



Bitte leer lassen – wird von der DSB ausgefüllt

Nummer:

DB.BS.

Eingangsdatum:

Per E-Mail an datenschutz@dsb.bs.ch

Meldung einer Datenschutzverletzung (data breach notification)

1 Art der Meldung (Zutreffendes ankreuzen)

Erstmeldung

Folgemeldung zur Erstmeldung

2 Um welchen Vorfall handelt es sich?

3 Verantwortliches öffentliches Organ

Name des verantwortlichen öffentlichen Organs und/oder Dienststelle

Strasse, PLZ Ort

Website

4 Meldende Person bzw. Ansprechperson

Anrede

Herr

Frau

keine Anrede

Name

Vorname

Funktion im verantwortlichen öffentlichen Organ

E-Mail-Adresse

Telefonnummer

Ist diese Person auch die Ansprechperson für die Datenschutzbeauftragte?

ja

nein

Wenn nein: Angaben der Ansprechperson:

Anrede

Herr

Frau

keine Anrede

Name

Vorname

Funktion im verantwortlichen öffentlichen Organ

E-Mail-Adresse

Telefonnummer

5 Details zum Data Breach (zur Datenschutzverletzung)

Was ist genau passiert?

Zeitraum/Zeitpunkt des Vorfalls (möglichst exakte Zeitangabe)

Zeitpunkt der Feststellung des Vorfalls

Ereignete sich der Data Breach bei einer Auftragsdatenbearbeiterin?

ja

nein

Name und Adresse der Auftragsdatenbearbeiterin

Falls zwischen der Feststellung des Vorfalls und der Erstmeldung mehr als 72 Stunden liegen: Was ist die Begründung dafür?

6 Schadensausmass

6.1 Anzahl der betroffenen Personen

Wie viele Personen sind vom Vorfall betroffen?

noch nicht bekannt

ca.

6.2 Anzahl der betroffenen Datensätze mit Personendaten

Wie viele Datensätze sind betroffen? (evtl. Schätzung)

noch nicht bekannt

ca.

6.3 Art der betroffenen Daten (alles, was zutrifft, ankreuzen)

noch nicht bekannt

Angaben über religiöse oder weltanschauliche Ansichten und Tätigkeiten

Angaben über politische oder gewerkschaftliche Ansichten oder Tätigkeiten

Angaben über die Gesundheit

Angaben über das Erbgut (genetische Daten)

Angaben über die persönliche Geheimsphäre

Angaben über die sexuelle Orientierung

Angaben über die ethnische Herkunft

Angaben über Massnahmen der sozialen Hilfe

Angaben über administrative oder strafrechtliche Verfolgungen und Sanktionen

Biometrische Daten: mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen

Resultate eines Profilings: mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, welche die eindeutige Identifizierung dieser Person ermöglichen oder bestätigen (biometrische Daten).

Daten, die einem Berufsgeheimnis unterstehen

Daten, die einem besonderen Amtsgeheimnis unterstehen

Vornamen und Namen

Geburtsdaten

Postadressen

E-Mail-Adressen

AHV-Nummer

Ausweisnummern (Pass, ID)

Kreditkartennummern

Passwörter

Fotos, Videos

Andere Personendaten:

Keine Personendaten → siehe Bemerkung zu Ziff. 7!

6.4 **Kategorien der betroffenen Personen** (alles, was zutrifft, ankreuzen)

noch nicht bekannt

Mitarbeiter:innen

Nutzer:innen

Kund:innen

Patient:innen

Kinder/Minderjährige

andere:

6.5 **Welche Folgen sind aufgrund der Datenschutzverletzung eingetreten?** (alles, was zutrifft, ankreuzen)

noch nicht bekannt

Verlust der Vertraulichkeit der Daten

Verlust der Integrität der Daten

Einschränkung der Verfügbarkeit der Daten

6.6 Mögliche Folgen für betroffene Personen (alles, was zutrifft, ankreuzen)

noch nicht bekannt

Diskriminierung, Stigmatisierung

Verlust des Arbeitsplatzes

Identitätsdiebstahl oder -betrug

Offenbarung eines Geheimnisses

Lebensgefährdung

Unbefugte Aufhebung von Pseudonymisierung

Finanzieller Schaden

Gesellschaftliche Nachteile

Rufschädigung

Wirtschaftliche Nachteile

Existenzgefährdung

Blossstellung

Sonstiges:

7 Einschätzung des Risikos für die betroffenen Personen

Wie hoch schätzen Sie anhand der möglichen Folgen (Ziff. 6.6 des Meldeformulars) das Risiko für die betroffenen Personen ein?

Noch keine Einschätzung möglich

kein Risiko

mittleres Risiko

hohes Risiko

Bemerkung: Wenn Sie nicht von einem Risiko für die Grundrechte der betroffenen Personen ausgehen, ist keine Meldung notwendig.

8 Bereits getroffene Abhilfemassnahmen

8.1 Getroffene Massnahmen

Welche Massnahmen wurden bisher bereits getroffen, um das Risiko für die Grundrechte der betroffenen Personen zu minimieren bzw. mögliche Sicherheitslücken zu schliessen?

8.2 **Kontaktierung anderer Stellen**

Vorgesetzte Stelle

ist bereits erfolgt
Datum:

wird erfolgen
Datum:

ist nicht geplant

IT Ihrer Organisation

ist bereits erfolgt
Datum:

wird erfolgen
Datum:

ist nicht geplant

Polizei, Staatsanwaltschaft

ist bereits erfolgt
Datum:

wird erfolgen
Datum:

ist nicht geplant

Nationales Cyber Security Center

ist bereits erfolgt
Datum:

wird erfolgen
Datum:

ist nicht geplant

Andere:

ist bereits erfolgt
Datum:

wird erfolgen
Datum:

ist nicht geplant

8.3 **Information der betroffenen Personen über den Vorfall und die Tatsache, dass sie betroffen sind**

Persönliche Information der betroffenen Personen

ist bereits erfolgt
Datum:

wird erfolgen
Datum:

ist nicht geplant

Falls nicht geplant: Begründung

8.4 **Proaktive Information über die Medien**

ist bereits erfolgt
Datum:

wird erfolgen
Datum:

ist nicht geplant

Begründung

8.5 Data Breach-Notfallplanung

Bestand für den Fall einer Datenschutzverletzung, wie sie nun geschehen ist, eine Notfallplanung?

ja nein, soll jetzt aber geschaffen werden ist nicht geplant

9 Zusätzliche Informationen an die Datenschutzbeauftragte

Ort, Datum

Unterschrift der meldenden Person:

Beilagen:

-
-
-
-