Merkblatt zur Meldung von Datenschutzverletzungen (§ 16a IDG)

Öffentliche Organe müssen Datenschutzverletzungen ab einer bestimmten Risikoschwelle der Datenschutzbeauftragten (DSB) melden. Unter gewissen Voraussetzungen, müssen auch die betroffenen Personen darüber informiert werden.

1 Adressat:innen dieses Merkblatts

Das vorliegende Merkblatt richtet sich – gleich wie die Meldepflicht selbst – an die öffentlichen Organe des Kantons Basel-Stadt, konkret an die dort jeweils für den Datenschutz zuständigen Personen, insbesondere auch an die Datenschutzberater:innen.

2 Meldepflicht

Das Informations- und Datenschutzgesetz des Kantons Basel-Stadt (IDG) enthält in § 16a eine Meldepflicht bei Datenschutzverletzungen:

> ***§ 16a*** *Meldung von Datenschutzverletzungen*
>
> *[1] Das verantwortliche öffentliche Organ meldet der oder dem Datenschutzbeauftragten ohne unangemessene Verzögerung eine Datenschutzverletzung.*
>
> *[2] Die Auftragsdatenbearbeiterin oder der Auftragsdatenbearbeiter informiert das auftraggebende öffentliche Organ unverzüglich über eine Datenschutzverletzung.*
>
> *[3] Eine Datenschutzverletzung liegt vor, wenn durch eine Verletzung der Informationssicherheit bearbeitete Personendaten unwiederbringlich vernichtet werden oder verloren gehen, unbeabsichtigt oder unrechtmässig verändert oder offenbart werden oder Unbefugte Zugang zu solchen Personendaten erhalten.*
>
> *[4] Eine Meldepflicht besteht nicht, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Person führt.*
>
> *[5] Das öffentliche Organ informiert die betroffenen Personen, wenn die Umstände dies erfordern oder der oder die Datenschutzbeauftragte es verlangt.*
>
> *[6] Die Benachrichtigung der betroffenen Personen kann ganz oder teilweise unterbleiben oder aufgeschoben werden, wenn eine Einschränkung gemäss § 29 zulässig ist.*

3 Meldepflichtige Organe

Zur Meldung von Datenschutzverletzungen verpflichtet sind nach § 16a IDG alle öffentlichen Organe des Kantons Basel-Stadt und seiner Gemeinden (§ 3 Abs. 1 IDG), also:

– die Organisationseinheiten der Verwaltung des Kantons und aller seiner Gemeinden (Einwohner-, Bürger- und Kirchgemeinden);

- die Organisationseinheiten der juristischen Personen des kantonalen und kommunalen öffentlichen Rechts, als die öffentlich-rechtlichen Anstalten (wie die Universität, die öffentlichen Spitäler, die IWB, usw.);

- Private, soweit ihnen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist (z.B. die Privatspitäler auf der gemeinsamen Spitalliste der Kantone Basel-Landschaft und Basel-Stadt mit Sitz in Basel-Stadt).
  (Hinweis: Privatspitäler auf der gemeinsamen Spitalliste der Kantone Basel-Landschaft und Basel-Stadt mit Sitz ausserhalb von Basel-Stadt melden Datenschutzvorfälle an die Datenschutzaufsichtsstelle des Sitzkantons.)

Weitere Hinweise:

- Private müssen nach Art. 24 des Bundesgesetzes vom 20. September 2020 über den Datenschutz (DSG, SR 235.1) Verletzungen der Datensicherheit auch an den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten EDÖB melden: https://www.edoeb.admin.ch/de/databreach

- Betreiberinnen von kritischen Infrastrukturen müssen Cyberangriffe künftig innert 24 Stunden nach Entdeckung auch dem Nationalen Cyber Security Center NCSC melden (Art. 74*a* ff. Bundesgesetz über die Informationssicherheit beim Bund, ISG, SR 128). Meldepflichtige Betreiberinnen sind u.a. Hochschulen, Bundes-, Kantons- und Gemeindebehörden sowie interkantonale, kantonale und interkommunale Organisationen, Organisationen mit öffentlich-rechtlichen Aufgaben in den Bereichen Sicherheit und Rettung, Trinkwasserversorgung, Abwasseraufbereitung und Abfallentsorgung, Unternehmen, die in den Bereichen Energieversorgung, Listenspitäler, konzessionierte Transportunternehmen.

Das Formular steht ausschliesslich den meldepflichtigen öffentlichen Organen zur Verfügung, nicht den vom Vorfall betroffenen Privatpersonen. Diese können eine Datenschutzverletzung mit einer aufsichtsrechtlichen Anzeige nach § 28a IDG geltend machen.

4 Meldepflichtige Datenschutzverletzungen

4.1 Risikoschwelle für die Meldepflicht

Meldepflichtig sind Datenschutzverletzungen die ein *bestimmtes Risiko für die Grundrechte der betroffenen Personen* bergen.

Ein solches Risiko liegt insbesondere vor, wenn den betroffenen Personen Folgen im Sinne von Ziff. 6.6 des Meldeformulars drohen: Diskriminierung, Stigmatisierung, Verlust des Arbeitsplatzes, Identitätsdiebstahl oder -betrug, Offenbarung eines Geheimnisses, Lebensgefährdung, unbefugte Aufhebung von Pseudonymisierung, finanzieller Schaden, gesellschaftliche Nachteile, Rufschädigung, wirtschaftliche Nachteile, Existenzgefährdung, Stigmatisierung etc.

Die Meldepflicht entfällt gemäss § 16a Abs. 5 IDG, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Grundrechte der betroffenen Person führt. Aufgrund einer vertieften Analyse der Bestimmung geht die Datenschutzbeauftragte davon aus, dass die Meldepflicht

grundsätzlich immer dann entfällt, wenn die Datenschutzverletzung *voraussichtlich zu keinen oder nur zu geringfügigen Risiken* für die Grundrechte der betroffenen Personen führt.

4.2 Beispiele

Es folgt eine Reihe von Beispielen zur Meldepflicht. Zu beachten ist, dass die Beispiele teilweise vereinfacht sind, um als Richtschnur zu dienen. Sie ersetzen deshalb nicht die konkrete Beurteilung im Einzelfall. Die Datenschutzbeauftragte rät dazu – in Anlehnung an den Ratschlag des Regierungsrates[1] – *im Zweifelsfall* eine Datenschutzverletzung zu melden.

Beispiele für *meldepflichtige* Datenschutzverletzungen:

- Verlust eines *unverschlüsselten* Datenträgers, worauf Personendaten gespeichert sind;
- Verlust eines *verschlüsselten* Datenträgers, worauf Personendaten gespeichert sind, sofern *kein Backup* der Daten besteht;
- Cyber-Angriff, sofern davon auszugehen ist, dass Personendaten Unbefugten zur Kenntnis gelangt sein könnten;
- Vernichtung von Personendaten, sofern keine Backups bestehen.

Beispiele für *nicht meldepflichtige* Datenschutzverletzungen:

- Verlust eines verschlüsselten Datenträgers, worauf Personendaten gespeichert sind, sofern ein Backup besteht;
- Kurzfristiger Unterbruch der Verfügbarkeit eines nicht kritischen Dienstes;
- Vernichtung von Personendaten, sofern diese mittels Backup innert kurzer Zeit wiederhergestellt werden können und aus dem Ausfall keine Nachteile für die betroffenen Personen zu erwarten sind;
- Cyber-Angriff, sofern aufgrund von implementierten Massnahmen davon auszugehen ist, dass kein Eindringen in das geschützte IT-System stattgefunden hat.

5 Frist für die Meldung von Datenschutzverletzungen

Die Meldung hat *so rasch wie möglich* zu erfolgen. «Ohne unangemessene Verzögerung» (§ 16a Abs. 1 IDG) bedeutet in der Regel *spätestens innert 72 Stunden*, nachdem dem verantwortlichen öffentlichen Organ die Verletzung bekannt geworden ist (Ratschlag vom 21. September 2021, S. 33).

[1] Ratschlag vom 21. September 2021, S. 34.

6 Erstmeldung – Folgemeldung

6.1 Erstmeldung

Melden Sie einen neuen Vorfall mit einer Erstmeldung. Geben Sie dabei den *aktuellen Stand der Information* wieder. Bei einem eingeschränkten Vorfall können im Moment der Erstmeldung bereits alle abgefragten Informationen vorliegen.

Füllen Sie das Meldeformular aus und senden Sie es als PDF-Dokument per E-Mail an: datenschutz@dsb.bs.ch oder ausgedruckt an die Postadresse der Datenschutzbeauftragten.

Wenn Sie noch nicht alle abgefragten Informationen vorliegen haben, dann speichern Sie das Formular der Erstmeldung auch als Word-Dokument bei sich ab.

Sie erhalten von der Datenschutzbeauftragten nach der Erstmeldung eine «Data Breach»-Nummer (DB.BS.xxxx.xxx). Bitte geben Sie bei Folgemeldungen an, zu welcher Erstmeldung die Folgemeldung gehört (Meldeformular Ziff. 1).

6.2 Folgemeldung

Bei einem schwereren Vorfall wird es in der Regel noch nicht der Fall sein, dass bei der Erstmeldung alle abgefragten Informationen schon bekannt sind. Dann reichen Sie die später erst vorliegenden Informationen in einer *Folgemeldung* zur entsprechenden Erstmeldung (siehe unten) nach. Nehmen Sie dazu die als Word-Dokument abgespeicherte Erstmeldung und löschen oder überschreiben Sie die nicht mehr aktuellen Informationen.

Kreuzen Sie bei der Art der Meldung «Folgemeldung» an und fügen Sie die «Data Breach»-Nummer ein, die sich von uns nach dem Eingang der Erstmeldung erhalten haben (oben Ziff. 5.1).

Eine erste Folgemeldung sollte spätestens innert eines Monats nach der Erstmeldung eingereicht werden. Bei schwereren Vorfällen ist das weitere Vorgehen gemeinsam mit der Datenschutzbeauftragten festzulegen.

7 Information der betroffenen Personen

7.1 Pflicht zur Benachrichtigung der betroffenen Personen

Gemäss § 16a Abs. 5 IDG hat das verantwortliche öffentliche Organ die betroffenen Personen über die Datenschutzverletzung zu informieren, wenn die Umstände dies erfordern oder die Datenschutzbeauftragte es verlangt.

Eine vertiefte Analyse lässt darauf schliessen, dass die Information der betroffenen Personen immer dann erforderlich ist, wenn sie den Schutz der betroffenen Personen fördert. Dieser Schutz kann insbesondere dadurch gefördert werden, dass die betroffenen Personen *durch die Information befähigt werden, risikominimierende Schutzvorkehrungen zu treffen*. Die Schutzvorkehrungen werden sich oftmals auf die konkrete, vorliegende Datenschutzverletzung beziehen, um die daraus unmittelbar ergehenden Risiken zu senken (z.B. das Ändern von Passwörtern). Allerdings sind

auch weniger unmittelbare, zukunftsorientierte Schutzvorkehrungen denkbar, wie etwa die zukünftige Nutzung eines anderen Kommunikationskanals (z.B. Vermeidung von unverschlüsselten E-Mails), der Wechsel zu einem anderen öffentlichen Dienstleister (sofern überhaupt mehrere Dienstleister vorhanden sind und ein Wechsel rechtlich möglich ist) oder – bei freiwilligen Angeboten (z.B. Umfragen) – der Verzicht auf künftige Teilnahmen.

Sind die betroffenen Personen aufgrund der Umstände in der Lage unmittelbare oder mittelbare Schutzvorkehrungen zu treffen, dann sind sie grundsätzlich so rasch wie möglich zu informieren. Wie auch die Meldepflicht entfällt die Informationspflicht, *sofern das Risiko für die betroffenen Personen bloss geringfügig ist*. Denn in solchen Fällen sind auch das Schutzbedürfnis und Informationsinteresse der betroffenen Personen bescheiden.

Unabhängig von der Informationspflicht gemäss § 16a Abs. 5 IDG kann eine Information der betroffenen Personen aus Transparenzgründen oder zur Vertrauensbildung sinnvoll sein.

7.2 Beispiele

Gleich wie die Beispiele vorne unter Ziff. 4.2 sind die folgenden Beispiele teilweise vereinfacht, um als Richtschnur zu dienen. Sie ersetzen deshalb nicht die konkrete Beurteilung im Einzelfall. Die Datenschutzbeauftragte rät dazu, *im Zweifelsfall* die betroffenen Personen von einer Datenschutzverletzung zu benachrichtigen.

Beispiele für Datenschutzverletzungen bei denen die betroffenen Personen informiert werden müssen:

- Zugangsdaten (z.B. Passwörter[2]) sind (möglicherweise) Unbefugten zur Kenntnis gelangt;
- Informationen über eine bestimmte Person sind Unbefugten zur Kenntnis gelangt und könnten zur Rufschädigung, Erpressung, zum Identitätsmissbrauch o.ä. missbraucht werden;
- Wesentliche Personendaten sind versehentlich gelöscht worden und können nicht wiederhergestellt werden.

Für Beispiele von Datenschutzverletzungen, bei denen die betroffenen Personen *nicht* informiert werden müssen, kann auf die Beispiele, bei denen die Meldepflicht an die Datenschutzbeauftragte entfällt, verwiesen werden (vgl. vorne unter Ziff. 4.2).

8 Zu einzelnen Ziffern im Meldeformular

*8.1 Ziff. 1 des Meldeformulars: Art der Meldung**

Siehe oben Ziff. 5.1 und 5.2.

8.2 Ziff. 2 des Meldeformulars: Um welchen Vorfall handelt es sich?

Geben Sie dem Vorfall einen kurzen, eindeutigen Titel.

[2] Unabhängig davon, ob die Passwörter allenfalls «gehasht» oder «gesalzen» sind.

8.3 Ziff. 3 des Meldeformulars: Verantwortliches öffentliches Organ

Bezeichnung des verantwortlichen öffentlichen Organs, in der Regel die Dienststelle, die Abteilung oder der Bereich.

8.4 Ziff. 4 des Meldeformulars

Name und Kontaktangaben der meldenden Person und, falls diese nicht die Ansprechperson für die Datenschutzbeauftragte ist, der Ansprechperson.

8.5 Ziff. 5 des Meldeformulars: Details zum Data Breach (zur Datenschutzverletzung)

Beschreiben Sie kurz den Vorfall: Was ist passiert, wann ist das passiert und wann ist der Vorfall festgestellt worden? Ist der Vorfall bei einer Auftragsdatenbearbeiterin geschehen? Falls zwischen der Feststellung des Vorfalls und der Erstmeldung mehr als 72 Stunden liegen: Was ist die Begründung dafür?

8.6 Ziff. 6 des Meldeformulars: Schadensausmass

8.6.1 Ziff. 6.1 des Meldeformulars: Anzahl der betroffenen Personen

Geben Sie an, wie viele Personen von dem Vorfall betroffen sind. Falls Sie das im Moment der (Erst- oder Folge-)Meldung noch nicht wissen, kreuzen Sie «noch nicht bekannt» an. Diesfalls ist die Information bei einer (weiteren) Folgemeldung nachzureichen.

Allenfalls gibt es direkt betroffene Personen (z.B. die Mitarbeiter:innen, deren Verzeichnisse an einem Speicherort gehackt worden sind) und indirekt betroffene Personen (die Klient:innen, über die in den gehackten Verzeichnissen Daten gespeichert sind). Sie können dies im Textfeld unterscheiden.

8.6.2 Ziff. 6.2 des Meldeformulars: Anzahl der betroffenen Datensätze mit Personendaten

Geben Sie an, wie viele Datensätze mit Personendaten betroffen sind, wenn z.B. eine Datenbank vom Vorfall betroffen ist.

8.6.3 Ziff. 6.3 des Meldeformulars: Art der betroffenen Daten

Geben Sie an, was für Daten betroffen sind. Kreuzen Sie alle zutreffenden Arten an. Falls Sie das im Moment der (Erst- oder Folge-)Meldung noch nicht wissen, kreuzen Sie «noch nicht bekannt» an. Diesfalls ist die Information bei einer (weiteren) Folgemeldung nachzureichen. Besondere Amtsgeheimnisse sind z.B. das Stimm-, Steuer-, Sozialhilfe-, Sozialversicherungs- oder Opferhilfegeheimnis oder das Geheimnis der grossrätlichen Kommissionen. Die Art der betroffenen Daten hat Auswirkungen auf die möglichen Folgen für die betroffenen Personen (Ziff. 6.6 des Meldeformulars).

8.6.4 Ziff. 6.4 des Meldeformulars: Kategorien der betroffenen Personen

Geben Sie an, welche Kategorien von Personen vom Vorfall betroffen sind. Kreuzen Sie alle zutreffenden Arten an. Falls Sie das im Moment der (Erst- oder Folge-)Meldung noch nicht wissen, kreuzen Sie «noch nicht bekannt» an. Diesfalls ist die Information bei einer (weiteren) Folgemeldung nachzureichen.

8.6.5 Ziff. 6.5 des Meldeformulars: Welche Folgen sind aufgrund der Datenschutzverletzung eingetreten?

Geben Sie an, welches Schutzziel (nach § 8 Abs. 2 IDG) vom Vorfall betroffen ist: Vertraulichkeit (die Informationen sind Unbefugten zur Kenntnis gelangt, weil z.B. eine Datenbank gehackt worden ist, oder weil die Finder:innen eines verlorenen Datenspeichers Zugang zu Informationen bekommen, die ihnen nicht zustehen), Integrität (die Informationen sind durch Unbefugte verändert worden) bzw. Verfügbarkeit (die Informationen sind nicht mehr vorhanden, weil sie z.B. gelöscht oder durch Hacker verschlüsselt worden sind). Kreuzen Sie alle zutreffenden Folgen an. Falls Sie das im Moment der (Erst- oder Folge-)Meldung noch nicht wissen, kreuzen Sie «noch nicht bekannt» an. Diesfalls ist die Information bei einer (weiteren) Folgemeldung nachzureichen.

8.6.6 Ziff. 6.6 des Meldeformulars: Mögliche Folgen für betroffene Personen

Geben Sie an, welche (negativen) Folgen der Vorfall für die betroffenen Personen haben kann. Kreuzen Sie alle zutreffenden möglichen Folgen an . Falls Sie das im Moment der (Erst- oder Folge-)Meldung noch nicht wissen, kreuzen Sie «noch nicht bekannt» an. Diesfalls ist die Information bei einer (weiteren) Folgemeldung nachzureichen.

8.7 Ziff. 7 des Meldeformulars: Einschätzung des Risikos für die betroffenen Personen

Geben Sie an, wie hoch Sie anhand der möglichen Folgen (Ziff. 6.6 des Meldeformulars) das Risiko für die betroffenen Personen einschätzen. Wenn Sie nicht von einem Risiko für die Grundrechte der betroffenen Personen ausgehen, ist keine Meldung notwendig (oben Ziff. 3).

8.8 Ziff. 8 des Meldeformulars: Bereits getroffene Abhilfemassnahmen

8.8.1 Ziff. 8.1 des Meldeformulars: Getroffene Massnahmen

Beschreiben Sie, welche Abhilfemassnahmen bereits getroffen worden sind, um den Vorfall zu beenden, um die Risiken für Ihre Aufgabenerfüllung und für die betroffenen Personen zu vermindern und um eine Wiederholung des Vorfalls zu vermeiden.

Bei einem schwereren Vorfall geht es im Moment der Erstmeldung um die getroffenen Sofortmassnahmen. Die weiteren, längerfristigen Massnahmen sind mit einer Folgemeldung nachzureichen.

8.8.2 Ziff. 8.2 des Meldeformulars: Kontaktierung anderer Stellen

Geben Sie an, welche anderen Stellen Sie schon kontaktiert haben oder noch kontaktieren werden.

Zu weiteren Meldepflichten siehe oben Ziff. 2.

8.8.3 Ziff. 8.3 des Meldeformulars: Information der betroffenen Personen über den Vorfall und die Tatsache, dass sie betroffen sind

Geben Sie an, ob Sie die vom Vorfall (direkt oder indirekt, vgl. oben Ziff. 6.6.1) betroffenen Personen schon informiert haben, noch informieren werden oder, falls nicht, warum Sie dies als nicht nötig erachten.

Denken Sie daran, dass die Information der betroffenen Personen eine vertrauensbildende Massnahme sein kann.

Die Datenschutzbeauftragte kann nach § 16a Abs. 5 IDG verlangen, dass das verantwortliche öffentliche Organ die betroffenen Personen informiert, falls es das nicht schon von sich aus getan hat.

8.8.4 Ziff. 8.4 des Meldeformulars: Proaktive Information über die Medien

Geben Sie an, ob Sie die Öffentlichkeit via die Medien schon informiert haben oder noch informieren werden (inkl. Begründung Ihres Entscheides).

8.8.5 Ziff. 8.5 des Meldeformulars: Data Breach-Notfallplanung

Geben Sie an, ob vor dem Vorfall eine Notfallplanung bestand, die bei der konkret vorgefallenen Datenschutzverletzung hilfreich war, ob eine solche nun geschaffen werden soll oder nicht.

8.9 Ziff. 9 des Meldeformulars: Zusätzliche Informationen an die Datenschutzbeauftragte

Wollen Sie uns sonst noch etwas zum Vorfall mitteilen?