



Leitfaden zur Datenschutz-Folgenabschätzung (DSFA-Leitfaden)

30. November 2023 (Stand am 1. Januar 2026)

Inhaltsverzeichnis

1	Empfänger des Leitfadens	2
2	Schritte zur Durchführung einer DSFA.....	2
2.1	Wer muss eine DSFA durchführen?	2
2.2	Wann muss eine DSFA durchgeführt werden?.....	3
2.3	Wann muss der EDÖB konsultiert werden?.....	4
2.4	In welcher Form und wie lange muss die DSFA aufbewahrt werden?	5
2.5	Muss die DSFA veröffentlicht werden?.....	5
3	Inhalt der DSFA	5
3.1	Vorbemerkungen: Grundlagen der DSFA und Methodik.....	5
3.2	Allgemeine Angaben	6
3.3	Beschreibung der geplanten Bearbeitung von Personendaten	7
3.4	Bewertung der Risiken für die Grundrechte der betroffenen Person.....	9
3.5	Identifizierung von Massnahmen, die zum Schutz der Grundrechte der betroffenen Person vorgesehen sind.....	13
3.6	Bewertung der Auswirkungen der vorgesehenen Massnahmen zur Einschätzung des Restrisikos.....	15
3.7	Konsultation des EDÖB bei hohem Restrisiko.....	16
3.8	Zusammenfassung und Ergebnisse der DSFA.....	17
Anhang: Checkliste zum Inhalt der DSFA		18
Erster Teil: Allgemeine Angaben		18
Zweiter Teil: Beschreibung der vorgesehenen Bearbeitung von Personendaten		18
Dritter Teil: Bewertung der Risiken für die Grundrechte der betroffenen Person.....		19
Vierter Teil: Identifizierung der vorgesehenen Massnahmen zum Schutz der Grundrechte der betroffenen Person.....		19
Fünfter Teil: Bewertung der Auswirkungen der vorgesehenen Massnahmen zur Beurteilung des Restrisikos.....		19
Sechster Teil: Zusammenfassung und Ergebnisse der DSFA		20

1 Empfänger des Leitfadens

Der DSFA-Leitfaden richtet sich in erster Linie an diejenigen Einheiten der zentralen Bundesverwaltung¹, die eine Datenschutz-Folgenabschätzung (DSFA) im Sinne von Artikel 22 des Bundesgesetzes vom 25. September 2020 über den Datenschutz (DSG)² und der Richtlinien des Bundesrates für die Risikoprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung (DSFA-Richtlinien)³ durchführen müssen.

Die Einheiten der dezentralen Bundesverwaltung⁴ sowie Personen, die mit öffentlichen Aufgaben des Bundes betraut sind, unterliegen zwar nicht den DSFA-Richtlinien, müssen aber dennoch das Datenschutzgesetz einhalten, da sie als Bundesorgane⁵ betrachtet werden. Diese verschiedenen Organe müssen daher eine DSFA durchführen, wenn die Bedingungen von Art. 22 DSG erfüllt sind. Dabei steht es ihnen frei, die Vorgaben der DSFA-Richtlinien und die begleitenden Instrumente wie diesen Leitfaden zu verwenden.

Mit der DSFA kann auch nachgewiesen werden, dass die geplante Bearbeitung von Personendaten im Einklang mit dem Datenschutzrecht (*privacy by design*)⁶ erfolgt. Zudem ermöglicht sie den Verantwortlichen zu überprüfen, ob die von ihnen bearbeiteten Daten den Datenschutzanforderungen entsprechen.

Abgrenzung zum Merkblatt zur Datenschutz-Folgenabschätzung (DSFA) nach den Art. 22 und 23 DSG des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten: Der DSFA-Leitfaden des BJ bezieht sich nur auf die Durchführung der Datenschutz-Folgenabschätzung durch die zentrale Bundesverwaltung. Hingegen richtet sich das [Merkblatt des EDÖB](#) in erster Linie an private Datenbearbeitungsverantwortliche, wobei es auch als Auslegungshilfe durch die Bundesorgane beigezogen werden kann.

2 Schritte zur Durchführung einer DSFA

2.1 Wer muss eine DSFA durchführen?

Das Gesetz besagt lediglich, dass der Verantwortliche eine DSFA erstellt. Bei der verantwortlichen Verwaltungseinheit handelt es sich gemäss Art. 5 Bst. j um diejenige Einheit, die allein oder zusammen mit anderen über den Zweck und die Mittel der Bearbeitung entscheidet. Die verantwortliche Verwaltungseinheit muss sicherstellen, dass die DSFA durchgeführt wird; sie ist aber nicht verpflichtet, die DSFA selbst durchzuführen.

Es ist wichtig, darauf hinzuweisen, dass die Durchführung einer DSFA spezifische Kenntnisse in verschiedenen Bereichen (Recht, Informatik usw.) erfordert. Daher sollte eine DSFA idealerweise

¹ Im Sinne von Art. 7 der Regierungs- und Verwaltungsorganisationsverordnung (RVOV, SR 172.010.1). Im Rahmen des Datenschutzrechts gelten diese Einheiten als Bundesorgane (siehe Art. 5 Bst. i DSG, der ein Bundesorgan als «Behörde oder Dienststelle des Bundes oder Person, die mit öffentlichen Aufgaben des Bundes betraut ist» definiert, SR 235.1).

² SR 235.1

³ BBI 2023 1882

⁴ Im Sinne von Art. 7a RVOV

⁵ Siehe Art. 5 Bst. i DSG

⁶ Art. 7 Abs. 1 und 2 DSG

von einem interdisziplinären Team durchgeführt werden, das über Kompetenzen in den Bereichen Datenschutz, Risikoidentifizierung sowie IT-Prozesse und -Systeme verfügt.

Ausserdem berät die Datenschutzberaterin oder der Datenschutzberater der Verwaltungseinheit den Verantwortlichen und überprüft die Durchführung der DSFA⁷. Für eine bessere Berücksichtigung des Datenschutzrechts ist es wichtig, dass die Datenschutzberaterin oder der Datenschutzberater während des gesamten Prozesses einbezogen wird. Zudem gilt zu beachten, dass er bzw. sie diese Funktion unabhängig von der verantwortlichen Verwaltungseinheit ausüben können muss, ohne Weisungen von dieser zu erhalten⁸.

Selbst wenn ein Verantwortlicher später beabsichtigt, die Bearbeitung von Personendaten an einen Auftragsbearbeiter zu übertragen, bleibt er für die Durchführung der DSFA verantwortlich.

Es ist zu präzisieren, dass eine DSFA auch dann durchgeführt werden muss, wenn beispielsweise ein Gesetzesentwurf die Datenbearbeitung durch Dritte regelt: Dabei wird insbesondere auf die Datenbearbeitung durch dem Bund nahestehenden Unternehmen im Rahmen einer Konzession Bezug genommen (z. B. Post, SBB, Swisscom, Skyguide). In diesem Zusammenhang obliegt es konkret der zuständigen Verwaltungseinheit, den Dritten zur Durchführung einer DSFA aufzufordern. Die verantwortliche Verwaltungseinheit sorgt somit für die Durchführung der DSFA und fügt deren Ergebnisse den Unterlagen für die Ämterkonsultation bei.

2.2 Wann muss eine DSFA durchgeführt werden?

Eine DSFA muss durchgeführt werden, wenn ein hohes Risiko für die Grundrechte einer betroffenen Person besteht. Um festzustellen, ob ein hohes Risiko besteht, sollte das vom Bundesamt für Justiz entwickelte [Instrument für die Risikoprüfung](#) herangezogen werden, in dem die wichtigsten Risikofaktoren aufgeführt sind.

Im Gegensatz zu privaten Verantwortlichen sieht Art. 22 DSG für Verwaltungseinheiten keine Ausnahmen vor, in denen von der Durchführung einer DSFA abgesehen werden kann. Ergibt sich aus dem Instrument für die Risikoprüfung, dass ein hohes Risiko für die Grundrechte der betroffenen Person vorliegt, so muss eine DSFA durchgeführt werden. Für mehrere ähnliche geplante Bearbeitungsvorgänge enthält Art. 22 Abs. 1 DSG die Möglichkeit, eine gemeinsame Datenschutz-Folgenabschätzung zu erstellen.

Art. 22 Abs. 1 DSG verlangt, dass die DSFA «vorgängig» erstellt werden muss. Dies bedeutet, dass die Risikoprüfung und die DSFA vor Beginn einer Bearbeitung von Personendaten durchgeführt werden müssen. Die DSFA wird idealerweise so früh wie möglich erstellt, auch wenn noch nicht alle Parameter der Bearbeitung von Personendaten bekannt sind.

Die DSFA sollte durchgeführt werden, sobald die verantwortliche Verwaltungseinheit eine neue Datenbearbeitung plant. Bei einer geplanten Bearbeitung von Personendaten kann es einerseits um die Einführung einer neuen Bearbeitung von Personendaten gehen. Andererseits kann es sich dabei auch um die Anpassung einer laufenden Bearbeitung von Personendaten handeln. Für Bearbeitungen, die bereits vor dem Inkrafttreten des neuen DSG im Gange sind, ist Art. 69 DSG einschlägig: Die Bestimmung sieht vor, dass für laufende Bearbeitungen nur dann eine

⁷ Art. 26 Abs. 2, Bst. a Ziff. 2 der Datenschutzverordnung (DSV), SR 235.11

⁸ Art. 26 Abs. 1 Bst. b DSV

Datenschutz-Folgenabschätzung erstellt werden muss, wenn sich der Bearbeitungszweck ändert oder wenn neue Kategorien von Daten beschafft werden.

Die Erstellung der DSFA ist somit Teil eines iterativen Prozesses. Die Analyse muss parallel zur Ausarbeitung der Rechtsgrundlage für die Datenbearbeitung erfolgen und im Laufe der Konkretisierung des Bearbeitungsprojekts angepasst werden (z. B. bei der Ausarbeitung einer Verordnung oder der Einrichtung von Systemen oder Datenregistern). Gemäss den geltenden Verfahren wird eine erste Fassung den Unterlagen für die Ämterkonsultation beigelegt und je nach Kontext dem EDÖB vorgelegt. Anschliessend muss die DSFA regelmässig aktualisiert werden, indem die vorherige Fassung ergänzt wird (wobei jedes Mal das Datum der neuen Fassung anzugeben ist), wenn neue Elemente hinzukommen.

Koordination mit dem Rechtsetzungsverfahren (Ziff. 4 DSFA-Richtlinien): Ist für die Datenbearbeitung eine neue Rechtsgrundlage oder die Anpassung einer bestehenden Rechtsgrundlage erforderlich, muss die DSFA vor der Erarbeitung oder Änderung der Rechtsgrundlage durchgeführt werden, da die Ergebnisse der DSFA den Unterlagen zur Ämterkonsultation beigelegt werden müssen. Wenn sich die Notwendigkeit einer DSFA oder einer Anpassung erst nach der Eröffnung der Ämterkonsultation herausgestellt hat, werden die Ergebnisse der DSFA den Unterlagen zur nachfolgenden Ämterkonsultation oder zum Mitberichtsverfahren beigelegt.

Koordination mit der Projektmanagementmethode HERMES⁹ (Ziff. 5 DSFA-Richtlinien): Erfolgt die Datenbearbeitung im Rahmen eines HERMES-Projekts, beginnt die Durchführung der DSFA in der Phase der Lösungsentstehung. Der Begriff der Lösungsentstehung bezieht sich sowohl auf die Anwendung der klassischen Methode als auch auf die Anwendung der agilen Methode. Ausserdem erlaubt es HERMES, dass weitere Methoden zur Anwendung gelangen. Allerdings wird auch in diesem Fall der Rahmen durch HERMES vorgegeben. Bei der Anwendung der klassischen Methode handelt es sich bei der Phase der Lösungsentstehung um die Phase des Konzepts. Kommt die agile Methode zur Anwendung, so muss die DSFA im Rahmen der Umsetzung durchgeführt werden. Idealerweise erfolgt die DSFA in diesem Fall zeitgleich wie das ISDS-Konzept.

2.3 Wann muss der EDÖB konsultiert werden?

Wenn die DSFA ergibt, dass die geplante Datenbearbeitung trotz der von der verantwortlichen Verwaltungseinheit vorgesehenen Massnahmen weiterhin ein hohes Risiko für die Grundrechte der betroffenen Person darstellt (zur Definition eines hohen Restrisikos siehe Kapitel 3.4.2 und 3.6), muss diese vor den EDÖB konsultieren.

Es ist zu beachten, dass die Konsultation des EDÖB einige Zeit in Anspruch nehmen kann. Die Übermittlung eines vollständigen Dossiers trägt daher zur Optimierung der Effizienz des Verfahrens bei. Der Leitfaden behandelt diese Fragen ausführlicher in Kapitel 3.7.

Im Falle einer Koordinierung mit dem Rechtsetzungsverfahren muss der EDÖB vor der Ämterkonsultation konsultiert werden (siehe Kasten oben).

⁹ www.hermes.admin.ch

2.4 In welcher Form und wie lange muss die DSFA aufbewahrt werden?

Das DSG und die Datenschutzverordnung (DSV)¹⁰ machen keine Vorgaben zur Form der DSFA. Vielmehr liegt es wie bei anderen Instrumenten des DSG und der DSV im Ermessen der verantwortlichen Verwaltungseinheit, in welcher Form sie die DSFA speichert. Wichtig ist allerdings, dass die verantwortliche Verwaltungseinheit den Nachweis erbringen kann, dass sie die DSFA durchgeführt hat. Ausserdem muss sie in der Lage sein, die DSFA nötigenfalls dem EDÖB vorzulegen und die Resultate der DSFA im Rahmen der Ämterkonsultation als Unterlage beizulegen. Hierfür muss die DSFA bzw. deren Resultate in einem gängigen Format lesbar sein.

Für die Aufbewahrung der DSFA bestimmt Art. 14 DSV, dass die verantwortliche Verwaltungseinheit die DSFA nach Beendigung der Datenbearbeitung mindestens zwei Jahren aufbewahren muss.

2.5 Muss die DSFA veröffentlicht werden?

Im DSG oder der DSV gibt es keine Pflicht, die DSFA zu veröffentlichen, da sie auch heikle Daten enthalten kann. Eine Veröffentlichung der DSFA ist aber mit Blick auf die Stärkung des Schutzes der Grundrechte der betroffenen Person, welches gerade das Ziel einer DSFA ist, in Betracht zu ziehen. So führt die Veröffentlichung zu einer erhöhten Transparenz bezüglich der Bearbeitung von Personendaten. Ausserdem wird dadurch das Vertrauen zwischen den betroffenen Personen und den Verantwortlichen gestärkt. Die Veröffentlichung liegt im Ermessen der verantwortlichen Verwaltungseinheit.

Im Übrigen gelten die Vorgaben des Öffentlichkeitsgesetzes¹¹ auch für die DSFA.

Koordination mit dem Rechtsetzungsverfahren (Ziff. 4 DSFA-Richtlinien) : Erfolgt die Durchführung der DSFA im Rahmen eines Rechtsetzungsverfahrens, sind die Ergebnisse¹² der DSFA den Unterlagen zur Ämterkonsultation beizulegen. Zudem informiert die verantwortliche Verwaltungseinheit (Departement oder BK) über die Ergebnisse der DSFA insbesondere im Antrag an den Bundesrat, im erläuternden Bericht, in der Botschaft, sowie in den Abstimmungserläuterungen.

3 Inhalt der DSFA

3.1 Vorbemerkungen: Grundlagen der DSFA und Methodik

Artikel 22 Absatz 3 DSG sieht Folgendes vor: «Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte».

Ziffer 3 Abs. 1 der DSFA-Richtlinien besagt zudem Folgendes: «Die DSFA besteht aus den folgenden Schritten:

¹⁰ SR 235.11

¹¹ SR 152.3

¹² Siehe nachstehende Ziffer 3.8 bezüglich der Ergebnisse der DSFA.

- a. Beschreibung der geplanten Datenbearbeitung;
- b. Bewertung der Risiken für die Grundrechte der betroffenen Person;
- c. Identifizierung der Massnahmen zum Schutz der Grundrechte;
- d. Bewertung der Auswirkungen der vorgesehenen Massnahmen, um zu beurteilen, ob ein hohes Restrisiko besteht.»

Die von der verantwortlichen Verwaltungseinheit durchgeführte DSFA muss mindestens die vier oben genannten Punkte abdecken.

Koordination mit der Projektmanagementmethode HERMES (Ziff. 5 DSFA-Richtlinien): Bei der Anwendung der Projektmanagementmethode HERMES erfolgen gewisse Teile der DSFA im Rahmen von HERMES: So sind die Rechtsgrundlageanalyse und die Instrumente, die bei Vorliegen eines erhöhten Schutzbedarfs erstellt werden,¹³ Bestandteil der DSFA.

3.2 Allgemeine Angaben

Die allgemeinen Angaben der DSFA beziehen sich im Wesentlichen auf die gleichen Bestandteile wie diejenigen im ersten Teil des [Instruments für die Risikoprüfung](#).

Sie müssen namentlich Informationen über die verantwortliche Verwaltungseinheit sowie über die Kontaktperson innerhalb dieser Einheit enthalten.

Die allgemeinen Angaben müssen auch die bestehenden oder geplanten Rechtsgrundlagen für die geplante Bearbeitung darlegen. Diese Analyse zeigt auf, ob und welche Rechtsgrundlagen bestehen, geschaffen oder angepasst werden müssen.¹⁴ Gegebenenfalls muss die verantwortliche Verwaltungseinheit die bestehenden Rechtsgrundlagen mit den geplanten Rechtsgrundlagen vergleichen (Ist-/Soll-Vergleich).

Koordination mit der Projektmanagementmethode HERMES (Ziff. 5 DSFA-Richtlinien): Bei der Anwendung der Projektmanagementmethode HERMES können die Ausführungen zu den bestehenden und vorgesehenen Rechtsgrundlagen aus der Rechtsgrundlageanalyse übernommen werden. Es muss sichergestellt werden, dass die Rechtsgrundlageanalyse noch aktuell ist.

Zudem ist in diesem Teil der Datenschutzberaterin oder des Datenschutzberaters der verantwortlichen Verwaltungseinheit anzugeben, und ob diese Person im Zusammenhang mit der DSFA konsultiert wurde.

Koordination mit dem Rechtsetzungsverfahren (Ziff. 4 DSFA-Richtlinien): In den allgemeinen Angaben muss die Verwaltungseinheit angeben, ob die DSFA im Rahmen eines Rechtsetzungsverfahrens, insbesondere im Rahmen einer Verordnungs- oder Gesetzesrevision erfolgt. Für die Koordination mit dem Rechtsetzungsverfahren sind die Vorgaben der Richtlinien des Bundesrats für die Risikoprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung zu beachten.

¹³ www.ncsc.admin.ch > Dokumentation > Informatiksicherheitsvorgaben Bund > Sicherheitsverfahren > Erhöhter Schutz

¹⁴ Die Analyse kann entsprechend der Rechtsgrundlageanalyse nach HERMES erfolgen: www.hermes.admin.ch

Koordination mit der Projektmanagementmethode HERMES (Ziff. 5 DSFA-Richtlinien): Bei den allgemeinen Angaben muss aufgeführt werden, ob die DSFA im Rahmen der Anwendung von HERMES erfolgt oder nicht. Die Koordination mit HERMES wird in den Richtlinien des Bundesrats für die Risikoprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung geregelt.

Übersicht über die allgemeinen Angaben

Verantwortliche Verwaltungseinheit(en)	
Kontaktperson (Name, Vorname, Tel., E-Mail)	
Bestehende oder vorgesehene Rechtsgrundlagen	
Datenschutzberaterin oder Datenschutzberater (Name, Vorname, Tel, E-Mail)	
Koordination mit dem Rechtssetzungsverfahren	Ja <input type="checkbox"/> Nein <input type="checkbox"/>
Anwendung von HERMES	Ja <input type="checkbox"/> Nein <input type="checkbox"/>

3.3 Beschreibung der geplanten Bearbeitung von Personendaten

Zunächst ist die geplante Bearbeitung zu beschreiben (Art. 22 Abs. 3 DSG). Im Allgemeinen bezieht sich der Teil der DSFA, der sich auf die Beschreibung der geplanten Bearbeitung von Personendaten bezieht, auf dieselben Bestandteile wie der zweite Teil des [Instruments für die Risikoprüfung](#) (mit der Überschrift «Angaben zur Datenbearbeitung»).

Diese Beschreibung umfasst die Art, den Umfang und den Zweck der Bearbeitung sowie die Umstände, unter denen sie stattfindet (Art. 22 Abs. 2 DSG). Die verantwortliche Verwaltungseinheit führt aus, wer welche Daten zu welchem Zweck wie bearbeitet. Bei der Erweiterung und Weiterentwicklungen von bestehenden Systemen und Anwendungen hat die Beschreibung der geplanten Bearbeitung auch einen Vergleich der bisherigen mit der geplanten Bearbeitung zu beinhalten (Ist-/Soll-Zustand).

Die detaillierte Beschreibung der geplanten Bearbeitung bildet die Grundlage für die nachfolgende Risikobewertung (vgl. Ziff. 3.4). Beim Eintreten eines Informationssicherheitsrisikos hat beispielsweise die geplante Bearbeitung von besonders schützenswerten Daten schwerwiegendere Auswirkungen für die betroffenen Person als die Bearbeitung von nicht besonders schützenswerten Personendaten.

Die verantwortliche Verwaltungseinheit muss angeben, wer die Daten bearbeitet. Es ist insbesondere darzulegen, ob mehrere Verantwortliche¹⁵ bestehen oder ob ein Auftragsbearbeiter¹⁶ eingesetzt werden soll.

Weiter muss ausgeführt werden, welche Art von Daten bearbeitet werden. Bei den Kategorien der Daten ist insbesondere anzugeben, ob und inwieweit die Bearbeitung Personendaten¹⁷ und

¹⁵ Art. 5 lit. j DSG definiert den Begriff des Verantwortlichen.

¹⁶ Art. 5 lit. k DSG definiert den Begriff des Auftragsbearbeiters.

¹⁷ Art. 5 Bst. a DSG enthält eine Umschreibung des Begriffs der Personendaten.

besonders schützenswerte Personendaten¹⁸ betrifft. Dabei muss auch angegeben werden, in welcher Form die Daten vorliegen (z.B. Schrift, Ton, Bild). Auch die Kategorien der betroffenen Personen (z. B. Angestellte, Versicherte) sind zu umschreiben. Dabei ist insbesondere zu berücksichtigen, ob Daten von besonders schutzbedürftigen Personen (z.B. Personen mit einer körperlichen oder psychischen Beeinträchtigung, Minderjährige, Seniorinnen und Senioren) bearbeitet werden und ob sich daraus ein besonderer Schutzbedarf aufgrund der Schutzbedürftigkeit dieser Personen ergeben kann.

Die Angaben umfassen auch eine Umschreibung der Art der Bearbeitung. Hier muss die verantwortliche Verwaltungseinheit darlegen, welche Art von Bearbeitung sie auszuführen gedenkt und wie die Bearbeitung(en) erfolgen soll(en). Dazu gehören zum Beispiel folgende Bearbeitungen: Beschaffung, Speicherung, Aufbewahrung, Verwendung, Veränderung, Bekanntgabe, Archivierung, Löschung oder Vernichtung von Daten.¹⁹ So ist zum Beispiel darzulegen, ob die Personendaten verdeckt (d.h. ohne Wissen der betroffenen Person) beschafft werden²⁰, ob die Personendaten mit Daten aus anderen Datenbanken zusammengeführt oder abgeglichen werden²¹ und ob und wie die Personendaten Dritten bekanntgegeben werden (z.B. über ein Abrufverfahren bzw. einen Online-Zugriff²² oder ins Ausland²³). Aus der Umschreibung muss erkennbar sein, ob ein Profiling bzw. ein Profiling mit hohem Risiko²⁴ geplant ist oder ob automatisierte Einzelentscheidungen²⁵ erfolgen. Die verantwortliche Verwaltungseinheit muss angeben, ob die Bearbeitung eine Überwachung von Personen beinhaltet.²⁶

Es muss umschrieben werden, mit welchen Technologien die Datenbearbeitung erfolgt. Es ist auszuführen, wie die Bearbeitung in technischer Hinsicht umgesetzt werden soll (z.B. Software, Netzwerk). Dabei ist auch zu berücksichtigen, ob die Datenbearbeitung auf neuen Technologien, basiert oder ob Technologien zur Anwendung gelangen, die zwar nicht neu sind, aber die mit Risiken für die Grundrechte der betroffenen Person verbunden sind oder deren Auswirkungen auf die Grundrechte der betroffenen Person nicht abgeschätzt werden können, wie z.B. der Anwendung künstlicher Intelligenz.²⁷

Der Umfang der Bearbeitung ist näher zu bestimmen. Aus den Angaben muss ersichtlich werden, ob eine grosse Menge von Daten bearbeitet werden, ob eine grosse Anzahl von Personen betroffen sind und ob die Bearbeitung in zeitlicher oder in räumlicher Hinsicht umfangreich ist.²⁸ In zeitlicher Hinsicht muss angegeben werden, wie lange die Personendaten bearbeitet und aufbewahrt werden. Für die Frage, ob eine Bearbeitung von Personendaten umfangreich ist, kann das Kriterium, ob es sich bei der Bearbeitung von Personendaten um die Haupttätigkeit der verantwortlichen Verwaltungseinheit handelt, mitberücksichtigt werden. Dieses Kriterium ist aber für sich allein

¹⁸ Art. 5 Bst. c DSGVO enthält eine abschliessende Liste von besonders schützenswerten Personendaten. Für Beispiele siehe das [Instrument für die Risikoprüfung](#).

¹⁹ Art. 5 Bst. d DSGVO

²⁰ Für Beispiele siehe das [Instrument für die Risikoprüfung](#).

²¹ Für ein Beispiel siehe das [Instrument für die Risikoprüfung](#).

²² Beim Abrufverfahren bzw. Online-Zugriff handelt es sich um eine spezifische Form der Bekanntgabe. Der Datenempfänger kann sich dabei selbstständig Zugriff auf Personendaten verschaffen, ohne dass der Verantwortliche tätig werden muss (Prinzip der Selbstbedienung).

²³ Art. 16 ff. DSGVO

²⁴ Art. 5 Bst. f und g enthalten die Begriffsdefinitionen des Profiling und des Profiling mit hohem Risiko. Für Beispiele siehe das [Instrument für die Risikoprüfung](#).

²⁵ Art. 21 Abs. 1 DSGVO umschreibt den Begriff der automatisierten Einzelentscheidung. Für Beispiele siehe das [Instrument für die Risikoprüfung](#).

²⁶ Für Beispiele siehe das [Instrument für die Risikoprüfung](#).

²⁷ Für weitere Beispiele siehe das [Instrument für die Risikoprüfung](#).

²⁸ Für Beispiele siehe das [Instrument für die Risikoprüfung](#).

nicht ausschlaggebend, sondern muss im Zusammenhang mit den anderen Kriterien betrachtet werden, um darauf zu schliessen, ob eine umfangreiche Bearbeitung vorliegt oder nicht.²⁹

Weiter muss die Umschreibung auch die Zwecke der Bearbeitung umfassen. Es ist anzugeben, zu welchen Zwecken die Personendaten beschafft und bearbeitet werden.

3.4 Bewertung der Risiken für die Grundrechte der betroffenen Person

Generell ist der Teil der DSFA über die Bewertung der Risiken für die Grundrechte der betroffenen Person mit dem dritten Teil des [Instruments für die Risikoprüfung](#) (mit der Überschrift «Gesamtbewertung des hohen Risikos») verknüpft. Diese Angaben können zwar hilfreich sein, sind jedoch nicht ausreichend. In der DSFA müssen die Risiken identifiziert werden, wobei für jedes Risiko zusätzlich die Eintrittswahrscheinlichkeit des Risikos sowie die Auswirkungen des Risikos auf die Grundrechte der betroffenen Person bestimmt werden muss. Für den Schweregrad bzw. die Auswirkungen des Risikos auf die Grundrechte der betroffenen Person können die im Instrument für die Risikoprüfung ermittelten Risikofaktoren ein Indiz sein.

3.4.1 Identifizierung der Risiken

Der Begriff des Risikos bezieht sich auf ein mögliches Ereignis, das Auswirkungen auf die Grundrechte der betroffenen Person hat oder haben kann. In der Risikobewertung wird beurteilt, mit welcher Wahrscheinlichkeit ein Risiko auftritt und welche Auswirkungen es für die betroffene Person hat bzw. haben kann. Zunächst müssen die möglichen Risiken einer geplanten Bearbeitung von Personendaten identifiziert werden.

Es gibt unterschiedliche Arten von Risiken. **Informationssicherheitsrisiken** stehen im Zusammenhang mit der Datensicherheit.

Beispiele (vgl. auch die Liste der Risiken in der detaillierten Risikoanalyse zum ISDS-Konzept³⁰):

- Verletzung der Integrität von Personendaten z.B. durch Manipulation oder Fehler im System
- Verletzung der Vertraulichkeit z.B. durch Schwachstellen im System, missbräuchliche Verwendung der Informationen oder ein Angriff auf das System
- Verletzung der Verfügbarkeit z.B. durch Ausfall der Systeme, Verlust der Informationen oder Ransomware
- Verletzung der Nachvollziehbarkeit z.B. durch Fälschung oder Verlust der Protokolle.

Datenschutzrisiken beziehen sich auf die einzelnen Datenbearbeitungsvorgänge. Sie gehen über die Datensicherheit hinaus.

Beispiele:

- unrechtmässige Beschaffung und Bearbeitung von Personendaten
- Verwendung von Personendaten zu nicht vorgesehenen Zwecken

²⁹ Für Beispiele siehe das [Instrument für die Risikoprüfung](#).

³⁰ Die Vorlage für die detaillierte Risikoanalyse zum ISDS-Konzept ist unter folgender Webseite abrufbar: www.ncsc.admin.ch > Dokumentation > Informatiksicherheitsvorgaben Bund > Sicherheitsverfahren > Erhöhter Schutz.

- Bearbeitung von inkorrekten Daten
- unbefugter Zugriff auf Personendaten
- übermässig lange Aufbewahrung von Personendaten
- Verweigerung der Rechte der betroffenen Personen

Die Identifizierung der Risiken hängt von den Umständen des Einzelfalls ab. So ist für jede geplante Bearbeitung separat zu untersuchen, welche Risiken bestehen bzw. bestehen könnten. Passend zu den jeweiligen Risiken werden mögliche Szenarien umschrieben. So ist beim Risiko eines unbefugten Zugriffs auf Personendaten denkbar, dass interne Mitarbeitende auf Personendaten zugreifen, die sie nicht zur Erfüllung ihrer Aufgaben benötigen. Gleichzeitig ist auch vorstellbar, dass externe Personen widerrechtlich auf Personendaten zugreifen (z.B. im Rahmen eines Hackerangriffs) (siehe die Beispielstabelle unten Kapitel 3.4.2).

Wichtig ist bei der Identifizierung der Risiken, dass die Risiken so definiert werden, dass sie in Bezug auf den Schutz von Personendaten auch relevant sind. Es sollen keine abstrakten Risiken aufgeführt werden, die lediglich indirekt einen Einfluss auf den Schutz von Personendaten haben (z.B. Erdbeben).

Ausserdem ist darauf hinzuweisen, dass bei der Identifizierung möglicher Risiken die vorgesehenen Massnahmen keine Rolle spielen. Beispielsweise ist die Regelung von Zugriffsberechtigung nicht im Rahmen der Identifizierung der Risiken zu berücksichtigen; sie kommt vielmehr erst dann zum Zug, wenn sich aus der Risikobewertung ergibt, dass Massnahmen vorgesehen werden müssen, um unbefugte Zugriffe zu verhindern.

Koordination mit der Projektmanagementmethode HERMES (Ziff. 5 DSFA-Richtlinien):

Ergibt die Schutzbedarfsanalyse einen erhöhten Schutzbedarf, so muss eine detaillierte Risikoanalyse zum ISDS-Konzept erstellt werden. Im Rahmen dieser Risikoanalyse werden die Informationssicherheitsrisiken identifiziert und bewertet. Das ISDS-Konzept bildet integraler Bestandteil der DSFA. Die Datenschutzrisiken müssen entweder separat oder im Rahmen des ISDS-Konzepts identifiziert und bewertet werden.

3.4.2 Risikobewertung

Im Rahmen der Risikobewertung wird beurteilt, mit welcher Wahrscheinlichkeit die identifizierten Risiken auftreten und welche Auswirkungen sie auf die Grundrechte der betroffenen Person haben bzw. haben können.

Die Risikobewertung kann mit Hilfe der 6 x 6- Risikomatrix, die auch im Rahmen der detaillierten Risikoanalyse zum ISDS-Konzept zur Anwendung gelangt,³¹ erfolgen.

³¹ Die Vorlage für die detaillierte Risikoanalyse zum ISDS-Konzept ist unter folgender Webseite abrufbar: www.ncsc.admin.ch > Dokumentation > Informatiksicherheitsvorgaben Bund > Sicherheitsverfahren > Erhöhter Schutz.

Auswirkungen	sehr hoch 6						
	hoch 5						
	wesentlich 4						
	moderat 3						
	gering 2						
	sehr gering 1						
		sehr unwahr- scheinlich 1	unwahr- scheinlich 2	selten 3	möglich 4	wahr- scheinlich 5	sehr wahr- scheinlich 6
		Eintrittswahrscheinlichkeit					

Bei den Auswirkungen kann es sich um physische Auswirkungen (z.B. eine fehlerhafte medizinische Behandlung aufgrund fehlerhafter Daten), materielle Auswirkungen (z.B. Verlust der Arbeitsstelle, Missbrauch der Kreditkarte, Erhebung ungerechtfertigter Gebühren) oder immaterielle Auswirkungen (Diskriminierungen, u.a. Rassismus, Sexismus, gesellschaftliche Nachteile, Stigmatisierung wegen Krankheit) handeln. Die Auswirkungen auf die Grundrechte der betroffenen Person oder der Schweregrad der Risiken können in sechs Stufen eingeteilt werden: sehr gering, gering, moderat, wesentlich, hoch oder sehr hoch. Die Stufen können wie folgt umschrieben werden.

- sehr gering: keine Auswirkung auf die Grundrechte; keine merklichen moralischen oder sozialen Verletzungen; kein adäquat kausaler finanzieller Schaden. z.B. geringfügige Überschreitung der zulässigen Aufbewahrungsdauer von Personendaten; unerwünschte Telefonanrufe oder Nachrichten ohne direkte oder indirekte Folgen.
- gering: vernachlässigbare Auswirkung auf die Grundrechte; kaum merkliche moralische oder soziale Verletzungen; evtl. adäquat kausaler minimaler finanzieller Schaden. z.B. Notwendigkeit, das eigene Internetkonto, die E-Mail-Adresse oder die Telefonnummer zu ändern.
- moderat: geringfügige langfristige oder schwerwiegende kurzfristige Auswirkung auf die Grundrechte; geringe psychische, moralische oder soziale Verletzungen; evtl. adäquat kausal finanzieller Schaden. z.B. intransparente, unzulässige Beeinflussung des Kaufverhaltens.
- wesentlich oder hoch³²: schwerwiegende langfristige Auswirkung auf die Grundrechte; mittelschwere physische, psychische, moralische oder soziale Verletzungen;

³² Die Nuancen zwischen diesen beiden Kategorien sind schwer zu bestimmen und hängen vom Einzelfall ab.

substanzieller adäquat kausal finanzieller Schaden. z.B. Verweigerung/Auflösung eines Vertragsverhältnisses; Reputationsschäden.

- sehr hoch: fatale Auswirkung auf die Grundrechte; schwerwiegende physische, psychische, moralische oder soziale Verletzungen; existenzgefährdender adäquat kausal finanzieller Schaden, z.B. folgenschwere falsche medizinische Behandlung aufgrund unrichtiger Patienteninformationen oder Patientenidentifikation; Risiko der grenzüberschreitenden Verfolgung aufgrund von persönlichen in den Herkunftsstaat gelangenden Daten von Asylsuchenden, mit Auswirkungen auf die betroffene Person oder ihre Familie (körperliche Unversehrtheit, Leben usw.).

Die Eintrittswahrscheinlichkeit ist eine Schätzung der Wahrscheinlichkeit für das Eintreten eines bestimmten Ereignisses in einem bestimmten Zeitraum in der Zukunft. Sie ist auch in sechs Stufen einzuteilen: sehr unwahrscheinlich, unwahrscheinlich, selten, möglich, wahrscheinlich, sehr wahrscheinlich. Bei der Beurteilung der Wahrscheinlichkeit kann die Legende, die im Rahmen der detaillierten Risikoanalyse zum ISDS-Konzept zur Anwendung gelangt,³³ herangezogen werden. Demnach ist die Wahrscheinlichkeit nach dem nachfolgenden Massstab zu bemessen.

- sehr unwahrscheinlich: über 10 Jahren
- unwahrscheinlich: alle 5-10 Jahre
- selten: alle 3-5 Jahre
- möglich: alle 2-3 Jahre
- wahrscheinlich: alle 1-2 Jahre
- sehr wahrscheinlich: mehrmals pro Jahr

Bei der Risikobewertung besteht die Schwierigkeit, die Risiken verlässlich einzuschätzen. Zum einen gibt es hier die Schwierigkeit, die Eintrittswahrscheinlichkeit der Risiken im Voraus einzuordnen, weil nicht vorhersehbar ist, ob und wann mit dem Eintritt eines Risikos zu rechnen ist. Zum anderen ist es unter Umständen schwierig, die Auswirkungen eines Risikos abzuschätzen. Im Fall eines unbefugten Zugriffs ist es denkbar, dass mit Mühe vorhergesagt werden kann, was mit den Personendaten passiert und welche Auswirkungen dies auf die Grundrechte der betroffenen Person hat. Trotz dieser Schwierigkeiten ist es dennoch von zentraler Bedeutung, die möglichen Risiken so gut wie möglich zu bestimmen, um in einem zweiten Schritt Massnahmen in Betracht ziehen zu können, mit denen die Grundrechte der betroffenen Personen am besten geschützt werden können.

Die grafische Darstellung in Form einer Risikomatrix ermöglicht es der für die Datenbearbeitung verantwortlichen Stelle, nicht erhöhte Risiken in grün von erhöhten Risiken in gelb oder rot zu unterscheiden:

- Risiken in grün in der Matrix können als akzeptabel angesehen werden, d. h. die Restrisiken sind zulässig, ohne dass Massnahmen ergriffen werden müssen.
- Gelb oder rot markierte Risiken in der Matrix sind als hoch einzustufen, d. h. für jedes identifizierte Risiko sind Massnahmen erforderlich, damit diese hohen Risiken so weit wie möglich zu grünen Risiken werden.

³³ Die Vorlage für die detaillierte Risikoanalyse zum ISDS-Konzept ist unter folgender Webseite abrufbar: www.ncsc.admin.ch > Dokumentation > Informatiksicherheitsvorgaben Bund > Sicherheitsverfahren > Erhöhter Schutz.

Bei der Anwendung von HERMES (siehe Kästchen oben, 3.4.1): Da die Informationssicherheitsrisiken bereits im Rahmen der detaillierten Risikoanalyse zum ISDS-Konzept identifiziert und bewertet werden, müssen einzig die Datenschutzrisiken noch entweder separat oder im Rahmen des ISDS-Konzepts identifiziert und bewertet werden. Bei den Informationssicherheitsrisiken ist zusätzlich sicherzustellen, dass sie auch bezüglich der Auswirkungen, die sie auf die Grundrechte der betroffenen Person haben, bewertet werden.

Beispiel (abstraktes Beispiel, muss im konkreten Fall präzisiert werden):

Szenario	Risiko	Eintrittswahrscheinlichkeit	Auswirkungen für die betroffene Person
interner Zugriff: mehrere Personen sind an der Bearbeitung von Personendaten beteiligt	unbefugter Zugriff auf die Personendaten	intern: schwierig zu bestimmen. Kann rechtskonformes Verhalten vermutet werden? Ist das Personal bereits für die Risiken sensibilisiert/geschult? Bisheriges Verhalten mitberücksichtigen	intern/extern: Personendaten gelangen an Unbefugte, unterschiedliche Auswirkungen je nach Art der Personendaten und Interesse an den Personendaten (z.B. Kreditkartenmissbrauch, Verwendung der Daten, wie z.B. E-Mail-Adresse, durch Dritte usw.)
externer Zugriff: mangelhafte Sicherheit des Systems (Hacking usw.)		extern: abhängig vom Interesse an den Personendaten	

3.5 Identifizierung von Massnahmen, die zum Schutz der Grundrechte der betroffenen Person vorgesehen sind

Sobald das Risiko bzw. die Risiken für die Grundrechte der betroffenen Person identifiziert wurden, kann eine Reihe von Massnahmen in Betracht gezogen werden, um diese Risiken zu verringern und die Grundrechte zu schützen. Im Gegensatz zu den vorherigen Kapiteln ist der Teil der DSFA, der sich auf die Ermittlung der vorgesehenen Massnahmen zum Schutz der Grundrechte der betroffenen Person bezieht, nicht im Instrument für die Risikoprüfung vorgesehen – dieses Instrument berücksichtigt nämlich die Massnahmen, mit denen die Risiken verringert werden könnten, nicht.

Bei der Identifizierung von Massnahmen geht es insbesondere darum, die Risiken für die Grundrechte der betroffenen Person zu minimieren. Mit den vorgesehenen Massnahmen soll sichergestellt werden, dass das Nettorisiko (Bewertung aufgrund der genannten Massnahmen) geringer ist als das Bruttorisiko (Bewertung unabhängig von den genannten Massnahmen). Gleichzeitig dient die DSFA aber auch dem Zweck, die festgestellten Risiken und die dafür vorgesehenen Massnahmen transparent auszuweisen.

Die Risikoverminderung kann entweder durch Beeinflussung der Eintrittswahrscheinlichkeit des auslösenden Ereignisses oder durch Einwirkung auf dessen Schweregrad bzw. Auswirkungen erfolgen.

Die Massnahmen können technischer Art sein (in der Praxis wird dies häufig auf IT-Massnahmen hinauslaufen), organisatorischer Art (Personal, Rollenverteilung, Verantwortlichkeiten,

Weisungen, Überwachung usw.) und/oder rechtlicher Art (Verabschiedung von Rechtsgrundlagen, Richtlinien, Reglementen, Verträgen usw.).

Eine Reihe von Massnahmen, insbesondere technischer und/oder organisatorischer Art, finden sich im DSGVO und in der DSV. Dazu gehören beispielsweise Datensicherheitsstandards, die Erstellung eines Bearbeitungsreglements und das Führen eines Verzeichnisses der Bearbeitungstätigkeit, die Begrenzung der Aufbewahrungsdauer, die Überprüfung der Richtigkeit der Daten usw.

Es geht darum, die geeignetsten Massnahmen für das erwartete Risiko zu finden. Dies kann eine gewisse Kreativität erfordern. Diese Massnahmen können sich direkt auf die Bearbeitung der Personendaten beziehen (Verschlüsselung, Anonymisierung, Pseudonymisierung, Zugriffskontrolle, Nachvollziehbarkeit usw.), auf das Bearbeitungssystem (Sicherheit der Hardware und der Software, Protokollierung, Backups usw.) oder auch auf die Governance im Bereich des Datenschutzes (Bearbeitungsreglement, Projekt- und Personalmanagement, sowie Umgang mit Datenschutzverletzungen).

In der Praxis gilt es, die relevanten Massnahmen zur Risikoverminderung in den gelben und roten Bereichen der Matrix zu finden. Für jede identifizierte Massnahme muss noch festgelegt werden, wer für ihre Umsetzung verantwortlich ist (Abteilung oder Funktion), ab wann und für wie lange die Massnahme umgesetzt werden muss, und schliesslich den finanziellen und personellen Aufwand der Massnahme.

Diese Informationen können z.B. in einer Tabelle wie folgt dargestellt werden:

Risiko	Massnahmen	Abteilung / Funktion	Zeitplan	Aufwand
Risiko 1	Massnahme 1	xy	Von... bis... /ab...	...
	Massnahme 2	ef	Von... bis... /ab...	...
	Massnahme 3	xy	Von... bis... /ab...	...
Risiko 2	Massnahme 2	ef	Von... bis... /ab...	...
Risiko 3	Massnahme 1	xy	Von... bis... /ab...	...
	Massnahme 4	ab	Von... bis... /ab...	...

Die Massnahmen, die im Rahmen des Grundschutzes zu ergreifen sind, sollten in der DSFA erwähnt werden, wenn sie dazu beitragen, dass sie das Risiko für die Grundrechte einer Person dadurch mindern. Allerdings müssen die für die Umsetzung berechneten Kosten nicht aufgeführt werden.

Bei der Anwendung von HERMES (siehe Kästchen oben, 3.4.1): Da die Massnahmen für die Informationssicherheitsrisiken bereits im Rahmen der detaillierten Risikoanalyse zum ISDS-Konzept festgelegt werden, sind nur für die Datenschutzrisiken Massnahmen entweder separat oder im Rahmen des ISDS-Konzepts vorzusehen. Bei den Informationssicherheitsrisiken ist

zusätzlich sicherzustellen, dass sie auch bezüglich der Auswirkungen, die sie auf die Grundrechte der betroffenen Person haben, bewertet werden.

Beispiel (abstraktes Beispiel, muss im konkreten Fall präzisiert werden):

Szenario	Risiko	Eintrittswahrscheinlichkeit	Auswirkungen für die betroffene Person	Massnahme
interner Zugriff: mehrere Personen sind an der Bearbeitung von Personendaten beteiligt	unbefugter Zugriff auf die Personendaten	intern: schwierig zu bestimmen. Kann rechtskonformes Verhalten vermutet werden? Ist das Personal bereits für die Risiken sensibilisiert/geschult? Bisheriges Verhalten mitberücksichtigen	intern/extern: Personendaten gelangen an Unbefugte, unterschiedliche Auswirkungen je nach Art der Personendaten und Interesse an den Personendaten (z.B. Kreditkartenmissbrauch, Verwendung der Daten, wie z.B. E-Mail-Adresse, durch Dritte usw.)	Regelung der Zugriffsberechtigungen, Protokollierung der Zugriffe, Schulung und Weisungen an die Mitarbeitenden, Überprüfung der Einhaltung der Weisungen
externer Zugriff: mangelhafte Sicherheit des Systems (Hacking usw.)		extern: abhängig vom Interesse an den Personendaten		Verbesserung der Systemsicherheit, Betroffene Personen werden über eine Datenschutzverletzung informiert

3.6 Bewertung der Auswirkungen der vorgesehenen Massnahmen zur Einschätzung des Restrisikos

Sobald die Massnahmen bestimmt sind, muss die verantwortliche Verwaltungseinheit für jedes identifizierte Risiko im gelben und roten Bereich der Matrix (siehe Kapitel 3.4, oben) eine neue Bewertung vornehmen, um festzustellen, ob die vorgesehenen Massnahmen das Risiko erfasst und reduziert haben, bzw. ob noch ein hohes Restrisiko besteht (Risiko im gelben oder roten Bereich der Matrix).

Dazu gehört zum Beispiel die Bewertung der vorgesehenen technischen und organisatorischen Massnahmen zur Datensicherheit, um die Eintrittswahrscheinlichkeit und den Schweregrad einer Verletzung der Datensicherheit trotz dieser Massnahmen zu bestimmen.

Zu beachten gilt, dass manche Risiken nicht oder kaum beeinflussbar sind. Denn selbst wenn verschiedene Massnahmen ergriffen werden, kann das Risiko gleich oder nahezu gleich bleiben.

Beispiel (abstraktes Beispiel, muss im konkreten Fall präzisiert werden):

Szenario	Risiko	Eintrittswahrscheinlichkeit	Auswirkungen für die betroffene Person	Massnahme	Auswirkungen der Massnahme (Restrisiko)
interner Zugriff: mehrere Personen sind an der Bearbeitung von Personendaten beteiligt	unbefugter Zugriff auf die Personendaten	intern: schwierig zu bestimmen. Kann rechtskonformes Verhalten vermutet werden? Ist das Personal bereits für die Risiken sensibilisiert/geschult? Bisheriges Verhalten mitberücksichtigen	intern/extern: Personendaten gelangen an Unbefugte, unterschiedliche Auswirkungen je nach Art der Personendaten und Interesse an den Personendaten (z.B. Kreditkartenmissbrauch, Verwendung der Daten, wie z.B. E-Mail-Adresse, durch Dritte usw.)	Regelung der Zugriffsberechtigungen, Protokollierung der Zugriffe, Schulung und Weisungen an die Mitarbeitenden, Überprüfung der Einhaltung der Weisungen	technische und organisatorische Massnahmen können Eintrittswahrscheinlichkeit weitgehend eindämmen, Auswirkungen können im Ereignisfall nur beschränkt eingedämmt werden
externer Zugriff: mangelhafte Sicherheit des Systems (Hacking usw.)		extern: abhängig vom Interesse an den Personendaten			Verbesserung der Systemsicherheit, Betroffene Personen werden über eine Datenschutzverletzung informiert

3.7 Konsultation des EDÖB bei hohem Restrisiko

Wie bereits in Kapitel 2.3 erwähnt, muss der EDÖB konsultiert werden, wenn trotz der vorgesehenen Massnahmen festgestellt wird, dass die geplante Bearbeitung noch immer ein hohes Risiko für die Grundrechte der betroffenen Person darstellt³⁴. Der für die Datenbearbeitung Verantwortliche muss diese Konsultation vor Beginn der Datenbearbeitung durchführen. Ausserdem muss sie die vom EDÖB bei seiner Konsultation vorgeschlagenen geeigneten Massnahmen berücksichtigen, um die betreffenden Daten bearbeiten zu dürfen.

Im Rahmen der Konsultation des EDÖB strukturieren verschiedene wichtige Fristen den Prozess:

- In einem ersten Schritt überprüft der EDÖB, ob die DSFA-Akte vollständig ist, und informiert die verantwortliche Verwaltungseinheit so schnell wie möglich über eventuelle Lücken.

³⁴ Art. 23 DSGVO

Diese Überprüfung dauert in der Regel zwei bis vier Wochen. Ist die von der verantwortlichen Verwaltungseinheit übermittelte Akte unvollständig, beginnt diese Frist mit jeder neuen übermittelten Fassung von Neuem.

- Hat der EDÖB in einem zweiten Schritt Einwände gegen die geplante Bearbeitung, schlägt er der verantwortlichen Verwaltungseinheit innerhalb der gesetzlichen Frist von zwei Monaten³⁵ geeignete Massnahmen vor. Diese Frist beginnt erst zu laufen, wenn die verantwortliche Verwaltungseinheit ihm ein vollständiges Dossier übermittelt hat. Bei komplexen Datenbearbeitungen kann sie um einen Monat verlängert werden.

Koordination mit dem Rechtsetzungsverfahren (Ziff. 4 DSFA-Richtlinien): Die Ergebnisse der DSFA sowie, im Fall eines hohen Restrisikos nach Artikel 23 DSG, die Stellungnahme des EDÖB sind den Unterlagen zur Ämterkonsultation beizulegen. Ergibt sich die Notwendigkeit zur Durchführung oder Anpassung einer DSFA nach der Ämterkonsultation, so sind die Ergebnisse der DSFA und allenfalls die **Stellungnahme des EDÖB** den Unterlagen zur nachfolgenden Ämterkonsultation oder zum Mitberichtsverfahren beizulegen.

Die verantwortliche Verwaltungseinheit (Departement oder BK) informiert über die Ergebnisse der DSFA und gegebenenfalls über die Stellungnahme des EDÖB, namentlich im Antrag an den Bundesrat, im erläuternden Bericht, in der Botschaft und in den Abstimmungserläuterungen.

3.8 Zusammenfassung und Ergebnisse der DSFA

Die Zusammenfassung enthält die wichtigsten Ergebnisse der DSFA, d.h. die Risiken (die sich im gelben und roten Bereich der Matrix befinden), die vorgesehenen Massnahmen zur Verminderung dieser Risiken und die allfälligen hohen Restrisiken.

Koordination mit dem Rechtsetzungsverfahren (Ziff. 4 DSFA-Richtlinien): Erfolgt die Durchführung der DSFA im Rahmen eines Rechtsetzungsverfahrens, sind die Ergebnisse der DSFA den Unterlagen zur Ämterkonsultation beizulegen. Zudem informiert die verantwortliche Verwaltungseinheit (Departement oder BK) über die Ergebnisse der DSFA insbesondere im Antrag an den Bundesrat, im erläuternden Bericht, in der Botschaft, sowie in den Abstimmungserläuterungen.

³⁵ Art. 23 Abs. 2 DSG

Anhang: Checkliste zum Inhalt der DSFA

Erster Teil: Allgemeine Angaben

Die allgemeinen Angaben der DSFA müssen folgende Bestandteile enthalten:

- Zuständige Verwaltungseinheit.
- Bestehenden oder geplanten Rechtsgrundlagen für die vorgesehene Bearbeitung von Personendaten.
- Datenschutzberaterin oder Datenschutzberater.
- Angabe, ob die vorgesehene Bearbeitung im Rahmen eines Rechtsetzungsverfahrens erfolgt.
- Angabe, ob die vorgesehene Bearbeitung im Rahmen eines HERMES-Projekts erfolgt.

Zweiter Teil: Beschreibung der vorgesehenen Bearbeitung von Personendaten

Der Teil des DSFA, der sich auf die Bearbeitung von Personendaten bezieht, muss Art, Umfang und Zweck der Bearbeitung sowie die Umstände, unter denen sie stattfindet, erkennen lassen.

- Identifizierung der an der Bearbeitung beteiligten Personen (z.B. mehrere Verantwortliche, Auftragsbearbeiter).
- Identifizierung und Beschreibung der Kategorien von Personendaten (z.B. Personendaten / besonders schützenswerte Daten, Form der Daten).
- Identifizierung und Beschreibung der Kategorien betroffener Personen (z.B. besonders schutzbedürftige Personen).
- Identifizierung und Beschreibung der geplanten Bearbeitung (z.B. Erhebung, Aufzeichnung, Aufbewahrung, Verwendung, Änderung, Weitergabe, Archivierung, Löschung oder Vernichtung von Daten).
- Identifizierung und Beschreibung der Art der Bearbeitung (z.B. Beschaffung von Personendaten ohne das Wissen der betroffenen Person, Zusammenführung oder Abgleich mit anderen Datenbanken, Bekanntgabe von Personendaten an Dritte, Profiling oder Profiling mit hohem Risiko, automatisierte Einzelentscheidung, Überwachung von Personen).
- Identifizierung und Beschreibung der verwendeten Technologien (z.B. Software, Netzwerk, Einsatz künstlicher Intelligenz).
- Identifizierung und Beschreibung des Umfangs der Bearbeitung (z.B. Menge der bearbeiteten Personendaten, Anzahl der betroffenen Personen, zeitlicher und geografischer Umfang).
- Identifizierung und Beschreibung des Zwecks der Bearbeitung.

Dritter Teil: Bewertung der Risiken für die Grundrechte der betroffenen Person

Der Teil der DSFA, der die Risikobewertung betrifft, muss folgende Aspekte enthalten:

- Identifizierung und Umschreibung der Informationssicherheits- und Datenschutzrisiken.
- Bewertung der Eintrittswahrscheinlichkeit der identifizierten Risiken.
- Bewertung und Umschreibung der Auswirkungen oder des Schweregrads der identifizierten Risiken für die Grundrechte der betroffenen Person

Für jedes identifizierte Risiko muss bestimmt werden:

- Ob das Risiko zumutbar ist (Risiko im grünen Bereich der Matrix).
- Ob das Risiko nicht zumutbar ist (Risiko im gelben oder roten Bereich der Matrix) → mögliche Korrekturmaßnahmen sind zu identifizieren (vgl. nächster Punkt).

Vierter Teil: Identifizierung der vorgesehenen Massnahmen zum Schutz der Grundrechte der betroffenen Person

Der Teil der DSFA, der sich auf die vorgesehenen Massnahmen zum Schutz der Grundrechte der betroffenen Person bezieht, muss die Frage beantworten, welche Massnahme das Brutto- auf ein Nettorisiko reduzieren kann.

Für jedes im gelben und roten Bereich der Matrix identifizierte Risiko (siehe Kapitel 3.4, oben):

- Identifizierung der relevanten Massnahme(n) zur Verringerung des Risikos.

Für jede identifizierte Massnahme müssen die nachfolgenden Angaben gemacht werden:

- Abteilung oder Funktion, die für die Umsetzung der Massnahme verantwortlich ist.
- Zeitplan für die Umsetzung der Massnahme.
- Aufwand (finanziell/personalbezogen) für die Umsetzung der Massnahme.

Identifizierung und Bewertung der Einhaltung:

- Grundsätze des Datenschutzrechts
- Pflichten des Verantwortlichen.

Fünfter Teil: Bewertung der Auswirkungen der vorgesehenen Massnahmen zur Beurteilung des Restrisikos

In diesem Teil soll festgestellt werden, ob trotz der vorgesehenen Massnahmen zum Schutz der Grundrechte der betroffenen Person ein hohes Restrisiko besteht.

Für jede vorgesehene Massnahme:

- Bewertung und Beschreibung der Auswirkungen der genannten Massnahmen

Für jedes im gelben und roten Bereich der Matrix identifizierte Risiko sollte Folgendes bestimmt werden:

- Ob ein hohes Restrisiko besteht
- gegebenenfalls den EDÖB konsultieren.

Sechster Teil: Zusammenfassung und Ergebnisse der DSFA

Dieser Teil soll eine Zusammenfassung der Ergebnisse darstellen.

- Beschreibung der identifizierten Risiken (Risiken aus dem gelben und roten Bereich der Matrix).
- Beschreibung der vorgesehenen Massnahmen zur Risikominimierung.
- Beschreibung der allfälligen hohen Restrisiken.