Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter
EDÖB

Datenschutz

Leitfaden des EDÖB betreffend die Meldung von Datensicherheitsverletzungen und Information der Betroffenen nach Art. 24 DSG

Vom 06. Februar 2025, zuletzt angepasst am 23. April 2025 (Version 1.2)

Versionen

Version 1.0	06.02.2025	Publikation
Version 1.1	26.02.2025	Sprachliche Klärung in Ziffern 1.2 und 1.7
Version 1.2	23.04.2025	Neue Ziffer 1.2 Meldender und sprachliche Klärung in (neu) Ziffer 1.4 Melderecht

Inhalt

Das Datenschutzgesetz (DSG) bezweckt gemäss seinem ersten Artikel den Schutz der Persönlichkeit und der Grundrechte von natürlichen Personen, über die Daten bearbeitet werden. Art. 24 DSG regelt die Pflichten der Verantwortlichen und Rechte der Betroffenen, wenn es bei einer solchen Bearbeitung von Personendaten zu einer Verletzung der Datensicherheit kommt. Nach Art. 5 lit. h DSG ist von einer Datensicherheitsverletzung auszugehen, wenn Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden.

Datensicherheitsverletzungen, die zwar zu schweren Beeinträchtigungen des Geschäfts- und Fabrikationsgeheimnisses, des Amtsgeheimnisses oder des Berufsgeheimnisses führen, aber keine Personendaten betreffen, fallen somit nicht in den Geltungsbereich von Art. 24 DSG. Das gilt in gleicher Weise für Daten, welche sich ausschliesslich auf verstorbene Menschen beziehen und keine persönlichkeitsverletzenden Rückschlüsse auf lebende Personen zulassen, da die Persönlichkeit laut Art. 31 Abs. 1 ZGB mit dem Tod endet.

Der vorliegende Leitfaden des EDÖB behandelt die rechtlichen Voraussetzungen für die Meldung von Datensicherheitsverletzungen an den EDÖB, insbesondere den Begriff des "voraussichtlich hohen Risikos" von Art. 24 Abs. 1 DSG. Er definiert auch die Voraussetzungen für die Information der betroffenen Personen bei einer Verletzung der Datensicherheit nach Art. 24 Abs. 4 DSG.

1 Meldungen von Datensicherheitsverletzungen an den EDÖB

1.1 Gegenstand der Meldung

Gegenstand der Meldung ist eine Schilderung von Tatsachen und Einschätzungen, mit welcher der Verantwortliche gegenüber dem EDÖB die Datensicherheitsverletzung beschreibt, indem er ihn namentlich über Art, Zeitpunkt, Dauer und Umfang der Verletzung und deren bereits bekannte und befürchteten Auswirkungen für die betroffenen Personen informiert. In Art. 15 Abs. 1 der Datenschutzverordnung (DSV) werden die notwendigen Angaben aufgeführt, die es dem EDÖB gegebenenfalls ermöglichen, zu Gunsten der von der Datensicherheitsverletzung Betroffenen nötige Schritte zu unternehmen, indem er z.B. deren Information über den Vorfall anordnet (vgl. Ziff. 2).

1.2 Meldender

Meldungen an den EDÖB (wie auch die Information der Betroffenen) obliegen dem Verantwortlichen. Der Auftragsbearbeiter hat seinerseits die Pflicht, den oder die Verantwortlichen über eine Verletzung der Datensicherheit zu informieren. Diese Informationspflicht ist nicht an eine Risikoabwägung wie in Art. 24 Abs. 1 DSG gebunden; der Auftragsbearbeiter hat den Verantwortlichen über jede Verletzung der Datensicherheit zu informieren, unabhängig davon, ob diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

1.3 Meldepflicht

Nach Art. 24 Abs. 1 DSG muss der Verantwortliche dem EDÖB eine Datensicherheitsverletzung nach Kenntnisnahme so rasch als möglich melden, wenn diese voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Wird für den Verantwortlichen nach der im Zuge der engen zeitlichen Umstände einer Datensicherheitsverletzung durchgeführten Risikoanalyse erkennbar, dass ein derartiges hohes Risiko voraussichtlich besteht und es nicht oder nicht innert kurzer Zeit mit abschliessender Gewissheit bestimmt werden kann (zur Frage des Risikos vgl. Ziff. 1.5), muss er dem EDÖB die Datensicherheitsverletzung mitteilen. Zum Beispiel wird bei Ransomware-Angriffen je nach Umständen in einer ersten Analyse von einem «voraussichtlich hohen Risiko» ausgegangen werden müssen. Der Verantwortliche muss nach dem Gesetz «so rasch als möglich» melden und kann demzufolge in solchen Fällen nicht die Durchführung länger dauernder Abklärungen abwarten, die das voraussichtlich hohe Risiko zweifelsfrei bestätigen oder ausschliessen können.

Die Pflichtmeldung muss sämtliche in Art. 15 Abs. 1 DSV enthaltenen Angaben enthalten, wobei unter den in Abs. 2 genannten Voraussetzungen auch Nachmeldungen zulässig sind (vgl. Ziff. 1.4).

Unterlässt der Verantwortliche diese Meldung, kann der EDÖB nach anderweitiger Kenntnisnahme vom Ereignis die Nachholung der Meldung verfügen (Art. 51 Abs. 3 Bst. f DSG).

Nach Eingang der Meldung prüft der EDÖB summarisch, ob die vom Verantwortlichen getroffenen oder geplanten Sofort- und Folgemassnahmen zum Schutz der Betroffenen und der Minderung von Nachteilen (vgl. Art. 15 Abs. 1 Bst. f DSV) geeignet, ausreichend und zeitlich angemessen erscheinen. Wenn nötig wird ihn der EDÖB vorerst auffordern, die geschilderten Tatsachen und Einschätzungen zu präzisieren und getroffene oder geplante Massnahmen zu ändern oder zu ergänzen. Gegebenenfalls wird der EDÖB mit dem Verantwortlichen auch in Kontakt treten um sicherzustellen, dass der Vorfall z.B. durch Sicherung von Protokolldaten dokumentiert wird. Er prüft zudem, ob betroffene Personen über den Vorfall und dessen Auswirkungen angemessen informiert werden (vgl. Art. 15 Abs. 3 und 4 DSV). Kommt der Verantwortliche den Aufforderungen des EDÖB nicht nach, kann Letzterer eine formelle Untersuchung nach Art. 49 DSG eröffnen und die Aufforderungen mit Massnahmen nach Art. 51 DSG durchsetzen.

Wenn es das öffentliche Interesse angezeigt erscheinen lässt, kann der EDÖB zudem gestützt auf Art. 57 Abs. 2 DSG die Öffentlichkeit über seine Feststellungen und Anordnungen informieren.

1.4 Melderecht

Die Praxis hat gezeigt, dass Verantwortliche dem EDÖB unter Umständen auch Datensicherheitsverletzungen anzeigen wollen, bei denen kein hohes Risiko identifiziert wurde. Der EDÖB nimmt auch solche freiwilligen Meldungen entgegen. Diese erweisen sich gerade in jenen Fällen für alle Beteiligten als sinnvoll und auch unter dem Blickwinkel des öffentlichen Interesses als zielführend, in denen zwar die Risikoanalyse aufgrund der betroffenen Daten ein tiefes Risiko ausweist, aber z. B. aufgrund der grossen Anzahl von betroffenen Personen ein mediales Interesse entstehen kann (vgl. Ziff. 1.5).

Nach summarischer Sichtung der Meldung entscheidet der EDÖB, ob er allfällige Massnahmen zur Information der Betroffenen oder der Öffentlichkeit anordnet bzw. selber ergreift.

1.5 Erstattung von Meldungen

Meldungen sind dem EDÖB so rasch als möglich zu erstatten und so zu formulieren, dass sie den der Datensicherheitsverletzung zugrunde liegenden Sachverhalt und dessen Auswirkungen möglichst vollständig wiedergeben. Ist es dem Verantwortlichen nicht möglich, alle Angaben gleichzeitig zu melden, so liefert er die fehlenden Angaben so rasch als möglich nach (vgl. Art. 15 Abs. 2 DSV).

Für obligatorische Meldungen stellt der EDÖB ein Meldeportal (*www.edoeb.admin.ch* > *Meldeportale* > *DataBreach*) zur Verfügung. Das Meldeportal stellt die gesicherte Übermittlung der Daten an den EDÖB sicher. Dank dem interaktiven Formular ist auch sichergestellt, dass die Meldung die Gesamtheit der in Art. 15 Abs. 1 DSV geforderten Angaben enthält und die Meldepflicht so korrekt erfüllt wird. Zudem stellt das Meldeportal eine Bestätigung über den Zeitpunkt der Meldung aus und erlaubt Folgemeldungen, mit denen die Meldung jederzeit ergänzt werden kann.

Freiwillige Meldungen erfolgen demgegenüber ausserhalb des Meldeportals und rufen, wie oben ausgeführt, keine Handlungen des EDÖB von Amtes wegen hervor.

1.6 Hohes Risiko nach Art. 24 Abs. 1 DSG

Nach Art. 24 Abs. 1 DSG muss der Verantwortliche dem EDÖB eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt, so rasch als möglich melden.

Das DSG verwendet die Begrifflichkeit des «hohen Risikos» sowie des «voraussichtlich hohen Risikos» in einer Vielzahl von Bestimmungen. Bei der Auslegung des «hohen Risikos» gilt es, den unterschiedlichen Zwecken dieser Bestimmungen gebührend Beachtung zu schenken.

Bei der Beurteilung des hohen Risikos nach Art. 24 Abs. 1 DSG sollen die Verantwortlichen erstens klären, in welchem Ausmass die eingetretene Datensicherheitsverletzung bereits zu Beeinträchtigungen

der Persönlichkeit oder Grundrechte natürlicher Personen geführt hat. Zweitens hält sie das in der Norm erwähnte Kriterium der «Voraussichtlichkeit» dazu an, auch die im Zeitpunkt der Beurteilung ihrer Meldeplicht weder abschliessend messbaren, noch sicher voraussagbaren Folgen der Datensicherheitsverletzung für die potenziell Betroffenen in ihre Beurteilung einzubeziehen.

Das voraussichtlich hohe Risiko nach Art. 24 Abs. 1 DSG ist ohne Berücksichtigung von Massnahmen zu identifizieren, die der Verantwortliche erst im Nachgang zur Datensicherheitsverletzung plant, ankündigt oder veranlasst hat. – In der bisherigen Praxis des EDÖB konnten hingegen bei der Beurteilung des Risikos Sofortmassnahmen berücksichtigt werden, die der Verantwortliche noch vor Erstatten der zeitgerechten Meldung treffen konnte und welche die befürchteten Auswirkungen einer potenziellen Persönlichkeitsverletzung nachweislich ausgeschlossen oder gemindert haben. So zum Beispiel, wenn der Verantwortliche durch ergriffene Sofortmassnahmen die Kontrolle über kurzfristig unzugängliche Personendatenbestände rasch wiedererlangt hat und anhand von Protokollen oder anderen Indizien innert Stunden mit hinreichender Wahrscheinlichkeit ausschliessen konnte, dass diese Daten zweckwidrig bearbeitet worden sind. In Situationen des Zweifels, der den Eintritt eines hohen Risikos nicht mit hinreichender Wahrscheinlichkeit ausschliesst, dürfen die Verantwortlichen jedoch nicht zuwarten, ihrer Meldepflicht nachzukommen. So ist eine Meldepflicht z.B. zu erfüllen, bevor der Verantwortliche vor oder nach Bezahlung von Lösegeld im Ungewissen darüber ist, wie wieder erlangte Personendaten von Cyberkriminellen bearbeitet worden sein könnten.

Kriterien für die Beurteilung der Höhe des sich aus der Datensicherheitsverletzung ergebenden voraussichtlichen Risikos sind:

1.6.1 Schwere der Folgen:

Zunächst gilt es, die Schwere der bereits eingetretenen oder befürchteten Beeinträchtigungen der Persönlichkeit oder Grundrechte der von der Datensicherheitsverletzung betroffenen natürlichen Personen abzuschätzen. Dabei ist die Intensität der Beeinträchtigung auf die am schwersten Betroffenen massgebend. Folgende Kriterien können bei der Beurteilung der Folgenschwere in Betracht gezogen werden:

- Schutzwürdigkeit der betroffenen Personendaten: Die Art der von der Datensicherheitsverletzung betroffenen Personendaten ist ein zentraler Aspekt der Prüfung. Je sensibler diese Daten sind, desto höher ist das Risiko, dass Betroffene in ihrer Persönlichkeit oder ihren Grundrechten verletzt werden. Sind besonders schützenswerte Personendaten nach Art. 5 lit. c DSG betroffen, z.B. Gesundheitsdaten, biometrische Daten oder Daten zur Sozialhilfe, ist in vielen Fällen von einem hohen Risiko auszugehen. Aber auch Daten, die nicht in diese Kategorie fallen, können ohne weiteres ein hohes Risiko bedeuten, so zum Beispiel der Verlust von (Kopien von) Identitätsdokumenten oder die Angaben der Kreditkarte. Je nach Kontext, in welchem die von einer Datensicherheitsverletzung betroffenen Personendaten bearbeitet werden, muss somit auch bei nicht besonders schützenswerten Personendaten von einem «voraussichtlich hohen Risiko» ausgegangen werden. So wenn von einer Datensicherheitsverletzung betroffene Kontakt- oder Adressdaten vom Berechtigten zu Zwecken wie der Strafverfolgung oder Massnahmen der sozialen Hilfebearbeitet wurden, bei denen regelmässig besonders schützenswerte Daten i.S.v. Art. 5 Bst. c. DSG anfallen. Waren die betroffenen Personendaten bereits vor der Datensicherheitsverletzung öffentlich zugänglich, ist das Risiko in der Regel nicht als hoch einzustufen.
- Art und Umstände der Verletzung sowie Kreis und Motive der unberechtigten Dritten: Hinsichtlich der Risikobeurteilung kann es einen Unterschied machen, ob ein menschlicher Fehler, eine kriminelle Absicht oder eine technische Störung zu einer Datensicherheitsverletzung geführt haben. Je nach Ursache kann die Einschätzung des Risikos unterschiedlich ausfallen. Werden abhanden gekommene Personendaten indessen z.B. über eine Publikation im Darknet einer breiten Öffentlichkeit zugänglich, führt dies zu einer tendenziell hohen Einschätzung des Risikos, und zwar unabhängig davon, ob die Daten durch einen technischen Störfall oder kriminelles Handeln dorthin gelangten. Ein tieferes Risiko indizieren kann hingegen die auf eine blosse Schädigungsabsicht zurückgeführte Löschung von Personendaten auf dem Server des Verantwortlichen. Ein nicht näher begründetes subjektives Vertrauen der Verantwortlichen in gute Absichten von unbekannten Datenempfängern vermag ein objektiv hohes Risiko indessen nicht auszuschliessen.

- Aufwand für die Bestimmung von Personen: Ein weiterer Indikator für die Risikoeinschätzung ist der Aufwand an Arbeit und Finanzen, der in Kauf genommen werden muss, um unrechtmässig behändigte und allenfalls einer breiten Öffentlichkeit z.B. über das Darknet zugänglich gemachte Informationen so zu bearbeiten, dass Rückschlüsse auf bestimmbare Personen möglich werden. Je einfacher es ist, aus den unrechtmässig erlangten Daten Rückschlüsse auf eine bestimmte Person zu ziehen, desto höher ist das Risiko für diese Person. Kommt bspw. «nur» eine Kundenummer abhanden, ohne dass weitere Daten verfügbar sind, die von der Kundennummer auf die Person schliessen lassen, ist das Risiko geringer, als wenn sprechende E-Mail-Adressen (Vorname.Name@XXXX.com) betroffen sind. Wurden von einer Datensicherheitsverletzung betroffene Personendaten vom Verantwortlichen wirksam verschlüsselt, bleiben sie für alle unlesbar, die den Schlüssel nicht besitzen. Solche Daten gelten damit datenschutzrechtlich für alle nicht zugriffsberechtigten Dritten als anonym, weshalb eine Meldepflicht nach Art. 24 Abs. 1 DSG entfällt. Demgegenüber gelten von einer Datensicherheitsverletzung betroffene Daten, die nur pseudonymisiert wurden, als Personendaten, die gegebenenfalls zu einer Meldepflicht nach dieser Bestimmung führen können.
- Menge und Bearbeitungsdauer: Zur Bestimmung der Intensität können die Menge und Bearbeitungsdauer der von einer Datensicherheitsverletzung betroffenen Informationen in Bezug auf eine gleiche Person ein massgeblicher Faktor sein.
- Ideelle und wirtschaftliche Nachteile: Von schweren Folgen für die einzelnen Betroffenen ist auszugehen, wenn eine Datensicherheitsverletzung Missbräuche wie Identitätsdiebstahl oder Kreditkartenbetrug ermöglicht, die Nachteile wie Rufschädigung, Diskriminierung oder Vermögenseinbussen nach sich ziehen, die bei den Betroffenen persönlichkeitsbeeinträchtigenden Unbill wie Sorgen oder Furchtzustände hervorrufen.
- Vulnerable Personen: Betrifft eine Datensicherheitsverletzung beispielsweise Daten von Minderjährigen oder Menschen mit Behinderungen kann dies ebenfalls schwere Folgen indizieren.
- Gesamtmenge der von der Datensicherheitsverletzung betroffenen Personen und Daten: Eine hohe Anzahl von betroffenen Personen oder grosse Mengen von Personendaten führen für sich alleine nicht zur Bejahung eines hohen Risikos. Bei Datensicherheitsverletzungen mit vielen Betroffenen kann indessen ein öffentliches und privates Interesse an deren Information vorliegen. In der Praxis verhält es sich denn auch so, dass die Verantwortlichen dem EDÖB solche Datensicherheitsverletzungen nicht selten freiwillig melden (vgl. Ziff. 1.3).

1.6.2 Wahrscheinlichkeit befürchteter Folgen:

Nachdem eine Datensicherheitsverletzung eingetreten und vom Verantwortlichen erkannt worden ist, gilt es für ihn, die Wahrscheinlichkeit einzuschätzen, dass noch nicht abschliessend beurteilte oder noch nicht eingetretene Auswirkungen der Datensicherheitsverletzung für die am meisten Betroffenen tatsächlich das befürchtete Beeinträchtigungspotenzial erreichen. Dieses Potenzial wird z.B. bei einem von einer Datensicherheitsverletzung betroffenen Spital, welches nebst administrativen und wissenschaftlichen Sachdaten eine hohe Anzahl besonders schützenswerter Personendaten bearbeitet, höher veranschlagt werden müssen, als z.B. bei einem Lebensmittelverteiler. Demzufolge darf ein betroffenes Spital mit der Meldung der Datensicherheitsverletzung an den EDÖB nicht zuwarten, bis Gewissheit besteht, dass von dieser nicht nur Sachinformationen, sondern auch Daten von Patientinnen und Patienten betroffen sind. Bei der Einschätzung der Eintretenswahrscheinlichkeit auszublenden sind Massnahmen, welche die Verantwortlichen erst nach Eintreten der Datensicherheitsverletzung geplant, angekündigt oder eingeleitet haben. Das bedeutet, dass die Verantwortlichen nicht die Durchführung und Auswertung zukünftiger Massnahmen abwarten dürfen, ehe sie den EDÖB über eine, wegen des hohen Schädigungspotenzials meldepflichtige Datensicherheitsverletzung informieren.

1.7 Meldungen von Datensicherheitsverletzungen an den EDÖB und das Öffentlichkeitsprinzip

Die Tätigkeit des EDÖB als Aufsichtsbehörde des Bundes für Datenschutz untersteht dem Bundesgesetz über das Öffentlichkeitsprinzip in der Verwaltung (Öffentlichkeitsgesetz, BGÖ; SR 152.3). Die Meldungen der Verantwortlichen, in welcher Form sie auch erfolgen mögen, sowie ein allfälliger Austausch zwischen dem EDÖB und dem Verantwortlichen oder seinen Auftragsbearbeitern sind im Grundsatz als amtliche Dokumente im Sinne des BGÖ zu betrachten. Amtliche Dokumente, die beim

EDÖB in Ausübung seiner gesetzlichen Aufgaben bei der Abwicklung von Datensicherheitsverletzungen anfallen, sind somit im Prinzip nach BGÖ für die Öffentlichkeit zugänglich. Dies gilt namentlich für alle Meldungen von Datensicherheitsverletzungen, ungeachtet ob sie unter der Meldepflicht nach Art. 24 Abs. 1 DSG oder freiwillig erfolgt sind. Im Rahmen der Behandlung von Zugangsgesuchen nach BGÖ prüft der EDÖB, ob und inwieweit ein allfälliger Zugang eingeschränkt oder aufgeschoben wird, basierend auf den Ausnahmebestimmungen von Art. 7 ff BGÖ. Im Rahmen des Verfahrens muss der EDÖB gegebenenfalls betroffene Dritte vorab anhören. Er entscheidet über den Zugang mittels Stellungnahme sowie auf Verlangen mittels Verfügung. Ein Schlichtungsverfahren nach Art. 13 f BGÖ wird nicht durchgeführt. (vgl. dazu das Urteil des Bundesverwaltungsgerichts A-4781/2019 vom 17. Juni 2020, E.3).

1.8 Meldepflicht und Sanktionen

Hätte der Verantwortliche den EDÖB nach Art. 24 Abs. 1 DSG über die Datensicherheitsverletzungen informieren müssen, hat dies aber unterlassen, kann der anderweitig in Kenntnis des Ereignisses gelangte EDÖB die Nachholung der Meldepflicht verfügen (Art. 51 Abs. 3 lit. f DSG). Der EDÖB kann im Zusammenhang mit einer Datensicherheitsverletzung auch weitere Verwaltungsmassnahmen aussprechen, z.B. wenn die Vorgaben von Art. 8 DSG nicht eingehalten wurden.

Die gänzliche oder teilweise Missachtung der Meldepflicht an sich ist nach DSG nicht strafbewehrt. Strafrechtlich relevant kann eine Datensicherheitsverletzung aber dann sein, wenn der Verantwortliche z.B. die Mindestanforderungen an die Datensicherheit nicht eingehalten hat (Art. 61 lit. c DSG). Art. 24 Abs. 6 DSG sieht dazu vor, dass Pflichtmeldungen im Strafverfahren ohne das Einverständnis der meldepflichtigen Person nicht verwendet werden dürfen. Dies gilt auch für freiwillige Meldungen (so auch Basler Kommentar Datenschutzgesetz, 4. Auflage [BSK] Art. 24 N 98 mit Verweis auf MÉTILLE/MEYER, in Meier/Métille (Hrsg.), Commentaire romand, Loi fédérale sur la protection des données, Basel 2023, Art. 24 N 35).

2 Information gegenüber den von der Datensicherheitsverletzung Betroffenen

Von der Meldepflicht des Verantwortlichen nach Art. 24 Abs. 1 DSG zu unterscheiden ist dessen Informationspflicht gegenüber der von der Datensicherheitsverletzung betroffenen Personen. Nach Art. 24 Abs. 4 DSG muss der Verantwortliche die betroffenen Personen über die Datensicherheitsverletzung informieren, wenn es zum Schutz dieser Personen erforderlich ist oder der EDÖB es verlangt.

Die Informationspflicht nach Abs. 4 gegenüber den Betroffenen ist unabhängig von Abs. 1 und der dort verwendeten Begrifflichkeit des hohen Risikos auszulegen (vgl. MATHYS/THOMANN, in Vasella/Blechta (Hrsg.), BSK Art. 24 N 63).

Kann der Verantwortliche glaubhaft machen, dass die Betroffenen bereits ohne zusätzliche Information hinreichend über eine Datensicherheitsverletzung und deren Folgen informiert sind und wissen, welche Massnahmen sie ihrerseits treffen können oder müssen, um sich zu schützen, kann die Informationspflicht als erfüllt gelten.

2.1 Pflicht zur Information aufgrund der Schutzbedürftigkeit der Betroffenen

Das in Art. 24 Abs. 4 DSG genannte Schutzbedürfnis für betroffenen Personen ist anzunehmen, wenn diese selber Handlungen vornehmen können oder müssen, um einen Schaden aus einer Datensicherheitsverletzung zu mindern oder abzuwenden. So wenn sie Zugangsdaten oder Passwörter ändern müssen (vgl. Botschaft zum revidierten DSG, BBl 2017 6941 ff., 7065). Das Schutzbedürfnis der Betroffenen kann aber auch in weiteren Fällen bestehen, z.B. wenn Kreditkarten gesperrt, Kontoauszüge oder Nachrichten und Anfragen, sprich Phishing-Mails, kritisch geprüft werden müssen (vgl. MATHYS/THOMANN, BSK, Art. 24 N 67).

Das «voraussichtlich hohe Risiko» nach Abs. 1 von Art. 24 DSG, das die Meldepflicht des Verantwortlichen an den EDÖB auslöst, ist keine rechtliche Voraussetzung für die Begründung einer Informationspflicht der Betroffenen nach Abs. 4 dieser Bestimmung. Eine solche Informationspflicht kann gerade auch dann bestehen, wenn der Verantwortliche ein objektiv hohes Risiko aufgrund seiner Insiderkenntnisse zwar mit vertretbaren Argumenten ausschliessen kann, die potenziell von einer Datensicherheitsverletzung Betroffenen in Unkenntnis der Lage jedoch mit dem Schlimmsten rechnen.

Umgekehrt wird das Vorhandensein eines voraussichtlich hohen Risikos im Sinne von Art. 24 Abs. 1 DSG in der Regel auch eine Informationspflicht nach Abs. 4 dieser Bestimmung indizieren.

2.2 Pflicht zur Information aufgrund einer Anordnung des EDÖB

Der EDÖB kann nach Art. 24 Abs. 4 DSG vom Verantwortlichen die Information der Betroffenen verlangen. Eine solche Aufforderung kann der EDÖB unabhängig davon aussprechen, ob ihm die Verletzung vom Verantwortlichen zuvor freiwillig oder als Pflichtmeldung nach Art. 24 Abs. 1 DSG mitgeteilt oder gar nicht notifiziert worden ist.

Der EDÖB wird vom Verantwortlichen eine Information der Beteiligten verlangen, wenn dies nach seiner Einschätzung die Schutzbedürftigkeit der von der Datensicherheitsverletzung Betroffenen erfordert. Er kann sie darüber hinaus aber auch verlangen, weil nach seinem Dafürhalten wegen der grossen Anzahl von Betroffenen oder einer medialen Berichterstattung ein öffentliches Interesse daran besteht, dass die Verantwortlichen die hohe Anzahl von Betroffenen und damit indirekt auch eine breite Öffentlichkeit in geeigneter Weise mit näheren Informationen zu den Folgen einer Datensicherheitsverletzung versorgen. Ein solches Interesse kann insbesondere gegeben sein, wenn Folgen, welche in einer breiten Öffentlichkeit zu Befürchtungen und Spekulationen Anlass gaben, verhindert oder massgeblich gemindert werden können. Gerade in solchen Fällen entschliessen sich die Verantwortlichen in der Praxis darum nicht selten zu freiwilligen Meldungen an den EDÖB, was dieser begrüsst (vgl. Ziff. 1.3 Melderecht).

Im Prinzip hat der EDÖB in diesen Fällen, gestützt auf Art. 57 Abs. 2 DSG, die Kompetenz, die Öffentlichkeit über seine diesbezüglichen Feststellungen zu informieren, da es sich hier um einen Fall von allgemeinem Interesse handelt. Die eigenständige Information der Betroffenen durch den Verantwortlichen selber ist aber in der Regel zielführender.

2.3 Durchführung der Information

Die Information der Betroffenen hat gemäss Art. 15 Abs. 3 DSV in «einfacher und verständlicher Sprache» zu erfolgen und muss mindestens die folgenden Angaben enthalten: die Art der Verletzung, also was ist passiert; die Folgen der Verletzung einschliesslich der Risiken für die betroffenen Personen, welche Massnahmen getroffen wurden oder vorgesehen sind, um einerseits den Mangel zu beheben und andererseits die Folgen zu mindern. Es muss auch ein Name und die Kontaktdaten einer Ansprechperson genannt werden.

Darüber hinaus gibt es keine Formvorschriften für die Information, und der Verantwortliche hat selber die geeignete Methode zu wählen.

Im Grundsatz werden die Betroffenen direkt und individuell informiert werden müssen. Eine Information durch eine öffentliche Bekanntmachung ist als Ausnahmetatbestand nach Art. 24 Abs. 5 lit. c DSG möglich, wenn die Information der einzelnen Betroffenen dabei in vergleichbarer Weise sichergestellt ist. Die Informationspflicht wird durch die öffentliche Bekanntmachung nicht aufgehoben, sondern nur modifiziert (vgl. CÉLIAN HIRSCH, Le devoir d'informer lors d'une violation de la sécurité des données. Avec un regard particulier sur les données bancaires, Genève 2023, p. 315).

2.4 Informationspflicht und Sanktionen

Hätte der Verantwortliche nach Art. 24 Abs. 4 DSG die Betroffenen infolge deren Schutzbedürftigkeit oder auf Aufforderung des EDÖB hin über eine Datensicherheitsverletzung informieren müssen, kann der EDÖB im Unterlassungs- und Weigerungsfall die Nachholung der Meldepflicht verfügen (Art. 51 Abs. 3 lit. f DSG). Der EDÖB kann im Zusammenhang mit einer Datensicherheitsverletzung auch weitere Verwaltungsmassnahmen aussprechen, z.B. wenn die Vorgaben von Art. 8 DSG nicht eingehalten wurden.