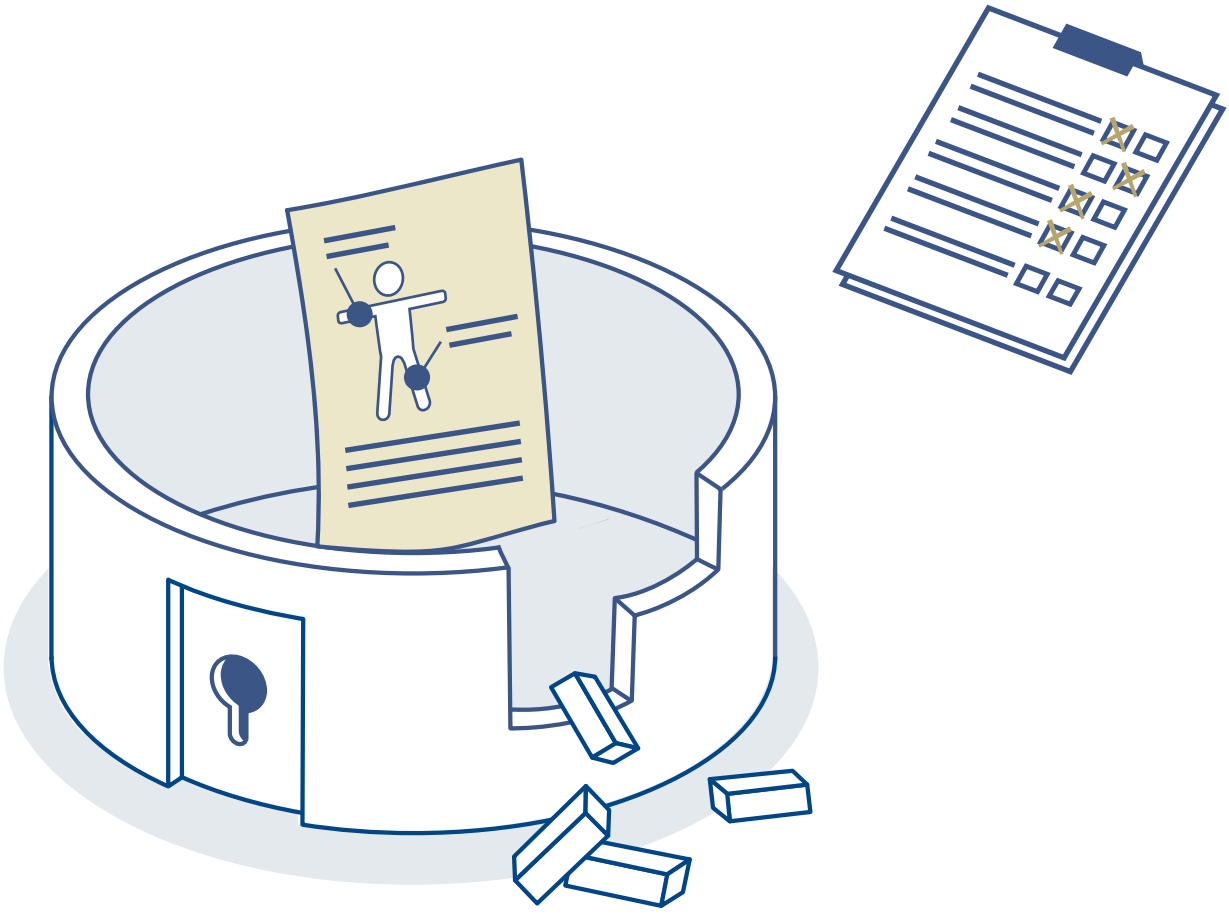
Checkliste und Prozessablauf bei Datenschutz-verletzungen



Version 03/2023

FMH · Verbindung der Schweizer Ärztinnen und Ärzte · Fédération des médecins suisses
Postfach · CH-3000 Bern 16 · Telefon +41 31 359 11 11 · info@fmh.ch · www.fmh.ch

Inhaltsverzeichnis

1 Allgemeines

Das vorliegende Dokument soll bei der Vorbereitung auf und der Abwicklung von Verletzungen der Datensicherheit behilflich sein und die Einhaltung der gesetzlichen Anforderungen sicherstellen. Neben Definitionen der Verletzung sowie der Meldepflicht umfasst das Dokument eine Checkliste zur Vorbereitung sowie einen Prozess zur Abwicklung eines Ereignisses.

Bei Themen, bei welchen das Gesetz keine Vorgabe erlassen hat, wurden Empfehlungen für ein mögliches Vorgehen formuliert. Um Redundanzen gegenüber den Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte, welche Empfehlungen sowie Massnahmen bei Sicherheitsvorfällen vorsehen, zu vermeiden, wird teilweise auf die einzelnen Empfehlungen (E) und Massnahmen (M-10.XX) des IT-Grundschutzes verwiesen.

1.1 Definition Verletzung der Datensicherheit

Analog den Zielen der Informationssicherheit besteht das Ziel der Datensicherheit darin, anhand geeigneter Massnahmen die Personendaten vor Verlust der Vertraulichkeit, der Integrität oder der Verfügbarkeit zu schützen.

Nach dem Datenschutzgesetz liegt eine Verletzung der Datensicherheit vor,

— wenn Personendaten unbeabsichtigt oder widerrechtlich verloren gehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden, z. B. bei Verlust eines Datenträgers wie Laptop, CD, USB-Stick etc. oder bei Zerstörung von Daten durch ein Naturereignis wie Überschwemmung, Feuer etc. oder durch einen Phishing-Angriff.

Indizien für eine mögliche Datensicherheitsverletzung sind zum Beispiel:

— Einbruch in die Praxis
— Brand

1.2 Meldepflicht

Falls die Verletzung der Datensicherheit ein hohes Risiko für die betroffenen Personen birgt, ist sie dem Eidgenössischen Daten- und Öffentlichkeitsbeauftragten (EDÖB) [1] zu melden. Ein hohes Risiko liegt gemäss Gesetz vor, wenn durch die Verletzung der Datensicherheit Grundrechte resp. die Persönlichkeit einzelner betroffener Personen voraussichtlich gefährdet werden.

Mögliche Beispiele für ein hohes Risiko könnten folgende sein:

— Die Server der Arztpraxis werden angegriffen und es wird angenommen, dass die Angreifer Zugang zu sämtlichen Gesundheitsdaten der Patientinnen und Patienten hatten.
— Durch eine technische Störung werden alle Gesundheitsdaten der Patientinnen und Patienten gelöscht und das Back-up kann nicht wiederhergestellt werden.
— Patientendaten werden ohne Einwilligung und unverschlüsselt per E-Mail an Dritte weitergeleitet.

[1] https://www.edoeb.admin.ch

1.3 Checkliste

Die nachfolgende Checkliste soll eine Hilfestellung dafür bieten, welche Punkte präventiv definiert werden sollten. Im Falle einer (vermuteten) Verletzung der Datensicherheit sind dadurch wichtige Prozessschritte bereits geklärt und die relevanten Entscheidungen getroffen.

Definition verantwortliche Person (Datensicherheitsverantwortliche)

Bei Verletzungen der Datensicherheit, insbesondere wenn eine Meldepflicht gemäss 1.2 angezeigt ist, ist der Inhaber der Arztpraxis umgehend zu informieren und gemeinsam mit ihm sind die erforderlichen Massnahmen umzusetzen.

Analog der Massnahme M-10.01 der Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte-D3 sollte eine Person definiert werden, welche im Rahmen von Datensicherheitsverletzungen die Verantwortung trägt (nachfolgend Datensicherheitsverantwortliche). Dabei kann es sich um dieselbe Person handeln, welche bereits für Sicherheitsvorfälle nach IT-Grundschutz benannt wurde (vgl. auch E1 der Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte-D3).

Merkblatt Datensicherheitsverletzung

Es wird empfohlen, vorgängig ein Merkblatt zu erarbeiten, welches die Mitarbeitenden dabei unterstützt, eine Verletzung der Datensicherheit zu erkennen. Zusätzlich als Hilfestellung könnten im Merkblatt mögliche Beispiele für Indizien einer Datensicherheitsverletzung aufgenommen werden. Als Orientierung kann oben Ziff. 1.1 Definition Verletzung der Datensicherheit dienen.

Weiter wird empfohlen, in diesem Merkblatt konkrete Handlungsanweisungen an die Mitarbeitenden zu definieren und zusätzlich die Mitarbeitenden zu sensibilisieren (vgl. unten Ziff. 2 Prozess Verletzung Datensicherheit).

Dokumentation

Das Datenschutzgesetz sieht vor, dass eine Verletzung der Datensicherheit von der Datensicherheitsverantwortlichen zu dokumentieren ist, sofern die Verletzung meldepflichtig ist.

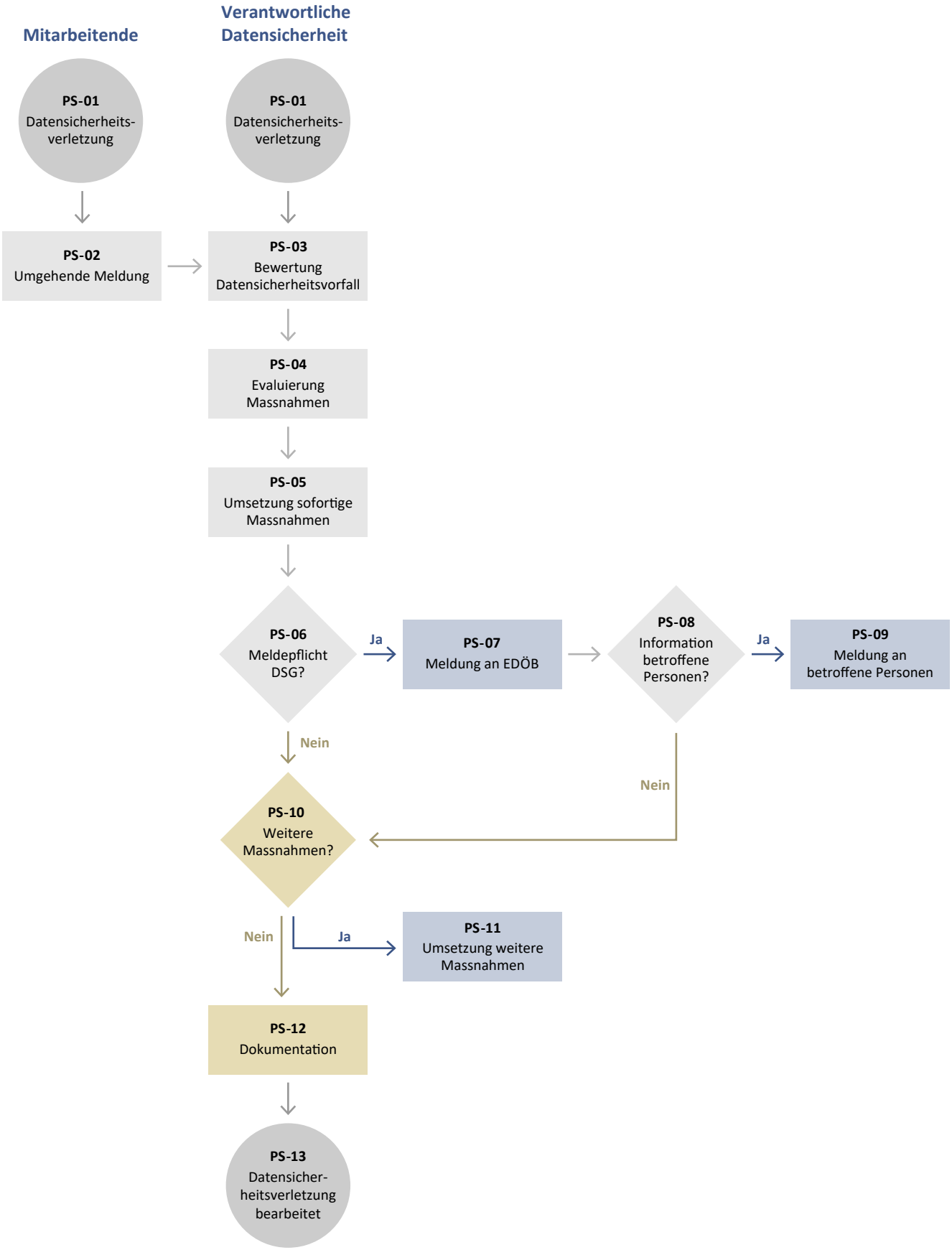
Die Dokumentation enthält mindestens:

— alle mit der Verletzung der Datensicherheit zusammenhängenden Tatsachen (vgl. auch unten Ziff. 2 Prozess Verletzung Datensicherheit Prozessschritt «PS-07, Meldung an EDÖB»),
— Auswirkungen der Verletzung der Datensicherheit und
— die ergriffenen Massnahmen für die Eindämmung oder die Beseitigung der Verletzung der Datensicherheit.

Ist die Verletzung der Datensicherheit nicht meldepflichtig, wird empfohlen, dass zusätzlich der Grund des Verzichts auf Meldung dokumentiert wird.

Ab Zeitpunkt der Verletzung der Datensicherheit ist die Dokumentation gemäss der Datenschutzverordnung mindestens während zwei Jahren aufzubewahren.

2 Prozess Verletzung Datensicherheit



Prozess-schritt (PS)	Aktivitäten	Beschreibung der Aktivität
PS-01	Datensicher-heitsverletzung	Eine Datensicherheitsverletzung ist eingetreten und wurde von der Datensicherheitsver-antwortlichen oder von einer/einem Mitarbeitenden erkannt (vgl. oben Ziff. 1.1 Definition Verletzung der Datensicherheit).
PS-02	Umgehende Meldung	Haben Mitarbeitende eine (potenzielle) Verletzung der Datensicherheit erkannt, ist die Datensicherheitsverantwortliche (vgl. oben Ziff. 1.3 Checkliste, Abschnitt «Definition ver-antwortliche Person») umgehend darüber in Kenntnis zu setzen.
PS-03	Bewertung Datensicher-heitsvorfall	Die Datensicherheitsverantwortliche bewertet die Meldung resp. die vermutete Verletzung der Datensicherheit. Für die Bewertung kann die Massnahme M-10.03 der Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte beigezogen werden.
PS-04	Evaluierung Massnahmen	Die Datensicherheitsverantwortliche beurteilt die Verletzung der Datensicherheit auf Basis des zu erwartenden Risikos und legt fest, ob und welche Massnahmen zur Behandlung der Verletzung notwendig sind. Bei der Definition von Massnahmen kann unterschieden werden zwischen Sofortmassnahmen zur Eindämmung des Vorfalls und Massnahmen zur langfristigen Adressierung der Ursache und Behandlung des Vorfalls.
PS-05	Umsetzung sofortige Massnahmen	Wurden in PS-04 Sofortmassnahmen definiert, werden diese direkt umgesetzt, um die Verletzung der Datensicherheit einzudämmen (bspw. Isolation oder Ausserbetriebnahme von einzelnen Diensten oder Systemen).
PS-06	Meldepflicht DSG?	Die Datensicherheitsverantwortliche prüft in einem weiteren Schritt, ob die Verletzung der Datensicherheit möglicherweise zu einem hohen Risiko für die betroffenen Personen führt (vgl. oben Ziff. 1.2 Meldepflicht) und dadurch eine Meldepflicht gegenüber dem EDÖB vorliegt.
PS-07	Meldung an EDÖB	Liegt eine Meldepflicht vor, wird die Meldung an den EDÖB vorbereitet. Das Datenschutz-gesetz sieht dabei vor, dass die Meldung über die Verletzung der Datensicherheit an den EDÖB mindestens folgende Punkte beinhaltet: — Art der Verletzung der Datensicherheit (z. B. Zerstörung der Daten, Diebstahl der Daten etc.); — sofern bekannt, Zeitpunkt und Dauer der Verletzung; — soweit möglich, die Kategorien der Personendaten und die ungefähre Anzahl der betroffenen Personendaten; — soweit möglich, die Kategorien der betroffenen Personen und die ungefähre Anzahl der betroffenen Personen; — Folgen der Verletzung der Datensicherheit, einschliesslich der allfälligen Risiken für die betroffenen Personen (z. B. kein Zugriff auf Krankengeschichten, folglich Nachvoll-ziehbarkeit der Behandlung nur noch teilweise möglich und folglich mögliche Gefähr-dung der Gesundheit der Betroffenen; Publikation der Krankengeschichten im Darknet, folglich Gefährdung der Persönlichkeit der Betroffenen); — ergriffene oder vorgesehene Massnahmen, um den Mangel zu beheben oder die Folgen zu mindern (z. B. Wiederherstellung des Back-ups bei digitalen Daten), und — Namen und Kontaktdaten einer Ansprechperson. Ist es nicht möglich, alle Informationen zur gleichen Zeit mitzuteilen, können die weiteren Informationen dem EDÖB in einem angemessenen Zeitrahmen schrittweise zur Verfügung gestellt werden. **Hinweis:** Für die Eruierung, welche betroffenen Personenkategorien und -daten von der Verletzung der Datensicherheit betroffen sind, könnte ein vorgängig erstelltes Verzeichnis der Bearbeitungstätigkeiten eine Hilfestellung bieten (siehe dazu auch den Leitfaden und die Vorlage für Verzeichnis der Bearbeitungstätigkeiten).

PS-08	Information betroffene Personen?	Die Datensicherheitsverantwortliche evaluiert, ob die von der Datensicherheitsverletzung betroffenen Personen zu informieren sind. Die betroffenen Personen sind zu informieren, wenn: — zu treffende Schutzmassnahmen nötig sind (z. B. Änderung von Zugangsdaten wie Passwörtern) oder — es der EDÖB verlangt. Die Datensicherheitsverantwortliche kann die Information der betroffenen Personen einschränken, aufschieben oder darauf verzichten, wenn: — dies aufgrund überwiegender Interessen erforderlich ist; — die Information aufgrund einer gesetzlichen Geheimhaltungspflicht verboten ist; — die Information unmöglich ist oder einen unverhältnismässigen Aufwand mit sich bringt oder — die Information der betroffenen Person durch eine öffentliche Bekanntmachung in vergleichbarer Weise sichergestellt ist.
PS-09	Meldung an betroffene Personen	Hat sich in PS-08 ergeben, dass eine Information der Betroffenen erforderlich ist, ist eine Meldung über die Datensicherheitsverletzung vorzubereiten. Die Meldung enthält mindestens folgende Angaben: — Art der Verletzung der Datensicherheit (z. B. Zerstörung der Daten, Diebstahl der Daten etc.). — Folgen der Verletzung der Datensicherheit, einschliesslich der allfälligen Risiken für die betroffenen Personen (z. B. kein Zugriff auf Krankengeschichten mehr möglich, folglich Nachvollziehbarkeit der Behandlung nur noch teilweise gegeben sowie allfällige Gefährdung der Gesundheit der Betroffenen; Publikation der Krankengeschichten im Darknet, folglich Gefährdung der Persönlichkeit der Betroffenen). — Ergriffene oder vorgesehene Massnahmen, um den Mangel zu beheben oder die Folgen zu mindern (z. B. Wiederherstellung des Back-ups bei Verlust digitaler Daten). — Namen und Kontaktdaten einer Ansprechperson.
PS-10	Weitere Massnahmen?	Wurden die Sofortmassnahmen umgesetzt und die Meldepflicht gegenüber dem EDÖB sowie den betroffenen Personen geprüft und allenfalls veranlasst, ist festzustellen, ob weitere Massnahmen notwendig sind. Gegebenenfalls besteht die Notwendigkeit weiterer Massnahmen, die jedoch mittel- oder langfristig umgesetzt werden können (siehe auch PS-04).
PS-11	Umsetzung weitere Massnahmen	Wurde weiterer Bedarf für Massnahmen ermittelt, kann die Umsetzung dieser erfolgen (vgl. auch M-10.07 sowie M-10.08 der Minimalanforderungen IT-Grundschutz für Praxisärztinnen und Praxisärzte).
PS-12	Dokumentation	Die Datensicherheitsverantwortliche dokumentiert in jedem Fall die Verletzung der Datensicherheit (vgl. oben 1.3 Checkliste).
PS-13	Datensicherheitsverletzung bearbeitet	Nach Umsetzung notwendiger Massnahmen, Erstattung einer allfälligen Meldung sowie der Dokumentation der Verletzung der Datensicherheit ist der Prozess abgeschlossen.

Impressum
Herausgeberin: FMH – Verbindung der Schweizer Ärztinnen und Ärzte, Bern
Publikation: März 2023
www.fmh.ch