Arbeitshilfe Datenschutz-Folgeabschätzung (DSFA)

Eine Datenschutz-Folgeabschätzung (Art. 35 DSGVO) ist kein neues Instrument des Datenschutzes. Sie entspricht der im deutschen Datenschutzrecht verankerten Vorabkontrolle (Art. 4 Abs. 5 BDSG a.F.). Die Datenschutz-Folgeabschätzung dient der Risikobewertung und Feststellung möglicher Folgen durch die Verarbeitung von Daten für die Rechte und Freiheiten des Betroffenen.

Eine DSFA ist immer dann durchzuführen, wenn insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen entsteht. Dieses könnte dann vorliegen, wenn umfangreiche besondere personenbezogene Daten verarbeitet werden. Besondere personenbezogene Daten sind: Ethnische Herkunft, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung natürlicher Personen, Gesundheitsdaten, Daten zum Sexualverhalten oder zur sexuellen Orientierung. Die Verarbeitung dieser Daten ist grundsätzlich untersagt. Ausnahmegründe werden in Art. 9 Abs. 2 lit. a – j DS-GVO genannt. Außerdem ist eine DSFA durchzuführen, wenn die Datenverarbeitung darauf abzielt, systematisch und umfassend die Persönlichkeit des Betroffenen, einschließlich Fähigkeiten, Leistungen oder sein Verhalten zu bewerten.

Die DSFA ist durch die/den Verantwortliche/n unter möglicher zur Hilfenahme der/des Datenschutzbeauftragten zu bewerten. Die Datenschutzbehörden können sogenannte Black- und/oder Whitelists (Negativliste, Positivliste) von Verfahren herausgeben, die eine Datenschutz-Folgeabschätzung ablösen bzw. nicht notwendig machen. Die Bundesdatenschutzbeauftragte hat eine Liste von Verarbeitungsvorgängen nach Art. 35 DS-GVO vorgelegt. Einzelne Landesdatenschutzbeauftragte haben entsprechende Listen von Verarbeitungsvorgängen (Baden-Württemberg, Brandenburg, Bremen, Hamburg bzw. nicht-öffentlicher Bereich, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen bzw. nicht-öffentlicher Bereich, Rheinland-Pfalz bzw. nicht-öffentlicher Bereich, Schleswig-Holstein, Thüringen, Abruf 11.06.2018) vorlegt. Bitte beachten Sie, dass die Aufsichtsbehörden die Listen nicht als abgeschlossen betrachten und somit diese als vorläufig anzusehen sind.

Laut einer ersten Einschätzung der Artikel-29-Datenschutzgruppe[1] haben folgende Kriterien ein hohes Risiko, die Rechte und Freiheiten einer Person zu berühren. Je mehr der Kriterien erfüllt sind, desto höher ist das Risiko, dass die Rechte einer Person eingeschränkt sind und daher eine DSFA notwendig ist. Sind weniger als zwei der Kriterien erfüllt, ist eine DSFA nicht unbedingt notwendig. Für ähnliche Verarbeitungsvorgänge kann eine gemeinsame DSFA erfolgen. Ziel der DSFA ist es, mögliche Risiken zu identifizieren und geeignete Maßnahmen zur Eindämmung der Risiken zu finden. Die Kriterien lauten:

- Scoring/Profiling[2]
- Automatische-Entscheidungen, die zu rechtlichen Folgen für die Betroffenen führen
- Systematische Überwachung
- Besondere personenbezogenen Daten (Art. 9 DS GVO)

[1] Die Artikel-29-Datenschutzgruppe ist ein Beratergremium der Europäischen Union. Die Teilnehmer sind unter anderem Vertreter der jeweiligen nationalen Datenschutzbehörden.

[2] Profiling jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen (aus Art. 4, Ziffer 4, DS-GVO 2018).

- Daten, die in großem Umfang verarbeitet werden (Kriterium: Anzahl der Betroffenen, Menge der Daten). Die Bundesdatenschutzbeauftragte (12.08.2018) hat folgende Auslösegrenze für die Erstellung einer DSFA formuliert: Es werden Daten von 5.000.000 Betroffenen verarbeitet oder es werden Daten von mindestens 40% der betroffenen Personengruppe verarbeitet.
- Zusammenführen/Kombinieren von Daten, die durch unterschiedliche Prozesse gewonnen wurden
- Daten geschäftsunfähiger oder beschränkt geschäftsfähiger Betroffener
- Einsatz neuer Technologien oder biometrischer Verfahren
- Datentransfer in Länder außerhalb der EU/EWR
- Die Datenverarbeitung hindert Betroffene an der Rechtsausübung (Art. 22 DS-GVO sowie Erwägungsgrund 91)[3].

Laut Art. 35 Abs. 7 DS-GVO muss eine DSFA folgende Punkte ansprechen:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Art. 35, Abs. 1 DS-GVO
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird
- den Nachweis erbringen, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird

Erstellung einer Datenschutz-Folgeabschätzung

Eine DSFA für wissenschaftliche Zwecke hat das Ziel, unbekannte Risiken und Eigenschaften einer Untersuchung (Technologiefolgenabschätzung) aufzudecken. Neben Aspekten des Daten- und Privatheitsschutzes werden ethische, ökonomische und Sicherheitsaspekte angesprochen. Da die DSFA zukünftige Risiken anspricht, ist das Vorgehen in etlichen Bereichen spekulativ. Die Erstellung einer DSFA erfolgt in drei Phasen: Vorbereitungs-, Bewertungs- sowie die Berichts- und Maßnahmenphase. Die DSFA ist ein zyklischer Prozess, der überwacht und fortgeschrieben werden muss.

Vorbereitungsphase

- Ist eine Datenschutz-Folgeabschätzung notwendig?
    - Wenn nein, Dokumentation der Entscheidung
    - Wenn ja, Eintritt in die Prüfungsplanung
- Teamzusammenstellung (IT, Datenschutzbeauftragte, Wissenschaftler, eventuell unabhängige und verantwortliche Personen)
- Was wird betrachtet (Systembeschreibung, Identifikation der Daten und Datenflüsse)?
- Wer ist betroffen? Welche Rechtsgrundlagen müssen beachtet werden?
- Dokumentation der Problem- und Aufgabendefinition

[3] Wenn die Kreditwürdigkeit von Kunden einer Bank vor der Vergabe eines Kredits mit Hilfe einer Datenbank geprüft werden (Stichwort: Schufaauskunft).

Was wird betrachtet?

Beschreibung des Prüfgegenstandes, Zweck, Kontext, Daten(-formate) beim Speichern und Transfer (Protokoll), IT-Systeme und deren Schnittstellen, Prozesse (z. B.: Datenübermittlung, Sicherstellen der Datenintegrität, Dokumentation, Behebung von Fehlern, Ansprache & Kontakt) und Funktionsrollen.

Beteiligte Akteure

Jeder der folgenden Gruppen ist zu beschreiben: Hersteller der Daten, Betreiber der Daten als Dienstleister, Mitarbeiter, betroffene Personen, Dritte (zufällig oder absichtlich; Sicherheitsbehörden usw.).

Maßgebliche Rechtsgrundlagen

DS-GVO, lokale gesetzliche Regelungen, AGBs, sonstige Verbraucherrechte, Minderjährigenschutz

Dokumentation

Die Ergebnisse der oben aufgeführten Maßnahmen müssen dokumentiert werden.

Bewertungsphase

- Identifikation von Schutzzielen
- Identifikation möglicher Angreifer, Angriffsmotive, Angriffsziele
- Identifikation von Bewertungskriterien und Bewertungsmaßstäben
- Bewertung des Risikos

Formulierung Schutzziele

Verfügbarkeit, Integrität[4], Vertraulichkeit, Nichtverkettbarkeit, Transparenz, Intervenierbarkeit sind die wesentlichen Schutzziele. Die Schutzziele stehen sich teilweise diametral gegenüber. So kann das Schutzziel Integrität der Daten durch das Schutzziel Intervenierbarkeit beeinträchtigt werden. Es muss eine Abwägung erfolgen, in welchem Umfang ein Schutzziel ein anderes beeinträchtigen darf.

Identifikation möglicher Angreifer

Hier ist die Betroffenenperspektive einzunehmen. Angreifer sind grundsätzlich externe Dritte und nicht interne regelkonform handelnde Nutzer. Als Risiko können alle datenverarbeitenden Organisationen inkl. Behörden oder Unternehmen betrachtet werden. Auch eine Überdehnung des Zweckes durch den Betreiber selbst muss behandelt werden. Man muss davon ausgehen, dass die vorliegenden Daten potenzielles Interesse auslösen. Daher muss überprüft werden, ob staatliche Organisationen, Unternehmen, Gesundheitswesen oder wissenschaftliche Organisationen ein Risiko darstellen.

Identifikation von Bewertungskriterien und –maßstäben

Schon die regelkonforme Datenverarbeitung stellt einen Eingriff in die Grundrechte der Betroffenen (Art. 7 & 8 der EU-Grundrechtecharta) dar. Der „normale“ Schutzbedarf ist also immer gegeben. Man kann drei Arten von Schutzbedarf unterscheiden:

1. Normal: Verarbeitung personenbezogener Daten mit normaler Eingriffsintensität
2. Hoch: Verarbeitung besonderer Arten von personenbezogenen Daten, z. B. Daten, die eine hohe Eingriffsintensität vorweisen (erhebliche Konsequenzen auf Seiten der Betroffenen, keine effektiven Selbstschutzmöglichkeiten auf Seiten der Betroffenen)
3. Sehr hoch: Verarbeitung personenbezogener Daten mit hohem Schutzbedarf; die Betroffenen sind von Entscheidung und Leistungen unmittelbar existenziell abhängig,

[4] Integrität der Daten fordert, dass gespeicherte, personenbezogene Daten nicht durch Fehlfunktionen des Systems oder Benutzereingriffe beschädigt werden können.

zusätzliche Risiken in der Informationssicherheit und unzulässige Zweckänderung durch die Organisation, die die Betroffenen nicht bemerken und/oder ändern können

Es sind Kumulationseffekte der Art möglich, dass getrennte Datenverarbeitungen mit einem normalen Schutzbedarf durch die Art der Verarbeitung zu Daten mit hohem Schutzbedarf werden (z. B. Big Data).

Bewertung des Risikos

Die folgende Aufstellung von Maßnahmen mit Referenzmaßnahmen basiert auf Empfehlungen des Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder. Die Aufstellung umfasst beispielhaft Schutzziele, Komponenten und mögliche Maßnahmen, die auf den unterschiedlichen Ebenen (Daten, System, Prozesse) eingesetzt werden können.

- Datenintegrität: Daten → Hash-Wertvergleich; Systeme → Einschränkung von Schreibrechten usw.; Prozesse → Festlegung von Referenzwerten (min/max usw.)
- Vertraulichkeit: Daten, Systeme → Verschlüsselung; Prozesse → Rechte- und Rollenkonzepte
- Nichtverkettbarkeit: Daten → Anonymisierung/Pseudonymisierung; Systeme → Trennung Daten und Prozesse;
- Transparenz: Daten → Dokumentation, Protokollierung; Systeme → Systemdokumentation, Protokollierung Konfigurationsänderungen, Prozesse → Dokumentation von Verfahren, Protokollierung
- Intervenierbarkeit: Daten → Zugriff auf Daten für den Betroffenen (Auskunft, Berichtigung, Sperrung, Löschung); Prozesse → Ansprechpartner, Helpdesk, Change-Management

Berichts- und Maßnahmenphase

- Identifikation passender Schutzmaßnahmen
- Bewertung der Maßnahmen
- Implementation der Schutzmaßnahmen
- Bericht Datenschutz-Folgeabschätzung
- Veröffentlichung Bericht
- Unabhängige Prüfung des Berichts

Identifikation passender Schutzmaßnahmen usw.

Ein Risiko ist mit dem Hinweis darauf, dass unter Umständen nur wenige betroffen sind, als akzeptabel einzustufen. Der Maßnahmenplan muss darlegen, wie die Grundrechtseingriffe minimiert bzw. vermieden werden sowie wie und wann Schäden durch welche Maßnahmen abgewehrt werden. Die verantwortliche Person für die Implementierung muss benannt werden. Der Erfolg einer Schutzmaßnahme muss bewertet werden. Es muss aufgeführt werden, wer die Bewertung durchführt.

Dokumentation

Der DSFA-Bericht beinhaltet gem. Art. 35 Abs. 7 DSGVO zumindest die systematische Beschreibung der geplanten Verarbeitungsvorgänge und ihrer Zwecke, die Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, die Beschreibung und Beurteilung der Risiken sowie der Abhilfemaßnahmen zur Risikoeindämmung. Die Dokumentation ist um eine Darstellung der Restrisiken samt Entscheidung über den Umgang mit diesen zu ergänzen. Der Abschlussbericht der DSFA dient ferner als Baustein einer umfassenden Dokumentation zur Umsetzung der in Art. 5 Abs. 2 DS-GVO normierten Rechenschaftspflicht. Es ist zu prüfen, inwieweit Teile des DSFA-Berichts im Sinne einer erhöhten Transparenz für die betroffenen Personen veröffentlicht werden sollen.

Unabhängige Prüfung

Die DFSA sollte von unabhängigen Beurteilern (ggf. Datenschutzbehörde) geprüft werden. Dabei sollten Interessenskonflikte angemessen gelöst worden sein, die Interessen der Betroffenen angemessen berücksichtig worden sein, die Öffentlichkeit informiert worden sein und die Schutzmaßnahmen auch tatsächlich implementiert worden sein.

URLs

Listen der Verarbeitungsvorgänge

Bundesbeauftragte für den Datenschutz und Informationsfreiheit

https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_Verarbeitungsvorgaenge.pdf?__blob=publicationFile&v=2

Baden-Württemberg: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorg%C3%A4ngen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf

Brandenburg: http://www.lda.brandenburg.de/media_fast/4055/DSFA_Muss-Liste_allgemein_180525.pdf

Bremen: https://www.datenschutz.bremen.de/

Hamburg: https://datenschutz-hamburg.de/assets/pdf/DSFA Muss-Liste f%C3%BCr den nicht-%C3%B6ffentlicher Bereich-HmbBfDI Version 1.0 (Entwurf).pdf

Mecklenburg-Vorpommern: https://www.datenschutz-mv.de/static/DS/Dateien/DS-GVO/Hilfsmittel zur Umsetzung/Liste von Verarbeitungsvorg%C3%A4ngen nach Art. 35 Abs. 4 DS-GVO/MV_DSFA_Muss-Liste.pdf

Niedersachsen:
http://www.lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/liste_von_verarbeitungsvorgaengen_nach_art_35_abs_4_dsgvo/liste-von-verarbeitungsvorgaengen-nach-art-35-abs-4-ds-gvo-164661.html

Nordrhein-Westfalen: https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Liste-Art-35-4-NRW-OeB_v1.pdf

https://www.ldi.nrw.de/mainmenu_Aktuelles/submenu_EU-Datenschutzreform/Inhalt/EU-Datenschutzreform/Liste-Art-35-4-NRW-NOeB_v1_.pdf

Rheinland-Pfalz:
https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_OE.pdf

https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSFA_-_Muss-Liste_RLP_NOE.pdf

Schleswig-Holstein:
https://datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf

Thüringen: https://www.tlfdi.de/mam/tlfdi/datenschutz/liste_der_verarbeitungstatigkeiten.pdf

Weitere Links

Arbeitskreises Technik der Datenschutzbeauftragten des Bundes und der Länder:
https://www.forum-privatheit.de/forum-privatheit-de/aktuelles/aktuelles/aktuelles_047.php

Artikel-29-Datenschutzgruppe: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

DS-GVO: https://dsgvo-gesetz.de/