KANTON LUZERN

Kantonaler Datenschutzbeauftragter
Bahnhofstrasse 15
6002 Luzern
Telefon 041 228 61 00
datenschutz@lu.ch
www.datenschutz.lu.ch

Merkblatt Datenschutz-Folgenabschätzung und Vorabkonsultation

1. Zweck des Merkblattes

Der Datenschutz ist bereits in der Planungsphase von Vorhaben und Projekten zu berücksichtigen. Öffentliche Organe des Kantons Luzern müssen Datenschutz-Folgenabschätzungen durchführen und Projekte und Vorhaben dem Datenschutzbeauftragten allenfalls zur Prüfung unterbreiten, wenn diese Datenbearbeitungen beinhalten, die für die betroffenen Personen mit hohen Risiken für ihre Rechte und Freiheiten verbunden sind. Mit der Vorabkonsultation soll die datenschutzkonforme Bearbeitung von Personendaten sichergestellt werden. Um die erforderlichen Massnahmen bei der Datenbearbeitung mit einem hohen Risiko einleiten zu können, bedarf es einer rechtzeitigen Prüfung im Vorfeld.

Dieses Merkblatt beinhaltet die wesentlichen Angaben zur Datenschutz-Folgenabschätzung und Vorabkonsultation sowie zu einer kurzen Checkliste, mit denen öffentliche Organe abklären können, ob sie im konkreten Fall eine Datenschutz-Folgenabschätzung durchführen müssen und die geplante Datenbearbeitung dem oder der Datenschutzbeauftragten zur Vorabkonsultation unterbreiten müssen.

2. Rechtsgrundlagen

- § 6 und § 7a Kantonales Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz, KDSG, SRL Nr. 38)
- § 6c Kantonale Datenschutzverordnung (KDSV SRL Nr. 38b)
- § 9 Informatikgesetz (SRL Nr. 26)

3. Definition

Mit der Datenschutz-Folgenabschätzung ist eine Prognose darüber zu machen, welche Folgen eine geplante Datenbearbeitung für die betroffenen Personen oder Personengruppen aufweist. Wenn sich aus der Abschätzung ergibt, dass die vorgesehene Datenbearbeitung ein hohes Risiko für die Persönlichkeits- oder die Grundrechte der betroffenen Personen zur Folge hat, obwohl rechtliche, technische und organisatorische Massnahmen vorgesehen sind, holt das Organ zum Vorhaben vorab die Stellungnahme des oder der Datenschutzbeauftragten ein, ob eine beabsichtigte Bearbeitung von Personendaten mit dem Datenschutz vereinbar ist (Vorabkonsultation).

Ein hohes Risiko besteht insbesondere, wenn für die Datenbearbeitung neue technische Bearbeitungsformen, wesentlich geänderte Prozesse oder ein Abrufverfahren vorgesehen sind oder besonders schützenswerte Personendaten in grossem Umfang oder von mehreren Organen in verknüpften Datenbanken bearbeitet werden.

4. Adressat

Alle Öffentliche Organe, die dem KDSG unterstehen und ein Vorhaben zur Datenbearbeitung planen, müssen grundsätzlich die Auswirkungen auf den Datenschutz überprüfen, gegebenenfalls eine Datenschutz-Folgenabschätzung durchführen und wenn ein hohes Risiko verbleibt, obwohl rechtliche, technische und organisatorische Massnahmen vorgesehen sind, den Datenschutzbeauftragten vorab konsultieren. Verantwortlich für die rechtzeitige Durchführung der Datenschutz-Folgenabschätzung und der Meldung zur Vorabkonsultation ist das für das geplante Vorhaben verantwortliche Organ.

Wurde eine Datenschutzberaterin oder ein Datenschutzberater ernannt, so sorgt diese für die Durchführung der notwendigen Datenschutz-Folgenabschätzungen und ist Ansprechperson des oder der Datenschutzbeauftragten.

5. Datenschutz-Folgenabschätzung

Eine vorgängige Datenschutz-Folgenabschätzung dient dazu, den Datenschutz bereits in der Planungsphase eines Vorhabens besser zu verankern. Bei heikleren Vorhaben soll eine risikobasierte Beurteilung des Datenschutzes durchgeführt und dokumentiert werden. Die Prüfung möglicher Auswirkungen einer geplanten Datenbearbeitung ist ein Beitrag zur Qualitätssicherung bei den organisatorischen und technischen Prozessen sowie den vertraglichen Rahmenbedingungen für die Datenbearbeitung innerhalb der Verwaltung.

Mittels Datenschutz-Folgenabschätzungen sollen Risiken identifiziert und bewertet werden, die durch den Einsatz von Technologien und Systemen im Rahmen der Datenverarbeitung entstehen. Die Datenschutz-Folgenabschätzung ist ausserdem die Grundlage für eine effiziente Durchführung der allenfalls notwendigen Vorabkonsultation (siehe unten 6).

5.1. Betroffene Datenbearbeitungen

Eine formelle Datenschutz-Folgenabschätzung ist nicht generell erforderlich aber nötig, wenn die vorgesehene Datenbearbeitung voraussichtlich zu einem hohen Risiko für die Persönlichkeits- oder die Grundrechte der betroffenen Personen führt. Mit der Abschätzung ist eine Prognose darüber zu machen, welche Folgen eine geplante Datenbearbeitung für die betroffenen Personen oder Personengruppen aufweist. Je umfangreicher die Bearbeitung oder je umfassender der Bearbeitungszweck oder je sensibler die bearbeiteten Daten, umso eher ist ein hohes Risiko anzunehmen. Ein hohes Risiko kann sich aber auch aus der Art der Bearbeitung ergeben, hauptsächlich, wenn neue Technologien oder Mechanismen verwendet werden, und in den meisten Fällen beim Profiling.

Betroffene Datenbearbeitungen sind nicht nur klassische Informatikprojekte, sondern auch andere Projekte und Initiativen, bei welchen personenbezogenen Daten bearbeitet werden wie zum Beispiel die Realisierung einer umfangreichen Videoüberwachung oder die Verwendung von Geräten, die eine Vielzahl von Gesundheitsdaten bearbeiten.

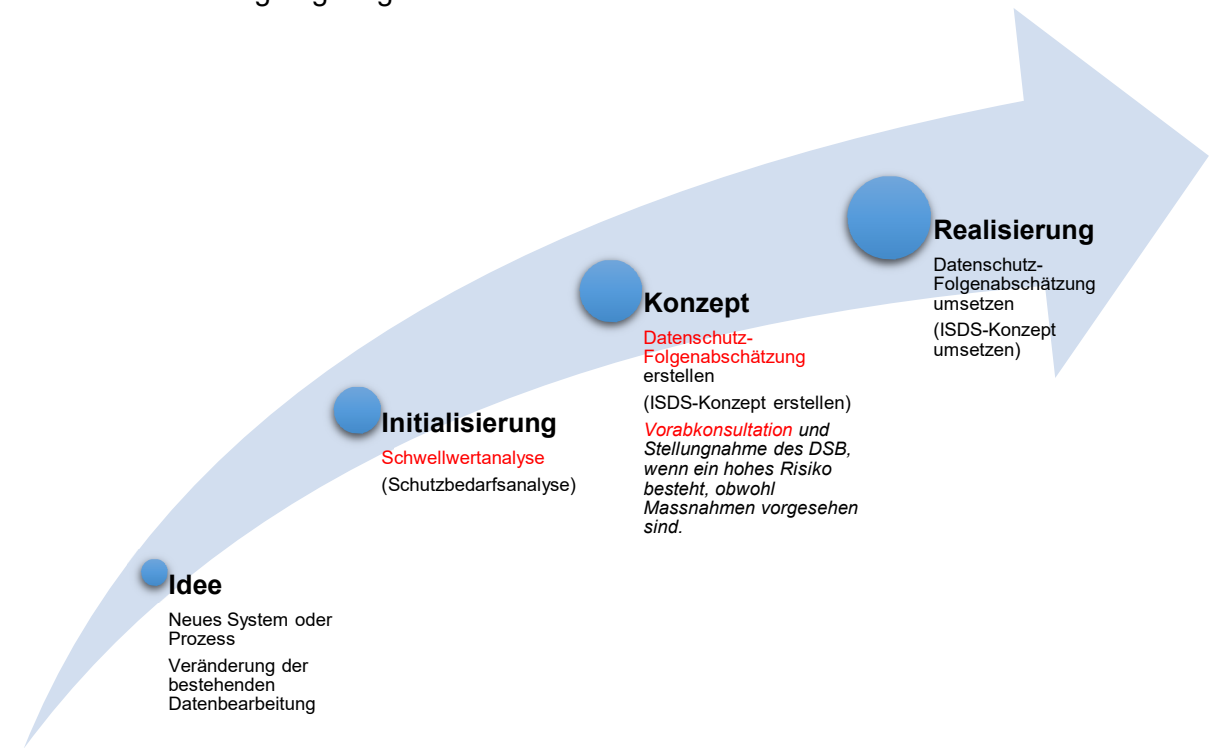
Die Pflicht zur Durchführung der Datenschutz-Folgenabschätzung ist mit der Schwellwertanalyse zu prüfen. Das Formular Schwellwertanalyse kann auf der Website des Datenschutzbeauftragten heruntergeladen werden.[1]

5.2. Zeitpunkt

Es ist zu empfehlen, den Datenschutz schon in der Idee-Phase einer beabsichtigten Bearbeitung zu berücksichtigen. Wenn die Datenschutzanforderungen frühzeitig identifiziert sind, können sie in

[1] Neues Kantonales Datenschutzgesetz - Kanton Luzern: https://datenschutz.lu.ch/themen/Neues_Kantonales_Datenschutzgesetz

der Initialisierungs- und Konzeptphase geplant werden. Im Gegenteil, wenn Datenschutz erst während der Realisierung eines Projekts berücksichtigt ist, kann es zu Verzögerungen und zusätzlichen Kosten und Aufwand führen, zum Beispiel, wenn die geplante Lösung verändert werden muss oder die bereits unterzeichneten Verträge neu verhandelt werden müssen, damit sie den Datenschutzanforderungen genügen.



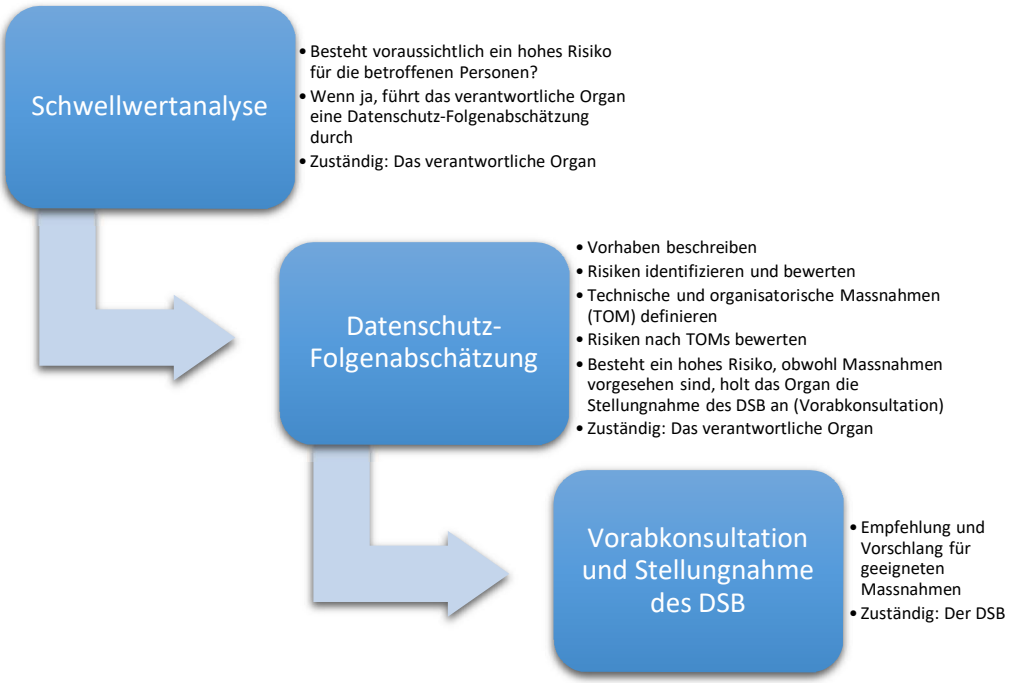
Berücksichtigung des Datenschutzes und der Informationssicherheit über alle Phasen eines Vorhabens[2]

5.3. Inhalt

Das öffentliche Organ ist verpflichtet, eine Prognose darüber zu machen, welche Folgen eine geplante Datenbearbeitung für die Betroffenen aufweist. Die Datenschutz-Folgenabschätzung enthält unter anderem eine allgemeine Beschreibung der geplanten Datenbearbeitung (z. B. Zweck, Bearbeitungsvorgänge und verwendete Technologie, Aufbewahrungsdauer der Daten), eine Bewertung der Risiken sowie eine Darstellung und Bewertung der geplanten Abhilfemassnahmen und anderen Vorkehren und Verfahren, durch die der Schutz der Grundrechte sichergestellt werden soll. Zur Durchführung der Datenschutz-Folgenabschätzung ist das Formular Datenschutz-Folgenabschätzung (Formulare Datenschutz-Folgenabschätzung) zu benutzen.[3]

Die Datenschutz-Folgenabschätzung kann dem Organ der Vorbereitung zum verlangten Nachweis der Einhaltung der Datenschutzvorschriften gemäss § 6 KDSG dienen. Das öffentliche Organ muss gegenüber der Aufsichtsstelle nachweisen können, dass es die Datenschutzbestimmungen bei der Datenbearbeitung einhält. Es ist möglich, mehrere ähnliche Bearbeitungsvorgänge in einer Datenschutz-Folgenabschätzung zu beurteilen.

[2] Schutzbedarfsanalyse und ISDS-Konzept (Informationssicherheits- und Datenschutzkonzept) sind bei Informatikprojekten nach HERMES zu erarbeiten.
[3] Kann hier heruntergeladen werden: https://datenschutz.lu.ch/themen/Neues_Kantonales_Datenschutzgesetz



6. Vorabkonsultation

6.1. Betroffene Datenbearbeitungen

Vorhaben, die eine Bearbeitung von Personendaten beinhalten, unterliegen der Vorabkonsultation durch den Datenschutzbeauftragten. Diese Datenbearbeitung muss zusätzlich mit hohen Risiken für die Persönlichkeits- oder die Grundrechte der betroffenen Personen verbunden sein. Die Pflicht zur Meldung zur Vorabkonsultation ist mit der Datenschutz-Folgenabschätzung zu prüfen (Formulare Datenschutz-Folgenabschätzung und Vorabkonsultation).

6.2. Zeitpunkt

Der oder die Datenschutzbeauftragte ist frühzeitig über eine beabsichtigte Bearbeitung von Personendaten zu informieren oder in ein solches Vorhaben einzubeziehen. Die Information zur Vorabkonsultation kann somit bereits im Stadium der Initialisierungs-, oder Konzeptphase erfolgen. Auf jeden Fall müssen grundlegende Informationen zum Projekt vorhanden sein (siehe unten 6.3). Dieses Vorgehen ermöglicht es dem Datenschutzbeauftragten, den passenden Zeitpunkt für die Vorabkonsultation mit dem verantwortlichen öffentlichen Organ zu vereinbaren.

6.3. Inhalt

Der Datenschutzbeauftragte prüft die rechtlichen, organisatorischen und technischen Rahmenbedingungen der geplanten Datenbearbeitung. Die Empfehlung und der Vorschlag für die geeigneten Massnahmen wird dem öffentlichen Organ innert angemessener Frist zugestellt. Für die Vorabkonsultation reicht das verantwortliche Organ die Datenschutz-Folgenabschätzung und die notwendige Dokumentation für die Beurteilung der rechtlichen, technischen und organisatorischen Massnahmen (siehe Formular Datenschutz-Folgenabschätzung) ein. Die Empfehlung des Datenschutzbeauftragten stellt sicher, dass die Risiken bei Datenbearbeitungsvorhaben rechtzeitig, vollständig und hinreichend abgeklärt sind und gegebenenfalls mit verhältnismässigen rechtlichen, organisatorischen oder technischen Massnahmen weiter reduziert werden können.

6.4. Risikomanagement

Ein zentrales Element der DSFA ist das Risikomanagement, wobei die zu bewertenden Risiken sich auf die Rechte und Freiheiten der von der Bearbeitung betroffenen natürlicher Personen beziehen. Wie bei jedem Risikomanagement geht es auch bei der DSFA darum, die Risiken zu identifizieren, zu bewerten und allenfalls durch geeignete rechtliche, technische und organisatorische Massnahmen zu reduzieren (mitigieren). Daraus ergibt sich, dass für die Durchführung einer DSFA ein interdisziplinär aufgestelltes Team benötigt wird, deren Mitglieder die verschiedenen Aspekte der benötigten Fachkenntnis abdecken können (Datenschutzrecht, IT-Sicherheit, Kenntnis des betroffenen Fachgebietes) und Entscheidungen bezüglich der Umsetzbarkeit von Massnahmen treffen können.
Das Formular DSFA stellt ein einfaches aber effizientes Werkzeug für das notwendige Risikomanagement bereit. Dabei werden in einem ersten Schritt die durch die geplante Bearbeitung entstehenden Risiken für die betroffenen Personen identifiziert und bewertet (Wahrscheinlichkeit des Eintritts und Schadensausmass bzw. Auswirkungen, siehe dazu Anhang 1). Nach dieser Risikobewertung sind die rechtlichen, technischen und organisatorischen Massnahmen zur Risikominimierung darzulegen. Daraus ergeben sich die Restrisiken, wenn die vorgesehenen rechtlichen, technischen und organisatorischen Massanahmen umgesetzt sind. Die Restrisiken werden wiederum bewertet und sofern die Restrisiken erhebliche Auswirkungen haben, obwohl die Massnahmen vorgesehen sind, kann die vorgesehene Datenbearbeitung ein hohes Risiko für die Persönlichkeit und/oder die Grundrechte zur Folge haben. Das verantwortliche Organ muss dann die Stellungnahme des Datenschutzbeauftragten einholen (Vorabkonsultation).

7. Formulare

Anhand des Formulars Schwellwertanalyse kann das verantwortliche Organ evaluieren, ob eine Datenschutz-Folgenabschätzung nötig ist. Ist eine Datenschutz-Folgenabschätzung notwendig, soll dazu das entsprechende Formular verwendet werden.[4] Die Formulare bieten für die meisten Fälle eine Orientierung, können aber nicht sämtliche Aspekte abdecken. Um späteren Aufwand zu verhindern, empfiehlt sich bei Fragen oder Unklarheiten eine frühzeitige Anfrage.

8. Fragen und Informationen

Für Fragen und weitere Informationen steht der Datenschutzbeauftragte gerne zur Verfügung.

Postadresse:	Datenschutzbeauftragter des Kantons Luzern Bahnhofstrasse 15 6002 Luzern
Telefon:	041 228 61 00
Fax:	041 228 69 13
E-Mail:	datenschutz@lu.ch
Internet:	www.datenschutz.lu.ch
Sicherer Dateiaustausch:	https://fxchange.lu.ch

Luzern, August 2021

[4] Kann hier heruntergeladen werden: Neues Kantonales Datenschutzgesetz - Kanton Luzern

Anhang 1 Risikobewertung

Wahrscheinlichkeit des Eintritts

gering	mittel	hoch
Fast unmöglich / nicht vorstellbar (unwahrscheinlicher Eintritt)	Mit gewissem / geringem Aufwand möglich (wahrscheinlicher Eintritt)	Einfach (fast sicherer Eintritt)

Auswirkungen (Schadensausmass, Schadenshöhe)

	Beschreibung der Auswirkungen	**Beispiele**
gering	Kleine Unannehmlichkeiten	Physische Schäden: - Leichte physische Beschwerden oder Krankheit Materielle Schäden und Finanzielle Verluste: - Zeitverlust bei Wiederholung der Formalitäten - Unverlangte E-Mails - Unerwartete Zahlungen (z.B. fehlerhafte Busse) Immaterielle Schäden: - Angst die Kontrolle über die Daten zu verlieren - Leichte psychische Beschwerden (Verleumdung, Reputation)
mittel	Grosse Unannehmlichkeiten oder wesentliche Folgen	Physische Schäden: - Ernsthafte physische Beschwerden oder Krankheit (z.B. Verschlechterung des Gesundheitszustands) Materielle Schäden und Finanzielle Verluste: - Verlust von Möglichkeiten (z.B. Ablehnung der Anstellung oder Studium) - Grosse finanzielle Verluste wegen Identitätsdiebstahls - Sachbeschädigung Immaterielle Schäden: - Verletzung die Grundrechte (z.B. Diskriminierung) - Ernsthafte psychische Beschwerden oder Krankheit (z.B. Depression) - Cyber-Mobbing oder Mobbing
hoch	Irreversible, schwerwiegende Folgen	Physische Schäden: - Langfristige oder permanente physische Beschwerden oder Krankheit, Tod Materielle Schäden und Finanzielle Verluste: - Arbeitsunfähigkeit - Verlust von Beweismaterial in Gerichtsprozess - Existenzbedrohende finanzielle Verluste - Verlust lebenswichtiger Infrastrukturdienste (Wasser, Elektrizität) Immaterielle Schäden: - Langfristige oder permanente psychische Beschwerden oder Krankheit - Verlust der Rechtsautonomie (Vormundschaft)

Risikomatrix

	Auswirkungen: gering	**Auswirkungen:** mittel	**Auswirkungen:** hoch
Wahrscheinlichkeit: hoch			
Wahrscheinlichkeit: mittel			
Wahrscheinlichkeit: gering			

Risiken Farben

Rot	Grosse Risiken deren Auswirkungen kritisch bis katastrophal sind. Diese Risiken müssen unbedingt reduziert werden.
Gelb	Risiken deren Auswirkungen erheblich sind und deshalb reduziert werden müssen.
Grün	Sind Risiken die vernachlässigt werden können. Sollen mit einfachen Massnahmen minimiert werden können.

Anhang 2 Weitere Informationen

Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“ (Der Europäische Datenschutzausschuss (EDSA)): https://edpb.europa.eu/our-work-tools/our-documents/guideline/data-protection-impact-assessments-high-risk-processing_de

Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO (Deutschland): https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf