Template zur Dokumentation von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO

Version zum RC06 vom 12. Oktober 2023

Inhalt

1 Vorwort

Liebe Nutzer:innen des Templates zur Dokumentation von Datenschutz-Folgenabschätzungen nach Art. 35 DSGVO,

Sie möchten oder müssen eine Datenschutz-Folgenabschätzung (DS-FA) für Ihr Projekt erstellen. Grundsätzlich ist die DS-FA immer dann durchzuführen, wenn eine geplante Datenverarbeitung vorliegt und dies voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Darüber hinaus ist sie zwingend durchzuführen, wenn eines der in Art. 35 EU-DSGVO in Abs. 3 bestimmten Regelbeispiele vorliegt. Hierzu gehört insbesondere die umfangreiche Verarbeitung von Gesundheitsdaten.

Diese Datei soll Sie beim Erstellen einer Risiko- und Schutzbedarfsanalyse der Datenschutz-Folgenabschätzung (DS-FA) für Ihr Projekt unterstützen. Machen Sie sich bitte zuerst mit den einzelnen Tabellenblättern und deren Inhalt vertraut und gehen Sie dann zur Erstellung der Risiko- und Schutzbedarfsanalyse mit Hilfe des Prozess-Templates über.

Die Erstellung der Risiko- und Schutzbedarfsanalyse erfolgt schrittweise und für jeden einzelnen Prozessschritt mit Hilfe einer Kopie des Prozess-Templates. Die Gesamtauflistung aller Prozessschritte wird abschließend im Tabellenblatt "Übersicht" zusammenfassend dargestellt und kann in das Datenschutzkonzept integriert bzw. diesem beigefügt werden. Grundsätzlich sind gelb markierte Felder/Zellen von Ihnen auszufüllen. Bitte denken Sie daran, das Prozess-Template vor der Bearbeitung zu kopieren, um die Vorlage zu erhalten.

Hinweis: Bitte lesen Sie vor dem Start noch die folgenden Abschnitte mit einer Beschreibung der einzelnen Tabellenblätter und der Vorgehensweise bei der Erstellung einer Risiko- und Schutzbedarfsanalyse im Rahmen einer DS-FA durch.

2 Aufbau des Templates

Im Folgenden sind die Bezeichnungen der Tabellenblätter im Template aufgeführt sowie deren Funktion und Inhalt erklärt.

2.1 Metadaten

Tabellenblatt zur Erfassung der Metadaten (Projektname, Datum, Version usw.) zu dieser Risiko-Analyse. Die Daten werden an relevanten Stellen in anderen Blättern eingeblendet.

2.2 Übersicht

Zusammenfassung und Darstellung aller beschriebenen Prozessschritte zum Einfügen in oder Anhängen an das Datenschutzkonzept. Hier werden übersichtlich die Prozessschritte, die dazugehörige(n) Gefährdung(en), sowie das Risiko vor und nach der Maßnahmenfestlegung dargestellt.

2.3 Projektstruktur

Dieses Tabellenblatt spiegelt Ihre projektspezifische Struktur wider. Die Inhalte sind dann in den Kopien des Prozess-Templates als Dropdown auswählbar. Bitte geben Sie dazu oben in Zelle E1 die Bezeichnung der ersten Gliederungsebene für Ihre Prozessbetrachtung bzw. die Strukturkategorie an (z.B. Standort, Szenario, Institution oder Verantwortungsbereich o.ä.). Ausgehend davon können Sie die Bezeichner innerhalb dieser ersten Gliederungsebene ab Zelle A2 nach rechts eingeben (z.B. Klinik, Treuhänder, Forschungsbank). In den Zeilen unterhalb der Bezeichner auf erster Gliederungsebene werden die jeweiligen Prozessschritte notiert, die für die Risiko-Analyse relevant erscheinen. Zum Beispiel könnte die Überschrift der ersten Gliederungsebene (Zelle E1) mit "Stelle" bezeichnet werden, ein Bezeichner innerhalb dieser Gliederungsebene könnte dann "Studienzentrum" sein (Zelle A2) und ein im Studienzentrum relevanter Prozess (Zelle A3) könnte die "Datenerhebung" sein.

2.4 Gefährdungen

Liste der Gefährdungen (bzw. Risiken) mit den dazugehörigen Risikoquellen und das dadurch gefährdete Gewährleistungsziel. Zu jeder Gefährdung und den Risikoquellen "interne menschliche Quelle", "externe menschliche Quelle" und "nichtmenschliche Quelle" sind Beispiele gelistet, die selbstständig angepasst bzw. auch gekürzt oder ergänzt werden können. Bitte dazu direkt die vorgesehenen Zellen bearbeiten (Farbcode beachten).

2.5 Maßnahmen

Dieses Tabellenblatt spiegelt Ihre projektspezifische Struktur wider. Die Inhalte sind dann in den Kopien des Prozess-Templates als Dropdown auswählbar. Bitte geben Sie dazu oben in

Zelle E1 die Bezeichnung der ersten Gliederungsebene für Ihre Prozessbetrachtung bzw. die Strukturkategorie an (z.B. Standort, Szenario, Institution oder Verantwortungsbereich o.ä.). Ausgehend davon können Sie die Bezeichner innerhalb dieser ersten Gliederungsebene ab Zelle A2 nach rechts eingeben (z.B. Klinik, Treuhänder, Forschungsbank). In den Zeilen unterhalb der Bezeichner auf erster Gliederungsebene werden die jeweiligen Prozessschritte notiert, die für die Risiko-Analyse relevant erscheinen. Zum Beispiel könnte die Überschrift der ersten Gliederungsebene (Zelle E1) mit "Stelle" bezeichnet werden, ein Bezeichner innerhalb dieser Gliederungsebene könnte dann "Studienzentrum" sein (Zelle A2) und ein im Studienzentrum relevanter Prozess (Zelle A3) könnte die "Datenerhebung" sein.

2.6 Gewährleistungsziele

Liste der Gewährleistungsziele mit einer jeweiligen Erläuterung und der Verankerung in verschiedenen Referenzen.

2.7 Risikoberechnung

Registerblatt mit einer Risikomatrix und den Risikokategorien nach einer Dokumentation zur Risiko-Analyse und Datenschutz-Folgenabschätzung des Bayerischen Landesbeauftragten für den Datenschutz. Ergänzend sind Listen für die Arbeit mit dieser Datei aufgeführt (Vgl. Abschnitte 4 - 6).

2.8 Prozess-Template

Mit Kopien dieses Arbeitsblatts erstellen Sie schrittweise die Risiko- und Schutzbedarfsanalyse. Erstellen Sie je Prozessschritt durch Kopieren ein neues Arbeitsblatt und legen per Dropdown-Menü die Zuordnung zu einem Bereich o.ä. und dem relevanten Prozess fest. Bitte benennen Sie die Kopie gleich sinnvoll um. Da bei der Bearbeitung viele Arbeitsblätter entstehen, ist eine strukturierte und kurze Benennung der Registerblätter erforderlich.

Zusätzlich sind sowohl Tabellenblätter als auch darin enthaltene Zellen durch einen Farbcode gekennzeichnet, der die Bearbeitung der Risiko- und Schutzbedarfsanalyse unterstützt:

grau	Alle Registerblätter ohne Eingabefelder sind farblich grau gekennzeichnet. Diese Registerblätter dienen der Unterstützung beim Erstellen und Bearbeiten der DS-FA.
gelb	Alle Registerblätter mit Eingabefeldern sind gelb gekennzeichnet. Die Registerblätter sind zum Bearbeiten und/oder Ergänzen. Die Registerblätter Gefährdungen und Maßnahmen können sich nach Bedarf ergänzen. Tragen Sie dazu Ihre Maßnahmen oder Gefährdungen in den gelb hinterlegten Feldern ein.

3 Vorgehensweise bei der Erstellung Ihrer Risiko- und Schutzbedarfsanalyse

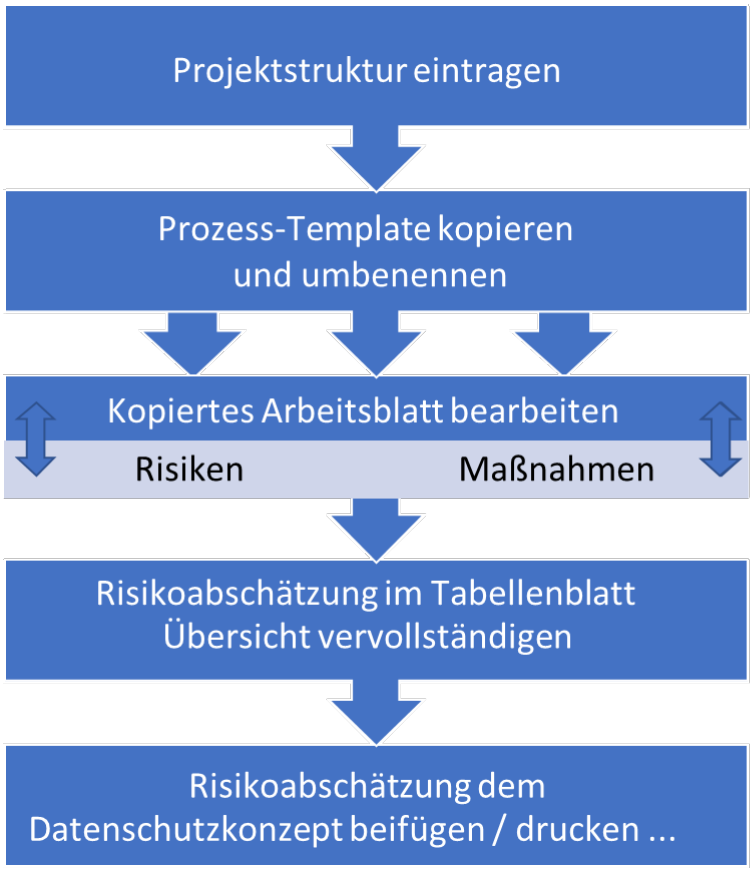

Abbildung 1: Schema der Erstellung einer Risiko- und Schutzbedarfsanalyse mittels Template

1. Bitte beschreiben Sie zuerst Ihre Projektstruktur in dem gleichnamigen Tabellenblatt.
2. Bitte prüfen Sie die Risiken- und Maßnahmenvorschläge in den Tabellenblättern Risiken und Maßnahmen ergänzen Sie diese bei Bedarf (siehe Beschreibungen zu Risiken und Maßnahmen)
3. Kopieren Sie nun bitte das Prozess-Template und benennen Sie es spezifisch. Da jedes Projekt typischerweise mehrere Stellen oder Bereiche umfasst und diesen jeweils mehrere Prozesse und diesen wiederum mehrere Gefährdungen zugeordnet sein können, werden Sie viele Tabellenblätter erzeugen. Legen Sie sich deshalb ein Benennungssystem mit Kürzeln oder Nummern für jede Stelle bzw. jeden Bereich sowie jeden Prozess zu. Wenn Sie je Prozess aufgrund vielfältiger Gefährdungen mehrere Arbeitsblätter benötigen, fügen Sie den Namen der Arbeitsblätter jeweils am Ende eine fortlaufende Zahl an.
4. Bearbeiten Sie die korrekt benannte Kopie des Prozess-Templates.

a. Wählen Sie zuerst die betroffene Stelle oder den betroffenen Bereich mit Hilfe des Dropdown-Menüs aus.
b. Wählen Sie anschließend den Prozessschritt und die zu beschreibende(n) Gefährdung(en) aus.
c. Nun wählen Sie bitte die hierdurch betroffenen Gewährleistungsziele aus. (Mehrfachnennung möglich)
d. Anschließend geben Sie bitte die potentielle(n) Risikoquelle(n) zu den Gefährdung(en) an. Nach Eingabe von Gefährdung und Risikoquelle, werden Ihnen Beispiele hierzu im mittleren Bereich angezeigt.
e. Wählen Sie bitte nun die Eintrittswahrscheinlichkeit und den Schweregrad vor Anwendung der geplanten Maßnahmen aus.
f. Wird Ihnen ein geringes oder tragbares Risiko angezeigt, so besteht kein weiterer Handlungsbedarf. Besteht ein hohes Risiko, müssen Sie Maßnahmen zur Risikominimierung ergreifen.
g. Im unteren Abschnitt können Sie geeignete Maßnahmen per Dropdown-Menü auswählen. Auch selbst hinzugefügte Maßnahmen sind auswählbar (siehe Beschreibung des Arbeitsblatts 'Maßnahmen').
h. Wählen Sie nun bitte die von Ihnen geschätzte Eintrittswahrscheinlichkeit und den Schweregrad zu den Gefährdungen nach Anwendung der Maßnahmen aus im oberen rechten Bereich aus.
i. Besteht NACH der Maßnahmenergreifung immer noch ein hohes Risiko, so müssen Sie entweder weitere Maßnahmen implementieren und hier zuordnen oder nach Art. 36 Absatz 1 DSGVO die zuständige Datenschutzbehörde konsultieren!

5. Sie können nun anderen Gefährdungen für diesen Prozessschritt beschreiben und anschließend mit weiteren Prozessschritten fortfahren. Wiederholen Sie dafür bitte die Schritte 3 bis 4 bis alle Gefährdungen in Ihrem Projekt identifiziert und beschrieben sind.
6. Im Tabellenblatt 'Übersicht' wird Ihnen eine Übersicht aller erarbeiteten Tabellenblätter mit Angabe des Prozessschrittes, der Gefährdung sowie der Risikobewertung VOR und NACH den ergriffenen Maßnahmen angezeigt. Dazu tragen Sie bitte in Spalte A die Bezeichnung der von Ihnen erarbeiteten Tabellenblätter ein. Die restlichen Spalten werden automatisch befüllt. Diese Übersicht können Sie dem Datenschutzkonzept beifügen. Bei Bedarf kann diese auch gedruckt werden.

4 Hilfestellungen zur Abschätzung des Schweregrads des Schadens

Die Schwere eines möglichen Schadens muss in jedem Einzelfall insbesondere unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung bestimmt werden (ErwGr. 76) / (Kurzpapier Nr. 18, DSK, 2018[1]). Im Folgenden finden Sie hilfreiche Beispiele mit Angabe der entsprechenden Quelle, die Ihnen die Einschätzung erleichtern können.

4.1.1 Wesentliche Faktoren (Kurzpapier Nr. 18, DSK, 2018):

- Verarbeitung besonders geschützter Daten im Sinne von Art. 9 und 10 DSGVO; z.B. Gesundheitsdaten
- Verarbeitung von Daten schützenswerter Personengruppen (z.B. Beschäftigte, Kinder)
- Verarbeitung nicht veränderbarer und eindeutig identifizierenden Daten (z.B. IDAT)
- Automatisierte Verarbeitungen, die eine systematische und umfassende Bewertung persönlicher Aspekte (z. B. Profiling) beinhalten
- Schaden ist nicht oder kaum reversibel
- Verarbeitung zur Ermöglichung einer systematischen Überwachung
- Anzahl der betroffenen Personen, die Anzahl der Datensätze, und die Anzahl der Merkmale in einem Datensatz

[1] https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf, Zugriff: 10.10.2023

Tabelle 1: Möglicher Grad der Schwere/des Schadens gemäß „Der Bayerische Landesbeauftragte für den Datenschutz: Risikoanalyse und Datenschutz-Folgenabschätzung. Systematik, Anforderungen, Beispiele.“ 2022. Version 1.0 (vergl. S. 23)[2]

Grad	**Bezeichnung des Grads**	**Schwere der Folgen / möglicher Schaden**	
		Beschreibung	**Beispiel**
1	geringfügig	Betroffene erleiden eventuell Unannehmlichkeiten, die sie aber mit einigen Problemen überwinden können	**immateriell**: leichte Verärgerung **materiell**: Zeitverlust **physisch**: vorübergehende Kopfschmerzen
2	überschaubar	Betroffene erleiden eventuell signifikante Unannehmlichkeiten, die sie aber mit einigen Schwierigkeiten überwinden können.	**immateriell**: geringe, aber objektiv nachweisbare psychische Beschwerden **materiell**: deutlich spürbarer Verlust an privatem Komfort **physisch**: minderschwere körperliche Schäden (z.B. leichte Krankheit)
3	substanziell	Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	**immateriell**: schwere psychische Beschwerden **materiell**: finanzielle Schwierigkeiten **physisch**: schwere körperliche Beschwerden
4	groß	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.	**immateriell**: dauerhafte, schwere psychische Beschwerden **materiell**: erhebliche Schulden **physisch**: dauerhafte, schwere körperliche Beschwerden

[2] https://www.datenschutz-bayern.de/dsfa/OH_Risiko.pdf, Zugriff: 06.10.2023

Tabelle 2: Übertragung der Schwere des möglichen Schadens auf das niedersächsische Schutzstufenkonzept (Quelle: „Die Landesbeauftragte für den Datenschutz Niedersachsen - Schutzstufenkonzept der LfD Niedersachsen“ Oktober 2018)[3]

Schutzstufe	**Personenbezogene Daten,**	**zum Beispiel**	**Schwere eines möglichen Schadens**
A	die von den Betroffenen freizugänglich gemacht wurden.	Telefonverzeichnis, Wahlvorschlagsverzeichnisse, eigene freizugänglich gemachte Webseite; frei zugängliche soziale Medien	geringfügig
B	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht; nicht frei zugängliche soziale Medien	
C	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen”).	Einkommen, Grundsteuer, Ordnungswidrigkeiten	überschaubar
D	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz”).	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Arbeitszeugnisse, **Gesundheitsdaten**, Schulden, Pfändungen, Sozialdaten, Daten besonderer Kategorien nach Art. 9 DSGVO	**substantiell**
E	deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, Zeugenschutzprogramm	groß

[3] https://lfd.niedersachsen.de/startseite/themen/technik_und_organisation/schutzstufen/schutzstufen-56140.html, Zugriff: 06.10.2023

5 Hilfestellungen zur Abschätzung der Eintrittswahrscheinlichkeit

Tabelle 3: Möglicher Grad der Eintrittswahrscheinlichkeit gemäß „Der Bayerische Landesbeauftragte für den Datenschutz: Risikoanalyse und Datenschutz-Folgenabschätzung. Systematik, Anforderungen, Beispiele.“ 2022. Version 1.0 (vergl. S. 23)

Grad	**Bezeichnung des Grads**	**Eintrittswahrscheinlichkeit**	
		Beschreibung	**Beispiel**
1	geringfügig	Schaden kann nach derzeitigem Erwartungshorizont nicht eintreten.	Befall durch Schadsoftware bei einem Stand-Alone-Rechner, der an keinem Netzwerk angeschlossen ist und an dem keine weiteren Medien angeschlossen werden können.
2	überschaubar	Schaden kann zwar eintreten, aus bislang gemachten Erfahrungen bzw. aufgrund der gegebenen Umstände scheint der Eintritt aber unwahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und nur mit einem BSI zertifizierten Firmennetzwerk verbunden ist.
3	substanziell	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände zwar möglich, aber nicht sehr wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem Rechner, der aktuell gehalten, mit aktueller Antivirensoftware ausgestattet und direkt mit dem Internet verbunden ist.
4	groß	Schadenseintritt scheint auf Basis bislang gemachter Erfahrungen bzw. aufgrund der gegebenen Umstände möglich und wahrscheinlich zu sein.	Befall durch Schadsoftware bei einem veralteten Windows-XP-Rechner ohne Antivirensoftware, der direkt mit dem Internet verbunden ist.

6 Risikomatrix zur Berechnung der Risikokategorie nach Eintrittswahrscheinlichkeit und Schwere des Schadens

Schwere des Schadens					
	groß	tragbares Risiko	tragbares Risiko	hohes Risiko	hohes Risiko
	substanziell	tragbares Risiko	tragbares Risiko	tragbares Risiko	hohes Risiko
	überschaubar	geringes Risiko	tragbares Risiko	tragbares Risiko	tragbares Risiko
	geringfügig	geringes Risiko	geringes Risiko	tragbares Risiko	tragbares Risiko
		geringfügig	überschaubar	substanziell	groß
		Eintrittswahrscheinlichkeit			

Abbildung 2: Risikomatrix zur Berechnung der Risikokategorie nach Eintrittswahrscheinlichkeit und Schwere des Schadens modifiziert nach „Der Bayerische Landesbeauftragte für den Datenschutz: Risikoanalyse und Datenschutz-Folgenabschätzung. Systematik, Anforderungen, Beispiele.“ 2022. Version 1.0 (vergl. S. 24)

7 Glossar

BSI Bundesamt für Sicherheit in der Informationstechnik (www.bsi.de)

DS Datenschutz

DSGVO Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung (Verordnung 2016/679)

DSK Datenschutzkonferenz – Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (www.datenschutzkonferenz-online.de)

EG Europäische Gemeinschaft

ErwGr Erwägungsgrund der EU-DSGVO (Auflistung: https://dsgvo-gesetz.de/erwaegungsgruende/)

EU-DSGVO Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG – Datenschutz-Grundverordnung (Verordnung 2016/679)

IDAT Identifizierende Daten (eines Patienten)

LfD Landesbeauftragte(r) für den Datenschutz