dsb
datenschutzbeauftragte
des kantons zürich

Leitfaden

Datenschutz-Managementsystem

Inhalt

Datenschutzbeauftragte des Kantons Zürich
Postfach, 8090 Zürich, +41 43 259 39 99
datenschutz@dsb.zh.ch, datenschutz.ch, twitter: @dsb_zh

1 Einleitung

In diesem Leitfaden werden die datenschutzrechtlichen Mindestanforderungen an ein Datenschutzmanagementsystem (DSMS), die Massnahmen sowie deren Umsetzung beschrieben.

Für die Mindestanforderungen gelten gemäss § 26 Verordnung über die Information und den Datenschutz (IDV, LS 170.41) die eidgenössischen Regelungen sinngemäss, sodass die folgenden Dokumente Anwendung finden:

- Richtlinien des Bundes über die Mindestanforderungen an ein Datenschutzmanagementsystem vom 19. März 2014
- Erläuterungen zu den Änderungen vom 19. März 2014 der «Richtlinien über die Mindestanforderungen an ein Datenschutzmanagementsystem»
- Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS vom 15. April 2014

Das DSMS basiert auf den Standards ISO/IEC 27001:2015 (ISO 27001), ISO/IEC 27002:2015 (ISO 27002) sowie ISO 9001:2015, die mit den datenschutzrechtlichen Anforderungen des Gesetzes über die Information und den Datenschutz (IDG, LS 170.4) ergänzt werden. Je nach Fachbereich sind spezialrechtliche Anforderungen zusätzlich zu berücksichtigen.

Falls bereits ein Informationssicherheits-Managementsystem (ISMS) oder ein Qualitätsmanagementsystem (QMS) besteht, können diese als Grundlage für ein DSMS dienen, indem lediglich Abweichungen analysiert und zusätzliche Massnahmen umgesetzt werden.

Die Planung, Umsetzung, Überprüfung, Instandhaltung und Verbesserung des DSMS nach ISO 27001 sind nicht Bestandteile dieses Dokuments. Diesbezüglich wird auf die Prozesse zu ISO 27001 verwiesen.

2 Datenschutzrechtliche Anforderungen

- Gesetzmässigkeit (§ 8 IDG)
  - Gesetzliche Grundlage für das Bearbeiten von Personendaten

- Verhältnismässigkeit (§ 8 IDG)
  - Verhältnismässige Bearbeitung

- Zweckbindung (§ 9 IDG)
  - Zweckbindung
  - Zweckänderung

- Erkennbarkeit (§ 12 IDG)
  - Erkennbarkeit
  - Informationspflicht

- Vermeidung des Personenbezugs (§ 11 IDG)
  - Datenvermeidung
  - Datensparsamkeit

- Informationssicherheit (§ 7 IDG)
  - Vertraulichkeit, Integrität und Verfügbarkeit
  - Zurechenbarkeit und Nachvollziehbarkeit
  - Weitere Massnahmen gemäss Informatiksicherheitsverordnung (LS 170.8)
  - Managementsysteme zur Umsetzung der Massnahmen

- Aufbewahrung und Archivierung (§ 5 IDG)
  - Aufbewahrung
  - Archivierung

- Datenbearbeitung im Auftrag (§ 6 IDG)
  - Datenbearbeitung durch Dritte

- Grenzüberschreitende Bekanntgabe von Personendaten (§19 IDG)
  - Angemessener Schutz

- Informationszugang (§ 20 IDG)
  - Informationszugangsrecht
  - Auskunftsrecht in Bezug auf eigene Personendaten

- Rechtsansprüche (§ 21 IDG)
  - Rechtsansprüche

- Datenschutz-Folgenabschätzung und Vorabkontrolle (§ 10 IDG)
  - Datenschutz-Folgenabschätzung
  - Vorabkontrolle

- Meldepflicht (§ 12a IDG)
  - Meldung von Datenschutzvorfällen

2.1 Gesetzmässigkeit (§ 8 IDG)

Personendaten dürfen durch das öffentliche Organ bearbeitet werden, wenn dies zur Erfüllung der gesetzlich umschriebenen Aufgabe geeignet und erforderlich ist. Das Bearbeiten besonderer Personendaten muss in einer formell-gesetzlichen Grundlage geregelt sein.

Gesetzliche Grundlage für das Bearbeiten von Personendaten

Massnahmen

- Sicherstellen, dass das Bearbeiten von Personendaten durch öffentliche Organe aus einer gesetzlich umschriebenen Aufgabe abgeleitet werden kann und geeignet und erforderlich ist (§ 8 Abs. 1 IDG).
- Sicherstellen, dass das Bearbeiten von besonderen Personendaten in einer hinreichend bestimmten Regelung in einem formellen Gesetz festgehalten ist (§ 8 Abs. 2 IDG).
- Sicherstellen, dass eine Datenbekanntgabe nur unter den Voraussetzungen der §§ 16 und 17 IDG erfolgt.

Umsetzung

- Das für die Datenbearbeitung verantwortliche Organ ist bekannt.
- Das Bearbeiten von Personendaten kann aus einem Gesetz, einer Verordnung oder einem anderen durch die Behörden erlassenen Reglement abgeleitet werden.
- Das Bearbeiten von besonderen Personendaten kann auf ein formelles Gesetz abgestützt werden. Das verantwortliche Organ, der Zweck der Bearbeitung, die Datenkategorien sowie die Datenempfänger sind bezeichnet.
- Ein Bearbeiten zu nicht personenbezogenem Zweck kann erfolgen, wenn die Personen-daten anonymisiert werden.
- Eine Datenbekanntgabe erfolgt nur unter den Voraussetzungen der §§ 16 und 17 IDG.

- Eine Datenbekanntgabe für nicht personenbezogene Zwecke kann erfolgen, wenn keine rechtliche Bestimmung entgegensteht.
- Personendaten werden nur durch ein Abrufverfahren zugänglich gemacht, wenn dies ausdrücklich in einem Erlass vorgesehen ist.
- Besondere Personendaten werden nur durch ein Abrufverfahren zugänglich gemacht, wenn dies in einem formellen Gesetz vorgesehen ist.
- Instrumente für Datensperren sind im Rahmen der rechtlichen Voraussetzungen von § 22 IDG vorhanden und können umgesetzt werden.

2.2 Verhältnismässigkeit (§ 8 IDG)

Personendaten dürfen bearbeitet werden, wenn die Bearbeitung verhältnismässig, das heisst für den Zweck geeignet und erforderlich ist.

Verhältnismässige Bearbeitung

Massnahmen

- Sicherstellen, dass nur diejenigen Personendaten bearbeitet werden, die für die Aufgabenerfüllung geeignet und erforderlich sind (§ 8 Abs. 1 IDG).
- Sicherstellen, dass die Prinzipien der Datenvermeidung und Datensparsamkeit eingehalten werden (§ 11 IDG).

Umsetzung

- Die Datenbeschaffung ist auf den Zweck und auf die Aufgabenerfüllung abgestimmt.
- Es werden keine für den Zweck ungeeigneten und nicht erforderlichen Personendaten erhoben.
- Personendaten, bei welchen sich nachträglich herausstellt, dass sie nicht erforderlich sind, werden gelöscht. Die Archivierungsvorschriften bleiben vorbehalten.
- Datenbearbeitungssysteme werden auf den Einsatz von Privacy Enhancing Technology (PET) überprüft.
- Personendaten werden anonymisiert.
- Ist eine Anonymisierung nicht möglich, wird eine Teilanonymisierung geprüft.
- Ist eine Anonymisierung oder Teilanonymisierung nicht möglich, wird eine Pseudonymisierung geprüft.

2.3 Zweckbindung (§ 9 IDG)

Das öffentliche Organ stellt sicher, dass Personendaten nur zu dem Zweck bearbeitet werden, zu dem sie erhoben wurden, eine rechtliche Bestimmung eine anderweitige Zweckverwendung vorsieht oder im Einzelfall eine Einwilligung der betroffenen Person vorliegt. Das öffentliche Organ gewährleistet, dass Personendaten zu einem nicht personenbezogenen Zweck nur bearbeitet werden, wenn diese anonymisiert werden und aus den Auswertungen keine Rückschlüsse auf betroffene Personen möglich sind.

Zweckbindung, Zweckänderung

Massnahmen

- Sicherstellen, dass die Bearbeitung der Personendaten nur zum dem Zweck erfolgt, zu dem sie erhoben wurden (§ 9 Abs. 1 IDG).
- Sicherstellen, dass beim Bearbeiten von besonderen Personendaten der Zweck in einem formellen Gesetz festgehalten ist (§ 8 Abs. 2 IDG).
- Bei einer Zweckänderung sicherstellen, dass diese aufgrund einer rechtlichen Bestimmung der Einwilligung erfolgt oder im Einzelfall auf der Einwilligung der betroffenen Person beruht (§ 9 Abs. 1 IDG).

Umsetzung
- Überprüfen, ob die Personendaten zu dem Zweck bearbeitet werden, zu dem sie erhoben wurden.
- Sicherstellen, dass jede nachträgliche Zweckänderung nachvollziehbar ist.
- Die Zweckverwendung durch Stichproben kontrollieren.
- Überprüfen, ob sich eine Änderung des ursprünglichen Zwecks auf eine rechtliche Grundlage oder die Einwilligung der Betroffenen stützt.
- Überprüfen, ob bei Statistiken keine Rückschlüsse auf Personen möglich sind.

2.4 Erkennbarkeit (§ 12 IDG)

Die Beschaffung von Personendaten und der Zweck ihrer Bearbeitung durch das öffentliche Organ müssen für die betroffenen Personen erkennbar sein. Bei der Beschaffung von besonderen Personendaten ist der Inhaber der Datensammlung verpflichtet, die betroffene Person über den Zweck der Bearbeitung zu informieren.

Erkennbarkeit und Informationspflicht

Massnahmen
- Sicherstellen, dass das öffentliche Organ Personendaten so beschafft, dass die Beschaffung und der Zweck der Bearbeitung für betroffene Personen erkennbar sind (§ 12 Abs. 1 IDG).
- Bei der Beschaffung von besonderen Personendaten muss der Inhaber der Datensammlung betroffene Personen über den Zweck der Bearbeitung informieren (§ 12 Abs. 2 IDG).

Umsetzung
- Das öffentliche Organ stützt seine Datenbeschaffungen auf eine Rechtsgrundlage ab.
- Werden besondere Personendaten beschafft, muss der Zweck der einzelnen Bearbeitung aus der Rechtsgrundlage ersichtlich sein.
- Das öffentliche Organ macht ein Verzeichnis der Informationsbestände, die Personendaten beinhalten (§ 14 Abs. 4 IDG).

2.5 Vermeidung des Personenbezugs (§ 11 IDG)

Das öffentliche Organ gestaltet Datenbearbeitungssysteme und -programme so, dass möglichst wenige Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig sind. Es löscht, anonymisiert oder pseudonymisiert solche Personendaten, sobald und soweit dies möglich ist.

Datenvermeidung, Datensparsamkeit

Massnahmen
- Datenbearbeitungssysteme und -programme müssen so entwickelt werden, dass möglichst wenig Personendaten anfallen (§ 11 Abs. 1 IDG).
- Sicherstellen, dass Datenbearbeitungssysteme mit Blick auf die Randdaten so entwickelt werden, dass, sobald und soweit möglich, Personendaten gelöscht, anonymisiert oder pseudonymisiert werden (§ 11 Abs. 2 IDG).

Umsetzung
- Datenbearbeitungssysteme werden auf den Einsatz von Privacy Enhancing Technology (PET) überprüft.
- Personendaten werden, wo möglich, anonymisiert.
- Ist eine Anonymisierung nicht möglich, wird eine Teilanonymisierung geprüft.
- Ist eine Anonymisierung oder Teilanonymisierung nicht möglich, wird eine Pseudonymisierung geprüft.

2.6 Informationssicherheit (§ 7 IDG)

Das öffentliche Organ muss seine Informationen durch angemessene organisatorische und technische Massnahmen so schützen, dass sie nicht unrechtmässig zur Kenntnis gelangen, richtig, vollständig und bei Bedarf vorhanden sind, einer Person zugerechnet werden können und Veränderungen erkennbar und nachvollziehbar sind.

Vertraulichkeit, Integrität und Verfügbarkeit

Für die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit sind die folgenden Massnahmen gemäss «Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS» aus ISO 27002 umzusetzen:

Vertraulichkeit

- Kapitel 6.1.5: Informationssicherheit im Projekt-Management
- Kapitel 6.2: Mobilgeräte und Telearbeit
- Kapitel 8.1-3: Wertemanagement
- Kapitel 9.1–4: Zugriffskontrollen
- Kapitel 10: Kryptographie
- Kapitel 11.1: Schutz vor physischem Zugang und Umwelteinflüssen
- Kapitel 11.2: Sicherheit von Betriebsmitteln
- Kapitel 12.4: Protokollierung und Überwachung
- Kapitel 13.1: Netzwerksicherheitsmanagement
- Kapitel 13.2: Informationsübertragung

Integrität

- Kapitel 12.2: Schutz vor Malware
- Kapitel 14.1–3: Anschaffung, Entwicklung und Instandhaltung von Systemen

Verfügbarkeit

- Kapitel 12.3: Datensicherungen
- Kapitel 17.1–2: Informationssicherheitsaspekte des Business Continuity Managements
- Kapitel 18.1.3 Schutz dokumentierter Informationen

Das Bundesamt für Sicherheit in der Informationstechnik (BSI, Deutschland) zeigt im BSI-Dokument Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz, wie die vor-geschlagenen Massnahmen den Zielsetzungen (Controls) zugeordnet werden.

Zurechenbarkeit und Nachvollziehbarkeit

Für die Schutzziele Zurechenbarkeit und Nachvollziehbarkeit gemäss § 7 IDG sind die folgenden Massnahmen aus ISO 27002 umzusetzen:

- Kapitel 6.1.1: Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit
- Kapitel 6.1.2: Aufgabentrennung
- Kapitel 7.1.2: Arbeitsvertragsklauseln
- Kapitel 7.2.1: Verantwortung des Managements

Weitere Massnahmen gemäss Verordnung über die Informationsverwaltung und -sicherheit

Für die Auswahl geeigneter Massnahmen wird das IT-Grundschutz-Kompendium des BSI unter Berücksichtigung der zuvor festgelegten Schutzstufen («1 – Grundschutz» und «2 – erhöhter Schutz» angewendet. Zusätzlich ist der Massnahmenkatalog und der Minimummassnahmenkatalog der Datenschutzbeauftragten zu beachten.

Managementsysteme zur Umsetzung der Massnahmen

Ein bestehendes Managementsystem, beispielsweise ein QMS oder ein ISMS, kann als Grundlage für das Umsetzen dieser Massnahmen dienen. Das ISMS stellt beispielsweise die notwendigen Verfahren und Regeln zur dauerhaften Steuerung, Kontrolle und Verbesserung der Sicherheitsziele bereit.

2.7 Aufbewahrung und Archivierung (§ 5 IDG)

Das öffentliche Organ bewahrt Informationen so lange auf, als es diese zur Erledigung seiner Aufgaben benötigt. Danach verbleiben sie noch höchstens zehn Jahre in der ruhenden Ablage, ausser wenn Rechts- oder Verjährungsfristen eine längere Aufbewahrung verlangen. Nach Ablauf der Aufbewahrungsfrist sind die Informationen dem zuständigen Archiv anzubieten. Informationen, die nicht archiviert werden, sind zu vernichten.

Aufbewahrung

Massnahmen

– Sicherstellen, dass das öffentliche Organ die Informationen nur so lange aufbewahrt, wie es diese benötigt. Die Aufbewahrungsfristen müssen durch das öffentliche Organ definiert und dokumentiert werden (§ 5 Abs. 2 und 3 IDG).

Umsetzung

– Aufbewahrungsfristen wurden definiert.
– Über die Aufbewahrungsfrist hinausgehende Verjährungs- und Rechtsmittelfristen wurden beachtet.
– Löschungsmechanismen sind Teil der technischen Lösung.

Archivierung

Massnahmen

– Sicherstellen, dass Informationen und Findmittel (Listen, Register, Verzeichnisse etc.) nach Ablauf der Aufbewahrungsfrist archiviert werden (§ 5 Abs. 2 IDG).

Umsetzung

– Das öffentliche Organ hat die Informationen unabhängig von Form und Träger nach Ablauf der Aufbewahrungsfrist dem zuständigen Archiv zur Archivierung angeboten oder nach den Vorgaben des Archivgesetzes (LS 170.6) archiviert.

2.8 Datenbearbeitung im Auftrag (§ 6 IDG)

Das Bearbeiten von Informationen kann Dritten übertragen werden, sofern keine rechtliche Bestimmung oder vertragliche Vereinbarung entgegensteht. Soweit die Informationsbearbeitung durch Dritte gesetzlich nicht geregelt ist, ergehen die Aufträge schriftlich. Das öffentliche Organ bleibt für den Umgang mit den Informationen verantwortlich.

Datenbearbeitung durch Dritte

Massnahmen

- Sicherstellen, dass sich das Bearbeiten von Informationen durch Dritte auf eine gesetzliche Grundlage stützt oder in einem schriftlichen Vertrag dokumentiert ist.
- Sicherstellen, dass einer solchen Auslagerung keine rechtlichen oder vertraglichen Bestimmungen entgegenstehen (§ 6 Abs. 1 IDG).
- Sicherstellen, dass die Personendaten nur so bearbeitet werden, wie dies das öffentliche Organ auch darf (§ 6 Abs. 2 IDG).
- Kontrollieren, ob die Anforderungen aus den Verträgen erfüllt werden und, falls nötig, Korrekturen einleiten.
- Sicherstellen, dass die Massnahmen gemäss A 15.1. «Sicherheit in Lieferantenbeziehungen» und A.15.2 «Management der Dienstleitungserbringung durch Lieferanten» umgesetzt werden.

Umsetzung

- Ein Gesetz oder eine vertragliche Vereinbarung gemäss § 25 IDV regeln das Bearbeiten im Auftrag.
- Die Verantwortung ist klar definiert.
- Es stehen keine gesetzlichen oder vertraglichen Geheimhaltungspflichten entgegen.
- Beim Bearbeiten im Auftrag mit besonderen Personendaten liegt eine Genehmigung durch die vorgesetzte Stelle vor (§ 25 Abs. 3 IDV).
- Der Geltungsbereich der IVSV ist abgeklärt und falls anwendbar, der Inhalt umgesetzt.
- Die Anwendbarkeit der AGB Auslagerung Informatikleistungen wurde abgeklärt und, falls bejaht, in die Verträge integriert.
- Finden die AGB Auslagerung Informatikleistungen keine Anwendung, wird ein gleichwertiger Schutz durch das Einbinden ebenbürtiger Vertragsklauseln gewährleistet.
- Erfolgt die Auslagerung ins Ausland, werden zusätzliche Massnahmen analog derjenigen in § 19 IDG und § 22 IDV umgesetzt.
- Die folgenden Massnahmen gemäss «Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS» aus ISO 27002 finden ergänzend Anwendung:
  - Kapitel 15.1: Sicherheit in Lieferantenbeziehungen
  - Kapitel 15.2: Management der Dienstleistungserbringung durch Lieferanten

2.9 Grenzüberschreitende Bekanntgabe von Personendaten (§ 19 IDG)

Personendaten dürfen an Empfängerinnen und Empfänger, die dem Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten nicht unterstehen, bekannt gegeben werden, wenn:

- der Empfängerstaat ein angemessenes Datenschutzniveau gewährleistet,
- eine gesetzliche Grundlage dies erlaubt, um bestimmte Interessen der betroffenen Person oder überwiegende öffentliche Interessen zu schützen
- oder vom öffentlichen Organ angemessene vertragliche Sicherheitsvorkehrungen getroffen wurden.

Angemessener Schutz

Massnahmen

- Sicherstellen, dass der Empfängerstaat das Europarats-Übereinkommen zum Schutz des-Menschen bei der automatischen Verarbeitung personenbezogener Daten ratifiziert hat, andernfalls
- Sicherstellen, dass der Empfängerstaat bei der grenzüberschreitenden Bekanntgabe von Personendaten ein angemessenes Datenschutzniveau gewährleistet (§ 19 IDG), andernfalls
- Prüfen, ob rechtliche Grundlagen bestehen oder sicherstellen, dass vertragliche Sicherheitsvorkehrungen getroffen werden, um die Persönlichkeitsrechte von Betroffenen zu schützen.

Umsetzung

- Eine Datenbekanntgabe ins Ausland erfolgt nur unter Einhaltung der zu den §§ 16 und 17 IDG zusätzlichen Voraussetzungen von § 19 IDG.
- Der Empfängerstaat hat das Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten ratifiziert (§ 19 IDG).
- Falls nicht, ist zu prüfen, ob der Empfängerstaat auf der durch den eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten publizierten Liste mit den Staaten mit angemessener Datenschutzgesetzgebung aufgeführt ist (§ 19 lit. a IDG).
- Fehlt eine angemessenes Datenschutzniveau, sind hinreichende Garantien zu verankern, die einen den Interessen angemessenen Schutz verankern (§ 19 lit. b und c IDG).
- Erfolgt eine grenzüberschreitende Übermittlung von Personendaten gestützt auf § 19 lit. c IDG, wird die Datenschutzbeauftragte vorab informiert (§ 22 Abs. 2 IDV).
- Im Einzelfall kann die Übermittlung gestützt auf die Einwilligung der betroffenen Person erfolgen (§ 22 Abs. 3 IDV).

2.10 Informationszugang (§ 20 IDG)

Das öffentliche Organ gewährleistet Zugang zu bei ihm vorhandenen Informationen und zu eigenen Personendaten.

Informationszugang

Massnahmen

- Sicherstellen, dass sowohl Ersuchen zu Informationen im Sinne des Öffentlichkeitsprinzips als auch Auskunftsersuchen betreffend die eigenen Personendaten durch das öffentliche Organ innert Frist behandelt und beantwortet werden (§§ 20, 28 IDG).

Umsetzung
- Das öffentliche Organ erstellt ein Verzeichnis der Informationsbestände, die Personendaten beinhalten (§ 14 Abs. 4 IDG).
- Das für den Informationsbestand verantwortliche Organ hat die Prozesse zur Behandlung von Auskunftsersuchen definiert und dokumentiert.
- Technische Systeme sind so gestaltet, dass Recherchen und eine vollständige Auskunft möglich sind.
- Auskünfte werden nur in den gesetzlich vorgesehenen Fällen verweigert, eingeschränkt oder aufgeschoben.
- Auskunftsverweigerungen oder -beschränkungen werden in einer Verfügung festgehalten.

2.11 Rechtsansprüche (§ 21 IDG)

Betroffene Personen können beim öffentlichen Organ Berichtigungs-, Vernichtungs-, Unterlassungs-, Beseitigungs- und Feststellungsansprüche geltend machen.

Rechtsansprüche

Massnahmen
- Sicherstellen, dass Berichtigungs-, Vernichtungs-, Unterlassungs-, Beseitigungs- oder Feststellungsbegehren von betroffenen Personen im Falle von unrechtmässigen Datenbearbeitungen überprüft, bearbeitet und beantwortet werden (§ 21 IDG).

Umsetzung
- Die Instrumente und Verfahren für die Ausübung des Berichtigungs-, Vernichtungs-, Unterlassungs-, Beseitigungs- und Feststellungsrechts wurden implementiert.
- Unrichtige Personendaten werden durch das öffentliche Organ berichtigt oder vernichtet.
- Widerrechtliche Datenbearbeitungen werden festgestellt, in der Folge unterlassen und die Folgen beseitigt.
- Die Widerrechtlichkeit wird festgestellt und dokumentiert.

2.12 Datenschutz-Folgenabschätzung und Vorabkontrolle (§ 10 IDG)

Das öffentliche Organ bewertet bei einer beabsichtigten Bearbeitung von Personendaten deren Risiken für die Grundrechte der betroffenen Personen (Datenschutz-Folgenabschätzung, DSFA). Datenbearbeitungen mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen sind der Datenschutzbeauftragten vorab zur Prüfung vorzulegen (§ 10 IDG).

Datenschutz-Folgenabschätzung

Massnahmen
- Sicherstellen, dass vor der Aufnahme einer neuen Datenbearbeitung oder einer wesentlichen Änderung einer Datenbearbeitung eine DSFA erstellt wird.

Umsetzung
- Geplante neue Bearbeitungen von Personendaten oder deren wesentliche Veränderung werden beschrieben.
- Eine Analyse der Risiken für die Grundrechte der betroffenen Personen (informationelle Selbstbestimmung, Privatsphäre) wird durchgeführt.
- Besondere Risikofaktoren, welche zu einer hohen Gefährdung von Grundrechten betroffener Personen führen können, werden identifiziert.
- Die Risiken werden nach Schwere des Eingriffs in die Grundrechte und Eintretenswahrscheinlichkeit bewertet, zum Beispiel mit niedrig, mittel, schwer, beziehungsweise niedrig, mittel, hoch.
- Die Massnahmen zur Bewältigung der Risiken, die bereits ergriffen wurden oder geplant sind, werden beschrieben.

Das öffentliche Organ unterbreitet eine beabsichtigte Bearbeitung von Personendaten mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen vorab der oder dem Beauftragten für den Datenschutz zur Prüfung.

Vorabkontrolle

Massnahmen
- Sicherstellen, dass Datenbearbeitungen mit besonderen Risiken für die Rechte und Freiheiten der Betroffenen der Datenschutzbeauftragten vorab zur Prüfung vorgelegt werden (§ 10 IDG).

Umsetzung
- Datenbearbeitungen, die ein im Sinne von § 24 IDV festgehaltenes Risiko beinhalten, wie z.B. ein Abrufverfahren, werden in der Planungsphase der Datenschutzbeauftragten zur Vorabkontrolle vorgelegt.

2.13 Meldepflicht (§ 12a IDG)

Ein Datenschutzvorfall liegt vor, wenn personenbezogene Daten
- unwiederbringlich vernichtet werden oder verloren gehen oder
- unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder
- Unbefugten zugänglich werden.

Ein Datenschutzvorfall muss der Datenschutzverantwortlichen gemeldet werden, wenn er zu einer Gefährdung der Grundrechte auf informationelle Selbstbestimmung beziehungsweise auf Privatsphäre von betroffenen Personen führen kann. Bestehen Zweifel, ob Grundrechte gefährdet sind, ist ebenfalls Meldung zu erstatten.

Meldung von Datenschutzvorfällen

Massnahmen
- Sicherstellen, dass Datenschutzvorfälle erkannt und der Datenschutzverantwortlichen gemeldet werden (§ 8 Abs. 1 IDG).

Umsetzung
- Datenschutzvorfälle werden erkannt und intern an die für die Erfüllung der Meldepflicht zuständige Stelle gemeldet.
- Die Datenschutzbeauftragte wird über meldepflichtige Vorfälle informiert.

V 3.2 / Oktober 2020