine Datenschutzaufsicht oder ein Datenschutzbeauftragter eine Datenverarbeitung im Wege einer sog. „Vorabkontrolle“ vorab geprüft hat. Derartige Prüf-entscheidungen bleiben in Kraft, bis diese geändert, ersetzt oder aufgehoben sind.

Vorgehensweise

1. Für jede Verarbeitung ist mittels einer systematischen Risikobewertung (sog. „Schwellenwertanalyse“) zu klären, <u>ob</u> eine Datenschutz-Folgenabschätzung durchgeführt werden muss. Das Ergebnis ist zu dokumentieren (z. B. bei der Beschreibung der Verarbeitung im sog. Verzeichnis von Verarbeitungstätigkeiten).
2. Für mehrere ähnliche Verarbeitungsvorgänge (umfasst alle Daten, Systeme [Hard- und Software] und Prozesse) reicht eine Abschätzung, sofern diese ein ähnlich hohes Risiko haben.
3. Vorstufe einer Risikobewertung ist eine Schutzbedarfsfeststellung der zu verarbeitenden personenbezogenen Daten anhand der Datenarten (Kundendaten, Mitarbeiterdaten, Steuerdaten, Gesundheitsdaten etc.):

Schutzbedarfskategorien – Schadensschwere

Schutz-bedarf	Klasse	Erläuterungen Beeinträchtigung des Persönlichkeits-rechts	Beispiele
Normal (Gering o-der mittel)	1	Wäre für Betroffene als tolerabel ein-zustufen. Ein möglicher Datenmiss-brauch hätte nur geringfügige Auswir-kungen (wirtschaftlich/gesellschaftspo-litisch) für Betroffene. • Nicht zur Veröffentlichung be-stimmte Daten • Geringfügige Schäden bei Veröf-fentlichung/Verfälschung	Gering: Öffentliche Register, An-schrift, Kontaktdaten Mittel: Daten über Geschäfts- und Vertragsbeziehungen, Kontostände, Prüfungser-gebnisse, Personaldaten (soweit nicht Stufe 2), Kre-ditauskünfte
hoch	2	Wäre für Betroffene als erheblich ein-zustufen. Ein möglicher Datenmiss-brauch hätte erhebliche Auswirkungen (wirtschaftlich/gesellschaftspolitisch, ggf. Beeinträchtigung der persönlichen Unversehrtheit) für Betroffene. • Sensible Daten • Hohe Folgeschäden bei Veröffentli-chung/Verfälschung	Steuerdaten, strafbare Handlungen; Daten, die ei-nem Berufs-, Geschäfts-, Fernmelde- oder Mandan-tengeheimnis unterliegen; Personaldaten (soweit nicht Stufe 1) wie z. B. Be-urteilungen, berufliche Laufbahn, Angaben über Behinderung etc.
sehr hoch	3	Wäre für Betroffene als besonders be-deutsam und als nicht tolerabel einzu-stufen. Ein möglicher Datenmiss-brauch bedeutet für Betroffene wirt-schaftlichen/gesellschaftspolitischen Ruin oder beeinträchtigt die persönli-che Unversehrtheit gravierend. • Hochsensible Daten • Veröffentlichung/Verfälschung ver-letzt Persönlichkeitsrechte, verur-sacht Schaden an Leib und Leben oder Ansehender Betroffenen	Adressen von polizeilichen V-Leuten, Adressen von Zeugen in bestimmten Strafverfahren

Bestandteile einer Datenschutz-Folgenabschätzung

1. <u>Risikobewertung</u>

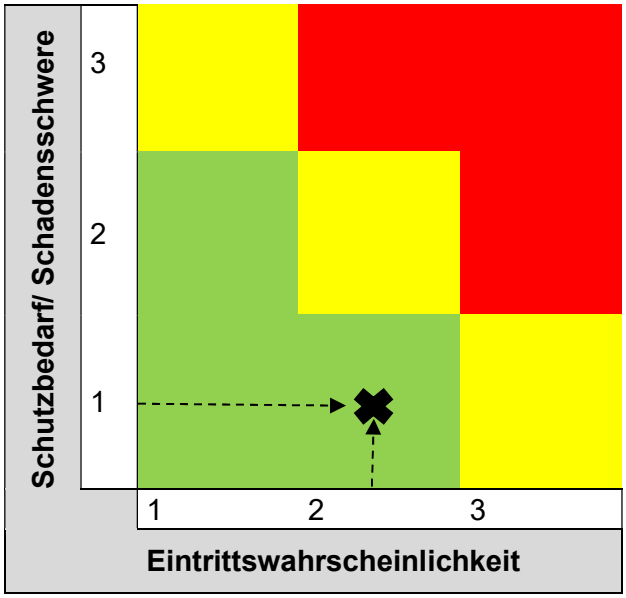
Das Datenschutzrisiko für den Betroffenen, dessen Daten verarbeitet werden (nicht ein Scha-densrisiko für das Unternehmen), ist anhand objektiver Kriterien (Art, Umfang, Umstände und Zwecke einer Verarbeitung) zu bestimmen

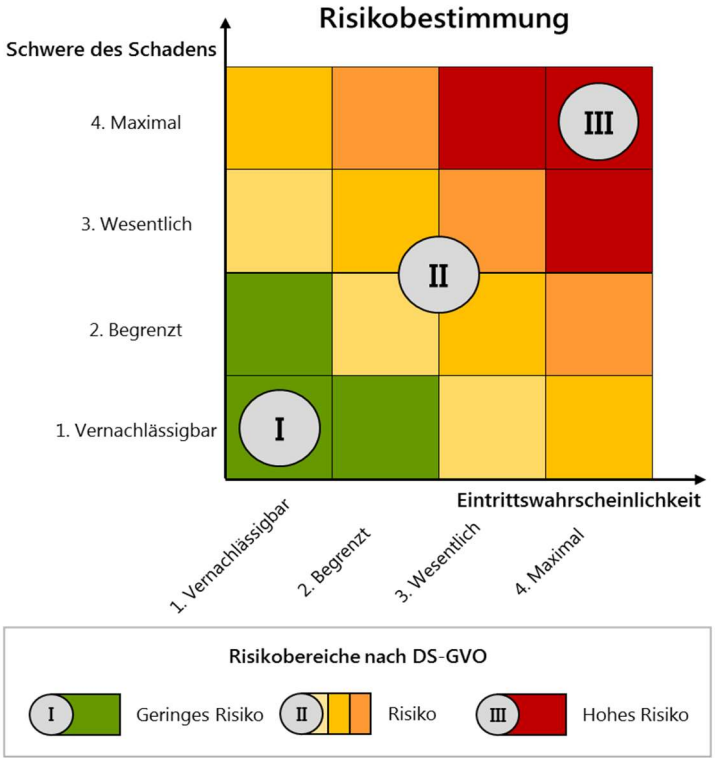
- nach der Eintrittswahrscheinlichkeit (zu berücksichtigen ist hier auch die Risiko-Quelle, also der Angreifer und ein durch diesen zu verursachender Schaden)
- nach der Schwere des Schadens
  - In einer Skalierung
    a) vernachlässigbar/begrenzt ○ (normal)
    b) wesentlich ○ (hoch)
    c) maximal ○ (sehr hoch)

Eine Datenschutz-Folgenabschätzung ist nur durchzuführen, wenn eine Risikobewertung ergibt, dass eine Datenverarbeitung ein hohes oder sehr hohes Risiko (in der Skalierung: ausschließlich die gelben und roten Felder) für die Betroffenen, deren Daten verarbeitet werden, zur Folge hat.
Ergebnis: Hohes Risiko + Sehr hohes Risiko ➔ Datenschutz-Folgenabschätzung

Verfahren zur Risikobestimmung

- Hierfür gibt es *keine einheitliche*, gesetzlich vorgeschriebene Methode. Daher sollte eine Risikobestimmung nach einem gängigen Verfahren (Best Practice: CNIL, ISO) erfolgen wie z. B. nach dem Standard-Datenschutzmodell oder dem Muster einer Datenschutzaufsicht.





Quelle: Bayerisches Landesamt für Datenschutzaufsicht

Praxis-Tipps:
- ✓ EU-weit anerkannte Vorgehensmodelle zur Risikobestimmung einsetzen.
- ✓ Das verwendete Vorgehensmodell muss das Verfahren gut dokumentieren (wichtiges Kriterium für einen massenhaften Einsatz).
- ✓ Maßnahmenkataloge (technisch-organisatorische Maßnahmen zur Verfügbarkeit, Vertraulichkeit, Integrität und Belastbarkeit) zur Behandlung von Risiken sollten gut dokumentiert und erprobt sein.

- Jedoch gibt es *einheitliche Kriterien* für eine Risikobestimmung. Die Art. 29-Datenschutzgruppe hat in den Leitlinien zur DSFA* Kriterien festgelegt, anhand deren geprüft werden sollte, ob eine DSFA durchgeführt werden muss. Dies soll umso wahrscheinlicher sein, wenn mindestens zwei und mehr der nachfolgenden und als besonders riskant eingestuften Kriterien erfüllt sind:

  - Scoring und Evaluierung, inkl. Profilbildung und Vorhersagen
  - Automatisierte Entscheidungen mit rechtlicher oder im Gewicht vergleichbarer Wirkung
  - systematische Beobachtung (z. B. von Arbeitsräumen)
  - Sensible Daten
  - Datenverarbeitung in großem Umfang
  - Datensätze, die abgeglichen oder kombiniert werden
  - Daten von besonders schutzbedürftigen Personen (z. B. Arbeitnehmer, Kinder)
  - Innovative Nutzung oder Verwendung von technologischen und organisatorischen Lösungen (z. B. eine Kombination aus Fingerabdruckscan und Gesichtserkennung)
  - Betroffene können ein Recht oder eine Dienstleistung ohne vorgeschaltete Datenverarbeitung nicht in Anspruch nehmen (z. B.: Eine Bank verlangt die Durchleuchtung von Daten eines potenziellen Kreditkunden vor einer Entscheidung über einen Vertragsabschluss)

2. <u>Schaden</u>

Ein Mensch kann durch eine Datenverarbeitung physische, materielle und immaterielle Schäden erleiden. Bezogen auf die geplante Anwendung ist zu klären, welche Schäden aus der Datenverarbeitung für Betroffene resultieren können.
Beispielhaft nennt die DS-GVO hier

- Diskriminierung
- Identitätsdiebstahl
- Rufschädigung
- Finanzieller Verlust
- Hinderung der Kontrolle über eigene Daten
- Profilbildung mit Standortdaten

3. <u>Risikominimierung</u>

Wer personenbezogene Daten verarbeiten will, ist verpflichtet, im Verhältnis zum Risiko nach dem Stand der Technik angemessene (nicht: neueste und teuerste) Maßnahmen zum Schutz der Daten zu ergreifen, diese regelmäßig, bei Bedarf sogar unverzüglich zu überprüfen und erforderlichenfalls upzudaten. In der Regel handelt es sich um eine Kombination aus

- organisatorischen Maßnahmen (z. B. Datenschutzschulung von Mitarbeitern, interne Regelungen zum Datenschutz, Notfallkonzept) und
- technischen Maßnahmen (z. B. Einsatz von Firewall und Virenscanner und deren zeitgemäßer Update, Verschlüsselung von Daten).

4. Nachweise hierüber erbringen (Dokumentation!)

Die Durchführung einer Datenschutz-Folgenabschätzung ist eine gesetzliche Pflicht. Deren Einhaltung müssen verantwortliche Stellen nachweisen. Der Nachweis ist Bestandteil der Rechenschaftspflicht. Diese verpflichtet verantwortliche Stellen, alle Vorgaben der DS-GVO einzuhalten, wirksam umzusetzen, zu überprüfen und bei Bedarf nachzubessern.

Zu dokumentieren sind:

- die Durchführung einer Risikobewertung,
- das Ergebnis der Analyse (normales, hohes, sehr hohes Risiko) und
- eine daraus ggf. abzuleitende DSFA

    - Ergebnis ➔ keine DSFA, da
        - Whitelist
          Datenschutzaufsichtsbehörden können (optional) eine Liste von Verarbeitungstätigkeiten (sog. Whitelist) veröffentlichen, die aus ihrer Sicht nie hochrisikobehaftet sind und damit keiner DSFA bedürfen.
          Offen ist, ob die Datenschutzaufsichtsbehörden von dieser gesetzlichen Möglichkeit Gebrauch machen werden.
        - Die Verarbeitungsvorgänge vor dem 25.05.2017 von einer Datenschutzaufsichtsbehörde oder einem Datenschutzbeauftragten im Wege einer Vorabkontrolle geprüft worden sind.
        - die Verarbeitung eine gesetzliche Aufgabe nach Art. 6 Abs. 1 c DS-GVO (Erfüllung einer rechtlichen Verpflichtung) oder Art. 6 Abs. 1 e DS-GVO (Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt) ist; eine allgemeine DSFA hierfür ist bereits bei Erlass der Rechtsgrundlage (z. B. Gewerberegister) vorgenommen worden, und der Mitgliedstaat hat die Durchführung einer DSFA für nicht notwendig erklärt.
        - Kein hohes Risiko als Ergebnis der Prüfung.

    - Ergebnis ➔ DSFA, da
        - Blacklist
          Datenschutzaufsichtsbehörden müssen eine sog. Blacklist veröffentlichen. Diese enthält Datenverarbeitungen, die aus Sicht der Datenschutzaufsicht generell ein hohes Risiko haben und daher stets (ohne weitere sonstige Prüfung) vor deren Einsatz eine Vorabkonsultation der Aufsicht erfordern.
        - Ergebnis der Risikobewertung:
          (sehr) hohes Risiko und eine Risikoreduzierung ist nicht möglich.

Führen geeignete technische und/oder organisatorische Maßnahmen dazu, dass für die Daten Betroffener ein (sehr) hohes Risiko in ein normales Risiko reduziert werden kann, ist keine Datenschutz-Folgenabschätzung durchzuführen. So muss ein hoher Schutzbedarf (z. B. biometrische Daten, Personalaktendaten) für sich allein nicht zwingend zu einem hohen Risiko führen, sondern nur dann, wenn gleichzeitig die Eintrittswahrscheinlichkeit für einen Vorfall hoch ist.

Mindestinhalt einer Datenschutz-Folgenabschätzung

Diesen legt die DSGVO wie folgt fest

- Systematische Beschreibung der Verarbeitungsvorgänge und Zwecke
- Notwendigkeit und Verhältnismäßigkeit der Verarbeitung im Verhältnis zum Zweck der Verarbeitung
- Risikobewertung (s. o.)
- Geplante Abhilfemaßnahmen zur Bewältigung der Risiken

➔ Verbleibt ein (sehr) hohes Restrisiko, bedeutet dies Folgendes:

- Der Verantwortliche hat eine Datenschutz-Folgenabschätzung durchzuführen.
- Ferner hat er **vor** einem Einsatz einer derartigen Datenverarbeitung die zuständige Datenschutzaufsichtsbehörde zu konsultieren und
- deren Entscheidung (z. B. Einsatz nur nach Ergreifung weiterer Schutzmaßnahmen, Verbot der geplanten Verarbeitung) zu beachten.

Rolle des Datenschutzbeauftragten
Hat eine verantwortliche Stelle freiwillig oder aufgrund gesetzlicher Vorgabe einen betrieblichen Datenschutzbeauftragten bestellt, so legt die DSGVO bezogen auf Datenschutz-Folgenabschätzungen Folgendes fest:

- Die verantwortliche Stelle hat den Rat des Datenschutzbeauftragten einzuholen.
- Zu den Aufgaben eines Datenschutzbeauftragten gehört auf Anfrage die Beratung im Zusammenhang mit der Durchführung einer DSFA und die Überwachung ihrer Durchführung.

Prozessschritte einer DSFA

1. DSFA-TEAM erstellen
2. Prüfplanung
3. Beurteilungsumfang festlegen
   z. B.
   a. Beschreibung des Verarbeitungsvorgangs
   b. inkl. der Datenflüsse und Zwecke der Verarbeitung in Abgrenzung zu anderen (Geschäfts-)Prozessen
4. Akteure und Betroffene identifizieren
   d. h. Datenschutzbeauftragten, Betriebsrat und ggf. Betroffene einbinden
5. Prüfung der Notwendigkeit/Verhältnismäßigkeit bezogen auf den Verarbeitungszweck
6. Rechtsgrundlagen für die Verarbeitung prüfen und dokumentieren
7. Risikoquellen identifizieren
   (Beweggründe, Ziele, Eintrittswahrscheinlichkeit)
8. Risikobewertung unter Berücksichtigung
   a. möglicher physischer, materieller oder immaterieller Schäden,
   b. deren Schwere sowie
   c. Eintrittswahrscheinlichkeit
9. Auswahl geeigneter Abhilfemaßnahmen
   a. u. a. durch technische und organisatorische Maßnahmen (toMs) und
   b. verbleibende Restrisiken eruieren und dokumentieren
10. DSFA-Bericht erstellen
11. Abhilfemaßnahmen umsetzen
12. Abhilfemaßnahmen auf Wirksamkeit testen
13. Dokumentation
    a. des DSFA-Berichts und
    b. der Überprüfung der Wirksamkeit der Maßnahmen
14. Freigabe der Verarbeitungsvorgänge
    inkl. Überprüfung und Audit einer DSFA und deren Aktualisierung
15. DSFA fortschreiben bei Aktualisierungsbedarf.

Publikationen

- *Artikel-29-Datenschutzgruppe: WP-29- Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“: 17/DE WP 248 rev.01 vom 04.04.2017 (Stand: 04.10.2017)
  http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- Kurzpapier Nr. 5 der Datenschutzkonferenz (DSK) – Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO
  https://www.lda.bayern.de/de/datenschutz_eu.html
- Bitkom e. V., Leitfaden „Risk Assessment & Datenschutz-Folgenabschätzung,
  https://www.bitkom.org/Bitkom/Publikationen/index.jsp
- Internationale Norm: ISO/IEC 29134 (project), Information technology – Security techniques – Privacy impact assessment – Guidelines, International Organization for Standardization (ISO) – enthält Leitlinien für Methodiken zur Durchführung einer DSFA
- Planspiel des ULD Schleswig-Holstein: https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20171106-Planspiel-Datenschutz-Folgenabschaetzung.pdf

Beispiele für EU-weite allgemeine Rahmenbedingungen

- Deutschland: Standard-Datenschutzmodell (SDM)
  https://www.datenschutzzentrum.de/sdm/
- Frankreich: Privacy Impact Assessment (PIA), Commission nationale de línformatique et des libertés (CNIL) – Leitlinien der französischen Datenschutzaufsichtsbehörde,
  https://www.cnil.fr/fr/node/15798

Beispiele für EU-weite branchenspezifische Rahmenbedingungen

- Privacy and Data Protection Impact Assessment Framework for RFID Applications32.[Rahmenvertrag für RFID-Anwendungen für die Datenschutz-Folgenabschätzung zu Methodiken.]
- http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Muster für die Datenschutz-Folgenabschätzung für intelligente Netze und intelligente Messsysteme33
  http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf