Stadt Bern

ombuds stelle daten schutz

Effingerstrasse 4
3011 Bern
Telefon 031 312 09 09

ombudsstelle@bern.ch
datenschutz@bern.ch

Vorabkontrolle – Allgemeine Informationen

Generelle Informationen

Dieses Merkblatt richtet sich insbesondere an die Verantwortlichen von IT-Projekten der städtischen Direktionen und Abteilungen. Wenn geplant ist, Personendaten einer grossen Anzahl von Personen elektronisch zu bearbeiten, sind Sie gesetzlich dazu verpflichtet, Projekte und Vorhaben der Datenschutz-Aufsichtsstelle der Stadt Bern (DSA) zur Prüfung vorzulegen. Mit der Vorabkontrolle soll die datenschutzkonforme Bearbeitung von Personendaten sichergestellt werden bzw. Datenschutz-Risiken wegen Neuanschaffung oder Adaption von Datenbearbeitungsprogrammen oder -systemen minimiert werden.

Die Verantwortung zur Einhaltung des Datenschutzes obliegt immer bei der datenbearbeitenden Behörde (Art. 8 KDSG).

Rechtsgrundlagen

Art. 17a Datenschutzgesetz (KDSG; BSG 152.04)
Art. 7 und 8 Datenschutzverordnung (DSV; BSG 152.040.1)

Vorabkontroll-bedürftige Datenbearbeitungen

Gemäss Art. 17a KDSG ist eine Vorabkontrolle vor Beginn der beabsichtigten Datenbearbeitung vorzunehmen, wenn Personendaten einer grösseren Anzahl von Personen elektronisch bearbeitet werden sollen und wenn:

- zweifelhaft ist, ob eine genügende Rechtsgrundlage besteht,
- besonders schützenswerte Personendaten bearbeitet werden,
- eine besondere Geheimhaltungspflicht (z.B. Sozialhilfegeheimnis) besteht *oder* die Rechte und Freiheiten der betroffenen Personen aufgrund der geplanten technischen Mittel besonderen Risiken ausgesetzt sind.

Technische Mittel mit besonderen Risiken für die Rechte und Freiheiten der betroffenen Personen liegen gemäss Art. 7 DSV insbesondere vor, wenn:

- Personendaten auf tragbaren Datenträgern gespeichert werden,
- Personendaten auf RFID-Chips (passive Funkfrequenzidentifikationstransponder) gespeichert werden,
- Personendaten über Drahtlosverbindungen übertragen werden (ausser bereits geprüfte Funktelefonverbindungen und Drahtlosverbindungen von Zahlterminals),
- Personendaten mit Bildaufzeichnungs- und Bearbeitungsgeräten erhoben werden,
- besonders schützenswerte Personendaten über öffentliche Netze übertragen werden *oder*
- Privaten aus dem Internet ein eingeschränkter Zugriff auf Daten aus einer Personendatenbank gewährt werden soll.

Zu beachten ist, dass nicht nur bei Einführung neuer Systeme, sondern auch bei Änderungen von bestehenden Datenbearbeitungen mit mindestens einem der oben erwähnten Risiken eine Vorabkontrolle durchgeführt werden muss (Art. 17a Abs. 2 KDSG).

Ausnahmen von der Vorabkontrolle

Eine Vorabkontrolle kann nach Art. 8 DSV entfallen, wenn:

- die eingesetzten Datenbearbeitungsprogramme oder –systeme bezüglich Datenschutz und Informatiksicherheit umfassend zertifiziert sind *oder*
- die Datenbearbeitung einschliesslich der elektronisch archivierten Datenbearbeitungen weniger als 500 Personen betrifft.

Den Entscheid darüber, ob eine Ausnahme vorliegt, trifft die DSA gestützt auf die konkreten Angaben zur geplanten Datenbearbeitung im Einzelfall.

Zeitpunkt

Die DSA ist frühzeitig über eine beabsichtigte Bearbeitung von Personendaten zu informieren oder in ein solches Vorhaben einzubeziehen. Dies ermöglicht es, konkrete Anforderungen an den Datenschutz bereits in der Konzeptphase aufzuzeigen, wodurch spätere Nachbesserungen bei der technischen Umsetzung oder gar ein Projekt-Stopp vermieden werden können.

- Ein erster Einbezug der DSA zwecks Abgabe einer datenschutzrechtlichen Grobbeurteilung kann bereits vor Projektstart im Rahmen des Digitalportfolio-Prozesses[1] der Stadt Bern erfolgen.
- Nach erfolgter Projektanmeldung kann die DSA in der Initialisierungsphase gemäss Projektleitfaden der ID[2] im Rahmen des Compliance Check Prozesses der ICT-Sicherheit für die Durchführung einer ISDS-Analyse beratend beigezogen werden.

  ISDS-Analyse kurz erklärt

  Die ISDS-Analyse dient der Beurteilung der Vorabkontrollpflicht des Vorhabens und liefert erste Grundlagen für die eigentliche Vorabkontrolle. Auf jeden Fall müssen grundlegende Informationen zum Projekt vorhanden sein (siehe «einzureichende ISDS-Dokumente»). Dieses Vorgehen ermöglicht es der DSA, den passenden Zeitpunkt für die Vorabkontrolle mit dem verantwortlichen öffentlichen Organ zu vereinbaren. Die eigentliche Vorabkontrolle erfolgt gestützt auf die relevanten ISDS-Dokumentationen (siehe «Einzureichende ISDS-Dokumente»), spätestens aber in der Realisierungsphase des Vorhabens und vor dessen Einführung.

- Wird der Prozess der Vorabkontrolle zu spät gestartet, kann die DSA keine Vorabkontrolle mehr durchführen, da allfällige Empfehlungen nicht mehr rechtzeitig vor der Produktivsetzung berücksichtigt werden könnten. Allfällig daraus folgende Projekt-Risiken, die bis zu einem Projekt-Stopp reichen können, sind durch die datenbearbeitenden Behörden zu tragen.

Inhalt und Verfahrensablauf

Die DSA prüft in der Vorabkontrolle, ob die für die Datenbearbeitung zuständige Behörde die Datenbearbeitung auf der Basis einer Rechtsgrundlage und mit angemessenen organisatorischen und technischen Schutzmassnahmen vornimmt. Das Resultat der Vorabkontrolle wird in einem Prüfbericht festgehalten und der verantwortlichen Behörde zunächst in Entwurf-Form zugestellt. Notwendige Verbesserungen des Datenschutzes hält die DSA in Form von Empfehlungen fest. Die verantwortliche Behörde erhält damit Gelegenheit, sich zum Entwurf des Vorabkontrollberichts und der Empfehlungen im Rahmen einer Stellungnahme zu äussern. Gestützt darauf verfasst die DSA den definitiven Vorabkontrollbericht. Bei Bedarf sind auch mehrere Iterationen möglich. Im Einzelnen verweisen wir auf unser Merkblatt «Vorabkontrolle – Die einzelnen Etappen».

[1] https://intranetbern.bgov.ch/digitales-und-informatik/digitalportfolio
[2] https://intranetbern.bgov.ch/digitales-und-informatik/projekte

Einzureichende ISDS-Dokumente

Für die Vorabkontrolle sind nachfolgende Dokumente und Angaben im Rahmen eines Informationssicherheits- und Datenschutzkonzeptes (ISDS-Konzept) gestützt auf die **Vorlagen ISDS-Paket der ICT-Sicherheit** einzureichen:

ISDS-Konzept mit folgenden Dokumenten und Angaben

- Verzeichnis der sicherheitsrelevanten Dokumente,
- Einstufung aufgrund der Schutzbedarfsanalyse,
- Darstellung der Rechtslage mit Nennung der Rechtsgrundlagen (evtl. Verweis auf Datenschutzbeurteilung im Rahmen des Compliance Check Prozesses),
- sicherheitsrelevante Systembeschreibung,
- Architektur und darin enthaltene Schnittstellen mit Datenflüssen,
- Risikoanalyse mit Sicherheitsmassnahmen zu den Risiken, Aufführung der Restrisiken,
- Bezeichnung und Unterschrift der Verantwortlichen, welche die Restrisiken übernehmen,
- (Referenz auf ein) Rollen- und Berechtigungskonzept,
- (Referenz auf ein) Archivierungs- und Löschkonzept etc.

Allfällig weitere projektspezifische Dokumente

- Auftragsdatenverarbeitungsvertag,
- Datenschutzerklärung,
- und weiter Dokumente.

Weiterführende Unterlagen

Weitergehende Informationen zu den einzelnen Etappen der Vorabkontrolle und zu den verschiedenen Rollen und Verantwortlichkeiten im Vorabkontroll-Verfahren sind **hier** auffindbar.

Datenschutz-Aufsichtsstelle der Stadt Bern, 08.03.2022 / EKR