BASEL LANDSCHAFT

Checkliste Vorabkontrolle

Diese Checkliste dient der Triage der Aufsichtsstelle Datenschutz, ob eine Bearbeitung von Personendaten der gesetzlich vorgeschriebenen Vorabkontrolle unterliegt. Gemäss § 12 des Informations- und Datenschutzgesetzes (IDG, SGS 162) sind die öffentlichen Organe verpflichtet, bestimmte – besonders risikoreiche - Datenbearbeitungsprojekte der Datenschutzbeauftragten zur Vorabkontrolle zu unterbreiten.

§ 9 der Informations- und Datenschutzverordnung (IDV, SGS 162.11) gibt präzisere Anhaltspunkte zur Frage, welche Projekte solche besonderen Risiken mit sich bringen (s. zweite Seite mit Fussnoten zu nachfolgenden Fragestellungen). Die Aufzählung der Risiken in § 9 IDV ist nicht abschliessend.

Projektname

.....

Verantwortliches Öffentliches Organ

.....

		Ja	Unklar	Nein
1	Beinhaltet das Vorhaben ein Abrufverfahren? [1]	☐	☐	☐
2	Werden besondere Personendaten bearbeitet? [2]	☐	☐	☐
3	Werden neue Technologien eingesetzt? [3]	☐	☐	☐
4	Ist von der Datenbearbeitung eine grosse Anzahl von Personen betroffen? [4]	☐	☐	☐
5	Ist vorgesehen, dass mehr als zwei Verwaltungseinheiten Personendaten gemeinsam bearbeiten? [5]	☐	☐	☐
6	Bestehen andere Gründe oder Hinweise, welche für ein Vorliegen von besonderen Risiken sprechen können? [6] Falls Ja oder Unklar: **Gründe oder Hinweise schriftlich festhalten**.	☐	☐	☐

Sofern nicht alle vorstehenden Fragen mit "Nein" beantwortet werden, klärt die Aufsichtsstelle Datenschutz in Zusammenarbeit mit der zuständigen Ansprechperson ab, ob und gegebenenfalls in welcher Weise eine Vorabkontrolle durchgeführt werden muss.

Verantwortliche Ansprechperson und Sicherheitsbeauftragter

Name, Vorname

.....

Telefon, E-Mail

.....

Funktion

Datum, Unterschrift

.....

Beilagen .....

[1] Unter einem **Abrufverfahren** wird ein automatisiertes Verfahren verstanden, welches Personen oder Stellen *ausserhalb* des verantwortlichen Organs einen Zugriff auf Personendaten durch Abruf ermöglicht. Abruf bedeutet, dass das Auslösen des Zugriffsvorganges durch den Datenempfänger erfolgt, dieser also die jeweiligen Daten beschaffen kann, ohne dass das verantwortliche öffentliche Organ die Berechtigung der konkreten Abfrage jeweils überprüfen kann. (Online-Zugriff auf einen Informationsbestand, automatisierte Datenabfrage- oder -austauschprozesse).

[2] **Besondere Personendaten** sind Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht, wie z.B., wenn diese sich auf religiöse, weltanschauliche oder politische Ansichten, medizinische Angaben, Massnahmen der sozialen Hilfe oder administrative oder strafrechtliche Verfolgung und Sanktionen beziehen (siehe §3 Abs. 4 IDG). Diese Beispiele sind nicht abschliessend, massgeblich ist die Gefahr der Grundrechtsverletzung. So können auch „normale" Personendaten wie zum Beispiel Adressen zu „besonderen" Personendaten werden, so zum Beispiel wenn die betroffene Person an einer Adresse wohnt, die Rückschlüsse auf dessen psychische Gesundheit ermöglicht. Bei der Beurteilung, ob eine besondere Gefahr einer Persönlichkeitsverletzung vorliegt und es sich somit um „besondere Personendaten" handelt, ist der Kontext, in welchem die Informationen erhoben und verwendet werden miteinzubeziehen. Der Persönlichkeitsschutz kann aber auch über den Datenschutz hinausgehen, zum Beispiel dann, wenn eine Person verfolgt oder bedroht wird und deshalb ihr Aufenthalt nicht bekannt werden darf. Das muss in der Schutzbedarfsanalyse berücksichtigt werden. Neben den sensiblen Personendaten gehören auch Persönlichkeitsprofile, d.h. Zusammenstellungen von Informationen, welche Aufschluss über viele Aspekte einer Persönlichkeit geben, zu den besonderen Personendaten.

[3] **Neue Technologien** bergen oft neuartige Risiken für die Rechte und Freiheit der betroffenen Personen. „Neu" heisst in diesem Falle nicht, dass eine Technologie noch nie eingesetzt wurde. „Neu" heisst vielmehr, dass mit dem Einsatz einer neuen Technologie in Bezug auf Datenbearbeitungen neue Möglichkeiten oder neue Risiken für die Grundrechte betroffener Personen geschaffen werden. Dabei handelt es sich oft um Technologien bzw. Funktionserweiterungen dazu, welche neue oder zusätzliche Informationen generieren.

[4] Die Tatsache, dass durch eine Datenbearbeitung eine **grosse Anzahl Personen betroffen** ist, kann zu besonderen Risiken für die Rechte und Freiheit der betroffenen Personen führen. Von einer grossen Anzahl von Personen ist die Rede, wenn die Datenbearbeitung nicht nur auf einzelne wenige, klar bestimmbare Personen eingeschränkt bleibt sondern im Endausbau des Informatiksystems potentiell weite Personenkreise wie alle Schüler/-innen, Mitarbeitenden, Verkehrsteilnehmenden, Anwohner/-innen etc. von einer Datenbearbeitung betroffen sein können. Das Kriterium „grosse Anzahl Betroffener" ist deshalb nur schwer mit einer bestimmten Zahl definierbar. Die Zahl 10'000 birgt sicher eine grosse Anzahl Betroffener, kann aber wie oben beschrieben nur bedingt als Grenzwert für dieses Kriterium gelten.

[5] Das Kriterium der **Datenbearbeitung durch mehrere öffentliche Organe** ist erfüllt, wenn mehrere Organe gemeinsam über Umfang und Art der Datenbearbeitung bestimmen und für diese gemeinsam die Verantwortung regeln müssen, da hier für ein adäquates Risikomanagement besondere Bearbeitungs- und Koordinationsregelungen erforderlich sind.

[6] Beispiele für **besondere Risiken**: Outsourcing der Datenbearbeitung (auch teilweise), Verknüpfung mit anderen Personendatenbeständen, Komplexität der geplanten Systemumgebung, Mobile Zugangspunkte, etc.

Zustellung dieser ausgefüllten *Checkliste* zusammen mit der *Schutzbedarfsanalyse* und - falls bereits vorhanden - der *Studie* und dem *Projekt(initialisierungs)auftrag* an

Aufsichtsstelle Datenschutz Basel-Landschaft (datenschutz@bl.ch) (ausser wenn alle Fragen zur Vorabkontrolle mit "nein" beantwortet werden)

Version 1.3 / Februar 2018

Aufsichtsstelle Datenschutz

Kanonengasse 20
4410 Liestal

T 061 552 64 30

datenschutz@bl.ch

www.bl.ch/datenschutz