Anleitung zur Datenschutz-Folgenabschätzung (DSFA) und Vorabkonsultation (VAK)

1 Einleitung

1.1 Zweck

Diese Anleitung richtet sich an öffentliche Organe im Kanton Basel-Stadt. Sie beschreibt das Vorgehen von der Schwellwertanalyse über die Datenschutz-Folgenabschätzung bis zur Vorabkonsultation.

Besteht bei einem Projekt/Vorhaben voraussichtlich ein hohes Risiko für die Grundrechte der betroffenen Personen, dann ist eine Datenschutz-Folgenabschätzung durchzuführen und das Projekt/Vorhaben der Datenschutzbeauftragten zur Vorabkonsultation vorzulegen (§ 12a und § 13 Abs. 1 lit. b revIDG).

Diese Instrumente sind Elemente des präventiven Datenschutzes mit dem Ziel, Datenschutzrisiken rechtzeitig zu erkennen und im Sinne von Datenschutz durch Technikgestaltung («privacy by design») und datenschutzfreundlichen Voreinstellungen («privacy by default») (§ 14 Abs. 1 und 2 des Informations- und Datenschutzgesetzes [IDG]) zu vermeiden, damit nicht später im Betrieb mühsam und i.d.R. kostenintensiv nachgebessert werden muss. Mit diesen Instrumenten soll im Sinne von § 12a und § 13 IDG und nach dem Projektleitfaden des Kantons bei Vorhaben sichergestellt werden, dass ein hohes Risiko für die Grundrechte der von einer Bearbeitung ihrer Daten betroffenen Personen vermieden oder auf ein tragbares Mass reduziert wird.

Die Verantwortung für den datenschutzkonformen Umgang mit Informationen trägt dasjenige öffentliche Organ (im Sinne von § 3 Abs. 1 IDG), das die Informationen zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet (§ 6 Abs. 1 IDG): die Dateneignerin. Die Datenschutz-Folgenabschätzung hilft der Dateneignerin, diese Verantwortung wahrnehmen zu können. Mit der Vorabkonsultation der Datenschutzbeauftragten wird die Einschätzung der Dateneignerin «von aussen» geprüft, was ihr wiederum helfen soll, ihre Verantwortung sachgerecht übernehmen zu können.

1.2 Begriffsklärungen

1.2.1 Vorhaben zur Bearbeitung von Personendaten

Mit «Vorhaben zur Bearbeitung von Personendaten» ist das systematische Bearbeiten von Personendaten durch ein öffentliches Organ gemeint, wie z.B. das Anlegen und Verwalten einer Datenbank mit Personendaten, die Einführung von M365, Nutzung von Transkriptionssoftware um Protokolle zu verschriftlichen, etc. Der Begriff «Vorhaben» ist dabei weit zu verstehen und umfasst sowohl geplante Datenbearbeitungen im gesamten Projektmanagementzyklus – von der Idee bis zum eigentlichen Projekt – als auch Datenbearbeitungen, die ausserhalb eines Projekts geplant werden. Der Begriff «Vorhaben» umfasst aber auch Anpassungen in bestehenden Anwendungen, welche zu Änderungen in der Bearbeitung von Personendaten führen (z.B. Major Release mit Anpassungen, die den Umfang und die Art der Bearbeitung von Personendaten signifikant verändern). Unerheblich dabei ist, ob die Datenbearbeitung digital oder – heutzutage eher selten – rein analog erfolgt.
Nicht erfasst sind jedoch einzelne, konkrete Bearbeitungen wie beispielsweise eine Einzelbekanntgabe von Personendaten.

1.2.2 Schwellwertanalyse (SWA)

Mit der **Schwellwertanalyse (SWA)** prüft das öffentliche Organ selber, ob bei einem Vorhaben der Schwellwert erreicht wird, ab dem eine Datenschutz-Folgenabschätzung durchzuführen ist (Details → Ziff. 2). Ergibt sich nach dem Ausfüllen des Fragebogens, dass keine Datenschutz-Folgenabschätzung durchzuführen ist, dann ist das unterzeichnete Formular in der Projektdokumentation abzulegen (zum weiteren Vorgehen: Ziff. 2.4). Es ist auf Verlangen der Datenschutzbeauftragten (DSB) vorzuweisen.

1.2.3 Datenschutz-Folgenabschätzung (DSFA)

Ergibt die SWA, dass ein Projekt/Vorhaben zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen kann oder es aus einem anderen Grund der DSB zur Vorabkonsultation vorzulegen ist, dann muss das für das Projekt/Vorhaben verantwortliche öffentliche Organ (bzw. in seinem Auftrag die Projektleitung) eine **Datenschutz-Folgenabschätzung (DSFA)** durchführen (Details → Ziff. 3). Voraussetzung dafür ist eine geeignete Projektbeschreibung und das Vorliegen einer Rechtsgrundlagenanalyse (Details → Ziff. 3.2.). Die DSFA als Risikoanalyse dient dazu, die datenschutzrelevanten Risiken zu eruieren, zu bewerten und in der Folge die notwendigen technischen, organisatorischen und/oder rechtlichen Schutzmassnahmen festzulegen, mit denen die datenschutzrelevanten Risiken vermieden oder auf ein tragbares Mass reduziert werden.

Diese Risikoanalyse ist wichtig für das verantwortliche öffentliche Organ: Deren Leitung muss schliesslich die Massnahmen abnehmen, das verbleibende Nettorisiko (Restrisiko) übernehmen oder, falls sie das Restrisiko als untragbar erachtet, auf das Vorhaben verzichten.

Eine Risikobeurteilung ist immer eine Momentaufnahme. Es können die Rechtsgrundlagen ändern, es können sich Risiken verändern (z.B., weil neue Angriffsformen entstehen), und es kann die Wirksamkeit von Massnahmen abnehmen (z.B. Verschlüsselung). Zum Risikomanagement gehört daher die regelmässige Überprüfung der Risikobeurteilung.

1.2.4 Vorabkonsultation (VAK)

Die **Vorabkonsultation (VAK)** schliesslich ist das Vorlegen der im Rahmen der DSFA erstellten Unterlagen an die DSB. Die DSFA ist die Vorbereitung der VAK (Details → Ziff. 4). Die Pflicht zur VAK – bis zum Inkrafttreten des revidierten IDG unter dem Namen Vorabkontrolle – besteht seit dem 1. Februar 2009.

Die DSB prüft aufgrund der eingereichten Unterlagen, ob ein Vorhaben **datenschutzkonform umsetzbar** ist. Sie gibt eine entsprechende Stellungnahme ab und kann zusätzliche oder andere Massnahmen empfehlen (§ 46 Abs. 1 IDG).

Die Leitung des verantwortlichen öffentlichen Organs trägt die Verantwortung, ob es die von der DSB empfohlenen Massnahmen umsetzen will oder nicht (§ 46 Abs. 2 IDG). Allerdings übernimmt sie damit auch – zusätzlich zum Nettorisiko (Details → Ziff. 3.3.2) – die Verantwortung für dieses spezifische Risiko, das mit der Nichtumsetzung der Massnahmen entgegen der Empfehlung der DSB verbleibt.

Die Datenschutzbeauftragte steht bei Fragen zur SWA, zur DSFA und zur VAK gerne zur Verfügung (061 267 16 40 / datenschutz@dsb.bs.ch).

2 Schwellwertanalyse (SWA)

2.1 Pflicht zum Erstellen der Schwellwertanalyse

Bei jedem Vorhaben, bei dem Daten bearbeitet werden, ist durch das verantwortliche öffentliche Organ das Formular «Schwellwertanalyse» auszufüllen.

2.2 Vorfrage: Personendaten

Ergibt sich bei der Vorfrage, dass mit dem geplanten Projekt/Vorhaben Personendaten (i.S.v. § 3 Abs. 3 IDG) bearbeitet werden, so muss anhand weiterer Fragen geklärt werden, ob ein hohes Risiko für betroffene Personen besteht und daher eine Datenschutz-Folgenabschätzung durchzuführen ist. Weiteres Vorgehen → Ziff. 2.3.

Mit dem geplanten Projekt/Vorhaben werden keine Personendaten bearbeitet. Weiteres Vorgehen → Ziff. 2.4.1.

2.3 Erläuterung zu den weiteren Fragen der Schwellwertanalyse

Ist eine der folgenden Fragen zu bejahen, muss eine DSFA durchgeführt und es müssen die dabei erarbeiteten Unterlagen der DSB zur VAK unterbreitet werden.

2.3.1 Frage 1: Abrufverfahren (§ 2 Abs. 1 lit. a IDV)

Ein Abrufverfahren (auch Onlinezugriff) erlaubt es einem öffentlichen Organ, ohne weitere Prüfung durch die Dateneignerin, **auf deren Daten zuzugreifen**, sich somit bei den Daten der Dateneignerin «zu bedienen». Daraus kann ein hohes Risiko für die betroffenen Personen resultieren, weil die Dateneignerin bei einem Onlinezugriff nicht prüfen kann, ob der konkrete Zugriff des anderen öffentlichen Organs rechtmässig und verhältnismässig ist.

Hinweis: Beschränkt sich das Projekt/Vorhaben **einzig** auf ein Abrufverfahren **im kantonalen Datenmarkt** (i.S.v. § 5 Abs. 1 lit. a Ziff. 1-3 der Datenmarktverordnung (DMV)), so findet die Vorabkonsultation im Rahmen des Autorisierungs-Workflow-Systems AWS statt. Wenn kein anderer Risikofaktor (Fragen 2–10) gegeben ist, muss keine Datenschutz-Folgenabschätzung durchgeführt werden.

2.3.2 Frage 2: Bearbeitung von besonderen Personendaten oder von Personendaten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen (§ 2 Abs. 1 lit. b IDV)

Das Bearbeiten von *besonderen Personendaten* (i.S.v. § 3 Abs. 4 IDG), also von Personendaten, die ein Stigmatisierungs- oder Diskriminierungspotenzial besitzen, führt zu einem hohen Risiko für die betroffenen Personen. Diese sogenannten *sensiblen Personendaten* sind insbesondere Angaben über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten; Angaben über die Gesundheit, das Erbgut (genetische Daten), die persönliche Geheimsphäre, das Sexualleben, die sexuelle Orientierung oder die ethnische Herkunft; Angaben über Massnahmen der sozialen Hilfe; Angaben über administrative oder strafrechtliche Verfolgungen und Sanktionen und biometrische Daten (mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder be-

stätigen) (§ 3 Abs. 4 lit. a IDG). Ebenfalls zu den besonderen Personendaten gehören *Persönlichkeitsprofile*, d.h. Zusammenstellungen von Informationen, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben (§ 3 Abs. 4 lit. b IDG). Zu beachten ist, dass besondere Personendaten nach § 9 Abs. 2 IDG nur aufgrund einer Grundlage in einem *Gesetz im formellen Sinn* bearbeitet (bzw. nach § 21 Abs. 2 IDG bekannt gegeben) werden dürfen.

Dasselbe gilt, wenn Personendaten bearbeitet werden sollen, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen (Art. 321 StGB bzw. Art. 320 StGB). *Berufsgeheimnisse* bestehen u.a. für Geistliche, Rechtsanwält:innen, Notar:innen, nach OR zur Verschwiegenheit verpflichtete Revisor:innen, Ärzt:innen, Zahnärzt:innen, Apotheker:innen, Hebammen, Psycholog:innen und ihre Hilfspersonen. *Besondere Amtsgeheimnisse* sind u.a. das Sozialhilfegeheimnis nach § 28 Sozialhilfegesetz, das Sozialversicherungsgeheimnis nach Art. 33 ATSG, die Schweigepflicht bei der Opferhilfeberatung nach Art. 11 Abs. 1 OHG, das Steuergeheimnis nach § 138 Abs. 1 StG (und nach § 75 Abs. 3 KV); das Stimmgeheimnis bei Wahlen und Abstimmungen nach § 43 Abs. 3 KV und § 6 Abs. 3 WahlG bzw. nach Art. 5 Abs. 7, 8 Abs. 1 und 8a Abs.2 BPR.

2.3.3 Frage 3: Profiling (§ 2 Abs. 1 lit. c IDV)

Profiling ist jede *automatisierte Auswertung von Informationen*, um wesentliche persönliche Merkmale zu *analysieren* oder Entwicklungen, insbesondere bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel, *vorherzusagen* (§ 3 Abs. 7 revIDG). Zu beachten ist, dass nach § 9 Abs. 2 revIDG ein Profiling nur aufgrund einer Grundlage in einem Gesetz im formellen Sinn zulässig ist bzw. nach § 21 Abs. 2 revIDG Resultate eines Profilings nur aufgrund einer formell-gesetzlichen Grundlage bekannt gegeben werden dürfen.

2.3.4 Frage 4: Bearbeiten von Daten von mehr als 10'000 Personen (vgl. § 2 Abs. 1 lit. d IDV)

Auch wenn keiner der anderen Risikofaktoren (Ziff. 2.3.1–2.3.3 und 2.3.5–2.3.10) vorliegt, kann die grosse Anzahl von Personen, über die Daten bearbeitet werden, zu einem hohen Risiko für die betroffenen Personen führen. Bereits bei der Schaffung von § 2 Abs. 1 lit. d IDV im Jahr 2011 hat der Regierungsrat die Zahl von 10'000 betroffenen Personen (im Endausbau) als Limite festgelegt (siehe Ratschlag 21.1239.01, S. 26). Wenn in einem System z.B. alle Einwohner:innen, alle im Kanton angemeldeten ausländischen Staatsangehörigen, alle Schüler:innen o.ä. erfasst werden sollen, ist von einem hohen Risiko auszugehen.

2.3.5 Frage 5: Auftragsdatenbearbeitung durch Dritte im Ausland in einem Staat ohne angemessenen Datenschutz (§ 2 Abs. 1 lit. e IDV)

Wenn ein öffentliches Organ Personendaten nicht selber bearbeitet, sondern durch Dritte bearbeiten lässt, bleibt es gegenüber den betroffenen Personen verantwortlich (§ 7 Abs. 2 IDG). Ein hohes Risiko für die Grundrechte der Betroffenen kann insbesondere dann entstehen, wenn die Auftragsdatenbearbeiterin dies in einem Staat tut, dessen Gesetzgebung keinen angemessenen Datenschutz gewährleistet. Für die Frage, ob ein Staat über ein angemessenes Datenschutzniveau verfügt, ist auf die vom Bundesrat im Anhang zur Datenschutzverordnung (DSV) veröffentlichte Liste der Staaten, Gebiete, spezifischen Sektoren in einem Staat und internationalen Organe mit einem angemessenen Datenschutz abzustellen.

2.3.6 Frage 6: Errichtung eines Datenpools (§ 2 Abs. 1 lit. f IDV)

Ein Datenpool (i.S.v. § 1a Abs. 1 IDV) liegt vor, wenn ein Informationsbestand mit Personendaten

a) zum Zweck der Aufgabenerfüllung von mindestens zwei öffentlichen Organen oder mindestens einem öffentlichen Organ und einem Dritten erstellt wird und

b) Informationen von mindestens zwei öffentlichen Organen oder mindestens einem öffentlichen Organ und mindestens einem Dritten enthält und

c) die in ihm enthaltenen Informationen von mehreren öffentlichen Organen und/oder Dritten gemeinsam verwendet werden, wobei die informationenbeziehenden und die informationenliefernden öffentlichen Organe und/oder Dritten nicht identisch sein müssen.

Wenn mit einem Projekt/Vorhaben ein solcher Datenpool geschaffen werden soll, dann kann das zu einem hohen Risiko für die Grundrechte der betroffenen Personen führen.

2.3.7 Frage 7: Automatisierte Einzelentscheidung (Liste der Bearbeitungsvorgänge, Ziff. 2.1)

Wenn automatisiert, also ohne Zutun von Menschen, über Ansprüche von Personen entschieden wird (d.h., wenn automatisiert eine Verfügung erlassen wird), kann ein hohes Risiko für die Grundrechte der Betroffenen entstehen. Dieses Risiko muss mit Transparenzmassnahmen und der Möglichkeit der betroffenen Personen, eine Überprüfung durch Menschen zu verlangen, auf ein tragbares Mass reduziert werden.

Der Regierungsrat hat im IDG-Revisions-Ratschlag die Meinung vertreten, dass eine spezifische Regelung für automatisierte Einzelentscheidungen (noch) nicht notwendig sei, da den betroffenen Personen im Vorfeld des Erlasses von Verfügungen ein Anspruch auf rechtliches Gehör zukommt und damit sichergestellt ist, dass die betroffenen Personen sich zur Einzelentscheidung äussern können. Offen bleibt, ob in Zukunft bereichsspezifisch automatisierte Einzelentscheidungen eingeführt werden, die nicht zum Erlass einer Verfügung führen, aber trotzdem rechtliche Wirkungen oder erhebliche Auswirkungen auf die betroffene Person haben. In solchen Fällen wird darauf zu achten sein, dass im entsprechenden Fachgesetz eine ausdrückliche und klare formell-gesetzliche Grundlage dafür geschaffen wird und dabei sichergestellt ist, dass den betroffenen Personen die Möglichkeit gegeben wird, sich zur automatisierten Einzelentscheidung und zu den bearbeiteten Daten zu äussern (IDG-Revisions-Ratschlag, S. 30 f.).

In der Beratung der IDG-Revision in der Justiz-, Sicherheits- und Sportkommission wurde in diesem Zusammenhang verlangt, dass die DSB solche Vorhaben prüft, sie sich also zur VAK vorlegen lässt, damit geprüft werden kann, ob und mit welchen technischen, organisatorischen und/oder rechtlichen Schutzmassnahmen dafür gesorgt wird, dass die datenschutzrelevanten Risiken vermieden oder auf ein tragbares Mass reduziert werden.

2.3.8 Frage 8: Systematische Übermittlung von Personendaten, die eine technische Überwachung ermöglichen (Liste der Bearbeitungsvorgänge, Ziff. 2.2)

Die Bekanntgabe von Personendaten ist nur zulässig aufgrund einer gesetzlichen Grundlage oder mit der ausdrücklichen Einwilligung der betroffenen Personen (§ 21 IDG). Viele Webseiten sammeln Daten, die zur Überwachung von Personen genutzt werden können, und senden diese an Dritte (wie z.B. bei der Verwendung von Google Analytics, Google Fonts, Meta Pixel u.ä.). Dadurch kann ein hohes Risiko für die betroffenen Personen entstehen,

- wenn die Personendaten nicht *vor* der Übermittlung anonymisiert werden oder

- wenn nicht *vor* der Übermittlung eine informierte Einwilligung der Betroffenen eingeholt wird und

– wenn die Erteilung der Einwilligung nicht oder nicht ohne wesentliche Einschränkung der Funktionalität der angebotenen Dienstleistung verweigert werden kann.

Andere Auswertungstools, die nachweisbar nur anonym(isiert)e Daten verwenden oder gar keine Daten an Dritte übermitteln, dürfen eingesetzt werden. In einem solchen Fall ist das in der Projektdokumentation nachvollziehbar zu dokumentieren.

2.3.9 Frage 9: Bearbeitung von Personendaten mit künstlicher Intelligenz ohne Garantie, dass Personendaten ausschliesslich lokal (on-prem) bearbeitet und nicht an Dritte übermittelt werden (Liste der Bearbeitungsvorgänge, Ziff. 2.3)

Bei der Beratung der IDG-Revision in der Justiz-, Sicherheits- und Sportkommission des Grossen Rats wurde darauf hingewiesen, dass ein hohes Risiko für die Grundrechte der betroffenen Personen auch entstehen kann, wenn Personendaten mit künstlicher Intelligenz bearbeitet werden. Die DSB müsse sich deshalb solche Systeme vorlegen lassen.

«Künstliche Intelligenz» ist zurzeit noch ein recht offener Begriff (vgl. dazu z.B. https://www.europarl.europa.eu/topics/de/article/20200827STO85804/was-ist-kunstliche-intelligenz-und-wie-wird-sie-genutzt), der zudem marketingmässig auch für vieles verwendet wird, was mit künstlicher Intelligenz wenig bis nichts zu tun hat. Bis der Begriff klarere Konturen gewinnt und die vorliegende Liste weiter konkretisiert werden kann, sind Vorhaben zur Personendatenbearbeitung vorabkonsultationspflichtig,

– wenn bei der Bearbeitung der Personendaten künstliche Intelligenz (insbesondere maschinelles Lernen) eingesetzt wird und

– nicht garantiert werden kann, dass Personendaten ausschliesslich lokal bearbeitet und nicht an Dritte übermittelt werden.

Die Information, ob künstliche Intelligenz eingesetzt wird bzw. ob garantiert ist, dass Personendaten ausschliesslich lokal bearbeitet und nicht an Dritte übermittelt werden, ist vom öffentlichen Organ bei der Anbieterin in Erfahrung zu bringen und nachvollziehbar zu dokumentieren.

Sobald der Begriff klarere Konturen hat und präziser beurteilt werden kann, welche Formen der Bearbeitung von Personendaten durch künstliche Intelligenz keine Datenschutzrelevanz haben, wird dieses Vorabkonsultations-Kriterium entsprechend «geschärft» werden können.

2.3.10 Frage 10: Basisdienste, bei denen nicht ausgeschlossen werden kann, dass (direkt oder indirekt) besondere Personendaten bearbeitet werden (Liste der Bearbeitungsvorgänge, Ziff. 2.4)

Basisdienste (wie z.B. E-Mail/Kalender, File-Ablagen, Tools für Terminvereinbarungen, eGov-Anwendungen wie Bezahl-Tools usw.) werden zentral für eine Vielzahl von öffentlichen Organen zur Verfügung gestellt. Kann nicht ausgeschlossen werden, dass in einem solchen System (direkt oder indirekt) besondere Personendaten bearbeitet werden, entsteht bei diesen Diensten ein hohes Risiko für die Grundrechte der Betroffenen. Nicht immer ist von Anfang an klar, welche öffentlichen Organe einen solchen Dienst nutzen werden. Er soll nicht von jedem interessierten öffentlichen Organ einzeln, sondern koordiniert nur einmal zur VAK gebracht werden. Dabei geht es insbesondere darum, eine Anwendung für die höchsten der angedachten Ansprüche (z.B. Nutzung des Terminvereinbarungstools durch öffentliche Organe, die von ihrer Aufgabe her regelmässig besondere Personendaten bearbeiten, z.B. die Sozialhilfe) zu beurteilen. Dadurch soll sichergestellt werden,

dass die erforderlichen Massnahmen den höheren Ansprüchen (z.B. erhöhter Schutzbedarf in Bezug auf die Schutzziele der Vertraulichkeit und/oder Integrität) genügen oder, falls das nicht erreicht werden kann, die Anwendung ausschliesslich für niedrigere Ansprüche (z.B. nur für Grundschutzbedarf) zugelassen und damit eine konsequente Umsetzung sichergestellt wird.

Eine andere Art von «Basisdienst» bilden vernetzte Dienste wie zum Beispiel *Identitäts- und Zugangs-Management-Systeme (IAM-Systeme),* die (indirekt) den Zugang zu anderen Systemen steuern, in denen u.U. besondere Personendaten bearbeitet werden. Zwar werden in einem IAM-System direkt keine besonderen Personendaten bearbeitet. Weil sein Inhalt jedoch eine Kernfunktion in der Steuerung des Zugangs zu Systemen mit u.U. sehr sensiblen (Personen-)Daten ausübt, sind bezüglich der Integrität von IAM-Systemen sehr hohe Anforderungen zu stellen. Wird das nicht korrekt geregelt und umgesetzt, entsteht daraus ein hohes Risiko für die Grundrechte der Personen, deren Daten in den durch das IAM-System gesteuerten Systemen bearbeitet werden. Darum sind solche vernetzten Dienste und IAM-Systeme der DSB zur VAK vorzulegen.

Dieser Vorabkonsultationsgrund betrifft primär IT BS und allenfalls die IT der Departemente. Sie sollen im Interesse der Verfahrensökonomie dafür sorgen, dass solche Vorhaben für Basisdienste, bei denen nicht ausgeschlossen werden, dass (direkt oder indirekt) besondere Personendaten bearbeitet werden, rechtzeitig zur VAK kommen.

IT BS und die IT der Departemente können sich für die Frage, ob solche Vorhaben vorabkonsultationspflichtig sind, an die DSB wenden, sobald eine Beschreibung des Vorhabens vorliegt, die eine Beurteilung möglich macht.

2.3.11 Hinweis: Vorabkonsultationspflicht durch Gesetz oder Verordnung vorgesehen

Vorhaben sind auch der DSB zur VAK zu unterbreiten, wenn ein Gesetz oder eine Verordnung dies vorschreibt.

Für Videoüberwachungen, die bei der Einrichtung bzw. Verlängerung der DSB zur VAK vorzulegen sind (§ 18 Abs. 4 IDG), ist nicht die hier verlangte Dokumentation einzureichen, sondern jene nach §§ 8 f. IDV.

2.4 Weiteres Vorgehen

2.4.1 Vorfrage verneint

Wenn die **Vorfrage verneint wird**, dann muss keine DSFA vorgenommen werden. Das ausgefüllte Formular ist durch die Leitung des verantwortlichen öffentlichen Organs zu unterzeichnen, mit der Projektdokumentation abzulegen und auf Verlangen der DSB vorzulegen.

2.4.2 Vorfrage bejaht und alle Fragen 1–10 verneint

Wenn **die Vorfrage bejaht und alle Fragen 1–10 verneint** werden, dann muss keine DSFA vorgenommen werden. Mit dem Vorhaben/Projekt sind in eigener Verantwortung die Grundschutzmassnahmen (und allenfalls weitere Schutzmassnahmen, die sich aus anderen als Datenschutz-Gründen ergeben) umzusetzen. Das ausgefüllte Formular ist durch die Leitung des verantwortlichen öffentlichen Organs, mit der Projektdokumentation abzulegen und auf Verlangen der DSB vorzulegen.

2.4.3 Vorfrage bejaht und mindestens eine der Fragen 1–10 bejaht

Wenn die **Vorfrage** und **mindestens eine der Fragen 1–10 bejaht wird**, dann ist eine DSFA nach § 12a revIDG vorzunehmen, wobei primär alle hier erkannten Risikofaktoren zu behandeln sind. Die dabei zu erarbeitenden Unterlagen sind anschliessend zeitnah der DSB zur VAK vorzulegen.

2.4.4 Die Rolle der/des zuständigen DSBer: Qualitätssicherung

Der/die DSBer übernimmt nicht die Verantwortung für das Vorhaben/Projekt – diese bleibt nach wie vor beim verantwortlichen öffentlichen Organ. Er/sie unterstützt und berät das verantwortliche öffentliche Organ dabei, dass die datenschutzrechtlichen Fragen im Formular korrekt ausgefüllt werden.

3 Datenschutz-Folgenabschätzung (DSFA, § 12a IDG)

Ergibt die Schwellwertanalyse, dass eine DSFA durchgeführt werden muss, sind folgende Dokumente zu erstellen.

3.1 Beschreibung des Vorhabens (Projektbeschreibung) (§ 4 lit. a IDV)

Hier ist das geplante Vorhaben verständlich zu beschreiben. Eine Zusammenfassung (z.B. «Ablösung der Geschäftsverwaltungs-Software») reicht dazu nicht aus. Auf der anderen Seite ist es auch nicht hilfreich, seitenweise Marketingbeschreibungen aus der Werbung der Anbieterin zu zitieren. Das Vorhaben muss in seinem wesentlichen Inhalt für die Verantwortlichen verständlich beschrieben werden, die in der Regel keine Spezialist:innen beispielsweise für IT sind.

Damit aus Datenschutzsicht eine Beurteilung vorgenommen werden kann, ist es unerlässlich, dass die Datenbearbeitungen beschrieben werden. Relevant sein können z.B.:

- Welche (Kategorien von) *Personendaten* (oder Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterstehen) werden zu welchem *Zweck* durch *wen* (durch das öffentliche Organ oder in seinem Auftrag durch Auftragsdatenbearbeiter:innen) bearbeitet?

- Bei wem bzw. aus welchem anderen System werden die Daten *erhoben*, und wem werden die Daten in welcher Form (identifizierend, pseudonymisiert, anonymisiert) zu welchem Zweck *bekannt gegeben*?

Bei IT-Systemen, insbesondere bei komplexeren, dienen auch Datenflussanalysen, Architekturskizzen, die Beschreibung der Schnittstellen zu Um- und Untersystemen der Beschreibung des Vorhabens.

Für diese Beschreibung sind allenfalls diejenigen Stellen beizuziehen, die hinreichend vertiefte Kenntnis haben von den Datenbearbeitungen im geplanten Vorhaben.

Ohne eine verständliche Beschreibung des Vorhabens können weder die Leitung des verantwortlichen öffentlichen Organs die Verantwortung übernehmen noch die DSB die notwendige Beurteilung vornehmen; die Dokumentation wird von der DSB zur Vervollständigung zurückgewiesen.

3.2 Darstellung der Rechtslage (§ 4 lit. b IDV)

Hier ist die Rechtslage für das geplante Vorhaben darzustellen (sog. Rechtsgrundlagenanalyse). Dazu reicht es nicht, Gesetze oder Verordnungen zu nennen. Es ist damit vielmehr zu belegen, welche Rechtsgrundlagen die **Datenbearbeitungen**, die oben in der Projektbeschreibung (Ziff. 3.1) aufgeführt werden, **gesetzmässig und verhältnismässig** erscheinen lassen. Falls noch keine hinreichend bestimmten Rechtsgrundlagen bestehen, sind diese im Rahmen des Projekts/Vorhabens allenfalls zu schaffen.

Das IDG verlangt für die Bearbeitung von Personendaten eine Rechtsgrundlage (§ 9 IDG bzw. für die Bekanntgabe von Personendaten: § 21 IDG), für das Bearbeiten von besonderen Personendaten oder ein Profiling eine Grundlage in einem Gesetz im formellen Sinn (§ 9 Abs. 2 IDG bzw. für die Bekanntgabe von besonderer Personendaten oder von Resultaten eines Profilings: § 21 Abs. 2 IDG). Die entsprechenden Rechtsgrundlagen finden sich regelmässig nicht im IDG, sondern in den jeweiligen Sachgesetzen oder -verordnungen, z.B. im Polizeirecht, Sozialversicherungsrecht, Schulrecht usw. Sie können in zwei Formen vorliegen:

- als *unmittelbare gesetzliche Grundlage*, die unmittelbar das Datenbearbeiten (oder -bekanntgeben) regelt, oder

- als *mittelbare gesetzliche Grundlage*, die eine Aufgabe statuiert, die nur erfüllt werden kann, wenn Personendaten bearbeitet (oder bekannt gegeben) werden dürfen, die also bloss mittelbar das Datenbearbeiten (oder -bekanntgeben) regelt.

Für die Darstellung der Rechtslage sind allenfalls die zuständigen Rechtsabteilungen oder Rechtsdienste beizuziehen.

Ohne eine nachvollziehbare Darstellung der Rechtslage können weder die Leitung des verantwortlichen öffentlichen Organs die Verantwortung übernehmen noch die DSB die notwendige Beurteilung vornehmen; die Dokumentation wird von der DSB zur Vervollständigung zurückgewiesen.

3.3 Übersicht über die Massnahmen zur Verhinderung von Persönlichkeitsverletzungen (§ 4 lit. c IDV)

3.3.1 Fokus der Risikoabwägung

Wenn die SWA in einem oder mehreren Bereichen ein hohes Risiko gezeigt hat oder wenn in der Schutzbedarfsanalyse (SCHUBAN) in Bezug auf ein Schutzziel oder auf mehrere Schutzziele § 8 Abs. 2 IDG: insb. Vertraulichkeit, Integrität und Verfügbarkeit) ein erhöhter Schutzbedarf festgestellt worden ist, dann ist vom verantwortlichen öffentlichen Organ – mit Fokus auf die erkannten Bereiche bzw. Schutzziele – eine **umfassende Risikoabwägung** vorzunehmen.

Die bei Vorhaben mit erhöhtem Schutzbedarf erforderliche Risikoabwägung beinhaltet zweierlei:

1. auf der einen Seite die *Informationssicherheit*, die (in der kantonalen Verwaltung) im Rahmen des Informationssicherheits-Managements-Systems (ISMS) bearbeitet werden kann, und

2. auf der anderen Seite die **Datenschutz-Folgenabschätzung**, die zu der in § 4 lit. c IDV erwähnten Übersicht über die Massnahmen zur Verhinderung von Persönlichkeitsverletzungen führt.

In diesem Rahmen sind Projektrisiken zu eruieren, aber – zusätzlich zu den üblicherweise betrachteten Projektrisiken wie z.B. dem Risiko, dass die Anbieterin in Konkurs geht – die mit dem geplanten Vorhaben verbundenen **Risiken für die Grundrechte der betroffenen Personen**. Dazu gehören insbesondere

- der Verletzung der *Vertraulichkeit* (Zugang zu Personendaten durch Unberechtigte) und/oder
- der *Integrität* von Personendaten (ungewollte oder ungerechtfertigte Veränderung der Personendaten),
- allenfalls auch der *Verfügbarkeit* (Verlust von Personendaten).

Betroffene sind die Personen, deren Personendaten im Rahmen des Projektes/Vorhabens bearbeitet werden, das sind regelmässig auch Mitarbeiter:innen.

3.3.2 Eruierung und Bewertung der Risiken, Massnahmen

Es sind die **Bruttorisiken** für die Grundrechte der Betroffenen zu eruieren und zu bewerten. Wenn die Risiken als hoch beurteilt werden, sind die **(technischen, organisatorischen und rechtlichen) Schutzmassnahmen** vorzusehen, die das Risiko vermeiden oder auf ein tragbares Mass vermindern. Das verbleibende **Nettorisiko** (das Bruttorisiko minus die Verkleinerung des Risikos durch die Schutzmassnahmen) ist von der verantwortlichen Stelle (der Leitung des öffentlichen Organs, das mit dem geplanten Vorhaben eine gesetzliche Aufgabe erfüllt, also der Dateneignerin nach § 6 IDG) zu übernehmen. Wird das Nettorisiko als nicht tragbar angesehen, ist auf das Vorhaben zu verzichten.

Die Risiken werden beurteilt nach der **Eintretenswahrscheinlichkeit** und der **Schadensschwere** und sind in einer Risiko-Matrix einzutragen – einmal in einer Matrix mit den Bruttorisiken und einmal, zusammen mit der Veränderung durch die Schutzmassnahmen, in einer Matrix mit den Nettorisiken.

Die **Massnahmen** sind den Risiken zuzuordnen: Mit welcher Massnahme soll welches Risiko vermieden oder vermindert werden? Ein Risiko kann durch mehrere Massnahmen angesprochen werden, und Massnahmen können verschiedene Risiken ansprechen. Massnahmen können ein Risiko in Bezug auf die Eintretenswahrscheinlichkeit und/oder das Schadensausmass beeinflussen.

Beispiele:

- Eine Verschlüsselung (technische Massnahme) eines Servers kann die Eintretenswahrscheinlichkeit eines Risikos (z.B. durch Hacking) reduzieren.
- Eine Beschränkung der Attribute der in einer Cloud ausgelagerten Daten mittels einer Weisung an die Anwender:innen eines Programms kann die Schadensschwere eines Risikos reduzieren (organisatorische Massnahme).

3.3.3 Darstellung

3.3.3.1 Tabelle

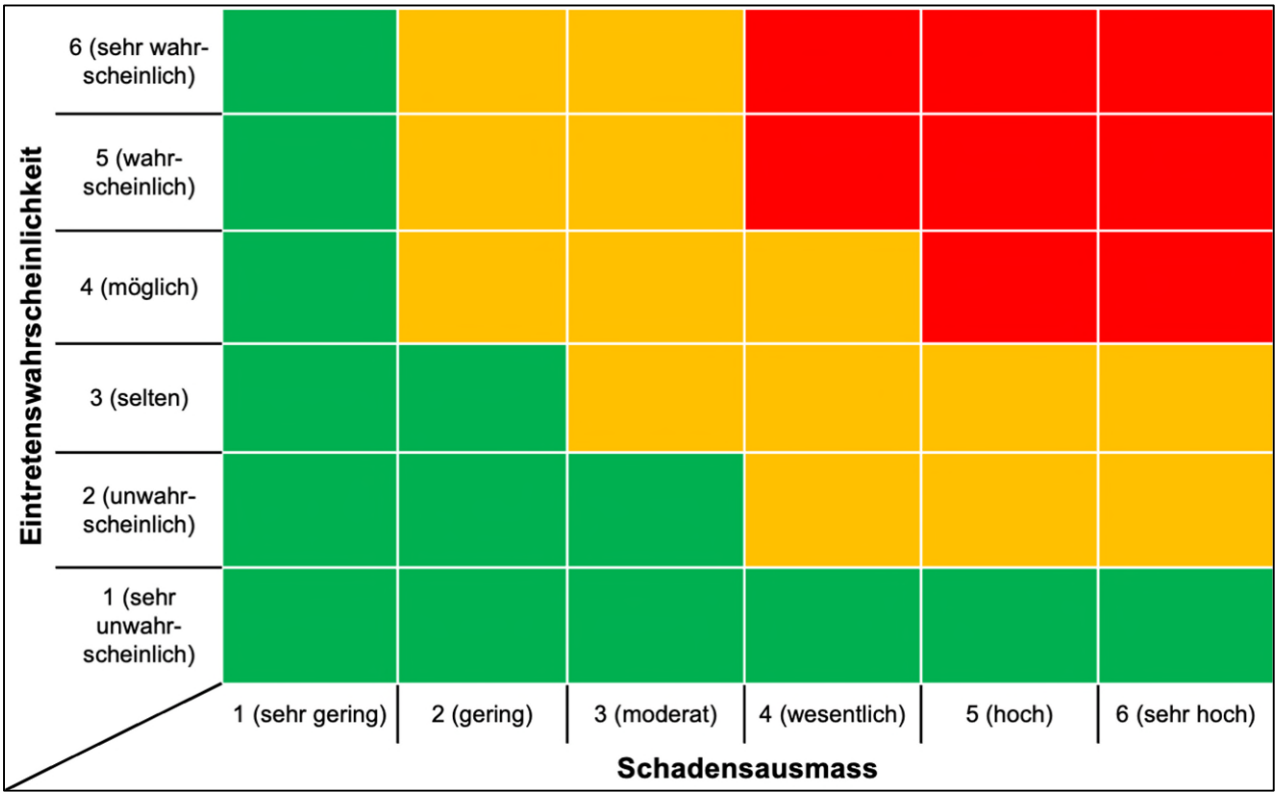
Wir empfehlen, die Risiken und dazugehörenden Massnahmen samt den Risikobewertungen (Bruttorisiko, Risikoreduktion, Nettorisiko (Restrisiko)) in einer oder mehreren Tabellen zu erfassen.

3.3.3.2 Bruttorisiko-Matrix und Nettorisiko-Matrix

Gleichzeitig sind im Interesse einer verständlichen Darstellung für das öffentliche Organ, das die Massnahmen abnehmen und das Restrisiko übernehmen muss, die Bruttorisiken und die Nettorisiken in einer Risikomatrix (Eintretenswahrscheinlichkeit x Schadensschwere) grafisch darzustellen. Wir empfehlen, dafür die folgende 6x6-Matrix zu verwenden, wie sie auch schon im ISMS für die Darstellung der Informationssicherheitsrisiken verwendet wird, mit den folgenden Stufen:

– für die **Eintretenswahrscheinlichkeit** 1: sehr unwahrscheinlich, 2: unwahrscheinlich, 3: selten, 4: möglich, 5: wahrscheinlich, 6 sehr wahrscheinlich;

– für die **Schadensschwere** 1: sehr gering, 2: gering, 3: moderat, 4: wesentlich, 5: hoch, 6: sehr hoch:



Dabei bedeuten die **Farben** in der **Bruttorisiko-Matrix** (Eintretenswahrscheinlichkeit x Schadensausmass):

Farbe	Punkte	Beschreibung, Konsequenz
rot	20-36	sehr hohes Risiko, auf jeden Fall mit Schutzmassnahmen zu verringern
orange	7-19	mittleres bis hohes Risiko, mit Schutzmassnahmen zu verringern
grün	<7	geringes Risiko, akzeptabel

In der **Nettorisiko-Matrix** (Eintretenswahrscheinlichkeit x Schadensausmass) bedeuten die **Farben**:

Farbe	Punkte	Beschreibung, Konsequenz
rot	20-36	weiterhin sehr hohes Risiko, nicht tragbar; wenn es nicht verringert werden kann, ist auf das Projekt/Vorhaben zu verzichten
orange	7-19	weiterhin mittleres bis hohes Risiko; muss von verantwortlichem öffentlichen Organ ausdrücklich übernommen werden, wobei es zu begründen hat, warum das Risiko nicht weiter verringert werden kann und wieso sich daraus für die betroffenen Personen keine untragbaren Risiken ergeben
grün	<7	geringes Risiko, akzeptabel

In der **Nettorisiko-Matrix** sollte zur besseren Nachvollziehbarkeit bei jedem Risiko die **Risikoreduktion** durch die beschlossenen Massnahmen durch einen Pfeil dargestellt werden:

- Ein **Pfeil nach links** zeigt, wie stark das Schadensausmass durch die beschlossenen Massnahmen reduziert wird (etwa, wenn im System statt besonderen Personendaten nur noch «gewöhnliche» Personendaten enthalten sind oder wenn Personendaten im System nur noch pseudonymisiert oder anonymisiert geführt werden);

- Ein **Pfeil nach unten** zeigt, wie stark die Eintretenswahrscheinlichkeit durch die beschlossenen Massnahmen reduziert wird (etwa, wenn durch eine Mehrfachauthentisierung das Risiko des Zugriffs durch Unbefugte reduziert wird);

- Ein **Pfeil nach links und nach unten** zeigt, wenn durch die beschlossenen Massnahmen sowohl das Schadensausmass als auch die Eintretenswahrscheinlichkeit reduziert werden.

4 Vorabkonsultation der DSB (§ 13 IDG)

4.1 Allgemeines

Wie erwähnt muss ein Vorhaben/Projekt, bei dem wegen des hohen Risikos für die Grundrechte der betroffenen Personen eine DSFA durchzuführen ist, *immer* auch der Datenschutzbeauftragten vorgelegt werden. Wenn sich im Laufe der DSFA herausstellt, dass (entgegen der Beurteilung im Rahmen der SWA, wonach voraussichtlich ein hohes Risiko besteht) tatsächlich kein hohes Risiko besteht, kann auch die Vorlage an die DSB zur VAK unterbleiben. Dies ist in der Projektdokumentation festzuhalten und der DSB auf Verlangen herauszugeben.

4.2 Fokus der VAK

Die bei der DSFA erstellte Dokumentation ist der DSB zur VAK vorzulegen. Diese hat zu beurteilen, ob – wenn die vorgesehenen Massnahmen umgesetzt werden – ein Vorhaben **datenschutzkonform umsetzbar** ist, oder zu empfehlen, dass (und allenfalls welche) weiteren Massnahme zu ergreifen sind, damit ein Vorhaben datenschutzkonform umsetzbar ist (§ 46 IDG).

4.3 Form der einzureichenden Dokumentation

In welcher Form diese Dokumentation eingereicht werden muss, ist nicht vorgeschrieben. Es sind nicht zwingend die drei wie oben Ziff. 3.1-3.3 beschriebenen Dokumente. Die nötigen Informationen müssen aber in der vorgelegten Dokumentation einfach auffindbar sein (Lesehilfe).

Es ist möglich (und sinnvoll), die Informationen zusammenzufassen in einem Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept). Dabei sind auch Verweise auf spezifische Teilkonzepte möglich.

Ein ISDS-Konzept muss (aus Datenschutzsicht) folgenden Mindestinhalt aufweisen:

- Beschreibung des Vorhabens (oben Ziff. 3.1);
- Darstellung der Rechtslage (oben Ziff. 3.2);
- Rollen- und Berechtigungskonzept;
- Regelung der Protokollierung (und ggf. der Auswertung der Protokolldaten);
- Backup- und Restore-Konzept;
- Aufbewahrungs-, Archivierungs- und Löschungskonzept;
- Gewährleistung der Datenschutzrechte der betroffenen Personen: Recht auf Zugang zu den eigenen Personendaten (§ 26 IDG), Anspruch auf Berichtigung bzw. Vernichtung unrichtiger Personendaten (§ 27 Abs. 1 lit. a IDG), auf Unterlassung eines widerrechtlichen Bearbeitens (§ 27 Abs. 1 lit. b IDG), auf Beseitigung der Folgen eines widerrechtlichen Bearbeitens, insb. Löschung der Daten oder Bekanntgabesperrung (§ 27 Abs. 1 lit. c IDG), auf Feststellung der Widerrechtlichkeit (§ 27 Abs. 1 lit. d IDG) samt jeweilige Mitteilung an Personen und Stellen, denen die Daten zuvor bekannt gegeben worden sind (§ 27 Abs. 1ter IDG), Recht auf Sperrung der Bekanntgabe von Personendaten an Private (§ 28 Abs. 1 IDG);
- Spezifische Konzepte, falls Auftragsdatenbearbeiter:innen beigezogen werden oder Cloud-Dienste genutzt werden.

Datenschutzrechtlich von Bedeutung sind auch die Vorkehrungen der **Informationssicherheit**. Zu einem ISDS-Konzept gehören insbesondere Aussagen zu den folgenden Aspekten:

- Beschreibung des Gesamtsystems (inkl. Systemarchitektur und Schnittstellen, Systemgrenzen);
- Datenflüsse (inkl. Beschreibung der zu bearbeitenden Informationen);
- Zugang für Benutzer:innen, Administrator:innen, Dritte;
- Authentisierungs- und Autorisierungsmechanismen;
- Verschlüsselung;
- Software Deployment;
- Viren- und Malwareschutz.

4.4 Nachweis der Datenschutzkonformität (§ 6 Abs. 3 IDG)

Mit dem korrekt erstellten ISDS-Konzept soll auch der **Nachweis** erbracht werden können, dass das öffentliche Organ bei der entsprechenden Datenbearbeitung die **Datenschutzvorschriften einhält** (§ 6 Abs. 3 IDG).