KANTON
LUZERN

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

Merkblatt Meldung einer Datenschutzverletzung

1. Zweck des Merkblattes

Verantwortliche Organe müssen mit technischen und organisatorischen Massnahmen die Einhaltung des Datenschutzes sicherstellen. Diese Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Rechte der betroffenen Personen mit sich bringt, angemessen sein. Eine der zentralen Komponenten der Datensicherheit ist neben der Fähigkeit, Datenschutzverletzungen soweit möglich zu verhindern, diese möglichst frühzeitig zu erkennen und zügig darauf zu reagieren.

Dieses Merkblatt beinhaltet die wesentlichen Angaben zu Melde- und Informationspflichten bei unbefugter Datenbearbeitung bzw. Datenschutzverletzungen sowie eine kurze Checkliste, mit der öffentliche Organe abklären können, ob sie die unbefugte Datenbearbeitung dem Datenschutzbeauftragten melden müssen.

2. Rechtsgrundlagen

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

3. Definition

Eine Datenschutzverletzung bzw. eine **unbefugte Datenbearbeitung** ist eine Verletzung der Datensicherheit (Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit), die Personendaten betrifft. Das Gesetz nennt dabei insbesondere Verlust, Fälschung, Entwendung und Kenntnisnahme durch nicht berechtigte Dritte als Beispiele unbefugter Datenbearbeitungen, wobei diese Liste nicht als abschliessend zu verstehen ist.
Von der **Meldepflicht** erfasst werden Datenschutzverletzungen, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führen, zum Beispiel, wenn Datenbestände verändert oder offenbart wurden, aber auch wenn sie ungesichert verloren gingen. Das Risiko ist im Einzelfall zu beurteilen.
Überdies besteht eine **Informationspflicht** der betroffenen Personen, anderer Organe oder Dritter, wenn es zum Schutz der betroffenen Personen erforderlich ist oder der Datenschutzbeauftragte es verlangt.

4. Adressat

Unter der Melde- und Informationspflicht stehen Organe, die Personendaten bearbeiten oder bearbeiten lassen und daher für den Datenschutz verantwortlich sind. Organe im Sinne des KDSG sind Behörden, Dienststellen und Verwaltungseinheiten, die für ein Gemeinwesen handeln, sowie private Personen, soweit ihnen öffentliche Aufgaben übertragen sind.

5. Melde- und Informationspflicht der Datenschutzverletzung

5.1. Meldepflicht gegenüber dem Datenschutzbeauftragten

Liegt eine unbefugte Datenbearbeitung vor, also eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für Persönlichkeits- oder Grundrechtsverletzungen führt, hat das verantwortliche Organ unverzüglich dem Datenschutzbeauftragten Meldung zu erstatten. Die unbefugte Datenbearbeitung kann sich in Verlust, Fälschung, Entwendung oder Kenntnisnahme durch nicht berechtigte Dritte manifestieren. In Frage kommen aber sämtliche Arten der Bearbeitung (vgl. § 2 Abs. 4 KDSG).
Ein hohes Risiko gemäss § 7 Abs. 1 KDSG besteht insbesondere, wenn besonders schützenswerte Personendaten oder eine grosse Anzahl von Personen betroffen sind oder wenn der mögliche Schaden für die betroffenen Personen schwerwiegend ist (§ 6b Abs. 2 KDSV). Neben dem Grundrecht auf informationelle Selbstbestimmung (Art. 13 Abs. 2 BV) können Persönlichkeits- oder Grundrechtsverletzungen aus physischem, materiellem oder immateriellem Schaden für natürliche Personen entstehen. Das Risiko ist im Einzelfall zu beurteilen. Möglicherweise hat das verantwortliche Organ jedoch bereits im Rahmen einer im Vorfeld des betreffenden Verarbeitungsvorgangs durchgeführten Datenschutz-Folgenabschätzung (DSFA) eine erste Einschätzung der möglichen Risiken vorgenommen, die eine Datenschutzverletzung mit sich bringen könnte.

Eine Meldepflicht ist beispielsweise anzunehmen, wenn Datenbestände verändert oder offenbart worden oder ungesichert verloren gegangen oder gelöscht worden sind und aus den Umständen dieses Vorgangs eine erhebliche Gefährdung für betroffene Personen eintreten kann. Verletzungen der Datensicherheit können fahrlässig oder missbräuchlich durch einen Mitarbeiter oder eine Mitarbeiterin der Verwaltung, aber auch durch einen Dritten (zum Beispiel Mitarbeiter oder Mitarbeiterin eines Auftragsbearbeiters) erfolgen.

Im Sinn der Risikoorientierung sind jedoch qualitativ und quantitativ unbedeutende Verletzungen der Datensicherheit nicht zu melden, auch solche, die durch nachträgliche Massnahmen vollständig behoben worden sind. So ist zum Beispiel eine kaum heikle, fälschlich zugestellte E-Mail an einen einzelnen Empfänger nicht zu melden, wenn der Empfänger die Löschung der E-Mail bereits bestätigt hat. Im Zweifelsfall sollte der Verantwortliche die Datenschutzverletzung sicherheitshalber melden.

5.2. Informationspflicht der betroffenen Personen

Die verantwortlichen Organe müssen die betroffenen Personen informieren, wenn es zu deren Schutz erforderlich ist oder der Datenschutzbeauftragte es verlangt, und soweit erforderlich auch andere Organe und Dritte. Unter Umständen kann die

Information der betroffenen Personen über eine Verletzung der Datensicherheit angezeigt sein. Auf diese Gefährdungen kann die betroffene Person nur reagieren, wenn sie von der Verletzung des Datenschutzes weiss. Eine betroffene Person kann allenfalls zur Abwehr des Schadens selber Schutzmassnahmen ergreifen indem sie zum Beispiel indem ihre Zugangsdaten oder Passwörter ändert.

Die Information kann eingeschränkt oder aufgeschoben oder es kann darauf verzichtet werden, wenn überwiegende öffentliche Interessen dies erfordern oder wenn die Information einen unverhältnismässigen Aufwand verursacht. Jedenfalls müssen betroffene Personen über Bagatellfälle oder Verletzungen der Datensicherheit, die hinreichend eingedämmt oder beseitigt werden konnten (z.B. die Wiederherstellung unbefugt gelöschter Daten durch ein technisches Back-up), nicht informiert werden. Die Information der Betroffenen kann aber auch trotz erfolgter Meldung an den Datenschutzbeauftragten unterbleiben, etwa zur Wahrung der öffentlichen Sicherheit, insbesondere wenn die Information den Zweck behördlicher Untersuchungen oder Verfahren in Frage stellen würde. Auf die Information ist ausserdem zu verzichten, wenn sie einen unverhältnismässigen Aufwand erfordern würde oder gänzlich unmöglich ist. An die Stelle der persönlichen Information kann unter Umständen eine öffentliche Bekanntgabe treten[1].

6. Inhalt und Zeitpunkt der Meldung

Zur Meldung ist das Formular Meldung der Datenschutzverletzung zu benutzen. Die Meldung soll den Vorfall und seine Auswirkungen so klar wie im Zeitpunkt der Meldung möglich erfassen. § 6b KDSV nennt als Mindestinhalt der Meldung

a. die Art der Verletzung der Datensicherheit,
b. die Kategorie der betroffenen Personendaten und der betroffenen Personen sowie, soweit möglich, die Anzahl der betroffenen Personen,
c. die wahrscheinlichen Auswirkungen für die betroffenen Personen,
d. umgesetzte oder geplante Schutzmassnahmen oder Massnahmen zur Behebung der Folgen der Verletzung der Datensicherheit.

Das verantwortliche Organ soll frühzeitig und unverzüglich, spätestens jedoch nach drei Tagen seit Erkennen dem Datenschutzbeauftragten die Verletzung melden. Das verantwortliche Organ soll die Meldung vornehmen, sobald es von der Datenschutzverletzung Kenntnis genommen und festgestellt hat, dass die Verletzung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen führt. Damit die Massnahmen zum Schutz der Personendaten rechtzeitig ergriffen werden können, sind auch die betroffenen Personen frühzeitig und unverzüglich zu informieren.

Die Meldung kann teilweise erfolgen, wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können. In diesem Fall kann das verantwortliche Organ die Informationen ohne unangemessene weitere Verzögerung schrittweise dem Datenschutzbeauftragte zur Verfügung stellen.

7. Dokumentation

Das öffentliche Organ muss gegenüber der Aufsichtsstelle nachweisen können, dass es die Datenschutzbestimmungen bei der Datenbearbeitung einhält. Dazu gehört

[1] Vgl. § 30 Abs. 1c Gesetz über die Verwaltungsrechtspflege (VRG) vom 3. Juli 1972

auch, dass das Organ alle Datenschutzverletzungen und die damit verbundene Risikobewertung dokumentiert.

8. Checkliste

Anhand der Checkliste kann das verantwortliche Organ evaluieren, ob eine Meldung oder Information erforderlich ist. Die Checkliste deckt nicht sämtliche Aspekte ab, bietet jedoch für die meisten Fälle eine Orientierung. Es existieren bereits diverse Informationen und Leitlinien anderer Organe zum Thema.[2] Um späteren Aufwand zu verhindern, empfiehlt sich bei Fragen oder Unklarheiten eine unmittelbare Anfrage.

Besteht eine Melde- oder Informationspflicht für eine Datenschutzverletzung?

1. Wurde der Schutz personenbezogener Daten bei Entdeckung eines Sicherheitsvorfalls verletzt? *Zum Beispiel*
   - *Personendaten wurden unbefugt verändert*
   - *Personendaten wurden unbefugt offenbart*
   - *Personendaten gingen ungesichert verloren oder sind langfristig unzugänglich*

   Ja weiter zu 2.
   Nein keine Meldungs- oder Informationspflicht

2. Führt die Datenschutzverletzung voraussichtlich zu einem hohen Risiko für Persönlichkeits- oder Grundrechtsverletzungen, beziehungsweise kann aus den Umständen eine erhebliche Gefährdung betroffener Personen eintreten? *Möglicherweise*
   - *Ist die Datenschutzverletzung für die betroffene Person lebensbedrohlich?*
   - *Sind sensible Personendaten (zum Beispiel die Gesundheitsdaten, Ausweisdokumente oder finanzielle Daten wie Kreditkarteninformationen) betroffen?*
   - *Ist eine grosse Anzahl von Personen betroffen?*
   - *Sind schutzbedürftige Personen (zum Beispiel Kinder) betroffen?*
   - *Können die betroffenen Personen leicht identifiziert werden?*
   - *Kann die Datenschutzverletzung zu einem besonders schwerwiegenden potenziellen Schaden für die betroffenen Personen führen (zum Beispiel Identitätsdiebstahl oder -betrug, Verletzungen, psychische Belastungen, Demütigung oder Rufschädigung)?*
   - *Können nicht berechtigte Dritte auf die Personendaten zugreifen?*

   Ja Meldepflicht gegenüber **dem Datenschutzbeauftragten** und weiter zu 3 und 4.
   Nein keine Melde- oder Informationspflicht

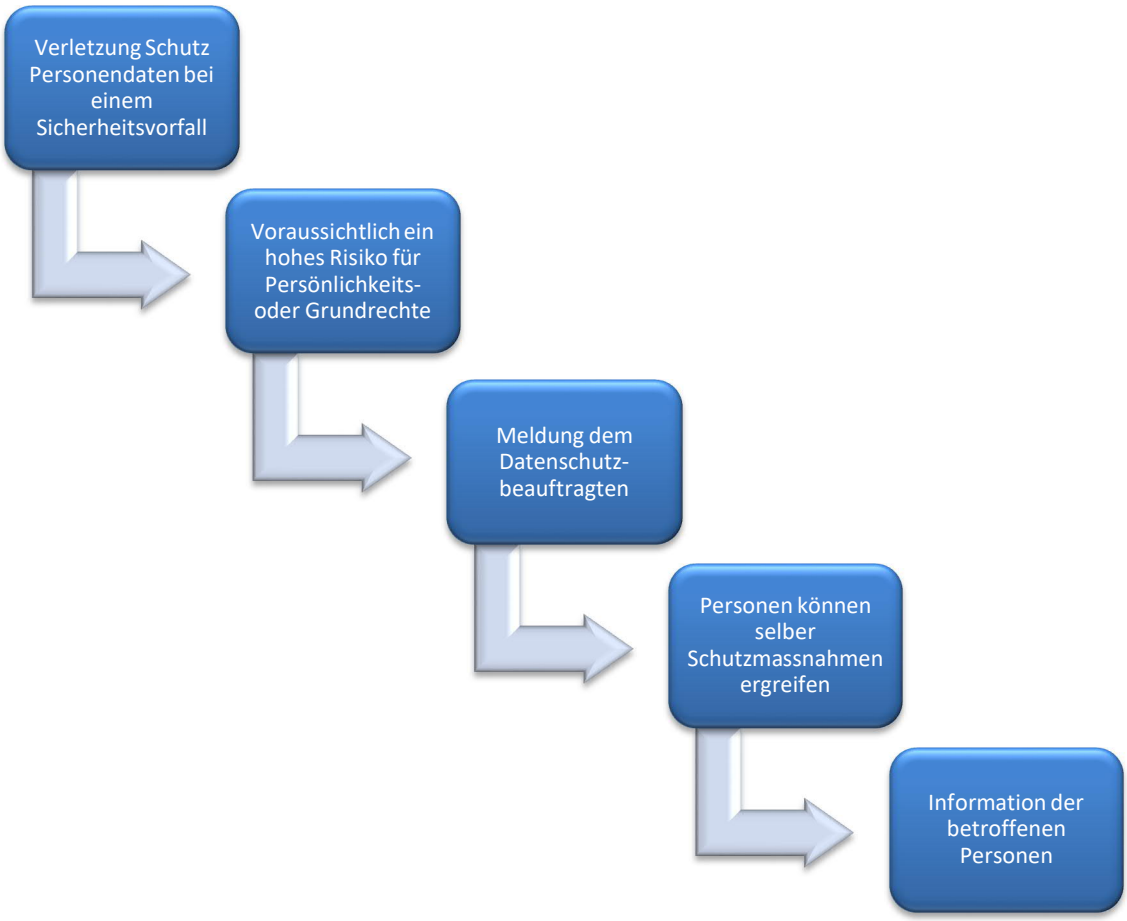
[2] Vgl. vom Europäischen Datenschutzausschuss (EDSA) die Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679.

3. Ist es zum Schutz der betroffenen Personen erforderlich, sie über die Datenschutzverletzung zu informieren? (Insbesondere gegeben, wenn sie selber Schutzmassnahmen ergreifen kann, um den Schaden zu minimieren)

   Ja Informationspflicht an die betroffene/n Person/en.
   Nein keine Informationspflicht

4. Sind andere Organe oder Dritte an der Datenbearbeitung beteiligt?

   Ja Informationspflicht gegenüber den beteiligten Organen oder Dritten
   Nein keine Informationspflicht



9. Fragen und Informationen

Für Fragen und weitere Informationen stehen Ihnen der Datenschutzbeauftragte gerne zur Verfügung.

Postadresse: Datenschutzbeauftragter des Kantons Luzern
Bahnhofstrasse 15
6002 Luzern
Telefon: 041 228 61 00
E-Mail: datenschutz@lu.ch
Internet: www.datenschutz.lu.ch

Luzern, August 2021