

Kantonaler Datenschutzbeauftragter

Bahnhofstrasse 15

6002 Luzern

Telefon 041 228 61 00

datenschutz@lu.ch

datenschutz.lu.ch

**Formular Schwellwerteanalyse und Formular Datenschutz-Folgenabschätzung**

Dieses Formular dient der Klärung, ob eine Bearbeitung von Personendaten1 der gesetzlich verlangten Datenschutz-Folgenabschätzung und Vorabkonsultation unterliegt.

Gemäss § 7a KDSG müssen Organe eine Datenschutz-Folgenabschätzung durchführen, wenn ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen besteht. Wenn die vorgesehene Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundreche zur Folge hätte, obwohl Massnahmen vorgesehen sind, ist solche Bearbeitung der Personendaten vorab dem oder der Datenschutzbeauftragten zur Prüfung zu vorgelegen.2 Der Begriff der hohen Risiken wird im Merkblatt Datenschutz-Folgenabschätzung und Vorabkonsultation mit den wichtigsten Anwendungsfällen beispielhaft konkretisiert (vgl. nachfolgende Fragestellungen).

**Anhang 1.** **Formular Schwellwertanalyse**

1. **Angaben des Vorhabens und verantwortliches Organs**

**Name des Vorhabens / des Projekts Verantwortliches Organ**

………………………………………………… ………………………………………………

|  |  |
| --- | --- |
| **Ja** | **Nein** |
| 1 | Beinhaltet das Vorhaben ein Abrufverfahren?3 | ☐ | ☐ |
| 2 | Wird Vielzahl von besonders schützenswerten Personendaten bearbeitet?4 | ☐ | ☐ |
| 3 | Ist vom Vorhaben eine grosse Anzahl von Personen betroffen?5 | ☐ | ☐ |
| 4 | Ist vorgesehen, dass mehr als zwei Verwaltungseinheiten (Dienstabteilungen der Stadt oder anderer Verwaltungen) Personendaten gemeinsam bearbeiten?6 | ☐ | ☐ |
| 5 | Werden neue Technologien/Mechanismen oder Profiling eingesetzt?7 | ☐ | ☐ |
| 6 | Werden umfangsreiche öffentliche Bereiche systematisch überwacht? | ☐ | ☐ |
| 7 | Werden Personendaten in Drittstaaten übermittelt, wenn die ausländische Gesetzgebung keinen angemessenen Schutz gewährleistet? | ☐ | ☐ |
| 8 | Kann eine grosse oder unbegrenzte Anzahl Personen auf die Daten zugreifen? | ☐ | ☐ |
| 9 | Bestehen andere Gründe oder Hinweise, welche für ein Vorliegen von besonderen Risiken sprechen können?  Falls "Ja": Gründe oder Hinweise schriftlich festhalten.  Klicken oder tippen Sie hier, um Text einzugeben. | ☐ | ☐ |

Sofern nicht alle vorstehenden Fragen mit "Nein" beantwortet werden, besteht voraussichtlich ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen. In dem Fall führt das Organ eine Datenschutz-Folgenabschätzung durch.

**Anhang 2. Formular Datenschutz-Folgenabschätzung**

1. **Angaben des Vorhabens und verantwortliches Organs**

**Name des Vorhabens / des Projekts Verantwortliches Organ**

………………………………………………… …………………………………………

1. **Allgemeine Beschreibung der geplanten Bearbeitungsvorgänge**

Beschreibung des Vorhabens (Projekt), Bearbeitungsvorgänge und verwendete Technologie:

Klicken oder tippen Sie hier, um Text einzugeben.

Kreis der betroffenen Personen und Kategorien von Personendaten:

Klicken oder tippen Sie hier, um Text einzugeben.

Zweck der Datenbearbeitung:

Nennung der Rechtsgrundlagen und Rechtsgrundlageanalyse der Datenbearbeitung:

Klicken oder tippen Sie hier, um Text einzugeben.

Aufbewahrungsdauer der Personendaten:

Klicken oder tippen Sie hier, um Text einzugeben.

Prüfung der Notwendigkeit und Verhältnismässigkeit in Bezug auf den Verarbeitungszweck:

Klicken oder tippen Sie hier, um Text einzugeben.

Empfänger der Personendaten (Datenbekanntgabe an anderen Organe und Auftragsbearbeitung):

Klicken oder tippen Sie hier, um Text einzugeben.

1. **Risikoidentifikation und -bewertung**
   1. **Identifikation**

Identifikation der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen, die zu physischen, materiellen oder immateriellen Schäden führen können (zum Beispiel Diskriminierung, Identitätsdiebstahl oder Betrug, finanzielle Verluste oder Reputationsverluste):

|  |  |
| --- | --- |
| **Ja** | **Nein** |
| **Generelle Datenschutzrisiken** | | | |
| 1 | Unberechtigter Zugriff zu Personendaten  (von einer internen oder externen Person oder einem System) | ☐ | ☐ |
| 2 | Unerwünscht Modifikation der Personendaten  (absichtlich oder unbeabsichtigt; z.B. von einer internen oder externen Person oder wegen einer Fehlkonfiguration) | ☐ | ☐ |
| 3 | Verlust der Personendaten  (absichtlich oder unbeabsichtigt; z.B. von einer internen oder externen Person) | ☐ | ☐ |
| **Prozessspezifische Risiken** | | | |
| 4 | Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Personendaten | ☐ | ☐ |
| 5 | Unbefugte Aufhebung der Pseudonymisierung | ☐ | ☐ |
| 6 | Andere Risiken. Falls "Ja": schriftlich festhalten:  Klicken oder tippen Sie hier, um Text einzugeben. | ☐ | ☐ |

* 1. **Risikobewertung8**

Bewertung der Risiken ohne die Einsetzung der Massnahmen zur Risikominimierung:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [Risiko 1.] |  | **Auswirkungen:**  gering | **Auswirkungen:**  mittel | **Auswirkungen:**  hoch |
| **Wahrscheinlich-keit:** hoch |  |  |  |
| **Wahrscheinlich-keit:** mittel |  |  |  |
| **Wahrscheinlich-keit:** gering |  |  |  |
| [Risiko 2.] |  | **Auswirkungen:**  gering | **Auswirkungen:**  mittel | **Auswirkungen:**  hoch |
| **Wahrscheinlich-keit:** hoch |  |  |  |
| **Wahrscheinlich-keit:** mittel |  |  |  |
| **Wahrscheinlich-keit:** gering |  |  |  |
| [Risiko 3.] |  | **Auswirkungen:**  gering | **Auswirkungen:**  mittel | **Auswirkungen:**  hoch |
| **Wahrscheinlich-keit:** hoch |  |  |  |
| **Wahrscheinlich-keit:** mittel |  |  |  |
| **Wahrscheinlich-keit:** gering |  |  |  |
| [Risiko 4.] |  | **Auswirkungen:**  gering | **Auswirkungen:**  mittel | **Auswirkungen:**  hoch |
| **Wahrscheinlich-keit:** hoch |  |  |  |
| **Wahrscheinlich-keit:** mittel |  |  |  |
| **Wahrscheinlich-keit:** gering |  |  |  |

1. **Vorgesehene rechtliche, technische und organisatorische Massnahmen zur Risikominimierung**

|  |  |  |
| --- | --- | --- |
| **Ja** | **Nein** | **N/A** |
| 1 | Datenminimierung (z.B. Reduzierung die Bearbeitungsfunktionalitäten, automatisierte Datenbearbeitung) | ☐ | ☐ | ☐ |
| 2 | Pseudonymisierung | ☐ | ☐ | ☐ |
| 3 | Information für die betroffenen Personen (z.B. Datenschutzerklärung) | ☐ | ☐ | ☐ |
| 4 | Instrumente und Verfahren für die Ausübung des Berichtigungs-, Vernichtungs- und Sperrungsrechts sowie das Recht auf die Anbringung eines Bestreitungsvermerks | ☐ | ☐ | ☐ |
| 5 | Vertragsanforderungen bezüglich Datenschutz und Datensicherung durch Auftragsbearbeiter | ☐ | ☐ | ☐ |
| 6 | Garantien für grenzüberschreitende Datenbekanntgabe | ☐ | ☐ | ☐ |
| 7 | Kontrolle der erfassten Personendaten (Datenrichtigkeit) | ☐ | ☐ | ☐ |
| 8 | Zugriffskontrolle (einschl. Zugriffsrollen und –verwaltung, geeignete Authentisierungsverfahren, Passwort-Richtlinie, Monitoring/Protokollierung) | ☐ | ☐ | ☐ |
| 9 | Netzwerksicherheit | ☐ | ☐ | ☐ |
| 10 | Physische Sicherheitsmassnahmen | ☐ | ☐ | ☐ |
| 11 | Physische und/oder logische Trennungsmassnahmen | ☐ | ☐ | ☐ |
| 12 | Verschlüsselung der Personendaten (bei der Übertragung / im Ruhezustand) | ☐ | ☐ | ☐ |
| 13 | Verschlüsselungsschlüsselmanagement ausschl. beim verantwortlichen Organ | ☐ | ☐ | ☐ |
| 14 | Datensicherungskopien | ☐ | ☐ | ☐ |
| 15 | Funktionen im IT-System für Garantieren der Datenintegrität | ☐ | ☐ | ☐ |
| 16 | Löschung der Personendaten (manuell oder automatisch) | ☐ | ☐ | ☐ |
| 17 | Betriebsanleitung für die Benutzer und/oder Benutzerschulung | ☐ | ☐ | ☐ |
| 18 | Regelmässige Überprüfung der Sicherheitsmassnahmen | ☐ | ☐ | ☐ |
| 19 | Datenschutzmanagementsystem | ☐ | ☐ | ☐ |
| 20 | Andere Massnahmen. Falls "Ja": schriftlich festhalten:  Klicken oder tippen Sie hier, um Text einzugeben. | ☐ | ☐ | ☐ |

1. **Restrisiken8**

Restrisiken, wenn die vorgesehene rechtliche, technische und organisatorische eingesetzt sind:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| [Risiko 1.] |  | **Auswirkungen:**  gering | **Auswirkungen:**  mittel | **Auswirkungen:**  hoch |
| **Wahrscheinlich-keit:** hoch |  |  |  |
| **Wahrscheinlich-keit:** mittel |  |  |  |
| **Wahrscheinlich-keit:** gering |  |  |  |
| [Risiko 2.] |  | **Auswirkungen:**  gering | **Auswirkungen:**  mittel | **Auswirkungen:**  hoch |
| **Wahrscheinlich-keit:** hoch |  |  |  |
| **Wahrscheinlich-keit:** mittel |  |  |  |
| **Wahrscheinlich-keit:** gering |  |  |  |
| [Risiko 3.] |  | **Auswirkungen:**  gering | **Auswirkungen:**  mittel | **Auswirkungen:**  hoch |
| **Wahrscheinlich-keit:** hoch |  |  |  |
| **Wahrscheinlich-keit:** mittel |  |  |  |
| **Wahrscheinlich-keit:** gering |  |  |  |
| [Risiko 4.] |  | **Auswirkungen:**  gering | **Auswirkungen:**  mittel | **Auswirkungen:**  hoch |
| **Wahrscheinlich-keit:** hoch |  |  |  |
| **Wahrscheinlich-keit:** mittel |  |  |  |
| **Wahrscheinlich-keit:** gering |  |  |  |

1. **Dokumentation**

|  |  |  |
| --- | --- | --- |
| **Ja** | **Nein** | **N/A** |
| 1 | Informationssicherheits- und Datenschutzkonzept mit Risikoanalyse  (obligatorisch für neue Anwendungen und Systeme, mit denen vertrauliche oder geheime Informationen bearbeitet werden) | ☐ | ☐ | ☐ |
| 2 | Schutzbedarfsanalyse | ☐ | ☐ | ☐ |
| 3 | Systemarchitektur / Übersicht der Anwendungen, Systeme Netzwerke, Schnittstellen und Prozesse, allgemeine Organisationskonzept | ☐ | ☐ | ☐ |
| 4 | Sicherheitsstrategie und Sicherheitskonzept | ☐ | ☐ | ☐ |
| 5 | Berechtigungs-, Zugriffs-, Protokollierungskonzept | ☐ | ☐ | ☐ |
| 6 | Löschungskonzept | ☐ | ☐ | ☐ |
| 7 | Detailkonzept und Massnahmenplan | ☐ | ☐ | ☐ |
| 8 | Dienstleistungsvereinbarung mit Auftragsbearbeiter | ☐ | ☐ | ☐ |
| 9 | Dienstleistungsvereinbarung über zentrale Datenbanken und Abrufverfahren | ☐ | ☐ | ☐ |
| 10 | Vertraulichkeitserklärung (Muster) | ☐ | ☐ | ☐ |
| 11 | Benutzeranleitung / -handbuch | ☐ | ☐ | ☐ |
| 12 | Andere Dokumentation. Falls "Ja": schriftlich festhalten:  Klicken oder tippen Sie hier, um Text einzugeben. | ☐ | ☐ | ☐ |

1. **Vorabkonsultationspflicht**

Sofern die Restrisiken (Frage 5) erhebliche oder kritische bis katastrophale (der gelbe und rote Bereich) Auswirkungen haben, obwohl die Massnahmen (Frage 4) vorgesehen sind, kann die vorgesehene Datenbearbeitung ein hohes Risiko für die Persönlichkeit und/oder die Grundrechte zur Folge haben, und das verantwortliche Organ muss die Stellungnahme des oder der Datenschutzbeauftragten einholen.

Sollten Zweifel an der Risikominimierung oder der Verhältnismässigkeit der rechtlichen, organisatorischen und technischen Massnahmen bestehen, ist es zu empfehlen, dass das verantwortliche Organ den oder die Datenschutzbeauftragten kontaktiert.

**Adressaten / Zustellung an dem / der Datenschutzbeauftragten des Kantons Luzern**

Unter Personendaten ist gemäss § 2 KDSG zu verstehen:

*Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen.*

2 Der Vorabkonsultation beim Datenschutzbeauftragten unterliegen alle Bearbeitungen von Personendaten mit besonderen Risiken, unabhängig davon,

- ob diese als Projekt, Vorhaben oder dgl. definiert werden;

- ob es sich um neue Bearbeitungen oder um Ablösungen handelt;

- ob diese dem städtischen IT-Controlling unterstehen.

3 Unter Abrufverfahren versteht man jedes automatisierte Verfahren (online, batch oder dgl.), welches Dritten einen Zugriff auf Personendaten (Übermittlung, Einsicht oder dgl.) durch Abruf ermöglicht. Abruf bedeutet, dass das Auslösen des Zugriffsvorganges durch den Datenempfänger erfolgt, dieser also die Daten selber beschaffen kann. Dritte sind alle Personen oder Stellen ausserhalb des verantwortlichen Organs (Dienstabteilung).

4 Unter besonders schützenswerten Personendaten ist gemäss § 2 Abs. 2 KDSG zu verstehen:

*Besonders schützenswerte Personendaten sind Angaben über natürliche Personen, bei welchen eine besondere Gefahr für Persönlichkeits- und Grundrechtsverletzungen besteht, insbesondere*

*1. die religiöse, weltanschauliche oder politische Haltung,*

*2. die Gesundheit,*

*3. die Intimsphäre,*

*4. das Erbgut,*

*5. die ethnische Zugehörigkeit,*

*6. mit speziellen technischen Verfahren gewonnen Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten),*

*7. Massnahmen der Sozialhilfe,*

*8. verwaltungs- oder strafrechtliche Massnahmen und Sanktionen sowie,*

*9. eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person (Persönlichkeitsprofil) erlaubt.*

Im Falle von Ziff. 9 (Zusammenstellung von Daten) ist das Erfordernis der Vielzahl von besonders schützenswerten Personendaten immer erfüllt.

5 Das Kriterium der *grossen Anzahl von Personen* kann nicht mit einer bestimmten Zahl definiert werden. Eine grosse Anzahl von Personen ist immer dann anzunehmen, wenn der Kreis der Betroffenen nicht von Beginn an auf einzelne wenige, klar bestimmbare Personen eingeschränkt bleibt. Massgebend ist das Ausmass der möglicherweise Betroffenen. Von einer grossen Anzahl von Personen ist zu sprechen, wenn - auch bloss in theoretischer Hinsicht - weite Personenkreise wie alle SchülerInnen, Mitarbeitenden, Verkehrsteilnehmenden, Anwohnenden usw. von einer Datenbearbeitung betroffen sein können. Nicht vorausgesetzt wird, dass besondere Personendaten (vgl. vorstehend Fussnote 2) bearbeitet werden.

6 Von einer gemeinsamen Bearbeitung ist immer dann die Rede, wenn ein Informationsbestand bzw. eine Datenbank der Aufgabenerfüllung mehrerer Organe dient. Mit anderen Worten: es liegt noch keine gemeinsame Datenbearbeitung vor, wenn Daten einer Dienstabteilung regelmässig anderen Organen bekannt gegeben werden. Voraussetzung ist vielmehr, dass mehrere Organe über Umfang und Art der Datenbearbeitung gemeinsam bestimmen und somit auch gemeinsam für die Datenbearbeitung Verantwortung tragen.

7Für den Begriff der "neuen Technologie" ist die Fragestellung massgebend, ob mit dem Einsatz einer bestimmten Technologie in Bezug auf Datenbearbeitungen neue Möglichkeiten oder neue Risiken geschaffen werden. Es sind somit insbesondere Technologien gemeint, welche dazu führen, neue oder zusätzliche Informationen zu generieren (bspw. Biometrie, Data Mining) oder weitergehende Bearbeitungen zu ermöglichen (bspw. RFID).

Profiling ist gemäss § 2 Abs. 4bis KDSG jede Art der automatisierten Bearbeitung von Personendaten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten. Insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person/der betroffenen Person zu analysieren oder vorherzusagen.

8 Anleitung für Risikobewertung in Merkblatt “Datenschutzfolgenabschätzung und Vorabkonsultation“ Anhang 1