Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Merkblatt

zur Datenschutz-Folgenabschätzung (DSFA) nach den Art. 22 und 23 DSG

Stand: August 2023

Quellenverzeichnis

- BBl 2017 6941 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017 (Botschaft)

- Lobsiger Adrian «Hohes Risiko – kein Killerargument gegen Vorhaben der digitalen Transformation», Schweizerische Juristenzeitung SJZ 6/119

Inhaltsverzeichnis

1 Zweck und Anwendungsbereich des Merkblatts

Das Merkblatt des EDÖB richtet sich in erster Linie an private Datenbearbeitungsverantwortliche, wobei es auch als Auslegungshilfe durch die Bundesorgane beigezogen werden kann. Für Verwaltungseinheiten der zentralen Bundesverwaltung hat das Bundesamt für Justiz auf seiner Website die Richtlinien des Bundesrats für die Risikovorprüfung und die Datenschutz-Folgenabschätzung bei Datenbearbeitungen durch die Bundesverwaltung (DSFA-Richtlinien), ein Instrument für die Risikovorprüfung sowie einen Leitfaden zur DSFA veröffentlicht. An diese Instrumente können sich auch private Verantwortliche anlehnen.

2 Gegenstand und Zwecke der DSFA

Ab dem 1. September 2023 gilt gemäss Art. 22 und 23 des revidierten Datenschutzgesetzes (DSG), dass bei hohen Bearbeitungsrisiken eine **Datenschutz-Folgenabschätzung (DSFA)** erstellt werden muss. Nach Art. 22 Abs. 1 DSG besteht diese Pflicht, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt.

Als Arbeitsinstrument des modernen Datenschutzrechts zielt die DSFA darauf ab, diese Rechte der Betroffenen in der sozialen Realität der Digitalisierung sicherzustellen. Wie Art. 22 Abs. 1 und Art. 23 Abs. 1 DSG zum Ausdruck bringen, sind Gegenstand der DSFA **vorab geplante Personendatenbearbeitungen**, womit der Gesetzgeber vorab an Grossprojekte der digitalen Transformation gedacht hat. Dabei muss es sich nicht zwingend um **neue Personendatenbearbeitungen** handeln. Gegenstand einer DSFA können auch Weiterentwicklungen und Erweiterungen **vorbestehender Personendatenbearbeitungen** sein.

Die DSFA bezweckt die **frühzeitige Erkennung hoher Projektrisiken**. Diese beziehen sich auf die **Eintrittswahrscheinlichkeit** und mit deren Quantifizierung als «hoch» die **Erheblichkeit** deren Auswirkungen an.

Der Zweck der DSFA erschöpft sich dabei nicht in der **Voraussehbarkeit und Bewertung «hoher» Projektrisiken**. Der praktische Nutzen des Arbeitsinstruments liegt vielmehr auch darin, die Herleitung und Analyse systemischer und sicherheitstechnischer Risiken nachvollziehbar zu **dokumentieren** und durch geeignete **Massnahmen** auf ein datenschutzrechtlich vertretbares Niveau zu senken.

3 Schutzobjekte der DSFA

Nach Art. 22 Abs. 1 und Art. 23 Abs. 1 DSG müssen sich die normrelevanten «hohen Risiken» auf die Persönlichkeits- oder die Grundrechte der betroffenen Personen beziehen. Damit spricht der Gesetzgeber den Persönlichkeitsschutz als Kernanliegen des Datenschutzes an, aus dem sich als **primäre Schutzobjekte** der DSFA die **Privatsphäre und informationelle Selbstbestimmung** ableiten, welche sowohl die Autonomie des Einzelnen als auch dessen Würde und Identität umfassen. Mit Blick auf das Schutzobjekt der informationellen Selbstbestimmung sagt die Gesetzesbotschaft denn auch, dass von einem «hohen Risiko» auszugehen ist, wenn die spezifischen Eigenschaften der geplanten Datenbearbeitung darauf

schliessen lassen, dass die Verfügungsfreiheit der betroffenen Person über ihre Daten in hohem Masse eingeschränkt wird oder werden kann.

Werden Personendaten rechtswidrig bearbeitet, kann dies physische und finanzielle **Folgeverletzungen** nach sich ziehen, die nebst den primären Schutzobjekten des Datenschutzes weitere Rechtsgüter und Grundrechte wie das Recht auf Leben, physische Unversehrtheit oder Eigentum beschlagen. Solche weiteren Verletzungen können sich bei den von der Bearbeitung Betroffenen, aber im weiteren Kausalverlauf auch bei den Verantwortlichen einstellen.

Zur Veranschaulichung folgendes fiktives Beispiel: Ein humanitär tätiger Verein betreibt ein digitales Projekt zur statistischen Bearbeitung von Daten über politisch verfolgte Migrantinnen und Migranten. Im Rahmen einer ersten Einschätzung der Risiken kommt der Verein zu folgenden Ergebnissen:

- *Die geplante Bearbeitung ist mit dem potentiell hohen Risiko für die Privatsphäre und informationelle Selbstbestimmung der davon betroffenen Migrantinnen und Migranten verbunden, dass mit dem datenschutzrechtlichen Bearbeitungszweck unvereinbare Rückschlüsse auf deren private Kontaktdaten möglich werden und in falsche Hände gelangen könnten (Primärrisiko für die Betroffenen).*
- *Mit der Realisierung Primärrisikos kann für die Betroffenen das Folgerisiko einhergehen, dass es zu deren widerrechtlichen Verfolgung bis hin zu Ermordungen kommen könnte (Folgerisiko für die Betroffenen).*
- *Die Realisierung dieses Folgerisikos für die Betroffenen könnte für den bearbeitungsverantwortlichen Verein die daran anknüpfende Gefahr begründen, dass Letzterer seinen guten Ruf einbüssen und die Betroffenen finanziell entschädigen müsste (Folgerisiken für den Verantwortlichen).*

Mit Blick auf die im Beispiel getroffene Unterscheidung zwischen **Primär- und Folgerisiken** empfiehlt der EDÖB den Verantwortlichen bei der Evaluation des «hohen Risikos»:

- in einem ersten Schritt die Risiken für die primären Schutzobjekte der Privatsphäre und informationelle Selbstbestimmung der Betroffenen
- und mit einem zweiten Schritt die Folgerisiken für deren übrigen Rechtsgüter und Grundrechte auszuweisen.

Soweit sich Folgerisiken **auf die Bearbeitungsverantwortlichen selbst auswirken**, erweisen sie sich aus aufsichtsrechtlicher Warte kaum relevant, weil das DSG in den Art. 1 und 22 Abs. 1 nicht auf den Schutz der Bearbeitungsverantwortlichen, sondern die Wahrung der Persönlichkeit und der Grundrechte der natürlichen Personen abzielt, über die Personendaten bearbeitet werden. Anders mag es sein, wenn der Eintritt dieser Folgerisiken auch die von den Betroffenen getragenen Schäden und Risiken vergrössern könnte. So etwa, wenn die Zahlungsunfähigkeit eines Verantwortlichen dazu führen könnte, dass er die Mittel für die Wartung der Infrastruktur zum technischen Schutz der von ihm bearbeiteten Personendaten nicht mehr aufbringen kann.

4 Charakterisierung des «hohen Risikos»

Abgesehen von den Bestimmungen zur DSFA in Art. 22 und 23 erwähnt das DSG Personendatenbearbeitungen mit einem «hohen Risiko» in den Regelungen:

- zum «Profiling mit hohem Risiko» nach Art. 5 Bst. g.;
- zur Pflicht, in der Schweiz eine Vertretung zu bezeichnen nach Art. 14 Abs. 1 Bst. d.;
- zur Meldung von Verletzungen der Datensicherheit nach Art. 24;

- zur Bearbeitung von Personendaten zur Prüfung der Kreditwürdigkeit nach Art. 31 Abs. 2 Bst. c. Ziff. 1.

Aufgrund seiner Auslegungsbedürftigkeit eröffnet der unbestimmte Gesetzesbegriff des «hohen Risikos» den Bearbeitungsverantwortlichen wie auch der Datenschutzaufsicht des Bundes einen weiten Anwendungsspielraum. Da auch der Verordnungsgeber von jeder begrifflichen Präzisierung abgesehen hat, wird sich diese erst mit der Etablierung der Praxis und Rechtsprechung verdeutlichen.

4.1 Allgemeine Definition des hohen Risikos (Art. 22 Abs. 2 erster Abschnitt DSG)

Es sollte nicht übersehen werden, dass der Gesetzgeber in Art. 22 Abs. 2 Auslegungshilfen bereitstellt. Gemäss dieser Bestimmung kann das «hohe Risiko» aus

- der Art,
- dem Umfang,
- den Umständen
- und dem Zweck

der Bearbeitung abgeleitet werden, was auf ein breites Rechtsanwendungsermessen hindeutet. Unter die **Art**, die typischerweise ein hohes Risiko mit sich ziehen kann, fällt beispielsweise das Profiling, wenn es im Sinne von Art. 5 Bst. g eine **Beurteilung wesentlicher Aspekte einer Persönlichkeit** der Betroffenen erlaubt. Zu einem hohen Risiko können auch andere Formen der automatisierten Bearbeitung wie die automatisierte Einzelentscheidung i.S.v. Art. 21 DSG führen. Im Rahmen der **Umstände** können z.B. Subordinationsverhältnisse zwischen Bearbeitungsverantwortlichem und Betroffenen ins Gewicht fallen.

4.2 Absolute Kriterien nach Art. 22 Abs. 2 Bst. a und b DSG

Nicht abschliessend werden in Art 22 Abs. 2 Bst. a und b DSG absolute Kriterien genannt, bei deren Erfüllung das «hohe Risiko» von Gesetzes wegen als gegeben gilt:

- die umfangreiche Bearbeitung besonders schützenswerter Daten
- die systematische und umfangreiche Überwachung öffentlicher Bereiche

5 Risikovorprüfung gemäss Art. 22 Abs. 1 und 2 DSG

Zeichnet sich ab, dass eine geplante Bearbeitung möglicher Weise mit potentiell hohen Risiken verbunden sein könnte, muss der Verantwortliche eine (summarische) Vorprüfung der mit dem Vorhaben verbundenen Gefahren durchführen. Wegleitend für die Risikovorprüfung sind die in Ziff. 3 genannten Kriterien, welche für die DSFA selbst gelten.

Die Vorprüfung ist so früh wie möglich, d.h. bereits bei der **Projektplanung** vorzunehmen, auch wenn die Einzelheiten der Datenbearbeitung noch nicht definiert sind. Es kann sich deshalb empfehlen, Varianten vorzusehen.

Es empfiehlt sich, ein Bearbeitungsverzeichnis sowie eine systematische Beschreibung der Bearbeitungsvorgänge und Zwecke der geplanten Bearbeitungen einschliesslich Geschäftsmodellen und anderen Absichten und Interessen der Projektverantwortlichen zu erstellen. Bei der Erweiterung und Weiterentwicklung **vorbestehender Applikationen** ist stets ein **Vergleich** der bisherigen mit der geplanten Bearbeitung vorzunehmen.

Das Ergebnis der Vorprüfung und die zugrunde gelegten Beurteilungen sind zu **dokumentieren**. Fällt das Ergebnis noch nicht eindeutig aus, empfiehlt es sich, eine DSFA durchzuführen.

Für den Ablauf und weitere Kriterien der Vorprüfung verweisen wir auf das Schema in Anhang 1.

6 Pflicht zur Durchführung der DSFA (Art. 22 Abs. 3 DSG)

Hat die Vorprüfung ergeben, dass eine geplante Bearbeitung mit einem potentiell hohen Risiko verbunden sein könnte, ist hernach eine DSFA zu erstellen. Aufgrund der Vorgaben von Art. 7 DSG (Privacy by Design und by Default) ist eine solche wie schon die Vorprüfung so früh wie möglich vorzunehmen. Da in aller Regel noch viele Details ausstehen, kann es sich wie bei der Vorprüfung empfehlen, Varianten zu erarbeiten, die im Laufe des Prozesses angepasst und reduziert werden.

Erhält der EDÖB Kenntnis von einer geplanten Bearbeitung und ist er der Auffassung, dass der Verantwortliche vor deren Realisierung eine Vorprüfung und hernach eine DSFA durchführen muss, kann er im Weigerungsfalle gegen die Realisierung der geplanten Bearbeitung aufsichtsrechtlich einschreiten (s. Ziff. 8 hinten).

6.1 Inhalte und Aufbau der DSFA

Nach Art. 22 Abs. 3 DSG muss eine DSFA eine

- **Beschreibung der geplanten Bearbeitung**,
- eine **Bewertung der Risiken**
- sowie die **Massnahmen**

zur Wahrung der Persönlichkeit und Grundrechte der Betroffenen resp. der primären und sekundären Schutzobjekte enthalten (s. vorne Ziff. 2). Für einen möglichen Aufbau einer DSFA verweisen wir auf Anhang 2.

6.2 Beschreibung der geplanten Bearbeitung

Zunächst sind die im Rahmen der Vorprüfung erstellten Beschriebe und Vergleiche nach Ziff. 4 zu aktualisieren und hernach im Rahmen der eigentlichen DSFA zu vertiefen. Für weitere Angaben verweisen wir auf Anhang 2.

6.3 Beschreibung und Bewertung der potentiell hohen Bruttorisiken

Die Beschreibung der potentiell hohen Primär- und Sekundärrisiken, die sich mit einer geplanten Personendatenbearbeitung realisieren könnten, und deren Bewertung nach Eintrittswahrscheinlichkeit und Schwere ergibt sich aus den vorgehenden Ziff. 1-3.

Werden Personendaten ins Ausland transferiert, unterliegt die Übermittlung einer eigenen Prüfung, welche in die DSFA zu integrieren ist. Besonders wenn die Exportstaaten über kein angemessenes Datenschutzniveau verfügen können in diesem Kontext potenziell hohe Risiken auftreten, die der Verantwortliche mangels faktischer oder rechtlicher Einflussmöglichkeiten **nicht nachweisbar beeinflussen** kann, sodass das in der DSFA auszuweisende

Restrisiko hoch bleibt. Dies kann etwa der Fall sein, wenn aufgrund faktischer Handlungsmöglichkeiten fremder Behörden unter fremdem Recht potenzielle Persönlichkeits- und Grundrechtsverletzungen drohen und der Bearbeitungsverantwortliche dieses Risiko weder mittels privatautonomer Vertragsgestaltung noch der Inanspruchnahme des Rechtswegs rechtssicher beeinflussen kann und er die Eintrittswahrscheinlichkeit und Schwere der drohenden Verletzung demzufolge auch nach Planung und Ausweisung entsprechender Massnahmen in der DSFA nicht verlässlich einzuschätzen vermag.

Zur transparenten Ausweisung derartiger Risikolagen in der DSFA gehört gegebenenfalls die Offenlegung des Umstands, dass sie nicht verlässlich einschätzbar sind. Diese Transparenzanforderungen können je nach Wirksamkeit der getroffenen technischen, rechtlichen und organisatorischen Massnahmen namentlich dann relevant werden, wenn Personendaten in Rechenzentren ausgelagert werden sollen, deren Betreiber zu Konzernen mit Sitz in Staaten gehören, deren Rechtsordnung kein mit dem schweizerischen Recht vergleichbares Datenschutzniveau ausweist.

6.4 Geplante Massnahmen zur Senkung der potentiell hohen Bruttorisiken

Die in Art. 22 Abs. 3 DSG verlangten Massnahmen zum Schutz der Persönlichkeit und Grundrechte der Betroffenen bezwecken, die mit der Realisierung der geplanten Bearbeitung befürchteten hohen Bruttorisiken auf ein angemessen tieferes Niveau zu senken, sodass es alsdann als weniger hoch oder geringer als hoch eingestuft werden kann. Bei der in Erwägung gezogenen Massnahmen darf eine Abwägung zwischen den Interessen der betroffenen Person und denjenigen des Verantwortlichen erfolgen. Diese Interessenabwägung ist in der DSFA ebenfalls aufzuführen und entsprechend zu begründen.

Für weitere Angaben zum Beschrieb der geplanten Schutzmassnahmen verweisen wir ebenfalls auf Anhang 2.

6.5 Verbleibende Nettorisiken

Art. 23 Abs. 1 DSG geht ausdrücklich davon aus, dass eine potenziell gefährliche Datenbearbeitung – je nach Umständen – auch nach Ergreifen der den Verantwortlichen angemessen und zumutbar erscheinenden Schutzmassnahmen immer noch die Schwelle des «hohen Risikos» überschreiten darf. Das DSG verlangt somit nicht, dass die Bearbeitungsverantwortlichen oder der EDÖB potenziell hohe Bearbeitungsrisiken auf ein von der Rechtsordnung konkret bezeichnetes Niveau senken oder gar für eine Eliminierung derselben sorgen müssten.

Die Verantwortlichen müssen jedoch die aus der DSFA resultierenden Nettorisiken verständlich, nachvollziehbar und vollständig ausweisen und herleiten und sich vergewissern, dass nach wie vor als «hoch» bewertete Nettorisiken einer geplanten Bearbeitung mit den Vorgaben der Datenschutzgesetzgebung als Ganzes vereinbar sind. Nur wenn diese Voraussetzung erfüllt ist kann sich die fragliche Bearbeitung hinsichtlich ihres geplanten Umfangs und ihrer Intensität als für die Betroffenen zumutbar und somit insgesamt als vertretbar erweisen.

Für weitere Angaben zu Beschrieb und Bewertung der resultierenden Nettorisiken verweisen wir auf Anhang 2.

7 Vorgehen nach Fertigstellung der DSFA

Je nach Bewertung des ausgewiesenen Nettorisikos ist weiter wie folgt vorzugehen:

7.1 Kein hohes Nettorisiko

a) Auch wenn das verbleibende Nettorisiko geringer als «hoch» ausfällt, muss der Verantwortliche prüfen, ob die geplante Bearbeitung mit sämtlichen Vorgaben der Datenschutzgesetzgebung vereinbar ist. Nur wenn diese Grundbedingung erfüllt ist, darf das Bearbeitungsvorhaben realisiert werden.

b) Der Verantwortliche muss die DSFA dem EDÖB nicht vorlegen.

Legt der Verantwortliche dem EDÖB die DSFA freiwillig vor, ist Letzterer nicht gehalten, darauf einzutreten und materiell Stellung zu nehmen. Er kann sich jedoch ausnahmsweise im Rahmen seiner Beratungstätigkeit zu nicht mehr hohen Restrisiken äussern. Für solche Beratungen muss der EDÖB Gebühren erheben (vgl. Art. 59 Abs. 1 Bst. e DSG).

7.2 Hohes Nettorisiko

a) Wenn die Datenbearbeitung trotz hohem Restrisiko durchgeführt werden soll, was grundsätzlich zulässig ist, muss das Restrisiko gegenüber den Betroffenen transparent ausgewiesen werden. Dazu gehört auch die Offenlegung von Risiken, die weder beeinflussbar noch verlässlich einschätzbar sind. Private Verantwortliche müssen mit Blick auf die rechtfertigende Einwilligung in hohe Nettorisiken beachten, dass eine solche nur dann rechtgültig erfolgen kann, wenn sie informiert, also auch in Kenntnis der in der DSFA auszuweisenden Restrisiken abgegeben worden ist.

b) Gemäss Art. 23 Abs. 1 DSG muss die DSFA dem EDÖB zur Stellungnahme vorgelegt werden. Die Stellungnahme ist gebührenpflichtig (Art. 59 Bst. c DSG).

Nach Abs. 4 können private Verantwortliche von einer Konsultation des EDÖB absehen, wenn sie ihren Datenschutzberater konsultiert haben. In diesem Fall kann die DSFA dem EDÖB indessen freiwillig vorgelegt werden. Tritt letzterer darauf ein, ist seine Beurteilung gemäss Art. 59 Abs. 1 Bst. c DSG gebührenpflichtig.

8 Vorgehen bei bereits erfolgenden Bearbeitungen mit hohem Risiko und einer Verletzung der Datensicherheit

Bestehen hinreichende Anzeichen dafür, dass Umstände eingetreten sein könnten, wonach eine bestehende oder weiterentwickelte Bearbeitung mit zusätzlichen, insgesamt als hoch einzuschätzenden Risiken verbunden sein könnte, muss der Verantwortliche je nach Umständen eine DSFA erstmals erstellen, oder eine solche – falls vorbestehend – aktualisieren. Auslöser für ein solches Tätigwerden können Expertenberichte, Beschwerden von Betroffenen, Medienberichte, abgewehrte oder ohne schädigende Absicht erfolgte Cyberattacken oder eine sonstige Verletzung der Datensicherheit sein. Weist die neue oder aktualisierte DSFA ein hohes Restrisiko aus, muss der Verantwortliche diese dem EDÖB inklusive eines Vergleichs der bisherigen und der zu erweiternden Applikationen zur Stellungnahme vorlegen.

Ist es im Zuge der bestehenden Bearbeitung von Personendaten zu einer gegenüber dem EDÖB meldepflichtigen Verletzung der Datensicherheit mit hohen Risiken für die Betroffenen

i.S.v. Art. 24 DSG gekommen, muss der Verantwortliche rechtzeitig die nötigen Massnahmen ergreifen, um den rechtmässigen Zustand wiederherzustellen und die Betroffenen über die eingetretenen oder drohenden Verletzungen ihrer Persönlichkeit oder Grundrechte zu informieren. Zeichnet sich ab, dass die Risiken der Bearbeitung bei deren Weiterführung hoch bleiben dürften, kann der EDÖB den Verantwortlichen auffordern, eine DSFA zu erstellen.

9 Stellungnahme des EDÖB nach Vorlage der DSFA

Der EDÖB prüft, ob die ihm vorliegende DSFA die ausgewiesenen hohen Nettorisiken verständlich, nachvollziehbar und vollständig ausweist und herleitet. Weiter prüft er, ob die geplante Bearbeitung unter Berücksichtigung der auszuweisenden Risiken mit den Vorgaben der Datenschutzgesetzgebung als Ganzes vereinbar ist, indem sie sich hinsichtlich des geplanten Umfangs und der Intensität als für die Betroffenen zumutbar und somit insgesamt als vertretbar erweist.

Innert der in Art. 23 Abs. 2 DSG genannten Ordnungsfrist von zwei Monaten teilt der EDÖB dem Verantwortlichen allfällige Einwände mit. Die Stellungahme des EDÖB ist gebührenpflichtig (Art. 59 DSG). Sie kann sich auf die geplanten Datenbearbeitung beziehen oder auch auf die Ausgestaltung der DSFA, z.B. wenn der Verantwortliche die imminenten Risiken nicht angemessen bewertet und ausweist, als auch die geplante Bearbeitung beziehen.

Die Stellungnahme des EDÖB hat empfehlenden Charakter und stellt deshalb keine Genehmigung oder Bewilligung der geplanten Durchführung dar.

Hat der EDÖB Einwände gegen die geplante Bearbeitung, schlägt er dem Verantwortlichen geeignete Massnahmen vor, sofern solche die festgestellten Risiken zu senken vermögen (Art. 23 Abs. 3 DSG).

10 Aufsichtsrechtliche Massnahmen des EDÖB

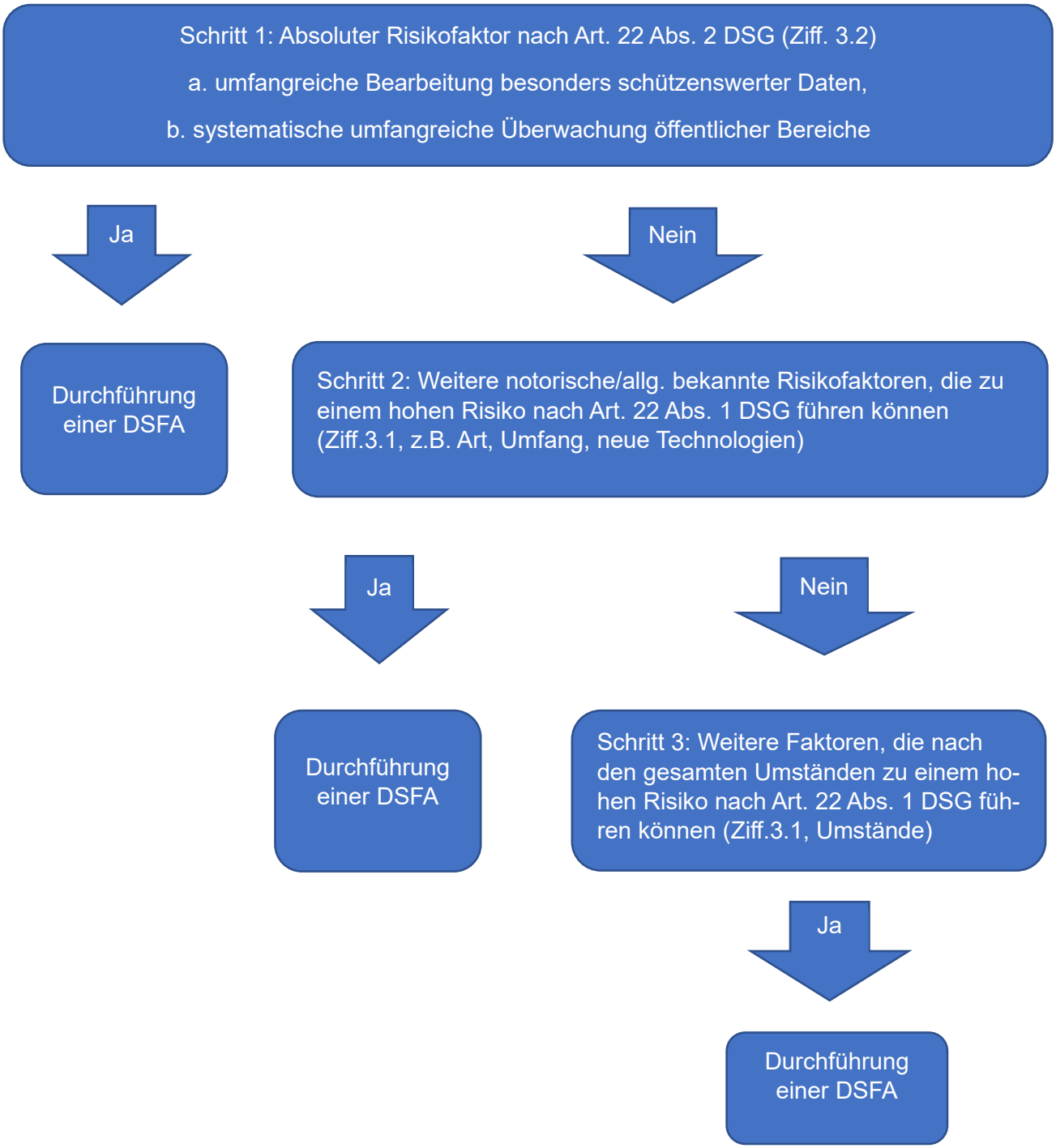
Weigert sich ein Verantwortlicher, wichtige Einwände und Anregungen des EDÖB zu befolgen, kann Letzterer eine Untersuchung eröffnen und angeregte Ergänzungen oder Änderungen bis hin zum Verbot der Bearbeitung zu gegebener Zeit formell verfügen. Dabei respektiert der EDÖB den Ermessensspielraum, der den fach- und branchenkundigen Verantwortlichen bei der Bewertung von Bearbeitungsrisiken zukommt.

Ein formelles Tätigwerden des EDÖB ist insbesondere angezeigt, wenn die Inkaufnahme eines Risikos namentlich aufgrund der Eintrittswahrscheinlichkeit und Schwere der Persönlichkeitsverletzungen nicht zumutbar ist und sich die geplante Bearbeitung demzufolge datenschutzrechtlich als unzulässig erweist. So etwa, wenn mit der Realisierung einer Bearbeitung mit hohem Restrisiko datenschutzrechtliche Grundsätze nach Art. 6 DSG wie die Verhältnismässigkeit oder Vorgaben an die technische Sicherheit nach Art. 8 DSG verletzt würden. Auch die Frage, ob und inwieweit Bearbeitungsverantwortliche den Betroffenen hohe Restrisiken zumuten dürfen, welche gemäss DSFA nicht verlässlich einschätzbar sind, lässt sich nicht aus den Bestimmungen zur DSFA, sondern nur nach Massgabe der Datenschutzgesetzgebung als Ganzes beantworten.

Anhang 1

Ablaufschema zur Vorprüfung, ob DSFA durchgeführt werden muss

Folgendes Ablaufschema kann für die Vorprüfung nach Art. 22 Abs.1 DSG herangezogen werden. Für Verwaltungseinheiten der zentralen Bundesverwaltung ist das Instrument für die Risikovorprüfung des Bundesamts für Justiz obligatorisch.



Erläuterungen zum Schema

Mit den nachfolgenden Schritten kann geprüft werden, ob eine DSFA zu erstellen ist.

Schritt 1:

Wenn mindestens einer der absoluten Risikofaktoren vorliegt, ist eine DSFA zu erstellen.

Falls kein absoluter Risikofaktor vorliegt: Schritt 2

Schritt 2:

Es ist zu prüfen, ob ein, mehrere oder andere notorische Risikofaktoren vorliegen (vgl. dazu auch nachfolgende, nicht abschliessende Liste).

- Liegt ein Profiling mit hohem Risiko vor?
- Wird eine automatisierte Einzelentscheidung vorgenommen?
- Kommen neue Technologien, inkl. künstliche Intelligenz zur Anwendung?
- Werden die Personendaten geheim (ohne Wissen der betroffenen Person) beschafft?
- Betrifft die Datenbearbeitung eine grosse Menge von Daten oder eine grosse Anzahl von Personen?
- Ist die Datenbearbeitung in zeitlicher oder geographischer Hinsicht umfangreich?
- Werden Datenbestände miteinander verknüpft oder abgeglichen?
- Werden die Personendaten an Dritte bekanntgegeben?
- Führt die Bearbeitung von Personendaten zu einer Überwachung betroffener Personen?
- Werden betroffene Personen daran gehindert, ein Recht auszuüben, eine Dienstleistung zu nutzen oder einen Vertrag zu erfüllen?

Wenn notorische Risikofaktoren gegeben sind, soll im Zweifelsfall eine DSFA durchgeführt werden.

Wenn kein notorischer Risikofaktor gegeben ist: Schritt 3

Schritt 3:

Es ist zu prüfen, ob unter Berücksichtigung der gesamten Umstände die Datenbearbeitung zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der Betroffenen führen kann (Ziff. 3.1, beispielsweise Subordinationsverhältnis).

Wenn ja, soll eine DSFA durchgeführt werden.

Wenn nein, kann von einer DSFA abgesehen werden.

Anhang 2

Möglicher Aufbau

Für den möglichen Aufbau einer DSFA kann folgende Liste verwendet werden, welche nicht als Vorgabe, sondern als Orientierungshilfe zu betrachten ist. Für Verwaltungseinheiten der zentralen Bundesverwaltung ist der Leitfaden des Bundesamts für Justiz zur DSFA, welcher das Vorgehen und den Inhalt der DSFA für Datenschutz-Folgenabschätzung durch die zentrale Bundesverwaltung erläutert, massgeblich.

1. Verantwortliche Person

- Verantwortliche Person
- Datenschutzberater
- Weitere interne beteiligte Stellen
- Auftragsbearbeiter
- Gemeinsam Verantwortliche

2. Kontext der Datenbearbeitung

- Beschrieb des Ist-Zustands
- Beschrieb des Soll-Zustands
- Bei vorbestehenden Applikationen, die erweitert werden: Vergleiche des Ist- und Soll-Zustands und Verweis auf bereits bestehende DSFAs

3. Datenbearbeitung

- Gesetzliche Grundlage (öffentlich) / Rechtfertigungsgrund (privat)
- Zweck der Datenbearbeitung
- Betroffene Personen
    - Art (Arbeitnehmer, Kunden, Patienten, etc.)
    - Involvierung (Opt-in/opt-out; automatisierte Bearbeitung; Transparenz)
- Art der Daten:
    - Schrift/Bild/Ton etc.
- Datenkategorien
    - Personendaten/besonders schützenswerte Daten etc.
- Umfang der Datenbearbeitung/Quantität der Daten
    - Zahl der betroffenen Personen
    - Datenvolumen pro betroffener Person
- Qualität der Daten
    - Quellen/Erhebung

- Bekanntgabe von Daten
- Geografisches Ausmass
- Dauer/Intensität der Bearbeitung
- Löschfristen
- Technische Umsetzung
    - Verwendete Technologien
    - Prozesse der Datenbearbeitung
    - Verschlüsselung
    - IT-Systeme und Schnittstellen
    - Zugriffsberechtigungen
- Einhaltung der Datenschutzgrundsätze
    - Rechtmässigkeit
    - Treu und Glauben
    - Zweckbindung
    - Verhältnismässigkeit
    - Transparenz
    - Datenrichtigkeit
    - Datensicherheit/Technische Risiken: evtl. ISDS Konzept etc.
- Umsetzung privacy by design/by default
- Auftragsbearbeiter

4. Potentiell hohe Risiken vor Massnahmen (Bruttorisiken)

- Art der Risiken
    - Systemische Risiken
    - Rechtliche Risiken
    - Sicherheitstechnische Risiken
    - Handelt es sich dabei um Primärrisiken für Privatsphäre und informationelle Selbstbestimmung der Betroffenen
    - Handelt es sich dabei um Sekundärrisiken für weitere Rechtsgüter oder Grundrechte der Betroffenen

- Analyse und Bewertung der potentiell hohen Bruttorisiken
    - Betroffene (Personen, über die Daten bearbeitet werden oder Verantwortliche)
    - Ausmass
    - Eintrittswahrscheinlichkeit

5. Massnahmen zur Senkung der potentiell hohen Bruttorisiken

- Rechtliche Massnahmen
    - Verträge, SCC etc.
- Organisatorische Massnahmen
    - Auswahl, Instruktion, Überwachung des Personals

    - Sensibilisierung, Ausbildung
- Technische Massnahmen gemäss Art. 3 DSV, bspw. Benutzerkontrolle

Risiken nach Massnahmen (Nettorisiken)

- Auswirkung der getroffenen Massnahmen auf die potentiell hohen Bruttorisiken
- Risiken durch Massnahmen des Verantwortlichen beeinflussbar
- Risiken durch Massnahmen des Verantwortlichen nicht beeinflussbar (z.B. Zugriffe durch fremde Behörden)
- Verhältnismässigkeit der Massnahmen/Interessensabwägung

6. Ergebnis

- Hohes Nettorisiko
- Hohes Nettorisiko datenschutzrechtlich akzeptabel oder inakzeptabel?
- Nicht mehr hohes Nettorisiko

7. Konsultation EDÖB

- Hohes Nettorisiko trotz Massnahmen
- Ausnahme: Konsultation interner Datenschutzberater