www.jusletter.ch

Ursula Uttinger / Ron Porath

Meldepflichten DSG und ISG

Mit der Revision des Datenschutzgesetzes des Bundes müssen seit 2023 Verletzungen der Datensicherheit an den EDÖB gemeldet werden. Eine solche Meldepflicht kennt man auch in den meisten kantonalen Gesetzen und auf europäischer Ebene. Neu dazugekommen ist dieses Jahr eine weitere Meldepflicht gestützt auf das Informationssicherheitsgesetz – wobei diese nur für bestimmte Branchen gilt. Wie diese Meldepflichten aussehen, wird nachfolgend genauer detailliert beschrieben.

Beitragsart: Wissenschaftliche Beiträge
Rechtsgebiete: Datenschutz

Zitiervorschlag: Ursula Uttinger / Ron Porath, Meldepflichten DSG und ISG, in: Jusletter 29. September 2025

Inhaltsübersicht

1. Gesetzliche Grundlagen

1.1. Datenschutz

[1] Mit der Revision des Bundesgesetzes über den Datenschutz (DSG – SR 235.1) ist eine Meldepflicht bei Verletzungen der Datensicherheit in Art. 24 statuiert worden (1. September 2023). Damit wurde die Anforderung gemäss den Änderungen des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV Nr. 223 – Europäische Datenschutzkonvention 108+)[1] aufgenommen. Gemäss dessen angepasstem Art. 7 Abs. 2 muss jede Vertragspartei sicherstellen, «dass der für die Verarbeitung Verantwortliche Verstösse gegen die Datensicherheit, welche die Rechte und Grundfreiheiten der betroffenen Person erheblich zu beeinträchtigen vermögen, ohne übermässige Verzögerung zumindest der zuständigen Aufsichtsbehörde nach Artikel 12bis meldet.» Die Schweiz hat das Übereinkommen am 7. September 2023 ratifiziert[2] – für das Inkrafttreten braucht es 38 Staaten; aktuell (Aug. 2025) fehlen noch 5 Staaten, damit dieses Übereinkommen in Kraft treten kann[3].

[2] Nebst dem Bundesgesetz über den Datenschutz, welches für private Personen und Bundesorgane gilt (Art. 2 Abs. 1 DSG), gelten für kantonale und kommunale Organe kantonale Datenschutzgesetze. Diese umfassen je nach Kanton nebst dem Datenschutz auch noch Regelungen zum Öffentlichkeitswesen (z.B. BL: IDG – SGS 162, SZ: ÖDSG – SRSZ 140.410), und zusätzlich

1 https://www.coe.int/de/web/conventions/full-list?module=treaty-detail&treatynum=223, Abruf 18. Juli 2025.

2 https://www.edoeb.admin.ch/de/08092023-schweiz-ratifiziert-konvention-108, Abruf 18. Juli 2025.

3 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223, Abruf 18. Juli 2025.

dem Archivwesen (z.B. Aargau: IDAG – SAR 150.700, AR: DIAG – GS 172.800). Die meisten kantonalen Gesetze kennen ebenfalls eine eigene Meldepflicht bei einer Verletzung der Datensicherheit bei den kantonalen Datenschutzbehörden.

[3] Auch die europäische Datenschutzgrundverordnung (DSGVO)[4] kennt in Art. 33 eine Meldepflicht an die Aufsichtsbehörde bei Verletzungen der Datensicherheit, sowie eine Informationspflicht an Betroffene, sofern «voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen » besteht (Art. 34 Abs. 1 DSGVO).

1.2. Informationssicherheitsgesetz

[4] Das Bundesgesetz über die Informationssicherheit (ISG – SR 128) hat per 1. April 2025 ein neues 5. Kapitel erhalten, in welchem es um den Schutz der Schweiz vor Cyberbedrohungen geht. Dies führte dazu, dass die Meldepflichten, bei einer Verletzung der Datensicherheit (Art. 24 DSG) um einen Absatz 5bis erweitert wurde: «Der EDÖB kann die Meldung mit dem Einverständnis des Verantwortlichen zur Analyse des Vorfalls an das Bundesamt für Cybersicherheit weiterleiten. Die Mitteilung kann Personendaten enthalten, einschliesslich besonders schützenswerter Personendaten über verwaltungs- und strafrechtliche Verfolgungen oder Sanktionen betreffend den Verantwortlichen.»

[5] In der Botschaft zur Revision des ISG steht in Bezug auf diese Anpassung des DSG, dass sich die Weiterleitung auf Daten beschränken soll, die für das Nationale Zentrum für Cybersicherheit (NCSC), welches seit dem 1. Januar 2024 Bundesamt für Cybersicherheit (BACS) heisst[5], relevant sei.[6] Dabei ist das Einverständnis der Meldenden zur Weiterleitung notwendig. Der Informationsaustausch ist einseitig – das BACS liefert keine Informationen.

[6] Mit dem revidierten ISG ist die Meldepflicht seit dem 1. April 2025 stark ausgeweitet worden: Die Liste der meldepflichtigen Behörden und Organisationen ist in Art. 74b ISG in den Buchstaben a–u als Liste zu finden: Angefangen bei Hochschulen (Bst. a), über Bundes-, Kantons- und Gemeindebehörden (Bst. b), Gesundheitseinrichtungen (Bst. f), Schweizer Radio- und Fernsehgesellschaften (Bst. j), Post (Bst. l), Eisenbahn (Bst. m) bis zu Anbieterinnen und Betreiberinnen von Diensten und Infrastrukturen, die der Ausübung der politischen Rechte dienen (Bst. s) (Aufzählung hier nur beispielhaft).

[7] Daneben gibt es für einzelne Branchen noch weitere Meldepflichten, beispielsweise:

[8] Meldepflicht für alle Bereiche des Finanzwesens, insbesondere Banken und Versicherungen an die FINMA – gemäss dem FINMA Rundschreiben 2023/1[7] sind Cybervorfälle unverzüglich zu melden bzw. eine Erstmeldung hat innert 24 Stunden und eine komplette Meldung gemäss

4 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (= DSGVO).

5 Vgl. https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/Startbundesamt2024.html, Abruf 18. Juli 2025.

6 BBl 2023, 84.

7 https://www.finma.ch/de/~/media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma-rs-2023-01-20221207.pdf, Abruf 1. September 2025.

Anforderungskatalog innert 72 Stunden zu erfolgen. Die Meldepflichten bei der FINMA gehen den beruflichen Schweigepflichten vor.[8]

[9] Gemeinschaften des elektronischen Patientendossiers (EPD) haben gegenüber dem Bundesamt für Gesundheit (BAG) eine Meldepflicht bezüglich datenschutz- und datensicherheitsrelevanter Vorfälle (Art. 12 Abs. 3 EPDV – SR 816.11).

[10] Meldung von Vorkommnissen, die eine Bedeutung für die nukleare Sicherheit haben – dies kann auch ein Cybervorfall sein[9] – beim eidgenössischen Nuklearsicherheitsinspektorat (ENSI).[10]

2. Datensicherheit und Verletzung Datensicherheit

[11] Bevor auf die Folgen einer Verletzung der Datensicherheit eingegangen wird, sollten die Begriffe im Kontext der Historie herausgearbeitet werden.

2.1. Begriffsklärung: IT-Sicherheit und Datensicherheit[11]

[12] IT-Sicherheit umfasst alle technischen und organisatorischen Massnahmen, die darauf abzielen, IT-Systeme und deren Dienste vor Vertraulichkeitsverletzungen, Manipulationen oder Störungen der Verfügbarkeit zu schützen. Das Ziel ist, wirtschaftliche, behördliche oder persönliche Schäden zu vermeiden. Sie wird oft als Zustand verstanden, in dem die IT-Infrastruktur exakt den vorgesehenen Zweck erfüllt und nicht für unerwünschte Zwecke missbraucht wird.

[13] Datensicherheit bezieht sich auf den Schutz von Daten jeglicher Art, vor Verlust, Manipulation und unbefugtem Zugriff, unabhängig davon, ob sie personenbezogen sind. Sie ist eine technische Voraussetzung für Datenschutz. Für die Betrachtung einer Verletzung der Datensicherheit[12] ist es unerheblich, ob diese absichtlich oder widerrechtlich erfolgt ist. Ebenso spielt es keine Rolle, ob sie durch eigene Handlungen, durch Dritte oder durch Mitarbeitende verursacht wurde.

2.2. Historische Entwicklung der Datensicherheit

[14] Die Notwendigkeit und Dringlichkeit für IT-Sicherheit und Datensicherheit wurde in den letzten Jahrzehnten aufgrund exponentiell zunehmender Datenmengen sowie zahlreicher Berichte über Hackerangriffe offensichtlicher.

[15] In den Anfangsjahren der IT bis in die 1980er Jahre wurden Benutzername und Passwort hauptsächlich von Behörden und Forschungseinrichtungen zur Anmeldung und Authentifizie-

8 Reto Ferrari-Visca/Thomas Nagel, Die Meldepflicht nach Art. 29 Abs. 2 FINMAG, 299 ff. in Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktaufsicht, 2024.

9 https://ensi.admin.ch/de/2020/02/21/nukleare-sicherung-schweiz-will-cybersicherheit-staerken/, Abruf 2. August 2025.

10 BBl 2023, 84, Botschaft zur Änderung des Informationssicherheitsgesetzes (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen), 19.

11 Claudia Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle, Berlin, München, Boston: De Gruyter Oldenbourg, 2014. 9. Auflage.

12 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6941, 7064.

rung verwendet. Verschlüsselungstechnologien waren aufgrund begrenzter Rechenleistung nur vereinzelt einsetzbar, und einfache Passwörter mit vier bis sechs Zeichen galten als ausreichend. Mit dem Aufkommen der nötigen Rechenleistung und Verfahren für die Verschlüsselung im Internet in den 2000er Jahren begann sich die Datensicherheit zu verbessern. Dennoch blieben viele private PCs und Mobilgeräte weiterhin ungeschützt. Fehlende Zugriffskontrollen in Firmen führten dazu, dass sensible Firmendaten entwendet und verkauft werden konnten, beispielsweise auch Steuerdaten von Bankkundinnen und -kunden.[13]

2.3. Technologische Fortschritte und organisatorische Massnahmen

[16] Um das Jahr 2010 verschärften sich die Anforderungen an sichere Passwörter und Unternehmen führten das Need-to-Know-Prinzip sowie umfassende Zugriffskontrollen ein, um sich gegen Cyberangriffe und Erpressungsversuche zu schützen.[14] Heute verfügen grosse Unternehmen und die meisten Behörden über gut ausgebaute Infrastrukturen, spezialisierte Softwarelösungen und Cloud-Dienste zur Gewährleistung der Datensicherheit. Dennoch bleiben menschliche Fehler ein grosses Risiko für die Datensicherheit.

[17] Privatpersonen und KMU hingegen haben auch aktuell oft noch nicht die Ressourcen oder das Wissen, um sich kontinuierlich um Datensicherheit zu kümmern. Sie sind daher zunehmend auf die Unterstützung durch grosse Konzerne angewiesen, die solche Angebote seit den 2020er Jahren vermehrt bereitstellen. Diese setzen dazu auch künstliche Intelligenz ein, welche die Erkennung von Angriffen in Echtzeit ermöglicht.

2.4. Definition und Klassifikation von Datensicherheitsvorfällen

[18] Ein «Datensicherheitsvorfall» (engl. security incident) folgt einem «Datensicherheitsereignis» (security event), welches bis zur Bewertung und Einschätzung der Kritikalität (criticality) neutral ist.[15] Ein «Datensicherheitsereignis» kann somit auch aufgrund einer autorisierten Nutzung der IT entstehen, welches dann nicht zu einem «Datensicherheitsvorfall» führt. Ein solcher Fall kann beispielsweise das Vertippen eines Passworts sein.

[19] Der Begriff «Datensicherheitsvorfall» ist ein Oberbegriff für unterschiedliche Szenarien, bei denen Daten unabsichtlich oder absichtlich entwendet, verändert, unbrauchbar gemacht oder Unbefugten zugänglich gemacht wurden und damit ein Verstoss gegen Sicherheitsrichtlinien (security policies) darstellen. Dabei wird mindestens eines der drei Hauptziele der Informationssicherheit (auch Schutzziele genannt[16]) – Vertraulichkeit, Verfügbarkeit und Integrität – beeinträchtigt oder diese können nicht mehr eingehalten werden.[17] Die Daten sind einerseits nicht mehr am vorgesehenen Ort für die berechtigten Personen zugänglich und andererseits möglicherweise anderen unbefugten Personen zugänglich.

---

13 https://www1.wdr.de/archiv/jahresrueckblick/steuercd342.html, Abruf 22. Juli 2025.

14 https://lehrerfortbildung-bw.de/st_recht/daten/ds_neu/technik/passwort/, Abruf 22. Juli 2025.

15 E. von Faber, IT und IT-Sicherheit in Begriffen und Zusammenhängen, Springer Vieweg Edition <kes>, 31.

16 Holger Kaschner, Cyber Crisis Management, 221, Springer Vieweg, Wiesbaden 2020.

17 Heinrich Kersten, Gerhard Klett, Business Continuity und IT-Notfallmanagement, 135, Springer Vieweg, Wiesbaden 2017.

[20] Ein Datensicherheitsvorfall ist dabei nicht auf personenbezogene Daten beschränkt, sondern berücksichtigt alle Daten, insb. auch Daten, welche nur für die betroffene Firma relevant sind wie beispielsweise geistiges Eigentum. Erst ab 2016 (DSGVO) und 2023 (DSG) wurde der Begriff der «Verletzung der Datensicherheit» für personenbezogene Daten in die Datenschutzgesetze aufgenommen.[18]

2.5. Ursachen von Datensicherheitsvorfällen

[21] Wenn Datensicherheitsvorfälle absichtlich herbeigeführt wurden, sind meist externe Akteure oder interne Mitarbeiter respektive Dienstleister involviert, welche neue oder noch nicht behobene Schwachstellen (vulnerabilities) ausnutzten. Die Methoden der absichtlichen Herbeiführung von Datensicherheitsvorfällen können vom einfachen Ausspähen von Passwörtern bis hin zu umfangreichen, mehrjährigen Vorbereitungen zur Infiltration von Software oder Personen reichen oder zum Zusammenbruch von IT-Systemen durch Überlastung führen. Dabei kann das Ziel sein, lediglich eine bestimmte Datei zu entwenden oder zu verändern, beispielsweise eine Lohnliste, oder sogar ein ganzes IT-Netzwerk zu kompromittieren, um Terabytes an Daten zu entwenden. Beispiele sind die von internen Bankmitarbeitern verkauften Bankdaten an ausländische Behörden[19] und die umfangreichen Datenlecks grosser Social Media Anbieter durch schwach geschützte Datenbanken[20], die im Internet zugänglich waren.

2.6. Schutzmassnahmen gegen Datensicherheitsvorfälle

[22] Gegen Datensicherheitsvorfälle durch Eingriffe von aussen, die über Malware, Phishing oder durch Ausnutzung von Schwachstellen oder schwach geschützten Servern und Datenbanken[21] vollzogen werden, helfen starke Passwörter, der flächendeckende Einsatz von 2FA und VPN, die Verschlüsselung von Daten und Backups sowie der Einsatz von Firewalls, Netzwerksegmentierung und Awareness-Kampagnen.[22]

[23] Datensicherheitsvorfälle durch interne Mitarbeiter oder Dienstleister entstehen meist durch erlaubten Zugriff auf unverschlüsselte Daten und können vor allem durch den Einsatz von Data Leakage Prevention[23], Firewalls, BackUps und Zero Trust[24], also dem Einfordern von Authentifizierung für jeden Zugang zu Daten und Systemen verhindert werden. Ausserdem sollte das Least-Privilege-Prinzip[25], auch bekannt als Need-to-Know-Prinzip, sicherstellen, dass jeder Benutzer nur Zugang zu für ihn relevanten Daten und Systemen erhält.

---

18 Célian Hirsch, Die Informationspflicht von Revisoren und Treuhändern bei einer Verletzung der Datensicherheit, in: TREX 2025, 169.

19 Z.B. https://www1.wdr.de/archiv/jahresrueckblick/steuercd342.html, Abruf 22. Juli 2025.

20 https://www.kaspersky.de/blog/top-five-data-breaches-in-history/31619/, Abruf 22. Juli 2025.

21 Ron Porath, Internet, Cyber- und IT-Sicherheit von A-Z, 289, Springer Vieweg, Wiesbaden 2020.

22 https://www.kaspersky.de/blog/top-five-data-breaches-in-history/31619/, Abruf 22. Juli 2025.

23 https://www.dataguard.de/blog/wie-sie-ihre-daten-im-unternehmen-effektiv-schuetzen, Abruf 22. Juli 2025.

24 https://www.microsoft.com/de-at/security/business/security-101/what-is-a-data-breach, Abruf 22. Juli 2025.

25 https://www.dataguard.de/blog/zero-trust-architektur-als-cybersicherheitsmassnahme, Abruf 22. Juli 2025.

2.7. Konsequenzen von Datensicherheitsvorfällen

[24] Die Konsequenzen von Datensicherheitsvorfällen können einerseits für die betroffene Firma Reputationsschäden, finanzielle Schäden und existenzbedrohende Schäden durch Verlust von geistigem Eigentum mit sich bringen, andererseits für betroffene Personen das Risiko von Identitätsmissbrauch, finanziellem Verlust oder auch weiteren personalisierten Phishing-Angriffen. Deswegen verlangen, wie in diesem Artikel beschrieben, diverse Gesetze als Reaktion die Meldung bestimmter Datensicherheitsvorfälle sowie Massnahmen, um die Ausbreitung und Auswirkungen von Datensicherheitsvorfällen zu minimieren und zu stoppen. Das BACS nimmt Meldungen zu Datensicherheitsvorfällen und allgemein zu Cybervorfällen und -bedrohungen entgegen und analysiert diese zum Schutz der Schweiz (Art. 74a Abs. 4 ISG). Gefundene Schwachstellen werden den Herstellern der Software oder Infrastruktur mit der Auflage gemeldet, diese innert Frist zu beheben.

3. Meldepflichten

3.1. Meldepflicht nach DSG

[25] Eine Meldepflicht nach DSG bedingt, dass Personendaten bearbeitet werden und das Datenschutzgesetz anwendbar ist. Werden anonymisierte Daten bearbeitet, ist das Datenschutzgesetz nicht anwendbar. Denn bei anonymisierten Daten handelt es sich nicht mehr um Personendaten.[26] Auch wenn Personendaten durch eine natürliche Person ausschliesslich zum persönlichen Gebrauch bearbeitet werden, ist das DSG nicht anwendbar (Art. 2 Abs. 2 lit. a DSG) und bedarf folglich keiner Meldung.

3.1.1. Hohes Risiko

[26] Kommt es zu einer Verletzung der Datensicherheit, muss diese gemeldet werden, sofern diese «voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt» (Art. 24 Abs. 1 DSG); in der Folge muss das betroffene Unternehmen bzw. die Bundesstelle eine erste Risikoabwägung machen. Eine Verletzung der Datensicherheit ist schnell gegeben, eine Meldepflicht besteht jedoch nur bei einem hohen Risiko; es soll verhindert werden, dass unbedeutende Verletzungen gemeldet werden.[27] Der Gesetzgeber folgt einem risikobasierten Ansatz.[28]

[27] Die Risikoabwägung – ähnlich auch bei einer Datenschutz-Folgenabschätzung (= DSFA, vgl. Art. 22 DSG) – ist nicht komplett objektiv, sondern beinhaltet eine subjektive Note.[29] Zu beachten ist, dass das Risiko im Zusammenhang mit einer DSFA nicht das gleiche Risiko ist wie bei einer Verletzung der Datensicherheit. Im Rahmen der Meldepflicht muss das Risiko im Zeitpunkt der Feststellung der Datensicherheitsverletzung beurteilt werden, wobei dies oft auch

26 Vgl. Keine Anwendung auf anonymisierte Daten – Erwägungsgrund 26 – DSGVO.

27 BBl 2017, 7064.

28 Adrian Bieri/Julian Powell, Kommentar zum Schweizerischen Datenschutzgesetz und weiteren Erlassen (OFK), Art, 24 N3 ff., Zürich 2023.

29 Ursula Uttinger/Thomas Geiser, Das neue Datenschutzrecht, Rz. 337 ff., Basel 2023.

nicht abschliessend geschehen kann, aufgrund noch fehlender Details. Gemäss Praxis des eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) dürfen bereits getroffene Sofortmassnahmen berücksichtigt werden. Im Zweifel sollte jedoch eine Meldung an den EDÖB erfolgen.[30]

[28] Bezüglich Risiko-Einschätzung sind grundsätzlich Eintrittswahrscheinlichkeit und Auswirkung zu berücksichtigen. Bei einer Verletzung der Datensicherheit ist das Ereignis bereits eingetreten, so dass nur noch die Auswirkungen im Fokus stehen. Sowohl im Leitfaden des EDÖB als auch in der Leitlinie des Europäischen Datenschutzausschusses[31] gibt es dazu einige Hinweise, wie die Risikobewertung vorgenommen werden kann.

[29] Bezüglich der Schwere der Folgen sind unter anderem folgende Elemente relevant:

- Schutzwürdigkeit der betroffenen Personendaten: Gesundheitsdaten sind sensibler als Adressdaten; aber nicht nur die besonders schützenswerten Daten gemäss Art. 5 Bst. c DSG, auch beispielsweise die Kopie von Identitätsdokumenten oder Kreditkarten können zu einem hohen Risiko führen;
- Art und Umstände sowie Motiv: Ein menschlicher Fehler dürfte weniger heikel sein, als wenn die Verletzung mit einer kriminellen Absicht begangen wurde;
- Identifizierbarkeit der betroffenen Person: Zu berücksichtigen ist, wie einfach die betroffenen Personen zu identifizieren sind;
- Schwere der Folgen für betroffene Personen: Kann die Verletzung der Datensicherheit zu einem Identitätsdiebstahl, zu Rufschädigung oder Demütigung führen?
- Besondere Eigenschaften der betroffenen Personen: Kinder, schutzbedürftige Personen oder auch Personen mit einem grösseren Bekanntheitsgrad können von einer Verletzung der Datensicherheit stärker betroffen sein;
- Menge und Bearbeitungsdauer: je mehr Daten über einzelne Person betroffen sind und je länger der Zeitraum dieser Bearbeitung ist, desto grösser wird auch das Risiko, dass dies für die betroffene Person weitergehende Auswirkungen hat.[32,33]

[30] Auch die Wahrscheinlichkeit des Eintritts von Folgen ist zu beurteilen, dabei kann man sich an der allgemeinen Lebenserfahrung und dem gewöhnlichen Lauf der Dinge orientieren: Je vertraulicher die Daten sind, umso höher ist die Wahrscheinlichkeit, dass diese auch missbraucht werden.

3.1.2. Keine Meldepflicht des Auftragsbearbeiters

[31] Wichtig ist in diesem Zusammenhang, dass Auftragnehmer keine Meldepflicht haben; selbst, wenn sie glauben, dass es sinnvoll wäre, dies zu melden, ist der verantwortliche Auftraggeber

30 Leitfaden des EDÖB betreffend die Meldung von Datensicherheitsverletzungen und Information der Betroffenen nach Art. 24 DSG vom 6. Februar 2024, S. 4, Version 1.2.

31 Leitlinie 09/22 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäss DSGVO, des Europäischen Datenschutzausschusses, Version 2.0.

32 Leitlinie 09/22 RZ 105 ff.

33 Leitfaden EDÖB, Ziff. 1.6.

dafür zuständig. Auftragsbearbeiter bearbeiten die Daten im Auftrag und haben keine eigene Hoheit über die Daten.[34]

[32] Jedoch müssen Auftragsbearbeiter die Verantwortlichen sofort informieren (Art. 24 Abs. 3 DSG), sobald eine Datensicherheitsverletzung bekannt wird; dies zeigt sich auch beim Meldeportal des EDÖB[35]: Nach dem Ankreuzen zur Bestätigung, dass man Auftragsbearbeiter sei, folgt nachfolgender Text: «Nur die für die Datenverarbeitung Verantwortlichen können gemäss dem Datenschutzgesetz Datensicherheitsverletzungen melden. Whistleblower und betroffene Personen können ihre Bedenken direkt auf der EDÖB-Kontaktseite melden. Auftragsbearbeiter melden Verletzungen der Datensicherheit bitte so rasch wie möglich dem Verantwortlichen.» Dabei ist zu beachten, dass ein Auftragsbearbeiter keinen Spielraum hat: Er muss jede Verletzung der Datensicherheit ohne einer vorgängigen Risikoabklärung dem Verantwortlichen melden.[36] Wie sinnvoll jede Meldung ist, wird in Frage gestellt;[37] dennoch ist es nachvollziehbar, dass nicht der Auftragnehmer entscheidet, was er dem Auftraggeber melden soll. Zu schnell könnte ein Vorfall als Bagatelle beurteilt werden, um eine Meldung verhindern zu können. Eine gute Fehlerkultur ist, obwohl eine solche immer wieder als äusserst wertvoll beurteilt wird, eher selten Realität, wenn es um die eigenen Fehler geht.[38] Für solche Situationen empfiehlt es sich, eine firmeninterne Regelung festzulegen und intern zu kommunizieren.

[33] Vereinzelt kann es vorkommen, dass Auftragnehmer versuchen, die Auftraggeber zu beruhigen, indem sie einen Vorfall selbst melden und damit den Eindruck erwecken wollen, der Meldepflicht sei damit Genüge getan. Zur Veranschaulichung ein konkretes Beispiel, das sich im Mai 2025 ereignet hat und von der Autorin als externe Datenschutzbeauftragte begleitet wurde: Eine Institution im Gesundheitsbereich liess ihre Webseite von einem IT-Unternehmen (Auftragnehmerin) betreiben. Auf dieser Webseite befand sich auch ein Anmeldeformular, in dessen Freitextfeld von den Nutzerinnen und Nutzern oftmals besonders schützenswerte Personendaten eingegeben wurden. Anfangs Mai 2025 ereignete sich bei der Auftragnehmerin ein Datenabfluss aus der Testumgebung des Webservers. Das IT-Unternehmen versuchte in der Folge, ihre Auftraggeberin zu beschwichtigen und hielt fest, dass der EDÖB bereits informiert worden sei – die Meldepflicht nach DSG sei damit erfüllt und die Sache nun erledigt. Auch wenn dies sicherlich gut gemeint ist: Die Aussage ist bzw. das Vorgehen war nicht korrekt. Denn Art. 24 Abs. 1 i.V.m. Abs. 3 DSG nimmt auch bei einer Auftragsdatenbearbeitung den Verantwortlichen in die Pflicht, sollte sich eine Verletzung der Datensicherheit ergeben. *In casu* hätte das IT-Unternehmen seine Auftraggeberin über den Abfluss informieren müssen – und die Auftraggeberin als Verantwortliche hätte ihrerseits die Meldung an den EDÖB vornehmen müssen, sofern der Abfluss voraussichtlich zu einem hohen Risiko für die Persönlichkeit der betroffenen Person geführt hätte. Die Auftraggeberin hat dann die Meldung auch selbst noch vorgenommen, da die Risikoabwägung ein hohes Risiko nicht ausschliessen konnte; ebenfalls wurden alle Betroffenen über den Vorfall informiert.

34 Eugen Roesle, Meldung von Data Breaches, S. 3, in RR-Comp 2/2022.

35 https://databreach.edoeb.admin.ch/report, Abruf 20. Juli 2025.

36 BBl 2017, 7065.

37 Adrian Bieri/Julian Powell, Meldung von Verletzungen der Datensicherheit, S. 783 f. in AJP 2021.

38 Exemplarisch: Fehlerkultur Report 2023 von EY.

3.1.3. Meldung

[34] Eine Meldung nach DSG hat keine absolute Frist – im Gegensatz zur DSGVO, die eine Frist von 72 Stunden vorsieht (Art. 33 Abs. 1 DSGVO), sie muss aber «so rasch als möglich» (Art. 24 Abs. 1 DSG) erfolgen. Das DSG gibt dem Verantwortlichen einen gewissen Ermessensspielraum; in dieser Zeit kann der Verantwortliche weitere Informationen über den Vorfall zusammentragen, um die Risikoabschätzung vornehmen zu können. Dabei gilt, dass je höher das Ausmass der Gefährdung für betroffene Personen und die Anzahl Betroffener ist, desto schneller die Meldung erfolgen sollte.[39]

[35] In Art. 24 Abs. 2 DSG werden die Mindestanforderungen definiert, detaillierter findet man sie in Art. 15 DSV (Verordnung über den Datenschutz, SR 235.11) aufgegliedert. Auch das Online-Formular[40] des EDÖB führt den Verantwortlichen durch die notwendigen, zu meldenden Elemente:

- Art der Verletzung,
- Zeitpunkt und Dauer der Verletzung,
- Kategorie und ungefähre Anzahl Personendaten sowie Anzahl Betroffener,
- Folgen der Verletzung- soweit dies möglich ist;
- geplante/getroffene Massnahmen.

[36] Zu beachten ist, dass es dabei um die Folgen für die betroffenen Personen geht, nicht die Folgen für den Verantwortlichen der Datenbearbeitung.[41] Die Verletzung der Datensicherheit kann insbesondere Verlust, Löschung, Veränderung und Bekanntgabe an Unbefugte beinhalten (Art. 5 lit. h DSG).

[37] Erfolgt keine Meldung an den EDÖB führt dies zu keinen strafrechtlichen Sanktionen; der EDÖB kann aber, sofern er von einer solchen Verletzung der Datensicherheit erfährt, eine nachträgliche Meldung gestützt auf Art. 51 Abs. 3 Bst. f DSG anordnen.[42] Wird diese Verfügung missachtet, droht eine Busse bis zu CHF 250'000 gestützt auf Art. 63 DSG (Missachten von Verfügungen). Der Täterkreis beschränkt sich allerdings auf private Personen, wobei in der Verfügung ausdrücklich auf die Strafandrohung von Art. 63 DSG hingewiesen wurde.

3.1.4. Information der betroffenen Personen

[38] In Absatz 4 und Absatz 5 von Art. 24 DSG geht es um die Informationspflicht an betroffene Personen. Eine solche Information ist grundsätzlich sinnvoll und zeigt die Professionalität der Firma in Bezug zum Datenschutz; es sollte verhindert werden, dass Betroffene erst mit Verspätung allenfalls aus der Zeitung erfahren, wie dies teilweise vor der Meldepflicht geschehen

39 BBl 2017, 7064.

40 https://databreach.edoeb.admin.ch/report, Abruf 20. Juli 2025.

41 BBl 2017, 7064 f.

42 Leitfaden EDÖB, Ziff. 1.8.

war.[43] Denn nur wer informiert ist, kann allenfalls eigene Massnahmen zur Schadensabwendung vornehmen.[44]

Kommunikation – ja oder nein

[39] Gemäss Gesetz kann die Information an betroffene Personen erfolgen, wenn es «zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt» (Art. 24 Abs. 4 DSG); die Information Betroffener sollte immer dann erfolgen, wenn diese dadurch selbst aktiv werden und handeln können, um einen Schaden zu reduzieren oder abzuwenden, indem sie beispielsweise Passwörter ändern oder die Kreditkarte sperren können.[45]

[40] In der Praxis empfiehlt sich demnach praktisch immer eine Information an Betroffene; es soll nicht sein, dass Betroffene allenfalls aus den Medien von einem Datenhack erfahren.[46] Dies gilt auch dann, wenn Daten versehentlich falsch verschickt wurden, es also nicht im engeren Sinne zu einer Verletzung der Datensicherheit gekommen ist, wie ein Fall aus dem Kanton Aargau zeigte: Eine Arztpraxis verschickte versehentlich Daten von einer Drittperson zusätzlich an eine Patientin. Statt die betroffene Person über den Vorfall zu informieren, hoffte die Praxis wohl – nachdem sie darüber informiert worden war – dass dies niemand erfahre. Doch genau in diesem Fall kannten sich die Empfängerin der Informationen und die Betroffene.[47]

Effektive Kommunikation

[41] Bezüglich Informationsinhalt an betroffene Personen besteht ein gewisser Ermessensspielraum.[48] Wichtig ist eine zeitnahe und adressatengerechte Kommunikation. Nur so kann die Kommunikationshoheit behalten werden. Adressatengerecht bedeutet, dass die Information in einfacher und verständlicher Sprache zu erfolgen hat; die DSGVO formuliert dies in Art. 34 klar: Die Benachrichtigung hat «in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten» zu erfolgen. Zu berücksichtigen ist auch der Umfang der Information: Ist die Information zu lang, kann dies zu einem Informationsoverkill führen, der nicht hilfreich ist.[49] Oft ist weniger mehr. Zudem sollte eine Ansprechperson für Rückfragen angegeben werden, die auf verschiedenen Kanälen erreichbar ist, technische Fachbegriffe sind zu vermeiden. Im Sinne der einfachen Sprache sollte der Text übersichtlich und die Sätze kurz sein. Auf komplizierte Wort- oder Satzkonstruktionen sollte verzichtet werden.[50]

[42] Grundsätzlich kann auch der EDÖB eine Information verlangen; es steht ihm zudem offen, die Information zu fordern, weil ein mediales Interesse daran bestehen könnte. Zudem könnte der EDÖB die Öffentlichkeit auch selbst informieren, gestützt auf Art. 57 Abs. 2 DSG.[51]

---

43 Vorfall noch nach altem DSG: https://www.republik.ch/2023/die-stille-nach-dem-datenklau, Abruf 27. Juli 2025.

44 Dominika Blonski, Stämpfli Handkommentar Datenschutz, Art. 24 N 36.

45 Leitfaden EDÖB, Ziff. 2.1.

46 https://www.srf.ch/news/schweiz/gehackte-gesundheitsdaten-datenleck-bei-spielsucht-beratung-ueber-1300-personen-betroffen, Abruf 27. Juli 2025.

47 https://www.aargauerzeitung.ch/aargau/freiamt/patientenakten-ld.2588599, Abruf 27. Juli 2025.

48 BBl 2017, 7065.

49 Kai von Lewinsky/Dirk Pohl, Kommunikation von Datenschutz – Recht und (gute) Praxis, S. 11.

50 https://portaleinfach.org/abc-der-einfachen-sprache/, Abruf 3. August 2025.

51 Leitfaden EDÖB, Ziff. 2.2.

Indirekte oder keine Information

[43] Gemäss Art. 24 Abs, 5 Bst. c DSG kann die Information auch mittels einer öffentlichen Bekanntmachung erfolgen. Hierzu gab es im Frühling 2023 den Fall eines Datendiebstahls bei verschiedenen Medienhäusern[52], welcher noch unter dem alten Datenschutzgesetz geschehen war – und damit die Information an Betroffene noch nicht Pflicht war. Dabei stellte sich die Frage, ob sich die Medienhäuser auf eine Berichterstattung in den eigenen Medien[53] beschränken dürften oder wo eine solche Publikation erfolgen müsste. Selbst bei einer nationalen Zeitung ist nicht sicher, ob die Information an Betroffene so sichergestellt ist. Sinnvollerweise müsste diese Information über mehrere Kanäle erfolgen, inklusive Internetseite und soziale Medien.[54]

[44] Ebenfalls kann auf eine Information an Betroffene verzichtet werden (Bst. b), wenn der Aufwand dazu unmöglich ist, weil Betroffene nicht erreicht werden können oder (noch) nicht klar ist, wer betroffen ist, oder der Aufwand unverhältnismässig gross ist (Kosten, Zeit) im Verhältnis zum Informationsgewinn der Betroffenen.[55]

[45] Ebenfalls als Grund für eine Einschränkung wird auf den nachfolgenden Art. 26 Abs. 1 Bst. b und Abs. 2 Bst. b oder auf eine gesetzliche Geheimhaltungspflicht verwiesen.

[46] Im Zusammenhang mit einer Meldung ist jedoch zu beachten, dass es nicht zu einer Selbstbelastung in einem Strafverfahren kommt: Deshalb dürfen solche Meldungen nur mit dem ausdrücklichen Einverständnis der betroffenen Person in einem Strafverfahren genutzt werden (Art. 26 Abs. 6 DSG).[56]

3.2. Meldepflicht nach kantonalen Datenschutzgesetzen

[47] Die meisten kantonalen Datenschutzgesetze wurden aufgrund des europäischen Rechts bereits angepasst; die Ausgestaltung der einzelnen Informationspflichten orientiert sich an der Meldepflicht gemäss der Modernisierung der Europarats-Konvention 108+ und dem Erlass der EU-Richtlinie 2016/680[57] für die justizielle und polizeiliche Zusammenarbeit.

[48] Per Ende Juli 2025 waren in 17 Kantonen die Anpassungen vorgenommen und die Gesetze revidiert worden.[58] In all diesen revidierten Gesetzen ist die Meldepflicht bei einer Verletzung der Datensicherheit an die kantonale Datenschutzbehörde hinterlegt. Unterschiede lassen sich in den Details finden. Erfolgen also Verletzungen der Datensicherheit bei kantonalen Organen – dies können auch Organisationen mit einem kantonalen Leistungsauftrag sein wie beispielsweise ein

52 https://www.persoenlich.com/medien/reduzierte-printausgaben-wegen-hackerangriff Abruf 27. Juli 2025.

53 In eigener Sache: Cyberangriff auf das Unternehmen NZZ, in NZZ vom 25. März 2025 https://www.nzz.ch/information/in-eigener-sache-cyberangriff-auf-das-unternehmen-nzz-ld.1732110, Abruf 27. Juli 2025.

54 Bieri/Powell, Art. 24 N23.

55 BBl 2017, 7065.

56 BBl 2017, 7965f.

57 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977.

58 Vgl. Liste Privatim – Stand 1. Juni 2025: https://www.privatim.ch/wp-content/uploads/2025/06/20250610_Revisionen_der_kantonalen_Datenschutzgesetze_-_Revisions_des_lois_cantonales_sur_la_protections_des_donnees.xlsx, Abruf 20. Juli 2025.

Spital oder eine soziale Einrichtung – ist die kantonale Datenschutzstelle die korrekte Meldestelle und nicht der EDÖB.

[49] Anbei die Liste sowie die entsprechenden Gesetzesartikel bezüglich Meldepflicht:

Kanton	Gesetz	Meldepflicht Verletzung Datensicherheit
Aargau	IDAG	§ 17c
Appenzell Innerhoden	DIAG	Art. 20
Appenzell Ausserhoden	Datenschutzgesetz	Art. 16a
Bern	KDSG	– –
Baselland	IDG	§ 15a
Baselstadt	IDG	§ 16a
Freiburg	DSChG/LPrD	Art. 43
Genf	LIPAD	– –
Glarus	IDAG	Art. 35
Graubünden	KDSG	– – (im revidierten Gesetz: Art. 21)
Jura/Neuenburg	CPDTE-JUNE	Art. 23c
Luzern	KDSG	§ 7
Obwalden	kDSG	– – (im revidierten Gesetz Meldepflicht vorgesehen)
St. Gallen	DSG	Art. 9a
Schaffhausen	Kantonales Datenschutzgesetz	Art. 14a
Schwyz	ÖDSG	§ 22a
Solothurn	InfoDG	– – –
Thurgau	TG DSG	– – –
Tessin	LPDP	– – –
Uri	KDSG	Art. 13
Waadt	LPrD	– – –
Wallis	GIDA	Art. 30a
Zug	DSG	§ 7c
Zürich	IDSG	§ 12a

[50] Bezüglich der Informationsflicht gegenüber Betroffenen sind die kantonalen Datenschutzgesetze unterschiedlich: Bei einzelnen kantonalen Datenschutzgesetzen besteht gegenüber den Betroffenen nur eine Informationspflicht, wenn die Verletzung der Datensicherheit voraussichtlich zu einem (hohen) Risiko führt – so beispielsweise bei Basel-Stadt und Basel-Land; bei einem allfälligen Vorfall sind die Vorgaben sorgfältig zu prüfen, wobei auch hier eine Information der Betroffenen grundsätzlich zu empfehlen ist.

3.3. Meldepflicht nach DSGVO

[51] Nicht alle Unternehmen in der Schweiz unterstehen den Regelungen der DSGVO; deren räumliche Anwendungsbereich ist in Art. 3 DSGVO definiert:

- Verarbeitung durch eine Niederlassung in der EU/EWR[59] – d.h. es besteht eine Einrichtung, in der eine Tätigkeit ausgeübt wird,[60]
- Auftragsverarbeiter in der EU/EWR,
- Marktortprinzip – d.h. Waren oder Dienstleistungen werden gezielt in der EU/EWR angeboten. Als Anknüpfungspunkt genügt nicht die Abrufbarkeit einer Internetseite oder der Gebrauch einer (EU-)Sprache; hingegen, wenn das Angebot mit einer (EU-)Währung verknüpft wird oder der Verweis auf Nutzer in der EU/EWR[61,62,]
- Verhaltensbeobachtung von Personen in der EU/dem EWR – beispielsweise durch Tracking-Cookies oder Browser-Fingerprints werden persönliche Vorlieben, Verhaltensweise oder Gepflogenheiten analysiert oder vorhergesagt.[63]

[52] Untersteht man der DSGVO, ist auch deren Meldepflicht zu beachten: Diese ist breiter formuliert und findet sich in Art. 33: «Im Falle einer Verletzung des Schutzes personenbezogener Daten. . . .»; in Art. 4 Ziff. 12 DSGVO wird der Begriff definiert – ähnlich wie im Schweizer Datenschutzgesetz: «. . . ..eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmässig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;». Es geht also auch in der DSGVO um eine Verletzung der Datensicherheit.[64]

[53] Analog zum schweizerischen Gesetz meldet ein Auftragsbearbeiter eine Verletzung sofort dem Verantwortlichen, welcher auch für die Risikoeinschätzung und allenfalls eine Meldung an die Behörde verantwortlich ist (Art. 33 Abs. 2 DSGVO).

[54] Unterschiede bestehen jedoch bei der Meldefrist, beim Risiko und bei der Strafe:

[55] Eine Meldung hat unverzüglich und möglichst innert 72 Stunden zu erfolgen (Art. 33 Abs. 1 DSGVO); zudem ist eine Meldung nicht nur bei einem *hohen* Risiko, sondern bei jedem Risiko notwendig.

[56] Die Risikobeurteilung ist auch in der DSGVO nicht dieselbe wie die in der Datenschutz-Folgenabschätzung der schweizerischen Gesetzgebung. Der Fokus liegt klar auf den Folgen der Verletzung der Datensicherheit/des Datenschutzes für die betroffenen Personen. Eintrittswahrscheinlichkeit und Auswirkungen sind zu beurteilen. Sobald wahrscheinlich ist, dass ein Risiko

---

59 EU/EWR: Grundsätzlich muss EU Recht im EWR-Raum übernommen werden – vgl. https://www.efta.int/de/eealaw#:{~}:text=Die%20EWR%2DEFTA%2DStaaten%20einigen%20sich%20auf%20einen%20Beschlussentwurf,auf%20einen%20Beschlussentwurf%20zur%20%C3%9Cbernahme%20des%20Rechtsakts, Abruf 15. August 2025.

60 Erwägungsgrund 22 DSGVO.

61 Erwägungsgrund 23 DSGVO.

62 Kurzpapier Nr. 7: Marktortprinzip: Regelungen für aussereuropäische Unternehmen – Datenschutzkonferenz.

63 Erwägungsgrund 24 DSGVO.

64 Kathrin Schürmann, Meldepflicht bei Datenschutzvorfällen: Wie sieht proaktiver Datenschutz aus? in: DATENSCHUTZ-BERATER 2022, 272.

besteht, muss dies gemeldet werden.[65] Bezüglich der Bewertungskriterien kann auf Ziffer 3.1.1 weiter oben verwiesen werden.

[57] Im Leitfaden der EU wird bezüglich der Risikobewertung folgendes Beispiel angeführt: Werden versehentlich personenbezogene Daten einem Dritten zugestellt, stellt dies grundsätzliche eine Verletzung dar. Ist der Empfänger eine interne Abteilung oder ein regelmässig beauftragter Lieferant, kann man darum bitten, die Unterlagen zurückzusenden oder zu vernichten. Aufgrund der langjährigen und kontinuierlichen Beziehung darf darauf vertraut werden, dass die Daten nicht gelesen oder/und missbraucht und entsprechend der Anweisung auch vernichtet werden. Man kann von einem kooperativen Verhalten ausgehen und dies entsprechend bei der Risikobewertung berücksichtigen. Eine Verletzung hat zwar stattgefunden, die Wahrscheinlichkeit eines Risikos könnte aber als nicht gegeben eingestuft werden und deshalb die Datenschutzbehörden nicht zu informieren sind.[66]

[58] Eine Benachrichtigung Betroffener ist gemäss Art. 34 Abs. 1 DSGVO nur notwendig, wenn «voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen» besteht.

[59] Erfolgt keine Meldung, können die Datenschutzaufsichtsbehörden verschiedene Massnahmen erlassen: Geldbussen nach Art. 83 Abs. 4 Bst. a DSGVO (bis zu 10'000'000 Euro bzw. 2% des weltweiten Jahresumsatzes) ansetzen oder Abhilfemassnahmen gemäss Art. 58 Abs. 2 DSGVO anordnen.

[60] Zuständig ist die Aufsichtsbehörde, in deren Hoheitsgebiet die Meldung unterlassen wurde. (Dies gilt wenn die Verarbeitung im Rahmen der Tätigkeiten im entsprechenden Hoheitsgebiet erfolgt ist.)[67]

3.4. Meldepflicht nach ISG

[61] Es ist unbestritten, dass Cyberangriffe zunehmen – gerade auch mithilfe der KI werden solche Angriffe immer erfolgreicher.[68] Dies ist mit ein Grund, weshalb aus dem Nationalen Cybersecurity-Center (NCSC) ein eigenes Bundesamt wurde: das Bundesamt für Cybersecurity (BACS).[69] Auch die Politik hat die Risiken erkannt und 2017 reichte Edith Graf-Litscher ein Postulat für eine Meldepflicht bei Sicherheitsvorfällen kritischer Infrastrukturen ein[70], welches vom Nationalrat angenommen und vom Bundesrat zur Annahme empfohlen wurde. Die Gesetzesanpassung des Bundesgesetzes über die Informationssicherheit beim Bund (Informationssicherheitsgesetz, ISG) ist eine Folge davon. Seit dem 1. April 2025 besteht eine Meldepflicht bei Cyberangriffen für bestimmte Behörden und Organisationen, die in Art. 74b ISG abschliessend aufgelistet sind. Es handelt sich dabei vorwiegend um «lohnende Ziele»; bewusst wurde die Definition

65 https://www.datenschutzstelle.li/datenschutz/themen-z/meldung-von-datenschutzverletzungen-art-33-dsgvo, Abruf 29. Juli 2025.

66 Leitfaden EU Rz. 114.

67 Erwägungsgrund 122 DSGVO.

68 Isabelle Wachter, Mit KI betrügen Kriminelle effizienter denn je, NZZ vom 23. Juli 2025.

69 https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2023/Startbundesamt2024.html, Abruf 30. Juli 2025.

70 Postulat 17.3475 von Edith Graf-Litscher: Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen.

kritischer Infrastrukturen breit gehalten. Mit dem breiten Adressatenkreis ist auch die Absicht verbunden, diesen nicht bereits in den nächsten Jahren ergänzen zu müssen. Ist eine Organisation unsicher, ob für sie eine Meldepflicht besteht, ist das BACS zur Unterstützung verpflichtet: Man kann nachfragen gestützt auf Art. 74a Abs. 2 ISG.

Ausnahmen von der Meldepflicht

[62] In der Cybersicherheitsverordnung (SR 128.51) hat der Bundesrat in Art. 12 CSV Ausnahmen von der Meldepflicht aufgelistet. Um von einer Meldepflicht ausgenommen zu sein, müssen diese Organisationen bestimmte Bedingungen erfüllen: Beispielsweise Hochschulen, sofern diese weniger als 2000 Studierende haben (Art 12. Abs. 1 Bst. a ISV), müssen einen Cybervorfall nicht melden. Dadurch ist der Kreis, der ausgewählten Organisationen auf kritische Infrastrukturen beschränkt und der Zusatz-Aufwand, der durch die Meldepflicht entsteht, nicht auf zu viele Organisationen ausgeweitet, wie dies in der Beratung vom Parlament gefordert worden ist.[71]

Kriterien Meldepflicht

[63] Die Meldepflicht soll sicherstellen, dass das BACS eine vollständige Übersicht über Cybervorfälle hat und so eine Frühwarnung möglich ist.[72] Dadurch sollen Cyberbedrohungen mit gezielten Massnahmen verhindert oder zumindest reduziert werden können.[73]

[64] Die Kriterien für eine Meldepflicht sind in Art. 74d ISG abschliessend umschrieben; die Kriterien wurden so gewählt, dass diese für die betroffenen Organisationen einfach feststellbar sind. So besteht eine Meldepflicht, wenn die Funktionsfähigkeit der kritischen Infrastruktur gefährdet (Bst. a), es zu einem Abfluss von Informationen gekommen ist (Bst. b), der Cyberangriff längere Zeit unentdeckt blieb und weitere Angriffe nicht ausgeschlossen werden können (Bst.c) sowie der Cyberangriff mit Erpressung, Drohung oder Nötigung verbunden ist (Bst. d). Diese Kriterien helfen dem BACS bei der Beurteilung der Bedrohungslage; was genau das Ziel dieser Meldepflichten ist.[74]

[65] Um der Bedrohungslage und einer Frühwarnung gerecht zu werden, ist eine Meldung nach ISG innert 24 Stunden nach Bekanntwerden zu machen. Die Meldung hat auf einer Plattform, dem sogenannten Cyber Security Hub (CSH), des BASC zu erfolgen, auf der man sich registrieren muss.[75] Eine frühzeitige Registrierung auf dieser Plattform empfiehlt sich für alle meldepflichtigen Organisationen, so dass bei einem Vorfall direkt die Meldung erfolgen kann. Diese Plattform ist nicht öffentlich zugänglich, die anmeldende Organisation wird vorgängig überprüft.[76] Nebst der Plattform sind aber auch weitere Kommunikationskanäle möglich, wie beispielsweise via E-Mail.

---

71 U.a. Marcel Dobler, NR, in der Debatte vom 16. März 2023 (https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=60152, Abruf 2. März 2025), bzw. Hans Wick, SR, in der Debatte vom 1. Juni 2023 (https://www.parlament.ch/de/ratsbetrieb/amtliches-bulletin/amtliches-bulletin-die-verhandlungen?SubjectId=60745, Abruf 2. August 2025).

72 BBl 2023, 84, 7.

73 Serdar Günal Rütsche/Jutta Sonja Oberlin/Sarah von Hoyningen-Huene, Die neue Meldepflicht für Cyberangriffe – ein Vorbild für den Umgang mit pädokriminellen Inhalten, in: Jusletter 16. Juni 2025.

74 BBl 2023, 84, 42 f.

75 https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht/informationen-csh.html, Abruf 2. August 2025.

76 https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht/informationen-csh.html#-324149790, Abruf 2. August 2025.

[66] Der CSH dient vor allem dem Informationsaustausch und soll die Zusammenarbeit zwischen verschiedenen Akteuren im Bereich der Cybersicherheit fördern; er soll bei der schweizweiten Strategie zur Stärkung der Cyber-Resilienz eine zentrale Rolle einnehmen.[77]

[67] Was zu melden ist, ist auf der Plattform erkennbar und in Art. 74e Abs. 2 ff. ISG beschrieben. Auf der Plattform gibt es auch Felder, die nicht zwingend auszufüllen, aber aus statistischen Gründen von Interesse sind.[78] Der Grundsatz «Nemo tenetur» gilt auch hier: Man muss sich nicht selbst belasten.

Sanktionen

[68] Auf den 1. Oktober 2025 treten zusätzlich die beiden Artikel 74 g und 74h ISG in Kraft treten: Dabei geht es einerseits um die Meldepflicht und andererseits um die Sanktionsmöglichkeiten. Das BACS ist aber gehalten, pragmatisch vorzugehen und die Meldepflichtigen erst auf die Pflichten aufmerksam zu machen und Kontakt aufzunehmen (Art. 74g Abs. 1 ISG). In einem nächsten Schritt ist eine Verfügung mit Strafandrohung zu erlassen (Art. 74g Abs. 2 ISG). Wird die Verfügung missachtet, droht eine Busse von bis zu CHF 100'000; zuständig sind die kantonalen Strafbehörden (Art. 74 h ISG). Bewusst wurde die Bussenhöhe nicht analog dem Datenschutzgesetz von CHF 250'000 gesetzt.[79]

[69] Seitens BACS wird der Fokus klar auf die Früherkennung von Cyberattacken gesetzt. Es ist nicht das Ziel, möglichst viele Strafverfahren zu initiieren. Um für eine Früherkennung möglichst viele Informationen zu haben, können auch private Personen, die nicht meldepflichtig sind, Vorfälle melden. Das BACS versteht sich als «Feuerwehr» und unterstützt betroffene Organisationen in einer ersten Phase, bei der Einschätzung der Lage und Wiederherstellung der Systeme. Unter den FAQ des BACS können die Informationen zur Meldeplicht übersichtlich abgerufen werden.[80] Insgesamt findet man auf der Internetseite des BACS viele Informationen – differenziert zwischen verschiedenen Anspruchsgruppen – zu Vorfällen, die laufend aktualisiert werden.[81] Der Vollständigkeit halber können sich insbesondere private Personen auch bei der Cybercrimepolice (www.cybercrimepolice.ch), einem gemeinsamen Engagement der verschiedenen Polizeikorps, bezüglich aktueller Cybervorfälle informieren.

4. Vergleich der Meldepflicht DSG und ISG

[70] Zwischen der Meldepflicht nach Datenschutzgesetz und nach Informationssicherheitsgesetz besteht ein wesentlicher Unterschied: Beim Datenschutz ist die betroffene Person im Zentrum und es geht um Personendaten. Demgegenüber ist die Meldepflicht nach ISG nicht mit einer Gefährdung der Persönlichkeit oder der Grundrechte Betroffener verknüpft. Vielmehr geht es um einen Cyberangriff gegen eine kritische Infrastruktur. Eine Meldung nach ISG hat immer zu

77 https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht/informationen-csh.html, Abruf 2. August 2025.

78 Onilne-Veranstaltung zu Meldepflichten: https://www.youtube.com/watch?v=KF7W7TbOaFo, Abruf 2. August 2025.

79 BBl 2023, 84, 47.

80 https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht/faq.html, Abruf 2. August 2025.

81 https://www.ncsc.admin.ch/ncsc/de/home.html, Abruf 2. August 2025.

erfolgen, wenn es zu einem Cyberangriff gekommen ist, der die Anforderungen von Art. 74c ISG erfüllt. Es muss keine Risikoabwägung vorgenommen werden.

[71] Weitere Unterschiede bestehen bei den Meldefristen und der Bussenhöhe: Während gemäss DSG eine Meldung *so rasch als möglich* zu erfolgen hat, muss dies gemäss ISG *innert 24 Stunden* nach Entdeckung geschehen. Verletzungen nach DSG sind mit einer Busse von maximal CHF 250'000 bedroht. Dabei wird die Meldepflicht selbst nicht direkt von einer Strafnorm umfasst, sondern erst die Missachtung einer Verfügung des EDÖB zur Meldung einer Datenschutzverletzung.

[72] Der EDÖB kann nämlich eine Information bei einer Verletzung der Datensicherheit anordnen (Art. 51 Abs. 3 Bst. f DSG) und muss auf die Strafandrohung von Art. 63 DSG bei Missachtung hinweisen. Auch gemäss ISG muss das BACS bei einer Verletzung der Meldepflicht eines Cyberangriffs eine Verfügung erlassen (Art. 74g ISG), die mit einem Hinweis auf eine mögliche Strafandrohung des Folgeartikels (Art. 74h ISG) versehen ist. Die Maximalbusse beträgt, wie bereits oben festgehalten, CHF 100'000.

[73] Gemeinsam ist beiden Meldepflichten der Grundsatz, sich nicht selbst belasten zu müssen (Art. 24 Abs. 6 DSG / Art. 74e Abs. 4 ISG); ebenfalls wird bei beiden Gesetzen auf die Möglichkeit hingewiesen, dass weitere Meldepflichten mit Einverständnis gleichzeitig erfolgen können: So kann der EDÖB gestützt auf Art. 24 Abs. 5bis DSG eine Meldung dem BACS weiterleiten. Das Meldesystem des BACS muss es ermöglichen, weitere Meldepflichten darin zu integrieren (Art. 74f Abs. 2 ISG). Dadurch sollen Meldende einen möglichst geringen Aufwand haben, wenn sie gegenüber mehreren Stellen meldepflichtig sind. Das System des BACS soll eine Art «One-stop-Shop» sein.[82]

4.1. Empfehlung

[74] Eine Organisation ist gut beraten, einen Prozessbeschrieb zu erstellen, der das Vorgehen bei einer Verletzung der Datensicherheit nach DSG festschreibt. Dabei muss das Unternehmen prüfen, ob es eine Organisation gemäss Art. 74b ISG ist; in einem nächsten Schritt sind die Ausnahmeregelungen von Art 12 ISV zu kontrollieren. Besteht eine Meldepflicht nach ISG, muss diese ergänzend aufgenommen werden. Wichtig ist in diesem Zusammenhang, dass eine Meldung innert 24 Stunden, also schneller erfolgen muss als gemäss DSG.

[75] Ein Prozess, der einzig auf Cybervorfälle ausgerichtet ist, ist bei Organisationen sinnvoll, die eine Meldepflicht nach ISG haben, aber keine Personendaten bearbeiten. Dies dürften jedoch Ausnahmefälle sein. Ein Meldeprozess «Verletzung Datensicherheit» wird empfohlen.

82 BBl 2023, 84, 45.

4.2. Tabellarischer Vergleich der wichtigsten Punkte

Thema	DSG	ISG	DSGVO
Was ist zu melden?	Art. 24 Abs.1 DSG: Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt	Art. 74d ISG: Cyberangriff, wenn dieser: a. die Funktionsfähigkeit der betroffenen kritischen Infrastruktur gefährdet; b. zu einer Manipulation oder zu einem Abfluss von Informationen geführt hat; c. über einen längeren Zeitraum unentdeckt blieb, insbesondere wenn Anzeichen dafür bestehen, dass er zur Vorbereitung weiterer Cyberangriffe ausgeführt wurde; d. mit Erpressung, Drohung oder Nötigung verbunden ist.	Art. 33 DSGVO: Verletzung des Schutzes personenbezogener Daten, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
Wo melden?	EDÖB	BACS	Zuständige, nationale Aufsichtsbehörde
Frist für Meldung	So rasch als möglich	Innert 24 Stunden nach Entdeckung des Cyberangriffs	Innert 72 Stunden, nachdem Verletzung bekannt wurde
Inhalt der Meldung	Art. 15 DSV	Art. 74e Abs. 2 ISG	Art. 33 Abs. 3 DSGVO

Thema	DSG	ISG	DSGVO
Information Betroffener	Art. 24 Abs. 4: Sofern zu deren Schutz notwendig oder auf Verlangen des EDÖB	– – – –	Art. 34 DSGVO: Sofern die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat
Strafrahmen bei Verletzung der Meldepflicht	Art. 63 DSG i.V.m. Art. 51 Abs. 3 Bst. f DSG: Maximal CHF 250'000	Art. 74 h ISG: Maximal CHF 100'000	Art. 83 Abs. 4 Bst. a i.V.m. Art. 33: Maximal Euro 10'000'000 bzw. 2% Jahresumsatz

Ursula Uttinger, lic. iur., exec. MBA HSG.

Ron Porath, Dr. rer. nat.