BASEL LANDSCHAFT

Checkliste Datenschutz-Folgenabschätzung / Vorabkonsultation Datenbearbeitung

Gemäss § 11a Abs. 1 IDG müssen alle öffentliche Organe prüfen, ob ein Vorhaben zur Bearbeitung von Personendaten voraussichtlich hohe Risiken für die von der Bearbeitung betroffenen Personen birgt. Ist dies der Fall, müssen sie eine Datenschutzfolgenabschätzung vornehmen (§ 11a Abs. 2 IDG) und das Vorhaben der ASD zur Vorabkonsultation vorlegen (§ 12 Abs. 1 IDG). Diese Checkliste mit den Fussnoten auf der Seite 2 definiert Kriterien gemäss § 12 Abs. 2 IDG, dient der ersten Risikoeinschätzung sowie der Triage der Aufsichtsstelle Datenschutz.

Projektname:……
Verantwortliches Öffentliches Organ:……

		Ja	Unklar	Nein
1	Werden besondere Personendaten bearbeitet? [1]	☐	☐	☐
2	Ist Profiling geplant? [2]	☐	☐	☐
3	Werden neue Technologien eingesetzt? [3]	☐	☐	☐
4	Ist von der Datenbearbeitung eine grosse Anzahl von Personen betroffen? [4]	☐	☐	☐
5	Ist vorgesehen, dass mehrere öffentliche Organe Personendaten gemeinsam oder in einem gemeinsam genutzten System bearbeiten? [5]	☐	☐	☐
6	Ist eine spezielle Form der Auftragsdatenbearbeitung geplant? [6]	☐	☐	☐
7	Bestehen andere Gründe oder Hinweise, welche für ein Vorliegen von besonderen Risiken sprechen können? [7] 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 Daten-schutz-Folgenabschätzung bzw. eine Vorabkonsultation durchgeführt werden muss.

Verantwortliche Ansprechperson und Sicherheitsbeauftragte/ -beauftragter

Name, Vorname …….

Telefon, E-Mail ……

Funktion

Datum, Unterschrift

……

Beilagen ……

[1] **Besondere Personendaten** sind Personendaten, bei deren Bearbeitung eine besondere Gefahr der Grundrechtsverletzung besteht, insbesondere Angaben über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, das Erbgut (genetische Daten), die Intimsphäre oder die ethnische Herkunft, Behinderungen, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen, mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten) (§ 3 Abs. 4 IDG). 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.

[2] **Profiling** ist jede Auswertung von Informationen, um wesentliche persönliche Merkmale zu analysieren oder Entwicklungen vorherzusagen, insbesondere bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, Intimsphäre oder Mobilität.(§ 3 Abs. 7 IDG)

[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 (bspw. Patientenportal, Internet der Dinge, Videoberatung, usw.) oder angepasste Massnahmen für die Gewährleistung der Informationssicherheit erfordern.

[4] Die Tatsache, dass durch eine Datenbearbeitung eine **grosse Anzahl Personen betroffen** ist, kann zu grösserem Schadensausmass 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 5'000 birgt sicher eine grosse Anzahl Betroffener, kann aber wie oben beschrieben nur bedingt als Grenzwert für dieses Kriterium gelten.

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

[6] **Spezielle Form der Auftragsdatenbearbeitung**. Droht aufgrund der Bearbeitung durch einen Dritten ein grösserer Steuerungs-/Kontrollverlust der Auftraggeberin oder sollen Services genutzt werden, bei welchen die AGB des Anbieters (ohne Anpassung an die kantonalen Datenschutzgesetze) akzeptiert werden müssen, können daraus grosse Risiken für die Rechte und Freiheit der betroffenen Personen entstehen. Dies gilt ausserdem für den Fall, dass die Auftragsdatenbearbeitung eine Bearbeitung bzw. Übermittlung in Staaten ohne angemessenes Schutzniveau beinhaltet (vgl. § 21 IDG).

[7] Beispiele für **besondere Risiken**: Verarbeitung personenbezogener Daten von Kindern oder anderen schutzbedürftigen Personen mit online-Diensten, Zusammenführen/Kombinieren von Personendaten, die durch unterschiedliche Prozesse generiert wurden, Abrufverfahren, Zugriff über nicht gemanagte Geräte, Komplexität der geplanten Systemumgebung, usw., Verwendung von Algorithmen zur Durchführung bzw. Unterstützung von personenbezogenen Entscheidungen.

Zustellung dieser ausgefüllten *Checkliste* zusammen mit der *Schutzbedarfsanalyse* und - falls vorhanden - der *Studie* und dem *Projekt(initialisierungs)auftrag* an die Aufsichtsstelle Datenschutz Basel-Landschaft (datenschutz@bl.ch) (ausser wenn alle Fragen zur Vorabkonsultation mit "nein" beantwortet werden).

Version 1.0 / Februar 2023

Aufsichtsstelle Datenschutz

Kanonengasse 20
4410 Liestal

T 061 552 64 30

datenschutz@bl.ch

www.bl.ch/datenschutz