Richtlinie
Data Breach Prozess

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 22.0

Fassung gemäß Vorstandsbeschluss vom 21.04.2022

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Richtlinie Data Breach Prozess
Version	22.0
Geltungsbereich	VAV Versicherungs-Aktiengesellschaft
Erstmalige Freigabe	23.03.2017
Verabschiedet durch (Datum)	Vorstand (21.04.2022)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	April 2022

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
1.0	23.03.2017	Erstellung	Sven Rabe
18.0	09.05.2018	Anpassungen an die DSGVO	Daniel Fürdauer
19.0	11.04.2019	Anpassungen an Neuerungen und Optimierungen des Prozesses	Daniel Fürdauer
20.0	28.07.2020	Redaktionelle Änderungen, Schnittstelle zu Informationssicherheit	Daniel Fürdauer
21.0	29.07.2021	Jährliches Review	Daniel Fürdauer
22.0	07.04.2022	Jährliches Review, Einführung der Bearbeitung von Datenschutzvorfällen mit geringem Schadenpotenzial durch den Datenschutzbeauftragten	Daniel Fürdauer

Art der Freigabe – VHV Konzern

Version	Datum	Wesentliche Änderungen	Bestätigt von
18.0	24.04.2018	Nein	Sina Rintelmann

19.0	10.04.2019	Nein	Sina Rintelmann (i.V. Carsten Kluge)
20.0	05.08.2020	Nein	Roman Lemke
21.0	30.07.2021	Nein	Roman Lemke
22.0	20.04.2022	Nein	Roman Lemke
Wesentliche Änderungen		→Nein: Bestätigung durch Konzerndatenschutzbeauftragter →Ja: Bestätigung durch Vorstand VHV Holding	

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

1. ALLGEMEINES

1.1. Grundlagen

Eine der wichtigsten Neuerungen der Datenschutzgrundverordnung (DSGVO) betreffen die in Art. 33 und 34 DSGVO festgelegte Informationsverpflichtungen über die Verletzung des Schutzes personenbezogener Daten:

1. **Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche […] binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der [Datenschutzbehörde], es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.**

2. **Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.**

1.2. Geltungsbereich

Der Geltungsbereich dieser Richtlinie bezieht sich auf die VAV Versicherungs-Aktiengesellschaft.

Die Richtlinie ist durch den Vorstand schriftlich zu genehmigen, bei wesentlichen Änderungen in dem jeweiligen Bereich unverzüglich anzupassen und zumindest einmal jährlich zu überprüfen.

Die vorliegende Richtlinie regelt das Vorgehen im Fall einer Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 und 34 DSGVO.

2. DATA-BREACH

2.1. Allgemeine Informationen

Ein Data Breach bzw. eine Datenschutz-Verletzung kann zum Beispiel aufgrund der folgenden Ereignisse eintreten:

- Unbefugter Zugriff auf Daten, z.B. durch einen Außentäter (Hacking-Angriff, Virenbefall, Ransomware,…) oder einen nicht berechtigten Mitarbeiter
- Verlust/Diebstahl/unbefugter Gebrauch von Schlüsseln, Notebook, Tablet, Smartphone, USB-Sticks, sonstigen Datenträgern, Dokumenten, sonstigen Unterlagen,…
- E-Mail/Brief an die falsche Person gesendet und/oder falschen Anhang gesendet
- Versand von Kundendaten an unberechtigte Dritte
- Bedrohung/Erpressung von Mitarbeitern
- Hacking, Spionage, Sabotage von IT-Systemen
- Unbefugter Zugriff von innen oder außen auf die VAV Systeme
- Unsachgemäße Entsorgung von Unterlagen
- Einbruch oder Ausfall des Zutrittsberechtigungssystems
- Im System wurden Daten falsch zugeordnet
- Die Löschung von Daten, die noch benötigt werden, oder durch eine nicht autorisierte Person
- Die Unmöglichkeit der Wiederherstellung eines Backups
- Nutzung der CC statt BCC-Funktion in E-Mails bei Empfängern, die sich nicht kennen.
- Jeder sonstige Fall, in dem offenkundig personenbezogene Daten aus der Verantwortung der VAV missbräuchlich verwendet oder unzulässig offengelegt werden.

Der Hinweis über Datenverluste, kann über verschiedene Kanäle erfolgen (demonstrative Aufzählung):

- Hinweise von dem Betroffenen selbst
- Hinweise von extern (z.B. per E-Mail oder Telefon)
- Hinweise durch die Medien
- Hinweise durch Auftragsverarbeiter, Vertriebspartner, anderer Versicherungen etc.
- Hinweise von Compliance
- Hinweise von Informationssicherheit

Zu beachten ist, dass der Schaden nicht bereits eingetreten sein muss. Es genügt die Möglichkeit, dass zukünftig daraus ein Schaden (z.B. in finanzieller Hinsicht, in Bezug auf das Ansehen oder hinsichtlich einer körperlichen Gefährdung des Betroffenen) entstehen könnte.
Die 72 Stunden gelten auch über das Wochenende. Es ist daher erforderlich die Informationen unverzüglich an die zuständigen Personen (Data-Breach-Krisenstab) weiterzuleiten.
Für die Meldung an die Datenschutzbehörde ist das Formular der Datenschutzbehörde in der aktuellen Fassung (abrufbar über die Homepage der DSB) zu verwenden. Bei Bedarf kann ein vergleichbares Formular selbst erstellt werden bzw. das Formular der Behörde ergänzt werden.
Die Information der Betroffenen kann grundsätzlich in jeder möglichen Form erfolgen. Abgesehen von direkten Kommunikationsformen, z.B. durch Brief- oder E-Mail-Versand, ist auch die Veröffentlichung in Tageszeitungen denkbar. Zu bedenken sind dabei aber die Nachprüfbarkeit der Benachrichtigung (die bei einem eingeschriebenen Brief gegeben ist, nicht aber bei einer einfachen E-Mail) und die möglichen negativen Auswirkungen auf den Ruf des Unternehmens, die z.B. bei einer breiten Veröffentlichung in der Zeitung eintreten könnten.

2.2. Interne Meldung der Datenschutzverletzung

Jeglicher Verdachtsfall von Datenverlust bzw. unrechtmäßige Verwendung von personenbezogenen Daten ist unverzüglich an die erste verfügbare Person mit dem Hinweis auf einen möglichen Data Breach (DB) gemäß dieser Meldekette zu melden.
Zumindest 2 der folgenden Personen bilden in weiterer Folge den Data-Breach-Krisenstab. Alternativ kann der Datenschutzbeauftragte geringe Datenschutzverletzungen alleine bearbeiten (siehe: 2.5).

1) Datenschutzbeauftragter
2) Informationssicherheitsbeauftragter
3) AL Compliance & Recht
4) AL IT, BO, FM
5) AL oder Datenschutzexperte der Fachabteilung(en), in der der etwaige Datenverlust aufgetreten ist
6) Sonstige fachlich qualifizierte Person (insbesondere Datenschutzexperten)
7) Wenn voraussichtlich keine der vorher genannten Personen innerhalb von 24 Stunden erreicht werden können (z.B. aufgrund des Wochenendes), ist der Vorstandsvorsitzende oder ein anderes Vorstandsmitglied unverzüglich über den Datenverlust zu informieren.

2.3. Grobanalyse der Datenschutzverletzung

Die jeweils erste verfügbare Person der Meldekette analysiert die Situation grob.
Bei eventuellem Erhärten des Verdachtsfalles informiert die Person eine weitere Person (1-6) innerhalb von 1 Stunde über den Vorfall. Ist keine Person verfügbar, ist eine andere qualifizierte Person hinzuzuziehen.

a) Der Verdacht erhärtet sich nicht:
   - Die Analyse der Situation ist von dem Datenschutzbeauftragten zu dokumentieren bzw. diesem zu übermitteln.
   - Wird bereits von der ersten Person ein eventuelles Erhärten ausgeschlossen, analysiert zusätzlich die 2. verfügbare Person der Meldekette die Situation und diese Analyse ist ebenfalls von dem Datenschutzbeauftragten zu dokumentieren.

b) Der Verdacht erhärtet sich:
   - Die Detailanalyse ist durchzuführen.

2.4. Detailanalyse der Datenschutzverletzung

Der DB-Krisenstab bewertet unverzüglich die vorgelegten Informationen und fordert alle Informationen an, um bei Bedarf die Meldung an die Behörde durchführen zu können.
Der DB-Krisenstab wird bei Bedarf und abhängig von dem Umfang um weitere Personen, insbesondere um jene, die bereits oben genannt wurden, erweitert. Im Zweifelsfall zieht der DB-Krisenstab externe Unterstützung von fachkundigen Dritten (z.B. IT-, Datenschutz-Spezialisten, Secur

Data) hinzu. Eventuelle Benachrichtigungen von Betroffenen und weiteren Personen sind bei Bedarf mit der Abteilung Unternehmenskommunikation abzustimmen.
Es ist dabei zu bewerten, ob voraussichtlich (a) kein, (b) ein oder (c) ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht.
Der DB-Krisenstab erstellt eine Entscheidungsvorlage für den Vorstand.

a) Bei der Feststellung keines Risikos für die Rechte und Freiheiten von natürlichen Personen erfolgt keine Meldung an die Datenschutzbehörde.
b) Bei der Feststellung eines Risikos für die Rechte und Freiheiten von natürlichen Personen erfolgt die Meldung an die Datenschutzbehörde (Kapitel 3).
c) Bei der Feststellung eines hohen Risikos für die Rechte und Freiheiten von natürlichen Personen erfolgt die Meldung an die Datenschutzbehörde (Kapitel 3) und Benachrichtigung der Betroffenen (Kapitel 4).

Der Vorstandsvorsitzende oder ein Vorstandsmitglied entscheidet auf Basis der Entscheidungsvorlage des DB-Krisenstabs über das voraussichtliche Risiko gemäß Art. 33 und 34 DSGVO.
Wenn weder der Vorstandsvorsitzende, noch ein Vorstandsmitglied bis 1 Stunde vor Ende der 72 Stunden Frist erreichbar ist, kann der Datenschutzbeauftragte über das voraussichtliche Risiko gemäß Art. 33 und 34 DSGVO entscheiden.

Der Datenschutzbeauftragte übernimmt die Kommunikation mit der Datenschutzbehörde.
Wenn der Datenschutzbeauftragte nicht verfügbar ist, legt der Vorstandsvorsitzende oder ein Vorstandsmitglied eine andere Person für die Kommunikation mit der Datenschutzbehörde fest.

Es ist darauf zu achten, dass es derzeit keine genauen Vorgaben gibt, wann ein Risiko vorliegt. Es ist stets eine Einzelfallbeurteilung vorzunehmen.
Ein hohes Risiko könnte zum Beispiel bestehen, wenn E-Mail-Adressen in Kombination mit Passwörtern, Gesundheitsdaten oder detaillierte Kreditkarteninformationen betroffen sind. Im Anhang finden sich die zu Art. 33 und 34 DSGVO und zu dieser Richtlinie passenden Erwägungsgründe.
Eine Meldung an die Datenschutzbehörde birgt immer das Risiko, dass die Datenverarbeitung unverzüglich eingestellt werden muss und dies zu einer Einstellung der Geschäftstätigkeit führen kann. Daher ist darauf zu achten, die ursprünglichen und zusätzlich unternommenen Schutz- sowie organisatorischen Maßnahmen möglichst detailliert zu beschreiben.

Zusätzlich ist durchzuführen:

- Evaluierung, ob eine BCM-Krisensituation gemäß der Geschäftsordnung des Krisenstabs vorliegt und ggf. die BCM-Krisensituation auszurufen ist.
- Eine allfällige Informationsverpflichtung an Auftraggeber/-nehmer ist zu beachten.
- Evaluierung, ob ein Informationssicherheits-Vorfall vorliegt.

2.5. Bearbeitung von Datenschutzverletzungen mit geringem Schadenspotenzial durch den Datenschutzbeauftragten

Der Datenschutzbeauftragte kann Datenschutzverletzungen, bei denen gemäß Art. 33 DSGVO voraussichtlich kein Risiko für die Rechte und Freiheiten natürlicher Personen besteht und die deshalb nicht an die Datenschutzbehörde gemeldet werden müssen, sowie deren Schadenspotenzial gering ist, alleine bearbeiten.
Dies gilt insbesondere für Datenschutzverletzungen, bei denen kein systematischer Fehler vorliegt, also beispielsweise nur ein Dokument an den falschen Empfänger versendet wurde, eine E-Mail an einen falschen Empfänger versendet wurde, weitere Empfänger einer E-Mail im CC statt BCC waren.
Der Datenschutzbeauftragte kann diese Datenschutzverletzungen alleine analysieren, bearbeiten und dokumentieren.
Der Vorstand wird zumindest jährlich über die aufgetretenen Datenschutz-Vorfälle informiert.

3. MELDUNG AN DIE DATENSCHUTZBEHÖRDE

3.1. Meldung

Die Meldung erfolgt mittels des Formulars der Datenschutzbehörde („Meldungen von Verletzungen des Schutzes personenbezogener Daten gemäß Art. 33 DSGVO“, verfügbar unter https://www.dsb.gv.at/dokumente).
Das ausgefüllte Formular ist an dsb@dsb.gv.at zu senden.
Das Formular umfasst dabei die rechtlichen Informationspflichten nach Art. 33 Abs. 3.
Wenn nicht alle Informationen zur Verfügung stehen, ist Art. 33 Abs. 4. zu beachten: „Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung schrittweise zur Verfügung stellen.“

4. BENACHRICHTIGUNG DER BETROFFENEN

4.1. Benachrichtigung

Die Benachrichtigung der betroffenen Personen muss unverzüglich erfolgen.

Die Benachrichtigung der betroffenen Personen ist nicht erforderlich, wenn eine der folgenden Bedingungen nach Art. 34 Abs. 3 erfüllt ist:

a) der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
b) der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht;
c) dies mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

Nach Art. 34 Abs. 4 kann die Datenschutzbehörde im Falle einer unterbliebenen Benachrichtigung der betroffenen Personen die Benachrichtigung verlangen, oder mit einem Beschluss feststellen, dass eine der genannten Bedingungen nach Art. 34 Abs. 3 erfüllt ist.

Die Benachrichtigung beschreibt in klarer und einfacher Sprache die Art der Verletzung und muss zumindest die folgenden Informationen enthalten:

a) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
c) eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Auf welchem Weg die Benachrichtigung des Betroffenen zu erfolgen hat, ist gesetzlich nicht geregelt. Die Art der Information muss jedenfalls geeignet sein, das primäre Ziel des Gesetzes, nämlich dem Betroffenen zu ermöglichen, Sicherheitsmaßnahmen rechtzeitig zu treffen, zu erreichen. Es ist daher grundsätzlich sowohl die Information durch E-Mail, ein herkömmliches Schreiben, ein Inserat oder ein Hinweis auf der Website möglich. Letztlich hängt es von den Umständen des Einzelfalls ab, welche Art der Information zu bevorzugen ist. Eine adäquate mediale Information käme allerdings etwa dann in Frage, wenn weder E-Mail Adresse noch Anschrift der Betroffenen bekannt sind. Zu bedenken ist bei der Auswahl der Art der Information auch, dass die Erfüllung der Informationsverpflichtung gegebenenfalls nachgewiesen werden können muss.

Von den gesetzlich erforderlichen Informationen ist der Name des Unternehmens nicht umfasst. Es ist daher prinzipiell denkbar bei einer Benachrichtigung der Betroffenen einen externen Datenschutzbeauftragten oder gar ein spezialisiertes, externes Call Center zu nutzen. Diese Möglichkeit sollte im Einzelfall geprüft werden. Es ist allerdings denkbar, dass das Fehlen des Unternehmensnamens beabsichtigt ist, da die Nennung des Unternehmens meistens nur zu einem PR-Schaden führt, die Sicherheit allerdings nicht erhöht wird bzw. dieser sogar schaden kann.

Der DB-Krisenstab schlägt dem Vorstand eine dem Vorgang angemessene Kommunikationsform für den Einzelfall vor. Der Vorstand entscheidet anschließend, bzw. unter vorheriger fachlicher Einschätzung durch den Datenschutzbeauftragten und/oder die AL Compliance & Recht oder einen fachkundigen Externen, über den geeigneten Kommunikationsweg.

5. ANHANG

5.1. Erwägungsgründe zu den Art. 33 und Art. 34 DSGVO und dieser Richtlinie:

(75) Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem physischen, materiellen oder immateriellen Schaden führen könnte, insbesondere wenn die Verarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einem finanziellen Verlust, einer Rufschädigung, einem Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden personenbezogenen Daten, der unbefugten Aufhebung der Pseudonymisierung oder anderen erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht oder daran gehindert werden, die sie betreffenden personenbezogenen Daten zu kontrollieren, wenn personenbezogene Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft hervorgehen, und genetische Daten, Gesundheitsdaten oder das Sexualleben oder strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln betreffende Daten verarbeitet werden, wenn persönliche Aspekte bewertet werden, insbesondere wenn Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel betreffen, analysiert oder prognostiziert werden, um persönliche Profile zu erstellen oder zu nutzen, wenn personenbezogene Daten schutzbedürftiger natürlicher Personen, insbesondere Daten von Kindern, verarbeitet werden oder wenn die Verarbeitung eine große Menge personenbezogener Daten und eine große Anzahl von betroffenen Personen betrifft.

(76) Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwe-cke der Verarbeitung bestimmt werden. Das Risiko sollte anhand einer objektiven Bewer-tung beurteilt werden, bei der festgestellt wird, ob die Datenverarbeitung ein Risiko oder ein hohes Risiko birgt.

(85) Eine Verletzung des Schutzes personenbezogener Daten kann — wenn nicht rechtzeitig und angemessen reagiert wird — einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person. Deshalb sollte der Verantwortliche, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Aufsichtsbehörde von der Verletzung des Schutzes personenbezogener Daten unverzüglich und, falls möglich, binnen höchstens 72 Stunden, nachdem ihm die Verletzung bekannt wurde, unterrichten, es sei denn, der Verantwortliche kann im Einklang mit dem Grundsatz der Rechenschaftspflicht nachweisen, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem

Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt. Falls diese Benachrichtigung nicht binnen 72 Stunden erfolgen kann, sollten in ihr die Gründe für die Verzögerung angegeben werden müssen, und die Informationen können schrittweise ohne unangemessene weitere Verzögerung bereitgestellt werden.

(86) Der für die Verarbeitung Verantwortliche sollte die betroffene Person unverzüglich von der Verletzung des Schutzes personenbezogener Daten benachrichtigen, wenn diese Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt, damit diese die erforderlichen Vorkehrungen treffen können. Die Benachrichtigung sollte eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten sowie an die betroffene natürliche Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung enthalten. Solche Benachrichtigungen der betroffenen Person sollten stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Aufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden wie beispielsweise Strafverfolgungsbehörden erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müssten betroffene Personen sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.

(87) Es sollte festgestellt werden, ob alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen getroffen wurden, um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können. Bei der Feststellung, ob die Meldung unverzüglich erfolgt ist, sollten die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren Folgen und nachteilige Auswirkungen für die betroffene Person berücksichtigt werden. Die entsprechende Meldung kann zu einem Tätig-werden der Aufsichtsbehörde im Einklang mit ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen führen.

(88) Bei der detaillierten Regelung des Formats und der Verfahren für die Meldung von Verletzungen des Schutzes personenbezogener Daten sollten die Umstände der Verletzung hinreichend berücksichtigt werden, beispielsweise ob personenbezogene Daten durch geeignete technische Sicherheitsvorkehrungen geschützt waren, die die Wahrscheinlichkeit eines Identitätsbetrugs oder anderer Formen des Datenmissbrauchs wirksam verringern. Überdies sollten solche Regeln und Verfahren den berechtigten Interessen der Strafverfolgungsbehörden in Fällen Rechnung tragen, in denen die Untersuchung der Umstände einer Verletzung des Schutzes personenbezogener Daten durch eine frühzeitige Offenlegung in unnötiger Weise behindert würde