Merkblatt

19.08.2018 (Stand 1. Juli 2020)

IDAG und VIDAG – Was ist neu? Datenschutz-Folgenabschätzung (DSFA)

Das Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (IDAG) vom 24. Oktober 2006[1] und die Verordnung zum Gesetz über die Information der Öffentlichkeit, den Datenschutz und das Archivwesen (VIDAG) vom 26. September 2007[2] wurden teilrevidiert. Die Änderungen sind am 1. August 2018 in Kraft getreten.

Das vorliegende Merkblatt richtet sich an die öffentlichen Organe des Kantons Aargau. Es erläutert, wann und wie eine Datenschutz-Folgenabschätzung bei der Einführung neuer elektronischer Datenbearbeitungen durchzuführen ist.

1. Was ist eine Datenschutz-Folgenabschätzung?

Vor Beginn einer vorgesehenen Bearbeitung von Personendaten hat das öffentliche Organ deren Folgen auf die Persönlichkeit und die Grundrechte der betroffenen Personen vorzunehmen, entsprechende Massnahmen zu treffen und diese zu dokumentieren.

Führt die vorgesehene Datenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person, ist gemäss § 17a Abs. 1 IDAG vor Aufnahme der Datenbearbeitungen eine Datenschutz-Folgenabschätzung (DSFA) vorzunehmen. Diese beschäftigt sich mit den Rechtsgrundlagen für die vorgesehenen Datenbearbeitungen sowie den technischen und organisatorischen Massnahmen zum Schutz der Personendaten vor unbefugten Zugriffen und ungewollten Datenverlusten. Erweist sich aufgrund der Datenschutzfolgen-Abschätzung, dass effektiv ein erhöhtes Risiko für die Persönlichkeit und die Grundrechte der betroffenen Person besteht oder wird das Risiko von Gesetzes wegen vermutet, hat das öffentliche Organ die Öffentlichkeits- und Datenschutzbeauftragte (ÖDB) zur Durchführung einer Vorab-Konsultation (vgl. Merkblatt IDAG und VIDAG – Was ist neu? Vorab-Konsultation) über das Resultat der DSFA in Kenntnis zu setzen (§ 17b IDAG). Dieses Vorgehen ersetzt die bisherige Vorabkontrolle durch die ÖDB und stärkt die Eigenverantwortung des öffentlichen Organs, indem dieses die DSFA selbst vorzunehmen hat.

[1] SAR 150.700
[2] SAR 150.711

2. Wann ist eine DSFA vorzunehmen?

2.1 Grundsatz

Eine DSFA ist vorzunehmen, wenn

- eine neue informatikgestützte Anwendung mit Personendaten eingeführt werden soll, oder
- eine bestehende informatikgestützte Anwendung mit Personendaten erweitert oder die verwendete Technologie geändert wird,

und

- die geplante Bearbeitung von Personendaten voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte der betroffenen Personen führt,
- die gesetzliche Grundlage der geplanten Datenbearbeitung eine DSFA nicht ausschliesst oder diese bereits im Gesetzgebungsverfahren durchgeführt worden ist (es können auch Teile der DSFA entfallen, wenn sie in der Rechtsgrundlage ausdrücklich vorgesehen ist, z.B. die zu bearbeitenden Daten oder die Datenempfänger aufgeführt werden).

Hinweis: Für am 1. August 2018 bereits laufende, unveränderte Bearbeitungen von Personendaten in informatikgestützten Systemen muss keine DSFA durchgeführt werden. Das öffentliche Organ ist trotzdem für die Rechtmässigkeit der Verarbeitung sowie ausreichende technische und organisatorische Massnahmen zur Wahrung der Datensicherheit verantwortlich und es hat deren Einhaltung zu dokumentieren. Für vor dem 1. August 2018 bestehende, unveränderte Informatikanwendungen die zu erhöhten Risiken für die Persönlichkeit und die Grundrechte betroffener Personen führen und die der Beauftragten nicht zur Vorabkontrolle nach altem Recht vorgelegt wurden, empfiehlt sich Durchführung einer Datenschutz-Folgenabschätzung auch ohne gesetzliche Verpflichtung.

Eine Erweiterung liegt vor, wenn eine signifikante Änderung der Anwendung stattgefunden hat, z.B. eine andere Technologie verwendet oder die Daten für einen geänderten Zweck bearbeitet werden. Eine Datenschutz-Folgenabschätzung muss überprüft werden, wenn sich die Risiken geändert haben (Änderung der Quellen der Risiken, der Bedrohungen) oder der Kontext der Bearbeitung. Eine erneute Datenschutz-Folgenabschätzung kann auch notwendig sein, wenn sich der organisatorische oder gesellschaftliche Kontext der Bearbeitung ändert, z.B. weil Personendaten in Länder ohne gleichwertiges Datenschutzniveau übermittelt werden sollen oder die Schutzbedürftigkeit bestimmter Personengruppen sich entwickelt hat.

Im Sinne eines guten Datenschutz-Managements sollten Datenschutz-Folgenabschätzungen bestehender Informatikanwendungen laufend durchgeführt werden, spätestens jedoch nach drei Jahren oder früher, abhängig von den Umständen der Bearbeitung.

2.2 Wann führt eine Personendatenbearbeitung voraussichtlich zu einem erhöhten Risiko für die Persönlichkeit und die Grundrechte?

Die nachfolgend aufgelisteten Umstände sind Indizien für ein erhöhtes Risiko. Nach einer Faustregel ist eine DSFA durchzuführen, wenn mindestens zwei der nachfolgend genannten Umstände zutreffen, d.h. wenn

- das System Profiling ermöglicht, also Daten ausgewertet werden können, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre oder Mobilität,
- besonders schützenswerte Personendaten[3] bearbeitet werden,
- die Bearbeitung von Personendaten nicht vom öffentlichen Organ selbst, sondern durch Auftragnehmer durchgeführt wird, insbesondere wenn Cloud Services von Cloud-Anbietern zum Einsatz kommen.
- zwei oder mehrere öffentliche Organe Personendaten in einem gemeinsamen elektronischen System bearbeiten,
- eine systematische Überwachung erfolgt,
- die Datenbearbeitungen umfangreich sind (wenn bspw. mehr als 1000 Personen betroffen oder viele Arten von Daten gesammelt werden),
- die Personendaten mit anderen Datenbeständen abgeglichen oder verknüpft werden können,
- Personendaten in Länder ohne gleichwertiges Datenschutzniveau übermittelt werden,
- Daten von besonders schutzbedürftigen Personen bearbeitet werden,
- webbasierte Techniken verwendet werden,
- neue Technologien verwendet werden (z.B. Fingerabdrucksensoren, Gesichtserkennung),
- optisch-elektronische Überwachungsanlagen verwendet werden (Videoüberwachung).

3. Wer ist für die Durchführung der DSFA verantwortlich?

Die verantwortliche Behörde hat zunächst zu entscheiden, ob eine DSFA durchzuführen ist (vgl. Ziff. 2.1). Ist dies nicht der Fall, sollte der Entscheid für die Dokumentation der Datensicherheit schriftlich festgehalten werden. Ist eine DSFA notwendig, ist sie von der verantwortlichen Behörde durchzuführen, d.h. von derjenigen Stelle, die befugt ist, über das Projekt zu entscheiden und welche die Verantwortung für die Datenbearbeitung über den Betrieb der Informatikanwendung trägt oder tragen wird.

4. Inhalt der DSFA

Die VIDAG enthält keine genauen Vorgaben, auf welche Art und Weise eine DSFA durchzuführen ist. § 6a Abs. 1 VIDAG regelt nur die Mindestanforderungen. Die DSFA muss enthalten:

a) das verantwortliche öffentliche Organ, die rechtliche Grundlage, den Zweck und eine systematische Beschreibung der geplanten Datenbearbeitungen,
b) eine Bewertung der Notwendigkeit und Verhältnismässigkeit der Datenbearbeitungen in Bezug auf den Zweck,

[3] Besonders schützenswerte Personendaten sind insbesondere Daten über
a) die religiösen, weltanschaulichen, persönlichen oder gewerkschaftlichen Tätigkeiten,
b) die Gesundheit, die Intimsphäre oder die ethnische Zugehörigkeit,
c) Massnahmen der sozialen Hilfe,
d) administrative oder strafrechtliche Verfolgungen und Sanktionen,
e) genetische Daten,
f) biometrische Daten.

c) eine Bewertung der Risiken für die Persönlichkeit und die Grundrechte der betroffenen Personen unter Beachtung der Schutzziele gemäss § 4 Abs. 1 VIDAG (sog. Schutzbedarfsanalyse) und
d) die technischen und organisatorischen Massnahmen, die zur Bewältigung der Risiken geplant sind (§ 4 Abs. 1 lit. a – j VIDAG, vgl. ausführlich dazu Ziffer 5 nachfolgend), unter anderem in Bezug auf Datenbearbeitungen durch beauftragte Dritte.

5. Datensicherheit

5.1 Schutzbedarfsanalyse (§ 4 Abs. 2 VIDAG)

Die organisatorischen und technischen Massnahmen zur Wahrung der Datensicherheit sind bei elektronischer Bearbeitung von Personendaten immer – nicht nur in Fällen einer erhöhten Gefährdung der Persönlichkeit und der Grundrechte – in einem Datensicherheitskonzept (Informationssicherheits- und Datenschutzkonzept, ISDS-Konzept) festzulegen. Die Massnahmen orientieren sich am Zweck, der Art und dem Umfang der Datenbearbeitung sowie den möglichen Gefahren für die Persönlichkeitsrechte betroffener Personen (§ 4 Abs. 2 VIDAG), d.h. an den Ergebnissen der Schutzbedarfsanalyse.

5.2 Informationssicherheits- und Datenschutzkonzept (ISDS Konzept); § 4 Abs. 1 VIDAG

Die technischen und organisatorischen Massnahmen bezwecken die Einhaltung der Vertraulichkeit, Integrität, Verfügbarkeit, Zurechenbarkeit und Nachvollziehbarkeit sowie der Löschfristen zu gewährleisten. Es sind folgende Massnahmen zu treffen (§ 4 Abs. 1 VIDAG):

a) Zugangskontrolle: unbefugten Personen ist der Zugang zu Einrichtungen, in denen Personendaten verarbeitet werden, zu verwehren,
b) Datenträgerkontrolle: unbefugten Personen ist das Lesen, Kopieren, Verändern oder Entfernen von Datenträgern zu verunmöglichen,
c) Transportkontrolle: bei der Bekanntgabe von Personendaten sowie beim Transport von Datenträgern ist zu verhindern, dass die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können,
d) Bekanntgabekontrolle: Datenempfänger, denen Personendaten mittels Einrichtungen zur Datenübertragung bekannt gegeben werden, müssen identifiziert werden können,
e) Speicherkontrolle: unbefugte Eingabe in den Speicher sowie unbefugte Einsichtnahme, Veränderung oder Löschung gespeicherter Personendaten sind zu verhindern,
f) Benutzerkontrolle: die Benutzung von automatisierten Datenverarbeitungssystemen mittels Einrichtungen zur Datenübertragung durch unbefugte Personen ist zu verhindern,
g) Zugriffskontrolle: der Zugriff der berechtigten Personen ist auf diejenigen Personendaten zu beschränken, die sie für die Erfüllung ihrer Aufgabe benötigen,
h) Eingabekontrolle: in elektronischen Systemen muss nachträglich überprüft werden können, welche Personendaten zu welcher Zeit und von welcher Person eingegeben wurden,
i) Wiederherstellung: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können,
j) Zuverlässigkeit, Integrität: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden und gespeicherte Personendaten nicht durch Fehlfunktionen des Systems beschädigt werden können.

Die oben genannten Massnahmen müssen zweck- und verhältnismässig sein. Sie orientieren sich am Zweck, der Art und dem Umfang der Datenbearbeitung sowie den möglichen Gefahren für die

Persönlichkeitsrechte betroffener Personen (§ 4 Abs. 2 VIDAG). Dabei ist eine Kombination von technischen und organisatorischen Massnahmen sowie der Massnahmen untereinander möglich. In Bezug auf die Datenträgerkontrolle bedeutet dies beispielsweise, dass durch Zugangskontrolle möglichst zu verhindern ist, dass unbefugte Personen Zugang zu Datenträgern (z.B. Laptops mit lokal gespeicherten Personendaten) haben, kombiniert mit der Zugriffskontrolle durch starken Passwortschutz und/oder der Benutzerkontrolle durch aktive Bewirtschaftung von Smartcards sowie regelmässiger Überprüfung der Berechtigung. Im Übrigen haben sich die Massnahmen am Stand der Technik zu orientieren.

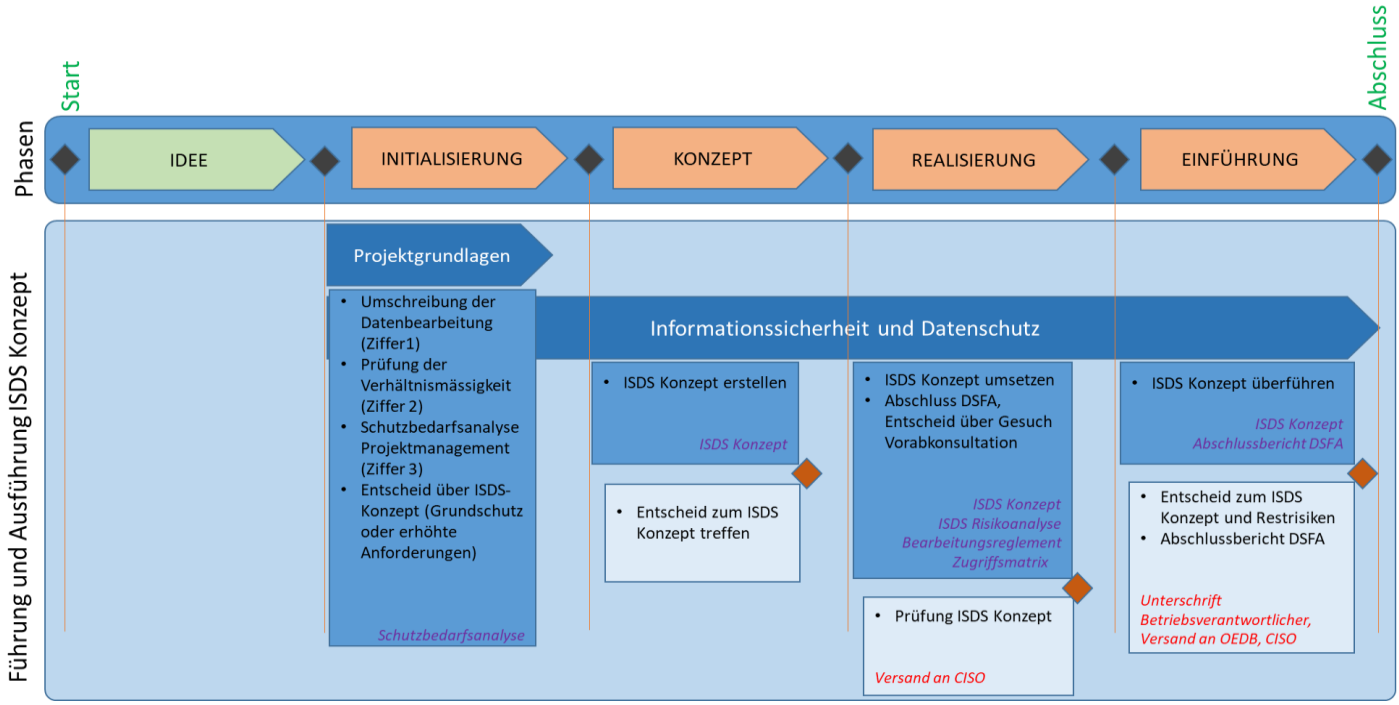
5.3 Grundschutzansatz

Verfolgt das öffentliche Organ einen Grundschutzansatz[4], ist ein besonderes Datenschutzkonzept nur dann erforderlich, wenn die Schutzbedarfsanalyse einen höheren Schutzbedarf ergibt als denjenigen, der durch den vom öffentlichen Organ definierten und umgesetzten Grundschutz abgedeckt wird. Das dokumentierte Grundschutz-Konzept mit Darstellung, welche Massnahmen auf welche Bedrohungen angewendet werden, ist der DSFA beizulegen. Bei erhöhtem Schutzbedarf ist die Dokumentation des Grundschutzes sowie das (ergänzende) ISDS-Konzept in die DSFA aufzunehmen.

[4] Beim IT-Grundschutz handelt es sich um eine Sammlung von Standards und Katalogen, die pauschalisierte Vorgehensweisen zum Schutz der eingesetzten Informationstechnik beschreiben. Ziel des IT-Grundschutzes ist es, die Mindestanforderungen für den normalen Schutzbedarf von IT-Anwendungen und IT-Systemen zu beschreiben und Methoden zu deren Umsetzung zu liefern. Das Konzept geht davon aus, dass bei den Anwendungen mit normalem Schutzbedarf individuelle Analysen und Sicherheitskonzepte zu aufwendig sind. Daher stellt der Grundschutz Standardmethoden und -massnahmen bereit und deckt die verschiedenen Bereiche Personal, Gebäude, Software, Hardware, Organisation und Kommunikationsnetze ab.

6. Erstellung der Datenschutz-Folgenabschätzung

Die Grafik zeigt in Bezug auf die Hermes-Projektmanagementmethode die Einbettung der Datenschutz-Folgenabschätzung in die Phasen der Erstellung eines Informatiksicherheits- und Datenschutzkonzepts auf.



Erläuterungen zum Schema:

1. Die Umschreibung der Datenbearbeitung enthält
   a) die Bezeichnung des verantwortlichen öffentlichen Organs,
   b) die rechtliche Grundlage der geplanten Datenbearbeitungen,
   c) den Zweck der Datenbearbeitungen,
   d) eine systematische Beschreibung der geplanten Datenbearbeitungen.

2. Prüfung der Verhältnismässigkeit der geplanten Datenbearbeitungen
Die Notwendigkeit und die Verhältnismässigkeit der geplanten Bearbeitungen sind in Bezug auf den Zweck zu bewerten.

3. Bedrohungs- und Schutzbedarfsanalyse
Die aufgrund der geplanten Datenbearbeitungen entstehenden Risiken für die Persönlichkeit und die Grundrechte der betroffenen Person sind im Hinblick auf die Schutzziele gemäss § 4 Abs. 1 VIDAG zu bewerten.

4. ISDS-Konzept
Bei jeder informatikgestützten Bearbeitung von Personendaten ist ein Informationssicherheits- und Datenschutzkonzept zu erstellen. Zur Ausnahme vergleiche Ziffer 5.3.

7. Abschluss der DSFA

Das Ergebnis der DSFA ist schriftlich festzuhalten und der ÖDB per Post oder E-Mail zuzustellen. Bei gegebenen Voraussetzungen ist ein Gesuch um Vorab-Konsultation zu stellen (vgl. Merkblatt IDAG und VIDAG – Was ist neu? Vorab-Konsultation).