

Merkblatt zur Meldung von Verletzungen der Sicherheit von Personendaten und zur Nutzung der Plattform

1. Meldung von Verletzungen der Sicherheit von Personendaten

Gemäss Artikel 30a des Gesetzes über die Information der Öffentlichkeit, den Datenschutz und die Archivierung, geändert am 16.03.2023 und in Kraft getreten am 01.01.2024 (nachfolgend GIDA), muss der Verantwortliche für die Datenbearbeitung dem kantonalen Datenschutz- und Öffentlichkeitsbeauftragten (nachfolgend KDÖB) unverzüglich die Fälle von Verletzungen der Sicherheit von Personendaten melden, die einen schweren Eingriff in die Grundrechte und Grundfreiheiten von Betroffenen darstellen können.

Zu diesem Zweck hat unsere Behörde beschlossen, eine Plattform für die Kommunikation dieser Daten zur Verfügung zu stellen, um deren Sicherheit zu gewährleisten. Die Kommunikation mittels unverschlüsselter E-Mails würde gegen das GIDA verstossen, so dass die Nutzung der Plattform erforderlich ist.

Die Meldung muss zumindest die Art der Verletzung der Sicherheit von Personendaten, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen enthalten.

Darüber hinaus sieht das Gesetz vor, dass der Auftragsbearbeiter dem Verantwortlichen für die Datenbearbeitung unverzüglich jede Verletzung der Sicherheit von Personendaten melden muss.

Ausserdem müssen die betroffene(n) Person(en) unverzüglich informiert werden, wenn dies zu ihrem Schutz erforderlich ist.

Schliesslich hat der Verantwortliche für die Datenbearbeitung die Möglichkeit, die Information an die betroffene Person einzuschränken, aufzuschieben oder darauf zu verzichten, wenn:

- a) ein überwiegendes öffentliches Interesse, insbesondere die innere oder äussere Sicherheit des Staates, dies erfordert oder wenn die Meldung eine Ermittlung, eine Untersuchung oder ein Verwaltungs- oder Gerichtsverfahren gefährden kann;
- b) die Information unmöglich ist oder einen unverhältnismässigen Aufwand erfordert;
- c) die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt werden kann;
- d) dies aufgrund überwiegender Interessen Dritter erforderlich ist.

2. Zugang zur Anwendung

Der Link, um auf die Anwendung zuzugreifen, befindet sich auf der Webseite des KDÖB.

Um die Nutzung dieser Anwendung zu vereinfachen ist für die Meldung einer Verletzung der Datensicherheit keine Anmeldung erforderlich.

3. Hauptfunktionen

Die Plattform erfüllt den Zweck, die Pflicht zur Meldung einer Verletzung der Sicherheit von Personendaten an den KDÖB zu erfüllen. Die Plattform ermöglicht es dem Verantwortlichen für die Datenbearbeitung jedoch nicht, Dritte über die Verletzung der Datensicherheit zu informieren. Es sei darauf hingewiesen, dass parallel zur Meldepflicht an den KDÖB jede Verletzung der Datensicherheit ebenfalls der Polizei gemeldet werden muss, die im Rahmen einer von der Staatsanwaltschaft eingeleiteten Strafuntersuchung tätig werden kann.

4. Auszufüllende Felder

i) Kontaktpersonen

(1) Verantwortlicher für die Datenbearbeitung

In diesen Feldern müssen Sie die Kontaktdaten des Verantwortlichen für die Datenbearbeitung im Sinne von Artikel 3 Absatz 6 GIDA angeben.

Sie müssen ebenfalls angeben, ob weitere Behörden an der Bearbeitung der Daten, die Gegenstand der Sicherheitsverletzung sind, beteiligt sind.

Es muss zudem angegeben werden, ob die Datenbearbeitung externalisiert wurde. Wenn dies der Fall ist, müssen die externen Beauftragten und ihre Kontaktdaten angegeben werden.

(2) Behördentyp

In diesem Feld müssen Sie den Behördentyp angeben, für den Sie eine Verletzung der Datensicherheit melden:

- kantonale Behörden (Legislativer, Exekutive, Judikative);
- Gemeinden;
- Burgergemeinden;
- öffentliche Anstalten und Körperschaften.

(3) Behörde

In diesem Feld müssen Sie die Behörde angeben, für die Sie eine Verletzung melden, d.h. eine staatliche Stelle, die Gemeinde oder die Burgergemeinde, oder wenn Sie eine Anstalt oder Körperschaft des öffentlichen Rechts sind, z.B. eine interkommunale Polizei oder eine interkommunale Betreuungsstelle, oder eine private Gesellschaft, die als Behörde im Sinne von Artikel 3 Absatz 1 Buchstaben b bis e GIDA gilt.

ii) Meldung einer Verletzung

In dieser Rubrik müssen Sie Folgendes angeben:

- das Datum des Beginns der Verletzung oder ob dieses Datum unbekannt ist;
- ob die Verletzung zum Zeitpunkt der Meldung noch andauernd ist;
- ob die Verletzung bei einem Auftragsbearbeiter erfolgte;
- das Datum der Feststellung der Verletzung durch den Verantwortlichen für die Datenbearbeitung oder durch einen Dritten;
- die Risikoeinschätzung (Es müssen nur Verletzungen, die die Rechte und Grundfreiheiten der betroffenen Person ernsthaft beeinträchtigen können, gemeldet werden.);
- das Mittel, mit dem die Verletzung der Datensicherheit entdeckt wurde;
- die Art der Verletzung der Datensicherheit (Dropdown-Listefeld);
- die Anzahl der durch diese Verletzung betroffenen Personen;
- ob andere öffentliche Organe durch diese Verletzung betroffen sind;
- die Beschreibung der betroffenen Datenbearbeitung;
- die Beschreibung dessen, was der Verantwortliche für die Datenbearbeitung zum Zeitpunkt der Meldung vom Vorfall Kenntnis hatte;
- Angaben zu den bereits bekannten Auswirkungen der Datenschutzverletzung;

- Kategorien der betroffenen Daten (Dropdown-Listenfeld);
- Konsequenzen der Verletzung der Datensicherheit für die betroffenen Personen (Dropdown-Listenfeld).

iii) Getroffene oder geplante Massnahmen

In dieser Rubrik müssen Sie Folgendes angeben:

- die Massnahmen, die nach der Feststellung der Verletzung der Sicherheit der Personendaten getroffen wurden;
- Die geplanten Massnahmen, die nach der Feststellung der Verletzung der Datensicherheit getroffen werden müssen;
- die vorgesehene Frist für die Umsetzung der geplanten Massnahmen.

iv) Kommunikation

(1) Kommunikation an die betroffenen Personen

In diesem Feld kann angegeben werden, ob die betroffenen Personen über die Verletzung der Datensicherheit informiert wurden. In einem Freitextfeld können Sie die Gründe für die Meldung oder den Verzicht auf die Meldung an die betroffenen Personen erläutern.

(2) Weitere Informationen oder Anhänge

Ein Freitextfeld ermöglicht es, dem KDÖB weitere Informationen mitzuteilen und Anhänge beizufügen, die von Nutzen sein könnten (z.B. Bericht über den Vorfall, Prüfbericht usw.).

5. Weiterer Austausch

Sobald die Meldung erfolgt ist, wird der KDÖB sie zur Kenntnis nehmen. Er kann diese bestätigen oder ablehnen. In diesem Zusammenhang wird der Verantwortliche für die Datenbearbeitung, der die Verletzung gemeldet hat, eine entsprechende E-Mail erhalten.

Ausserdem kann der KDÖB bei Bedarf telefonisch Kontakt mit dem Verantwortlichen für die Meldung aufnehmen, um das weitere Vorgehen und die zukünftige Übermittlung von Dokumenten zu besprechen. Der KDÖB kann auch telefonisch oder per Post zusätzliche Dokumente anfordern.

Die Meldung der Verletzung wird in keinem Katalog veröffentlicht.