

---

## Melde- und Informationspflicht

---

### Wann spricht man von einer Datenschutzverletzung?

---

Eine Datenschutzverletzung liegt vor, wenn Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet, verändert, Unbefugten offengelegt oder zugänglich gemacht werden. Die Gefahr einer Verletzung geht nicht nur von böswilligen Dritten wie bspw. Hackern aus, sondern auch von Mitarbeitenden, die ihre Kompetenzen missbrauchen oder fahrlässig handeln oder ungenügenden technischen und organisatorischen Sicherheitsmassnahmen.

---

### Meldepflicht innert 72 Stunden

---

Gemäss **DSGVO** müssen solche Meldungen von Verletzungen innert 72 Stunden an die zuständige Datenschutzaufsichtsbehörde gemeldet werden (Art. 33 f. **DSGVO**).

→ Schnell handeln und vorbereitet sein mit allen Unterlagen.

Öffentliche Stellen:

- In der Schweiz: [Eidgenössischer Datenschutz – und Öffentlichkeitsbeauftragter \(EDÖB\)](#)
  - o Informationsstelle Bund: Tel 058 462 43 95 – Herr Jörg
    - «[DataBreach \(admin.ch\)](#)» = Meldestelle  
[www.edoeb.admin.ch/edoeb/de/home/meldeportal/databreach.html](http://www.edoeb.admin.ch/edoeb/de/home/meldeportal/databreach.html)
- EU: [Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit](#)
  - o [Informationen zu der Meldung](#) von Datenschutzverstössen
  - o [Informationen zu der eigentlichen Meldung](#)
    - [Meldung über das Internet](#)

---

### Definition einer Datenschutzverletzung

---

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 berechnigte 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.

---

## Melde- und Informationspflicht

---

### Adressat

Unter der Melde- und Informationspflicht stehen Organe, die Personendaten bearbeiten oder bearbeiten lassen und daher für den Datenschutz verantwortlich sind.

---

### 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 die verantwortliche Person dies dem Datenschutzbeauftragten zu melden. Die unbefugte Datenbearbeitung kann in Verlust, Fälschung, Entwendung oder Kenntnisnahme durch nicht berechnigte Dritte stattfinden.

Ein hohes Risiko 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.

Das Risiko ist im Einzelfall zu beurteilen. Eine Datenschutz-Folgeabschätzung von Gästedaten (FM-DSFA\_KMU\_Tool\_de) einer ersten Einschätzung der möglichen Risiken wurde durchgeführt.

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:innen 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.

---

### Informationspflicht der betroffenen Personen

Der Datenschutzbeauftragte muss die betroffenen Personen informieren, wenn es zu deren Schutz erforderlich ist. Eine betroffene Person kann allenfalls zur Abwehr des Schadens selber Schutzmassnahmen ergreifen indem sie zum Beispiel indem ihre Zugangsdaten oder Passwörter ändert.

Jedenfalls müssen betroffene Personen über Bagatellfälle oder Verletzungen der Datensicherheit, die hinreichend eingedämmt oder beseitigt werden konnten (z.B. die Wiederherstellung unbefugter 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 In-

---

## Melde- und Informationspflicht

formation 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.

---

### Inhalt und Zeitpunkt der Meldung

Die Meldung soll den Vorfall und seine Auswirkungen so klar wie im Zeitpunkt der Meldung möglich erfassen (\*).

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

(\*) Die Meldung muss so schnell mit der Beantwortung der obigen Fragen an den Datenschutzbeauftragten [andrea.durrer@gaiahotel.ch](mailto:andrea.durrer@gaiahotel.ch) plus Whats up gemeldet werden, damit sie die nötigen Sachen weiter veranlassen kann. Die Meldung muss umgehend gemacht werden, damit ....

→ Dies muss innert 72 Stunden erfolgen.

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.

→ Siehe Punkt «Meldepflicht»

---

### Wie kann ich einen Datenschutzverletzung verhindern?

Vorweg: einen 100%igen Schutz wird es nie geben. Aber da eine Datenschutzverletzung in ganz unterschiedlichen Formen auftreten kann, müssen einerseits organisatorische Massnahmen getroffen werden, um eine Verletzung des Schutzes personenbezogener Daten umgehend entdecken zu können. Es sind also organisatorische und technische Massnahmen zu implementieren, die sicherstellen, dass nicht datenschutzkonforme Bearbeitungstätigkeiten oder Datenverluste bemerkt werden.

## Melde- und Informationspflicht

### Kleine 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.

### 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 berechnete Dritte auf die Personendaten zugreifen?*

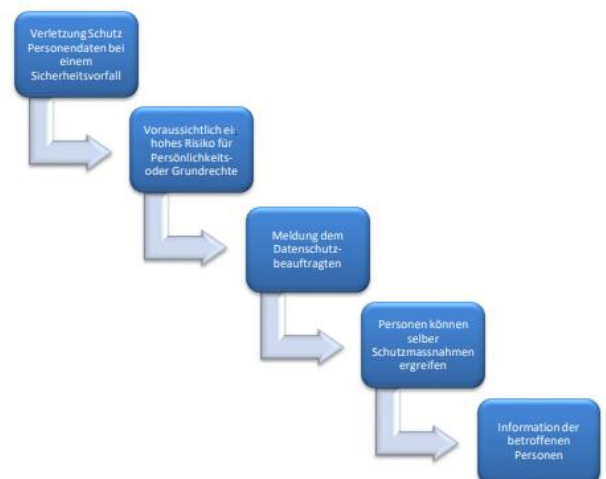
**Ja** Meldepflicht gegenüber dem **Datenschutzbeauftragten** und weiter zu 3 und 4.  
**Nein** keine Melde- oder Informationspflicht

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



Quelle:

<https://datenschutz.lu.ch/>

[/media/Datenschutz/Dokumente/Merkblaetter/neuesKDSG/Merkblatt\\_Meldung\\_einer\\_Datenschutzverletzung\\_V10.pdf?la=de-CH](https://media/Datenschutz/Dokumente/Merkblaetter/neuesKDSG/Merkblatt_Meldung_einer_Datenschutzverletzung_V10.pdf?la=de-CH)