kanton glarus

Telefon 055 646 60 19
E-Mail: elias.krummenacher@gl.ch
www.gl.ch

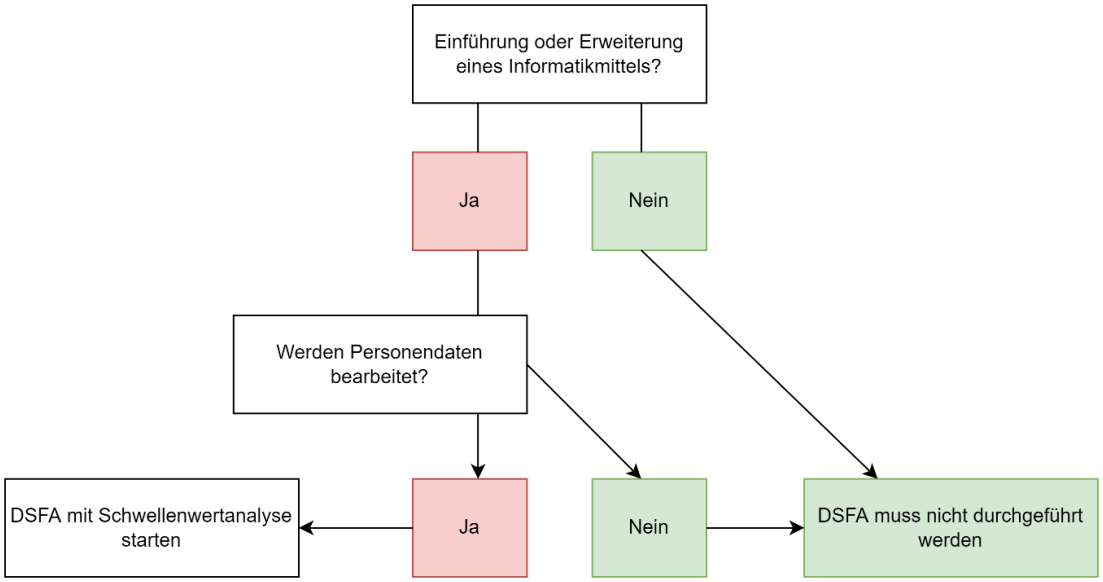
Staatskanzlei
Fachstelle Datenschutz
Rathaus
8750 Glarus

Version 1.0 – Dezember 2022

Merkblatt Datenschutz-Folgenabschätzung

1. Einleitendes

Dieses Merkblatt unterstützt die öffentlichen Organe des Kantons Glarus beim Bearbeiten des Formulars Datenschutz-Folgenabschätzung (nachfolgend auch DSFA). Die Pflicht zur Erstellung einer DSFA liegt beim öffentlichen Organ, das für die beabsichtigte Datenbearbeitung verantwortlich ist (Art. 32 IDAG). Eine Datenschutz-Folgenabschätzung muss grundsätzlich bei Einführung oder Erweiterung von Informatikmitteln erstellt werden. Sofern die beabsichtigten Informatikmittel keine Personendaten bearbeiten, muss die DSFA hingegen nicht durchgeführt werden (Art. 23 Abs. 1 VIDAG).



2. Zeitpunkt der Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung ist erforderlicher Bestandteil des Informatik-Projektantrags (Art. 17 Abs. 4 Verordnung über die Informatik). Für jedes Informatikmittel, das neu beschafft oder erweitert werden soll, ist demnach eine Datenschutz-Folgenabschätzung durchzuführen. Zusammen mit dem Projektantrag ist der Hauptabteilung Informatik die Schwellenwertanalyse bzw. die finalisierte DSFA vorzulegen. Bei Nichteinreichung der Datenschutz-Folgenabschätzung gilt der Informatik-Projektantrag als unvollständig. In der Folge bliebe dieser unberücksichtigt.

Die Datenschutz-Folgenabschätzung ist mit genügendem zeitlichem Vorsprung zum Antrag Informatik-Projektantrag durchzuführen, um in Erfahrung bringen zu können, ob die beabsichtigte Datenbearbeitung trotz risikominimierenden Massnahmen ein hohes Risiko für die Verletzung der Persönlichkeit oder der Grundrechte von Betroffenen mit sich bringt. Sollte dies der Fall, so muss die geplante Datenbearbeitung der Fachstelle Datenschutz (nachfolgend auch DSB) zur Vorab-Konsultation vorgelegt werden (Art. 34 Abs. 1 IDAG). Die frühzeitige Ermittlung des mit der Datenbearbeitung einhergehenden Risikos dient dem verantwortlichen öffentlichen Organ dabei, abwägen zu können, ob bzw. unter Berücksichtigung welcher risikominierenden Massnahmen die Beschaffung eines Informatikmittels angezeigt ist.

Wird die Datenschutz-Folgenabschätzung hingegen erst durchgeführt, wenn der Beschaffungsprozess bereits fortgeschritten oder gar abgeschlossen ist, so trägt das verantwortliche öffentliche Organ das

Risiko, dass im Zuge einer allfälligen Vorab-Konsultation festgestellt wird, dass die Datenbearbeitung ganz oder teilweise Vorschriften über den Datenschutz verletzt. Im äussersten Fall kann empfohlen werden, ein bereits beschafftes Informatikmittel nicht zu nutzen (Art. 58 Abs. 3 IDAG).

Gleiches gilt, wenn die Datenschutz-Folgenabschätzung ohne eigentliche Sachkenntnisse über das zu beschaffende Informatikmittel durchgeführt wird. Wird bspw. nachträglich festgestellt, dass das in der Datenschutz-Folgenabschätzung ermittelte Risiko fälschlicherweise als zu niedrig eingestuft wurde, so ist das öffentliche Organ für allfällige Verletzungen von Datenschutzvorschriften verantwortlich. Um sich hinreichend mit dem zu beschaffenden Informatikmittel vertraut machen zu können, ist es sinnvoll, frühzeitig die entscheidrelevante Dokumentation (siehe etwa Formular Datenschutz-Folgenabschätzung 9. Bereits vorhandene Dokumentation) einzuholen und potenzielle Anbieter rückfrageweise zu konsultieren.

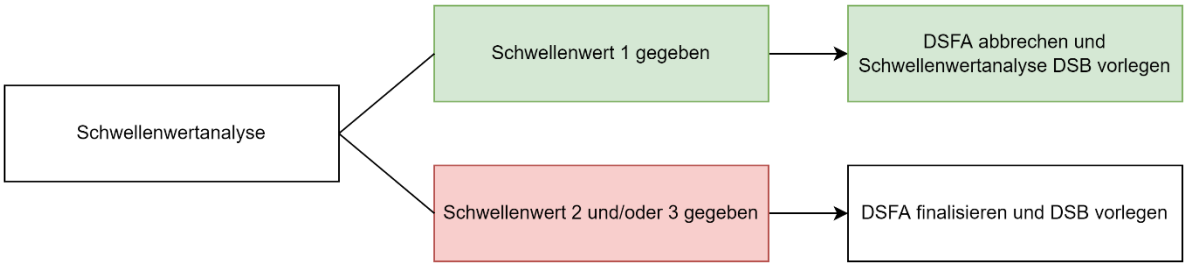
Die Fachstelle Datenschutz steht, unter Mitwirkung der Hauptabteilung Informatik, bei der Bearbeitung der Datenschutz-Folgenabschätzung beratend zur Verfügung.

3. Ablauf der Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung ist zweigeteilt, um eine Triage der relevanten Datenbearbeitungen zu ermöglichen. Mittels der Schwellenwertanalyse wird bestimmt, ob eine rechtliche Ausnahme von der bzw. eine rechtliche Pflicht zur Datenschutz-Folgenabschätzung besteht.

3.1. Schwellenwertanalyse

Während der Schwellenwert 1 die rechtlichen Ausnahmen von der DSFA umfasst, beinhalten die Schwellenwerte 2 und 3 jene beabsichtigten Datenbearbeitungen, die eine DSFA verpflichtend machen. Zeigt die Schwellenwertanalyse auf, dass die rechtliche Pflicht zur DSFA besteht, muss das Formular Datenschutz-Folgenabschätzung finalisiert werden (weiter ab 3.2. Finalisierung der Datenschutz-Folgenabschätzung). Ergibt die Schwellenwertanalyse hingegen, dass keine DSFA erforderlich ist, muss das Formular nicht weiterbearbeitet werden. Die DSFA ist somit abgeschlossen. So oder so ist das Ergebnis der Fachstelle Datenschutz (DSB) vorzulegen.



Die DSFA muss nicht erarbeitet werden, wenn für die beabsichtigte Datenbearbeitung ein Datenschutznachweis vorliegt (Art. 32 Abs. 2 IDAG; Art. 33 Abs. 3 IDAG; Art. 22 VIDAG) oder für die beabsichtigte Datenbearbeitung eine ausdrückliche gesetzliche Grundlage vorliegt (Art. 23 Abs. 3 VIDAG).

Eine Datenschutz-Folgeabschätzung muss hingegen durchgeführt werden, wenn die beabsichtigte Datenbearbeitung zu Testzwecken erfolgt (Art. 29 Abs. 2 IDAG) und/oder die beabsichtigte Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte führt. Ob ein Informatikmittel voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte von betroffenen Personen führt, muss teilweise antizipiert werden. Sofern bei der Beurteilung Probleme oder Fragen auftauchen, soll die Fachstelle Datenschutz beratend hinzugezogen werden. Eine eingehende Auseinandersetzung mit dem Aspekt des voraussichtlich hohen Risikos ist bei der Erarbeitung der Datenschutz-Folgenabschätzung zentral.[1]

[1] Zu den einzelnen Risiken siehe Formular Datenschutz-Folgenabschätzung, Schwellenwert 3 sowie das hier enthaltene Kapitel 3.3.4. Erläuterungen zu den voraussichtlichen Risiken für die Persönlichkeit und die Grundrechte.

3.2. Finalisierung der Datenschutz-Folgenabschätzung

Ergibt die Schwellenwertanalyse, dass die DSFA fortgeführt werden muss, hat das verantwortliche öffentliche Organ die beabsichtigte Datenbearbeitung im Formular Datenschutz-Folgenabschätzung weiter zu beschreiben. Folgende weiteren Aspekte sind hierbei zu thematisieren:

3.2.1. Angaben zur rechtlichen Grundlage

Im Formular Datenschutz-Folgenabschätzung ist die gesetzliche Grundlage oder – sofern nicht gegeben – die gesetzliche Aufgabe, die zur beabsichtigten Datenbearbeitung ermächtigt, zu benennen. Im Formular sollen der einschlägige Rechtserlass sowie die Artikel des Rechtserlasses präzise aufgeführt werden. Im Merkblatt «Voraussetzungen und Grundsätze für die Bearbeitung von Personendaten» sind ebenfalls weiterführende Erläuterungen zu finden.

3.2.2. Beschreibung der geplanten Datenbearbeitung

Erläuterungen hierzu finden sich im Formular Datenschutz-Folgenabschätzung. Grundsätzlich gilt, dass die Beschreibung so ausführlich wie nötig und so kurz und präzis wie möglich sein soll.

3.2.3. Beschreibung der Verhältnismässigkeit der Datenbearbeitung

Erläuterungen hierzu finden sich im Formular Datenschutz-Folgenabschätzung. Grundsätzlich gilt, dass die Beschreibung so ausführlich wie nötig und so kurz und präzis wie möglich sein soll. Im Merkblatt «Voraussetzungen und Grundsätze für die Bearbeitung von Personendaten» sind ebenfalls weiterführende Erläuterungen zu finden.

3.2.4. Erläuterungen zu den voraussichtlich hohen Risiken für die Persönlichkeit und die Grundrechte

Die unter dem Schwellenwert 3 genannten Risiken und allenfalls weitere Risiken sollen im Formular so ausführlich wie nötig und so kurz und präzis wie möglich beschrieben werden. Ein Risiko für die Persönlichkeit und die Grundrechte der Betroffenen ist insbesondere dann zu vermuten, wenn die beabsichtigte Datenbearbeitung zu physischen oder psychischen, materiellen und/oder immateriellen Schäden für natürliche Personen führen könnte. Personen, die einen entsprechenden Schaden erlitten haben, weil datenschutzrechtliche Vorschriften verletzt wurden, können denn auch Schadenersatz- bzw. Genugtuungsansprüche gemäss dem Staatshaftungsgesetz geltend machen (Art. 61 IDAG).

Physische und psychische Schäden können etwa aufgrund unrichtiger Daten bzw. Datenbearbeitungsvorgängen eintreten, bspw., wenn daraus eine fehlerhafte medizinische Behandlung resultiert. Auch psychische Schäden sind in der DSFA zu erfassen, bspw. Angstzustände, Depressionen oder andere psychische Schädigungen bspw. als Folge einer (unrechtmässigen) polizeilichen Überwachung. Führt eine Datenbearbeitung zu einer schwerwiegenden Grundrechtsverletzung, etwa, weil eine Prognose über künftiges deliktisches Verhalten falsch ist, können daraus für Betroffene psychische Schäden entstehen. Weitere: Vertraulichkeitsverlust von Adressdaten führt zu Stalking etc.

Immaterielle Schäden können etwa gesellschaftliche und soziale Nachteile sein, sofern sie Folge der Datenbearbeitung sind (Rufschädigungen, automatisierte Entscheidungen betreffend Zugang zu einer Dienstleistung etc.). Unter die immateriellen Schäden fallen etwa auch Einschüchterungseffekte, wobei Betroffene aus Angst vor staatlichen Repression davor zurückschrecken, ihre verfassungsmässigen Rechte auszuüben (bspw. Meinungsfreiheit, Versammlungsfreiheit, ungestörte Ausübung der Religionszugehörigkeit etc.). Auch Profiling kann zu immateriellen Schäden führen, etwa wenn eine mangelnde Integrationsfähigkeit in den Arbeitsmarkt analysiert wird. Weitere: Verlust der Kontrolle über eigene Daten, Vertraulichkeitsverlust von Gesundheitsdaten etc.

Materielle Schäden sind primär wirtschaftlicher Natur. In Betracht kommen bspw. berufliche und damit einhergehende finanzielle Nachteile (unrechtmässige Leistungs- und Verhaltenskontrolle durch den Arbeitgeber gefolgt von entgangener Beförderung, erfolgter Abmahnung oder Jobverlust), Beschneidung staatlicher Leistungen (Sozialhilfeleistungen, Taggelder bei Arbeitslosigkeit etc.), Diskriminierung (bspw. bei der Festlegung des Invaliditätsgrades), Identitätsdiebstahl oder –betrug etc. Materielle Schäden können auch durch Analysen von persönlichen Merkmalen (Profiling) oder aufgrund von Vorhersagen von Entwicklungen (Prognose) entstehen, um etwa die Arbeitsleistung oder die Integrationsfähigkeit in den Arbeitsmarkt zu beurteilen. Weitere: Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Personendaten und damit einhergehender Reputationsverlust etc.

Mögliche Schäden bzw. Risiken sollen in dem Umfang im Formular erläutert werden, als dass sie bereits antizipiert werden können. Nachfolgend ein Beispiel zur Umschreibung eines möglichen Risikos für die Persönlichkeit oder die Grundrechte von Betroffenen:

Materieller, immaterieller und psychischer Schaden durch Profiling: Die beabsichtigte Datenbearbeitung ermöglicht die Integrationsfähigkeit von Arbeitslosen in den Arbeitsmarkt automatisiert zu analysieren. Je nach ermittelter Einstufung der Integrationsfähigkeit erhalten Arbeitsuchende umfassende oder aber reduziertere Fördermassnahmen zugesprochen. Eine fehlerhafte Datenbearbeitung hätte zur Folge, dass die Integrationsfähigkeit falsch ermittelt und bestimmte Personen bei der Integration in den Arbeitsmarkt benachteiligt würden. Die Schäden können materieller (Einkommenseinbussen), immaterieller (soziale Nachteile im privaten Umfeld) und psychischer Natur sein (fehlende Beschäftigung führt zu Desintegration, Vereinsamung, Depressionen etc.). Zwar ist der Kreis der Betroffenen bestimmbar (alle Arbeitsuchenden), jedoch können durch den Einsatz der beabsichtigten Datenbearbeitung viele Personen von den negativen Folgen bzw. Risiken betroffen sein.

3.2.5. Bewertung der Risiken hinsichtlich Schwere des Eingriffs in die Persönlichkeit oder die Grundrechte von Betroffenen

Die ermittelten Risiken bzw. potenziellen Schäden sollen im Formular Datenschutz-Folgenabschätzung hinsichtlich ihrer Schwere beurteilt werden. Dabei stehen drei Schweregrade pro Risiko zur Auswahl: gering, normal, hoch. Zudem soll erläutert werden, weshalb das ermittelte Risiko im entsprechenden Schweregrad eingestuft wurde.

Sofern die Risiken bzw. potenziellen Schäden eintreten sollten, ist die Schwere des Eingriffs in die Persönlichkeit oder die Grundrechte der Betroffenen als hoch einzustufen, da für sie materielle, immaterielle und psychische Schäden drohen. Zudem ist der Kreis möglicher Betroffener zwar bestimmbar, jedoch wäre eine Vielzahl von Personen von den genannten Risiken betroffen.

3.2.6. Bewertung der Eintretenswahrscheinlichkeit der identifizierten Risiken

Das verantwortliche öffentliche Organ prüft die beabsichtigte Datenbearbeitung mit Blick auf die Eintretenswahrscheinlichkeit der identifizierten Risiken. Im Formular Datenschutz-Folgenabschätzung sind die wesentlichen Erkenntnisse hinsichtlich Eintretenswahrscheinlichkeit aufzuführen (Textfeld «Risiko und Begründung zur Bewertung benennen»). Die Ausführungen dazu sollen so ausführlich wie nötig und so kurz und präzis wie möglich sein. Zudem soll die Eintretenswahrscheinlichkeit pro ermitteltem Risiko als tief, normal oder hoch ausgewiesen werden.

Die Wahrscheinlichkeit, dass genannte Risiken eintreten ist als hoch einzustufen, da die automatisiere Analyse nicht überprüft werden kann (fehlende Transparenz hinsichtlich Algorithmus oder Algorithmus kann nicht nachvollzogen werden) und folglich kann Diskriminierung basierend auf Geschlecht, Rasse, Alter etc. nicht ausgeschlossen werden.

3.2.7. Geplanten Massnahmen zur Bewältigung der ermittelten Risiken

Es sind die angemessenen technischen und organisatorischen Massnahmen, die zur Minimierung der ermittelten Restrisiken ergriffen werden sollen, zu benennen (zu den einzelnen organisatorischen und technischen Massnahmen siehe Art. 12 Abs. 1 und 13 VIDAG). Für jede geplante Massnahme ist zudem zu erläutern, inwiefern diese das Risiko hinsichtlich ermittelter Schwere und Eintretenswahrscheinlichkeit reduzieren kann. Hierbei ist darauf zu achten, dass die zu ergreifenden Massnahmen effektiv, umsetzbar, einhaltbar und überprüfbar sind (Art. 12 Abs. 2 und 3 VIDAG), was aus der entsprechenden Erläuterung auch hervorgehen soll. Die Ausführungen dazu sollen so ausführlich wie nötig und so kurz und präzis wie möglich sein.

Als organisatorische Massnahme ist geplant, dass die Auswertungen zur Integrationsfähigkeit von Arbeitsuchenden nicht ausschliesslich automatisiert erfolgen soll und eine Fachperson die Ergebnisse einer individuellen Bewertung unterzieht. Somit wird dem Risiko, dass die automatisierte Analyse fehlerhaft oder diskriminierend sein kann, zu einem gewissen Teil Rechnung getragen.

3.2.8. Neubewertung der ermittelten Risiken

Ziel der Datenschutz-Folgenabschätzung ist es, die verbleibenden Restrisiken unter Berücksichtigung der geplanten technischen und organisatorischen Massnahmen neu zu bewerten. Die hier ermittelten Restrisiken sollen einzeln als tief, normal oder hoch ausgewiesen werden.

Aufgrund der ergriffenen organisatorischen Massnahme (individuelle Bewertung durch Fachperson) ist im Ergebnis von einer mittleren bis hohen Eintretenswahrscheinlichkeit der Risiken auszugehen.

3.2.9. Bereits vorhandene Dokumentation

Grundsätzlich bedarf es einer Dokumentation zur beabsichtigten Datenbearbeitung. Je nach Datenbearbeitung können sich die Anforderungen an die Dokumentation ändern. Typischerweise basiert eine eingehende Risikobeurteilung von Informatikmitteln auf der Grundlage eines sogenannten Informations- und Datenschutz-Konzepts (nachfolgend ISDS-Konzept), welches durch das verantwortliche öffentliche Organ, unter Mitwirkung der Hauptabteilung Informatik, zu erstellen ist (Art. 11 Abs. 1 VIDAG). Es beinhaltet im Wesentlichen eine Schutzbedarfs- und Risikobeurteilung und benennt die Eintretenswahrscheinlichkeit und die möglichen Folgen einer Verletzung der Datensicherheit (Art. 11 Abs. 1 VIDAG). Zusätzlich beschreibt es angemessene technische und organisatorische Massnahmen, die zur Minimierung der ermittelten Restrisiken ergriffen werden sollen (Art. 11 Abs. 2 VIDAG). Das ISDS-Konzept ist der Fachstelle Datenschutz im Falle einer rechtlichen Pflicht zur Vorab-Konsultation vorzulegen. Ebenfalls typischerweise einzureichen ist eine hinreichend klar skizzierte bzw. umschriebene Systemarchitektur, worin eine Übersicht der Systeme, Schnittstellen und Prozesse aufgezeigt wird. Hiermit kann etwa festgestellt werden, an welche Umsysteme bzw. über welche Schnittstellen Daten an wen bekanntgegeben werden und ob ein Auftragsdatenbearbeitungsvertrag erstellt werden muss. Eine nichtabschliessende Liste der möglichen Dokumentation ist im Formular Datenschutz-Folgenabschätzung auffindbar. Weitere prüfrelevante Dokumente sind in Absprache mit der Fachstelle Datenschutz, und unter Mitwirkung der Hauptabteilung Informatik, zu ermitteln.

3.3. Abschluss der DSFA

3.3.1. Abschluss der DSFA ohne Konsultationspflicht

Ergibt sich aus der Datenschutz-Folgenabschätzung kein hohes Risiko für die Verletzung der Persönlichkeit oder der Grundrechte von betroffenen Personen, so hat das öffentliche Organ die beabsichtigte Datenbearbeitung nicht zur Vorab-Konsultation an die Fachstelle Datenschutz vorzulegen. Das öffentliche Organ teilt der Fachstelle Datenschutz (DSB) das dokumentierte Ergebnis der Datenschutz-Folgenabschätzung jedoch unabhängig davon mit, ob die Einführung oder Erweiterung von Informatikmitteln eine Vorab-Konsultation bedingt oder nicht (Art. 23 Abs. 4 VIDAG).

3.3.2. Abschluss der DSFA und Pflicht zur Vorab-Konsultation

Sofern trotz Einsatz von technischen und organisatorischen Massnahmen ein oder mehrere identifizierte Risiken hinsichtlich ermittelter Schwere und/oder Eintretenswahrscheinlichkeit als hoch bewertet wurden (*siehe dazu oben Beispiel unter Ziff. 3.2.8, wofür eine mittlere bis hohe Eintretenswahrscheinlichkeit ermittelt wurde*), so liegt ein hohes Risiko für die Verletzung der Persönlichkeit oder der Grundrechte von betroffenen Personen vor. In diesem Fall informiert das verantwortliche öffentliche Organ die Fachstelle Datenschutz gemäss Art. 34 Abs. 1 IDAG, wobei zusammen mit dem Gesuch um Vorab-Konsultation das dokumentierte Ergebnis der Datenschutz-Folgenabschätzung einzureichen ist (Art. 25 Abs. 1 VIDAG). Sofern bereits vorhanden, sollen auch weitere Dokumente, wie bspw. das ISDS-Konzept eingereicht werden. Die Fachstelle Datenschutz prüft, ob die Datenschutz-Folgenabschätzung vollständig ausgefüllt ist und teilt dem öffentlichen Organ mit, welche weiteren Dokumente einzureichen bzw. zu erarbeiten sind. Die Vorab-Konsultation und die dreimonatige Prüffrist beginnt im Moment, in welchem alle prüfrelevanten Dokumente (vgl. Formular Datenschutz-Folgenabschätzung, 9. Bereits vorhandene Dokumentation) vollständig eingereicht wurden (Art. 34 Abs. 1 IDAG)).

Das Ergebnis der Vorab-Konsultation wird in einem Prüfbericht festgehalten und dem verantwortlichen öffentlichen Organ – sofern erforderlich – zunächst in Entwurf-Form zugestellt. Das öffentliche Organ erhält damit Gelegenheit, zum Berichtsentwurf und darin enthaltenen Empfehlungen Stellung zu nehmen. Sofern angezeigt, sind auch mehrere Iterationen möglich. Werden mit der beabsichtigten Datenbearbeitung datenschutzrechtliche Vorschriften verletzt, lässt die Fachstelle Datenschutz erforderliche Vorkehrungen und/oder Massnahmen als Empfehlung ergehen (Art. 58 Abs. 3 IDAG). Anderenfalls erklärt sie das Informatikmittel als datenschutzkonform. Es gilt, dass die geplante Datenbearbeitung erst nach Abschluss der Konsultation durchgeführt werden darf (Art. 25 Abs. 3 VIDAG).

Anhang: Verfahrensablauf Datenschutz-Folgenabschätzung und Vorab-Konsultation