Der Bayerische Landesbeauftragte
für den Datenschutz

Meldepflicht und Benachrichtigungspflicht des Verantwortlichen

Erläuterungen zu Art. 33 und 34 Datenschutz-Grundverordnung

Orientierungshilfe

Herausgeber:

Der Bayerische Landesbeauftragte für den Datenschutz
80538 München | Wagmüllerstraße 18
Telefon: +49 89 21 26 72-0
E-Mail: poststelle@datenschutz-bayern.de
https://www.datenschutz-bayern.de

Bearbeiter:

Dr. Kai Engelbrecht

Version 1.0 | Stand: 1. Juni 2019

Diese Orientierungshilfe wird ausschließlich in elektronischer Form bereitgestellt. Sie kann im Internet auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018“ abgerufen werden.

Die PDF-Datei ist für den doppelseitigen Ausdruck optimiert.

Vorwort

Die Datenschutzreform 2018 hat eine Meldepflicht für Verletzungen des Schutzes personenbezogener Daten eingeführt (Art. 33 Datenschutz-Grundverordnung – DSGVO[1]). Unter bestimmten Voraussetzungen wird diese Meldepflicht um eine Pflicht zur Benachrichtigung betroffener Personen über eine Datenschutzverletzung ergänzt (Art. 34 DSGVO). Diese Vorgaben gelten grundsätzlich auch für bayerische öffentliche Stellen. Die neuen Regelungen haben sich in der Datenschutzpraxis bereits etabliert. Ich erhalte von bayerischen öffentlichen Stellen nahezu täglich Meldungen nach Art. 33 DSGVO. Die Melde- und die Benachrichtigungspflicht sind zudem immer wieder Gegenstand von Beratungsanfragen.

Die vorliegende Orientierungshilfe erläutert die Bestimmungen in Art. 33 und 34 DSGVO. Schwerpunkte liegen beim Merkmal der Datenschutzverletzung – das nicht mit einem Verstoß gegen datenschutzrechtliche Vorschriften gleichzusetzen ist, vielmehr den Aspekt der Datensicherheit in den Blick nimmt – sowie bei der Risikobeurteilung, die sowohl Art. 33 wie auch Art. 34 DSGVO erfordert. Zur Sprache kommt ferner der Handlungsablauf von der Feststellung einer Datenschutzverletzung in einer arbeitsteiligen Organisation bis zur Erfüllung der Melde- und der Benachrichtigungspflicht. Hinweise zum Umgang mit dem auf meiner Internetpräsenz bereitgestellten Online-Meldeformular runden die Orientierungshilfe ab. Berücksichtigung finden auch Besonderheiten im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz (RLDSJ).[2]

Um die Benutzung der Orientierungshilfe zu erleichtern, sind die einschlägigen Normtexte vorangestellt. Merkmale oder Merkmalsgruppen in den Vorschriften sind mit Verweisen auf die Randnummern der Erläuterungen versehen. Verbesserungsvorschläge sind willkommen und erreichen mich unter orientierungshilfen@datenschutz-bayern.de.

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, ABl. L 119 vom 4. Mai 2016, S. 1, berichtigt ABl. L 314 vom 22. November 2016, S. 72, und ABl. L 127 vom 23. Mai 2018, S. 2).

[2] 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 (ABl. L 119 vom 4. Mai 2016, S. 89).

Inhaltsverzeichnis

I. Erste Orientierung ... 13

II. Datenschutzverletzung als Anknüpfungspunkt von Meldepflicht und Benachrichtigungspflicht ... 14
1. Verletzungsverhalten ... 14
a) Nichtbeachtung von normativen Vorgaben ... 14
b) Überwindung technischer Vorkehrungen ... 15
c) Organisatorisches Fehlverhalten ... 15
2. Verletzungserfolg ... 17
a) Beeinträchtigung der Datenverfügbarkeit ... 17
b) Beeinträchtigung der Datenintegrität ... 18
c) Beeinträchtigung der Datenvertraulichkeit ... 18
3. Datenschutzverletzung bei unklarer Tatsachengrundlage ... 19

III. Risikobeurteilung bei Meldepflicht und Benachrichtigungspflicht ... 21
1. Erster Schritt: Gewinnung der Beurteilungsgrundlage ... 22
a) Datenschutzverletzung und Umgebungsbedingungen ... 22
b) Art, Sensibilität und Umfang der betroffenen personenbezogenen Daten ... 23
c) Identifizierbarkeit betroffener Personen ... 24
d) Besondere Eigenschaften betroffener Personen ... 25
e) Besondere Eigenschaften des Verantwortlichen ... 25
f) Zahl betroffener Personen ... 25
2. Zweiter Schritt: Risikoanalyse ... 25
a) Mögliche Nachteile ... 26
b) Bewertung der möglichen Nachteile ... 28
aa) Bewertung der möglichen Nachteile nach ihrer Schwere ... 29
bb) Bewertung der möglichen Nachteile nach ihrer Eintrittswahrscheinlichkeit ... 31
3. Dritter Schritt: Gesamtbewertung, Ergebnis der Risikobeurteilung ... 32

IV. Meldepflicht des Verantwortlichen gegenüber der Datenschutz-Aufsichtsbehörde (Art. 33 DSGVO) ... 34
1. Verantwortlicher, zuständige Aufsichtsbehörde ... 34
2. Entstehen der Meldepflicht ... 35
a) Zeitpunkt ... 35
b) Kenntniszurechnung ... 36
3. Erfüllung der Meldepflicht ... 37
a) Grundsatz ... 37
b) Insbesondere: Berechnung der 72-Stunden-Frist ... 38
c) Umfang der Meldung ... 39
4. Organisatorische Vorkehrungen ... 40

V. Meldepflicht des Auftragsverarbeiters ... 41

Inhaltsverzeichnis

VI. Benachrichtigungspflicht des Verantwortlichen gegenüber der betroffenen Person (Art. 34 DSGVO) 42
1. Verantwortlicher, betroffene Personen 42
2. Entstehen der Benachrichtigungspflicht 42
3. Ausschluss der Benachrichtigungspflicht 43
a) Ausschluss bei vorsorglicher Risikoabschirmung 43
b) Ausschluss bei nachträglicher Risikominimierung 43
c) Ausschluss bei unverhältnismäßigem Aufwand 44
d) Ausschluss zum Schutz bestimmter rechtlich geschützter Belange 44
aa) Abwehr von Nachteilen zulasten der Allgemeinheit 44
bb) Verfolgung von Straftaten und Ordnungswidrigkeiten 45
cc) Abwehr von Nachteilen zulasten Dritter 45
3. Erfüllung der Benachrichtigungspflicht 46

VII. Meldepflicht und Benachrichtigungspflicht im Bereich der Datenschutz-Richtlinie für Polizei und Strafjustiz 47
1. Grundgedanken der Umsetzung 47
2. Regelungen im Einzelnen 48

VIII. Dokumentation 50
1. Allgemeines 50
2. Hinweise zur Nutzung des Online-Meldeformulars 50
a) Art der Meldung 50
b) Zeitpunkt der Meldung 51
c) Art der Verletzung des Schutzes personenbezogener Daten 52
d) Betroffene personenbezogene Daten 56
e) Folgen der Verletzung des Schutzes personenbezogener Daten 59
f) Beschreibung der ergriffenen oder geplanten Maßnahmen 60
aa) Maßnahmen zur Behebung des Vorfalls und zur Abmilderung von nachteiligen Auswirkungen 61
bb) Information der betroffenen Personen 62

IX. Folgen von Pflichtverstößen 64

Normtexte

Datenschutz-Grundverordnung

Art. 4 – Begriffsbestimmungen – Auszug –

Im Sinne dieser Verordnung bezeichnet der Ausdruck

[…]

12. „Verletzung des Schutzes personenbezogener Daten“ Rn. 4 ff. eine Verletzung der Sicherheit Rn. 6, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, Rn. 11 zur Veränderung, Rn. 14 oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang Rn. 16 zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

[…].

Art. 33 – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

(1) Im Falle Rn. 17 ff. einer Verletzung des Schutzes personenbezogener Daten Rn. 4 ff. meldet der Verantwortliche Rn. 63 f. unverzüglich Rn. 74 und möglichst binnen 72 Stunden Rn. 76 ff., nachdem ihm die Verletzung bekannt wurde Rn. 68 ff., diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde Rn. 65, es sei denn, Rn. 68 ff. dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko Rn. 21 ff. für die Rechte und Freiheiten Rn. 47 natürlicher Personen Rn. 46 führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, Rn. 76 ff. so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich. Rn. 88 ff.

(3) Die Meldung gemäß Absatz 1 enthält zumindest folgende Informationen:

a) eine Beschreibung der Art Rn. 29 ff., 129 ff. der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, Rn. 35 ff., 38, 41 der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze; Rn. 144 ff.

b) den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten; Rn. 45 ff., 159 ff.

d) 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. Rn. 31, 57, 97 f., 165 ff.

(4) 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. Rn. 85, 124 f., 143

(5) Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, von deren Auswirkungen und der ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen dieses Artikels ermöglichen. Rn. 121 ff.

Art. 34 – Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten Rn. 4 ff. voraussichtlich ein hohes Risiko Rn. 21 ff. für die persönlichen Rechte und Freiheiten Rn. 47 natürlicher Personen Rn. 46 zur Folge, so benachrichtigt der Verantwortliche Rn. 63 f. die betroffene Person unverzüglich Rn. 74 von der Verletzung.

(2) Die in Absatz 1 genannte Benachrichtigung der betroffenen Person beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält zumindest die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Maßnahmen. Rn. 107

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen 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, Rn. 96 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; Rn. 97

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. Rn. 99 f.

(4) Wenn der Verantwortliche die betroffene Person nicht bereits über die Verletzung des Schutzes personenbezogener Daten benachrichtigt hat, kann die Aufsichtsbehörde unter Berücksichtigung der Wahrscheinlichkeit, mit der die Verletzung des Schutzes personenbezogener Daten zu einem hohen Risiko führt, von dem Verantwortlichen verlangen, dies nachzuholen, oder sie kann mit einem Beschluss feststellen, dass bestimmte der in Absatz 3 genannten Voraussetzungen erfüllt sind. Rn. 173

Verordnung (EWG, EURATOM) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine

Artikel 1

Diese Verordnung gilt, soweit nichts anderes bestimmt ist, für die Rechtsakte, die der Rat und die Kommission auf Grund des Vertrages zur Gründung der Europäischen Wirtschaftsgemeinschaft oder des Vertrages zur Gründung der Europäischen Atomgemeinschaft erlassen haben bzw. erlassen werden. Rn. 76

Artikel 2

(1) Für die Anwendung dieser Verordnung sind die Feiertage zu berücksichtigen, die als solche in dem Mitgliedstaat oder in dem Organ der Gemeinschaften vorgesehen sind, bei dem eine Handlung vorgenommen werden soll.

Zu diesem Zweck übermittelt jeder Mitgliedstaat der Kommission die Liste der Tage, die nach seinen Rechtsvorschriften als Feiertage vorgesehen sind. Die Kommission veröffentlicht im Amtsblatt der Europäischen Gemeinschaften die von den Mitgliedstaaten übermittelten Listen, die durch Angabe der in den Organen der Gemeinschaften als Feiertage vorgesehenen Tage ergänzt worden sind.

(2) Für die Anwendung dieser Verordnung sind als Arbeitstage alle Tage außer Feiertagen, Sonntagen und Sonnabenden zu berücksichtigen.

Artikel 3
– Auszug –

(1) Ist für den Anfang einer nach Stunden bemessenen Frist der Zeitpunkt maßgebend, in welchem ein Ereignis eintritt oder eine Handlung vorgenommen wird, so wird bei der Berechnung dieser Frist die Stunde nicht mitgerechnet, in die das Ereignis oder die Handlung fällt. Rn. 77 f.

Ist für den Anfang einer nach Tagen, Wochen, Monaten oder Jahren bemessenen Frist der Zeitpunkt maßgebend, in welchem ein Ereignis eintritt oder eine Handlung vorgenommen wird, so wird bei der Berechnung dieser Frist der Tag nicht mitgerechnet, in den das Ereignis oder die Handlung fällt.

(2) Vorbehaltlich der Absätze 1 und 4 gilt folgendes:

a) Eine nach Stunden bemessene Frist beginnt am Anfang der ersten Stunde und endet mit Ablauf der letzten Stunde der Frist. Rn. 79

b) Eine nach Tagen bemessene Frist beginnt am Anfang der ersten Stunde des ersten Tages und endet mit Ablauf der letzten Stunde des letzten Tages der Frist.

[…]

(3) Die Fristen umfassen die Feiertage, die Sonntage und die Sonnabende, soweit diese nicht ausdrücklich ausgenommen oder die Fristen nach Arbeitstagen bemessen sind. Rn. 80

(4) Fällt der letzte Tag einer nicht nach Stunden bemessenen Frist auf einen Feiertag, einen Sonntag oder einen Sonnabend, so endet die Frist mit Ablauf der letzten Stunde des folgenden Arbeitstags. Rn. 80

Diese Bestimmung gilt nicht für Fristen, die von einem bestimmten Datum oder einem bestimmten Ereignis an rückwirkend berechnet werden.

(5) Jede Frist von zwei oder mehr Tagen umfaßt mindestens zwei Arbeitstage. Rn. 81 f.

Bayerisches Datenschutzgesetz

Art. 6 – Zweckbindung (zu Art. 6 Abs. 3 und 4 DSGVO) – Auszug –

(2) Eine Verarbeitung zu anderen Zwecken als zu denjenigen, zu denen die Daten erhoben wurden, ist unbeschadet der Bestimmungen der DSGVO zulässig, wenn
[…]
3. die Verarbeitung erforderlich ist
   a) zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und Ordnung, Rn. 102 ff.
   b) zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen, Rn. 103 f.
   […]
   d) zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person, Rn. 106
   […].

Art. 13 – Benachrichtigung bei Datenschutzverletzungen (zu Art. 34 DSGVO)

Die Benachrichtigung kann auch unter den Voraussetzungen des Art. 6 Abs. 2 Nr. 3 Buchst. a, b oder Buchst. d unterbleiben. Rn. 101

Art. 28 – Anwendungsbereich dieses Kapitels – Auszug –

(1) [1]Die Vorschriften dieses Kapitels gelten, soweit nichts anderes bestimmt ist, für die Verarbeitung personenbezogener Daten durch
1. die Polizei,
2. die Gerichte in Strafsachen und die Staatsanwaltschaften,
3. die Strafvollstreckungs- und Justizvollzugsbehörden,
4. die Behörden des Maßregelvollzugs

zum Zwecke der Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. [2]Die Vorschriften dieses Kapitels gelten auch für sonstige Behörden im Sinne des Art. 1 Abs. 1 Satz 1, soweit diese personenbezogene Daten verarbeiten, um Straftaten oder Ordnungswidrigkeiten zu verfolgen oder zu ahnden. Rn. 111

(2) [1]Unbeschadet anderer Rechtsvorschriften finden auf Verarbeitungen nach Abs. 1 abweichend von Art. 2 nur Anwendung:
[…]
3. aus dem Kapitel IV DSGVO über Verantwortliche und Auftragsverarbeiter die Art. 24 Abs. 1 und 2, Art. 25 Abs. 1 und 2, Art. 28 Abs. 1 bis 4, 9 und 10, Art. 29, 31, 34, 36 Abs. 4, Art. 37 Abs. 1 und 3 bis 7, Art. 38 und 39 DSGVO, Rn. 112 f.

[…]
[2]Im Übrigen finden aus dem Kapitel II DSGVO über Grundsätze Art. 9 Abs. 1 und 2, aus dem Kapitel IV DSGVO über Verantwortliche und Auftragsverarbeiter die Art. 26, 30, 32 und 33 DSGVO Rn. 112 f. sowie aus dem Kapitel VI DSGVO über unabhängige Aufsichtsbehörden die Art. 57 und 58 DSGVO nach Maßgabe der nachfolgenden Vorschriften dieses Kapitels Anwendung.

Art. 33 – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Wenn Daten von oder an den Verantwortlichen eines anderen Mitgliedstaates übermittelt wurden, sind die Informationen nach Art. 33 Abs. 3 DSGVO unverzüglich auch an diesen zu melden. Rn. 115 f.

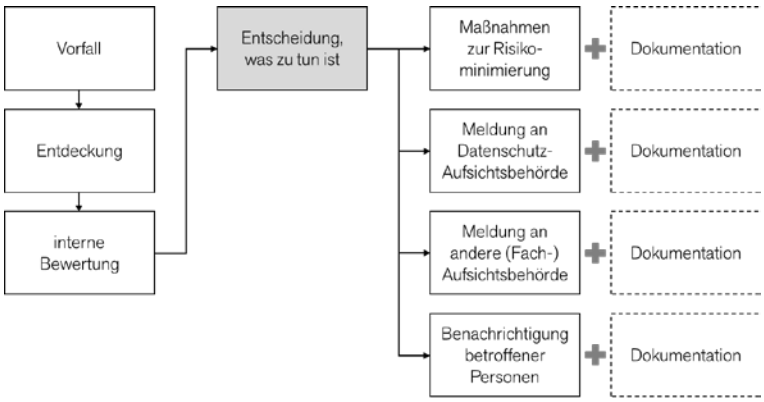
Art. 36 – Vertrauliche Meldung von Datenschutzverstößen

[1]Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können. Rn. 117 ff. [2]Art. 12 Abs. 2 gilt für die zur Entgegennahme dieser Meldungen betraute Stelle entsprechend. Rn. 118 f.

I. Erste Orientierung

Jeder Verantwortliche ist stets bestrebt, Datenschutzverletzungen zu vermeiden. Ereignen sie sich bei bayerischen öffentlichen Stellen, sind regelmäßig personenbezogene Daten von Bürgerinnen und Bürgern oder von Beschäftigten betroffen. Eine Datenschutzverletzung enttäuscht Vertrauen. Sie verursacht Mehrarbeit und Kosten. Auch das beste Risikomanagement – unter Einschluss sorgfältig erstellter und anschließend handlungsleitend gewordener Datenschutz-Folgenabschätzungen – kann Datenschutzverletzungen nie vollkommen ausschließen. 1

Daher sollte jeder Verantwortliche den Fall einer Datenschutzverletzung in seinen Planungen von vornherein berücksichtigen. Er sollte insbesondere über eine Aufbau- und Ablauforganisation verfügen, die dabei hilft, mit einer Datenschutzverletzung adäquat umzugehen. Der Verantwortliche muss in der Lage sein, Datenschutzverletzungen frühzeitig zu erkennen, in Bezug auf die mit ihnen verbundenen Risiken einzuschätzen und die erforderlichen Maßnahmen zu ergreifen. Das sind in erster Linie Vorkehrungen, die den durch die Datenschutzverletzung geschaffenen Risiken entgegenwirken. Zudem muss der Verantwortliche Melde- und Benachrichtigungspflichten nach der Datenschutz-Grundverordnung erfüllen, daneben auch fachrechtliche Benachrichtigungspflichten sowie Dokumentationspflichten. Die Datenschutz-Grundverordnung verlangt bei einer Datenschutzverletzung also eine komplexe, insgesamt auf eine Ausschaltung von Risiken gerichtete Reaktion. Der Grundsatz „Melden befreit“ gilt für den Verantwortlichen gerade nicht. 2



Die vorliegende Orientierungshilfe befasst sich mit zwei Pflichten aus diesem Pflichtenkreis: der Meldepflicht, die Art. 33 DSGVO dem Verantwortlichen im Fall einer Datenschutzverletzung auferlegt, sowie der Benachrichtigungspflicht, die ihm nach Maßgabe von Art. 34 DSGVO gegenüber betroffenen Personen auferlegt ist. 3

II. Datenschutzverletzung als Anknüpfungspunkt von Meldepflicht und Benachrichtigungspflicht

4 Anknüpfungspunkt für die Meldepflicht nach Art. 33 DSGVO und die Benachrichtigungspflicht nach Art. 34 DSGVO ist eine „Verletzung des Schutzes personenbezogener Daten". Eine solche Verletzung liegt nicht in jedem Verstoß gegen datenschutzrechtliche Vorschriften, sie bezieht sich vielmehr gerade auf die **Datensicherheit**. Art. 4 Nr. 12 DSGVO bestimmt:

> „‚Verletzung des Schutzes personenbezogener Daten' [ist] 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".

5 Bei der Feststellung einer Datensicherheitsverletzung – hier einer gängigeren Terminologie folgend als „Datenschutzverletzung" bezeichnet – sollten **Verletzungsverhalten** (1.) und **Verletzungserfolg** (2.) unterschieden werden. Schwierigkeiten kann eine unklare **Tatsachengrundlage** bereiten (3.).

1. Verletzungsverhalten

6 Das **Verletzungsverhalten** ist in Art. 4 Nr. 12 DSGVO nach der „Angriffsart" (etwa: Nutzen ausspionierter Passwörter, Einschleusen von Schadsoftware) nicht näher spezifiziert. Gleichwohl begründet nicht jede Handlung oder Unterlassung eine Datenschutzverletzung, so sie nur einen tatbestandsmäßigen Verletzungserfolg nach sich zieht. Es muss sich bei ihr vielmehr um eine **„Verletzung der Sicherheit"** (von personenbezogenen Daten) handeln. Ein Verhalten ist als Verletzung der Sicherheit zu werten, wenn die betreffende Person normative – insbesondere organisatorische – Vorgaben nicht beachtet oder technische Vorkehrungen überwindet, die der Verantwortliche jeweils nach Art. 32 DSGVO getroffen hat. Ein Verschulden ist nicht erforderlich. **Drei Konstellationen** sollten unterschieden werden:

a) Nichtbeachtung von normativen Vorgaben

7 Die **Nichtbeachtung von normativen Vorgaben** des Verantwortlichen hinsichtlich der Datensicherheit (Art. 32 DSGVO) ist ein Verletzungsverhalten, das typischerweise Personen aus der Sphäre des Verantwortlichen verwirklichen. Dabei kann es sich insbesondere um eigene Beschäftigte handeln oder um Beschäftigte, die für einen Auftragsverarbeiter des Verantwortlichen tätig sind. Sind die Vorgaben dagegen berücksichtigt – hat die Person insbesondere die ihr nach dem Berechtigungskonzept zukommende Rolle nicht verlassen –, so

begründet ein (sonst) rechtswidriger Datenumgang grundsätzlich keine Verletzung der Sicherheit. Dies gilt selbst dann, wenn ein Verletzungserfolg eintreten sollte.

Beispiel 1: Ein Personalsachbearbeiter in einer Gemeinde nutzt einen privaten USB-Stick an seinem dienstlichen PC; dabei wird ohne sein Wissen eine Schadsoftware aufgespielt, die sich im gemeindlichen Netzwerk alsbald weiter verbreitet. Die Nutzung externer Datenträger am dienstlichen PC war durch Dienstanweisung untersagt. – Verletzung der Sicherheit, weil eine Vorgabe nicht beachtet wurde, die das System vor unkontrolliert eingebrachter Software schützen soll.

Beispiel 2: Eine Beamtin verschafft sich an einem verlassenen und nicht gesperrten PC eines Kollegen einen im Berechtigungskonzept ihrer Dienststelle nicht vorgesehenen Zugang zu einer dienstlichen Datei und teilt Inhalte einem Dritten mit. – Verletzung der Sicherheit, weil die Beamtin außerhalb ihrer Zugriffsberechtigung agiert; unter Umständen auch Verletzung der Sicherheit, wenn ihr Kollege bei Abwesenheit seinen PC entgegen einer Dienstanweisung nicht gesperrt hat, oder wenn die Behörde eine solche Regelung versäumt hat.

Gegenbeispiel: Der Personalsachbearbeiter erteilt einem einzelnen Gemeinderatsmitglied Auskunft aus der Personalakte eines Kollegen, obwohl Art. 108 Bayerisches Beamtengesetz (BayBG) dies nicht zulässt. – Keine Verletzung der Sicherheit; zwar ist Art. 108 BayBG nicht beachtet und die Vertraulichkeit der Personalaktendaten beeinträchtigt; dies beruht jedoch nicht auf einer Handlung, die (gerade) Vorgaben nach Art. 32 DSGVO außer Acht lässt.

b) Überwindung technischer Vorkehrungen

Die **Überwindung technischer Vorkehrungen** (Art. 32 DSGVO) ist dagegen ein Verletzungsverhalten, das typischerweise externe Angreiferinnen oder Angreifer verwirklichen. Solche Personen sind im Allgemeinen nicht berechtigt, mit den beim Verantwortlichen vorgehaltenen personenbezogenen Daten umzugehen. Datenschutzverletzungen im Sinne von Art. 4 Nr. 12 DSGVO müssen daher nicht gegen (sonstige) Datenschutzverstöße abgegrenzt werden. Die Kenntnisnahme durch den Verantwortlichen unbeabsichtigt oder unrechtmäßig bereitgestellter Informationen gehört in diese Fallgruppe ebenso wenig wie die Nutzung „an die Öffentlichkeit gelangter" Zugangspasswörter. 8

Beispiele: Ein Nichtberechtigter dringt mittels eines „Wörterbuchangriffs" in das Ratsinformationssystem einer Stadt ein und lädt Unterlagen für nichtöffentliche Stadtratssitzungen herunter. – Eine Angreiferin schickt unter dem Namen eines Arztes einen Befundbericht mit Bilddateien an ein Krankenhaus. Die Bilddateien werden gutgläubig geöffnet. In der Folge stellt sich heraus, dass in ihnen ein Datenträger verschlüsselndes Schadprogramm versteckt ist.

c) Organisatorisches Fehlverhalten

Nur der Verantwortliche – genauer: eine Person, welche Aufgaben des Verantwortlichen wahrzunehmen hat – kann einen Verletzungserfolg durch **organisatorisches Fehlverhalten** verursachen. Der Verantwortliche versäumt es hier gerade, die nach Art. 32 DSGVO erforderlichen Maßnahmen – insbesondere eine Implementierung organisatorischer Stan- 9

dards in entsprechenden Vorgaben, etwa Dienstanweisungen, oder eine Implementierung von Vorkehrungen nach dem Stand der Technik, etwa der Konfiguration eines Internetbrowsers oder E-Mail-Clients – zu treffen. Eine solche Datenschutzverletzung kann auch zweiaktig sein: Der Verantwortliche unterlässt gebotene Vorkehrungen zur Gewährleistung der Datensicherheit; Beschäftigte oder außenstehende Personen nutzen das Defizit, um „ungehindert" einen Verletzungserfolg herbeizuführen.

Beispiel 1 (einaktig): Ein öffentliches Krankenhaus will einen Befund einem nachbehandelnden Arzt zuleiten. Eine Hilfskraft steckt das Schreiben ins Telefaxgerät und tippt neben einem Telefongespräch schnell die schon hundertmal gewählte Nummer ein – ohne hinzusehen. Das Telefax geht einem anderen Empfänger zu, der sich an den behördlichen Datenschutzbeauftragten wendet. Dieser stellt fest, dass eine Regelung zum Versand von Befunden per Telefax nicht getroffen ist. – Verletzung der Sicherheit, weil der Verantwortliche technisch-organisatorische Maßnahmen[3] versäumt hat, die bei der Nutzung einer fehleranfälligen Technologie zu treffen sind.

Beispiel 2 (ebenfalls einaktig): Eine Kuvertiermaschine ordnet auf Grund fehlerhafter Einstellungen adressierte Bescheide anders adressierten Umschlägen zu oder legt in Umschläge mehrere Schriftstücke an verschiedene Adressaten ein. – Verletzung der Sicherheit, weil anzunehmen ist, dass der Verantwortliche bei den Einstellungen nachlässig war und/oder keine Ursachenerforschung betrieben hat.

Beispiel 3 (zweiaktig): Den Zugang zum Ratsinformationssystem einer Gemeinde haben alle Gemeinderatsmitglieder mit demselben voreingestellten Passwort bekommen. Die meisten haben das Passwort nicht geändert. Mittlerweile ist es ortsbekannt. Interessierte nutzen das Passwort, um Zugang zu den Sitzungsunterlagen der nichtöffentlichen Gemeinderatssitzungen zu erlangen, unter denen sich – entgegen den Empfehlungen der zuständigen Datenschutz-Aufsichtsbehörde[4] – auch Informationen zu Personalangelegenheiten in Einzelfällen befinden. – Verletzung der Sicherheit; die Interessierten nutzen nur allgemein zugängliche Informationen, allerdings hat es die Gemeinde versäumt, ein den fachlichen Standards entsprechendes Berechtigungskonzept[5] einzurichten.

10 Das organisatorische Fehlverhalten tritt nicht selten in mehreren „an sich" unscheinbaren Ereignissen zutage. So können insbesondere wiederkehrende, auf fehlerhafter Rechtsanwendung beruhende Datenübermittlungen darauf hinweisen, dass der Verantwortliche bislang keine ausreichenden technisch-organisatorischen Maßnahmen zur Minimierung von Rechtsanwendungsfehlern – wie etwa die Anordnung des „Vier-Augen-Prinzips", der stichprobenartigen Kontrolle durch Vorgesetzte oder einer nachvollziehbaren Protokollierung –

[3] Zum organisatorischen Standard siehe Bayerischer Landesbeauftragter für den Datenschutz, Datensicherheit beim Telefax-Dienst, im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Themengebiete – Technik und Organisation – Datensicherheit beim Telefax-Dienst".

[4] Siehe dazu Bayerischer Landesbeauftragter für den Datenschutz, 21. Tätigkeitsbericht 2004, Beitrag Nr. 16.2 „Personaldaten im Gemeinderat", im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Tätigkeitsberichte".

[5] Vgl. etwa Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, ORP.4 Identitäts- und Berechtigungsmanagement, im Internet abrufbar auf https://www.bsi.bund.de in der Rubrik „Themen – IT-Grundschutz – IT-Grundschutz-Kompendium".

getroffen hat. Daher sollte der Verantwortliche sicherstellen, dass Ereignisse dieser Art intern an eine zentrale Stelle weitergegeben und diese Hinweise auf Unregelmäßigkeiten in festen Zeitabständen ausgewertet werden. Bei dieser Auswertung kann sich ergeben, dass ein organisatorisches Fehlverhalten vorliegt, welches die Meldepflicht nach Art. 33 Abs. 1 DSGVO auslöst.

2. Verletzungserfolg

a) Beeinträchtigung der Datenverfügbarkeit

Die **Verfügbarkeit der personenbezogenen Daten** ist in den Fällen der Vernichtung und des Verlustes betroffen: **11**

– Nach einer **Vernichtung** kann niemand mehr auf die Daten zugreifen, weil sie nicht mehr vorhanden sind.

  Ein **typisches Verletzungsverhalten**, das zu diesem Verletzungserfolg führt, ist das nicht revidierbare Löschen oder Überschreiben eines Datenträgers sowie dessen endgültige physische Zerstörung. Wegen Art. 2 Satz 1 Bayerisches Datenschutzgesetz (BayDSG) gilt dies auch für die Entsorgung einer Papierakte mittels Aktenvernichter.

– Beim **Verlust** bleiben die Daten erhalten, jedoch lösen sich die faktischen Zugriffsmöglichkeiten so von den seitens des Verantwortlichen erteilten Zugriffsberechtigungen, dass der Verantwortliche oder seine Beschäftigten entweder gar nicht mehr oder jedenfalls nicht mehr ohne Mitwirkung eines nichtberechtigten Dritten auf die personenbezogenen Daten zugreifen können.

  Ein **typisches Verletzungsverhalten**, das zu diesem Verletzungserfolg führt, ist der Eingriff in die vom Verantwortlichen vorgesehene Ordnung der Zugriffsberechtigungen eines Dateisystems durch Externe („Hacker“) oder nichtberechtigte Interne. Auch Verhaltensweisen, die sich auf Schlüssel für einzelne verschlüsselte Dateien beziehen, kommen in Betracht, so das Vergessen des Passworts durch den einzigen Zugriffsberechtigten oder ein Angriff mittels Ransomware, aber auch das Abhandenkommen von Datenträgern (einschließlich Papierakten).

Eine Verletzung des Schutzes personenbezogener Daten kann auch dann vorliegen, wenn die **Verfügbarkeit** personenbezogener Daten lediglich **vorübergehend eingeschränkt** ist. Bei der Einordnung eines Vorfalls sollte berücksichtigt werden, für welchen Zeitraum die Verfügbarkeit beeinträchtigt ist, außerdem, ob und inwieweit die Situation beherrschbar ist. **12**

Eine **„planmäßige“ Einschränkung der Verfügbarkeit** im Rahmen von Wartungsmaßnahmen des Verantwortlichen ist grundsätzlich nicht als Datenschutzverletzung[6] zu werten. **13**

[6] Ein alternativer Lösungsansatz ist das Ausscheiden bagatellmäßiger Verfügbarkeitsdefizite im Rahmen der Risikobeurteilung, so wohl Artikel 29-Datenschutzgruppe, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679, WP 250 (rev.01), S. 9 f., im In-

Auch eine kurzzeitige Störung bei den Zugriffsmöglichkeiten, die vom Verantwortlichen nach einer erprobten Handlungsroutine behoben werden kann, muss nicht als Datenschutzverletzung anzusehen sein. Dies gilt jedenfalls dann, wenn sie nicht auf einem Eingriff durch Externe oder nichtberechtigte Interne beruht. Dagegen stellt eine vorübergehende Beeinträchtigung der Verfügbarkeit personenbezogener Daten, die den Verantwortlichen „aus heiterem Himmel" trifft, eine spezifische Ursachenerforschung sowie spezifische Gegenmaßnahmen erfordert, eine Datenschutzverletzung dar.

b) Beeinträchtigung der Datenintegrität

14 Die **Integrität der personenbezogenen Daten** wird durch eine **Veränderung** beeinträchtigt. Hier bleibt ein Zugriff durch den Verantwortlichen und seine Beschäftigten unverändert möglich, doch „sagen" die Daten nun „etwas anderes aus" als vor der Einwirkung.

15 Ein **typisches Verletzungsverhalten**, das zu diesem Verletzungserfolg führt, ist der Austausch, das (partielle) Löschen und das Hinzufügen von personenbezogenen Daten in einer Datei oder einer Papierakte unter Missachtung organisatorischer Vorgaben oder unter Überwindung technischer Vorkehrungen des Verantwortlichen.

c) Beeinträchtigung der Datenvertraulichkeit

16 Die **Vertraulichkeit der personenbezogenen Daten** ist berührt, wenn die Datenschutzverletzung zu einer unbefugten Offenlegung von oder einem unbefugten Zugang zu personenbezogenen Daten führt.

– Bei einer **unbefugten Offenlegung** werden personenbezogene Daten unter Missachtung rechtlicher Vorgaben der Öffentlichkeit oder einem zu weiten Benutzerkreis bereitgestellt.

  Ein **typisches Verletzungsverhalten**, das zu diesem Verletzungserfolg führt, ist die fehlerhafte Adressierung eines Briefs oder einer E-Mail mit der Folge, dass Dritte von Daten einer betroffenen Person Kenntnis erhalten können, oder die nicht ordnungsgemäße Entsorgung von Papierakten, beispielsweise durch Einwurf von ärztlichen Befunden in eine gewöhnliche Mülltonne. Gleiches gilt für eine nicht ordnungsgemäße Planung oder Verwaltung von Zugriffsberechtigungen. Für den Verletzungserfolg ist es nicht erforderlich, dass Dritte von den unbefugt offengelegten Daten Kenntnis nehmen. Der Nachweis, dass diese Möglichkeit bestand, ist ausreichend.

  Grundsätzlich liegt dagegen keine Verletzung der Datensicherheit vor, wenn eine Mitarbeiterin oder ein Mitarbeiter einer Behörde personenbezogene Daten infolge fehlerhafter Anwendung einer Übermittlungsbefugnis an eine Stelle gelangen lässt, die von Gesetzes wegen in der konkreten Situation keine Kenntnis erlangen darf. In diesem Fall verstößt die Weitergabe allerdings anderweit gegen datenschutzrechtliche Vorschriften.

ternet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Orientierungs- und Praxishilfen – Meldung von Datenschutzverletzungen".

– Bei einem **unbefugten Zugang** steht demgegenüber das Handeln Externer im Vordergrund, die Schwachstellen in den vom Verantwortlichen ergriffenen Sicherheitsvorkehrungen ausnutzen.

  Ein t**ypisches Verletzungsverhalten**, das zu diesem Verletzungserfolg führt, ist das Ausspionieren – auch das unberechtigte Nutzen – von Benutzerpasswörtern oder von Schlüsseln, die für die Kenntnisnahme bestimmter Dateien erforderlich sind, ferner das Einschleusen von Spyware. Beschäftigte können etwa durch Behalten von Benutzerpasswörtern über das Ende ihrer Tätigkeit hinaus unbefugten Zugang erlangen oder durch Einräumung einer Zugangsmöglichkeit an einen Dritten gewähren. Unbefugten Zugang eröffnet in der analogen Welt ein nicht abgeschlossener Schrank, in dem Unterlagen mit personenbezogenen Daten aufbewahrt werden.

3. Datenschutzverletzung bei unklarer Tatsachengrundlage

Die Meldepflicht nach Art. 33 DSGVO knüpft an eine konkrete Datenschutzverletzung (Art. 33 Abs. 1 DSGVO: „[i]m Falle einer Verletzung des Schutzes personenbezogener Daten“). Entsprechendes gilt für die Benachrichtigungspflicht nach Art. 34 DSGVO. Unproblematisch ist daher der Fall, dass die Datenschutzverletzung in Verletzungsverhalten und Verletzungserfolg offen zutage liegt. 17

In **„atypischen“ Konstellationen** sollte eine bayerische öffentliche Stelle aus aufsichtsbehördlicher Sicht die folgenden Hinweise beachten: 18

– **Rückschluss aus einem eingetretenen Nachteil:** Ein die Meldepflicht auslösender Nachteil ist eingetreten; eine Datenschutzverletzung ist dafür Voraussetzung. Allerdings kann die Datenschutzverletzung nicht näher beschrieben werden; der Verantwortliche findet nicht heraus, wie sie zustandegekommen ist.

  Beispiel: Eine örtliche Tageszeitung veröffentlicht ein Dokument aus der Beilhilfeakte eines Gemeindebediensteten. Die behördliche Datenschutzbeauftragte kann lediglich feststellen, dass das Dokument nicht von dem Bediensteten selbst weitergegeben worden ist. Es muss „irgendwie“ aus der Personalakte – auf Grund einer Datenschutzverletzung oder durch eine schlicht rechtswidrige Übermittlung – an die Zeitung gelangt sein. Aus dem eingetretenen Nachteil – Kenntnisnahme zeitunglesender Personen von Gesundheitsdaten des Bediensteten – kann auf die immerhin mögliche Datenschutzverletzung rückgeschlossen werden.

  Reaktion: Der Verantwortliche erfüllt seine Pflichten nach Art. 33 und 34 DSGVO, soweit die weiteren Voraussetzungen gegeben sind.

– **Unbekanntes Verletzungsverhalten:** Ein Verletzungserfolg ist eingetreten. Der Verantwortliche kann aber das Verletzungsverhalten nicht näher beschreiben; er kann nicht ermitteln, was den Verletzungserfolg bewirkt hat.

  Beispiel: Einer behördlichen IT-Stelle fällt auf, dass ein Server ungewöhnlich hohe Datenmengen ins Internet verschickt. Sie kann ermitteln, dass Pakete mit personenbezo-

genen Daten abgeflossen sind, nicht jedoch, was die Ursache hierfür war. Fest steht nur, dass der Datenversand nicht beabsichtigt war. Von einer möglichen Datenschutzverletzung ist daher letztlich nur der Verletzungserfolg bekannt.

Reaktion: Von dem feststellbaren Verletzungserfolg kann jedenfalls auf ein solches Verletzungsverhalten rückgeschlossen werden, das zu seinen möglichen Ursachen gehört. Ist ein ausgeschlossen, dass ein Datenabfluss beabsichtigt war, kann dieser Symptom für die Aktivität einer Schadsoftware sein, jedoch auch für die Fehlfunktion einer technischen Komponente. Der Verantwortliche wird in einem solchen Fall annehmen, dass ein nach Art. 4 Nr. 12 DSGVO tatbestandsmäßiges Verletzungsverhalten vorliegt. Er erfüllt seine Pflichten nach Art. 33 und 34 DSGVO, soweit die weiteren Voraussetzungen dieser Vorschriften gegeben sind.

- **Verletzungsverhalten nachweisbar ohne Verletzungserfolg:** Ein (potenzielles) Verletzungsverhalten ist nachweisbar, ein Verletzungserfolg ist nachweislich nicht eingetreten. Reaktion: Eine Datenschutzverletzung ist nicht eingetreten, sodass weder eine Pflicht nach Art. 33 DSGVO noch eine Pflicht nach Art. 34 DSGVO zu erfüllen ist.

- **Verletzungsverhalten ohne nachweisbaren Verletzungserfolg:** Ein (potenzielles) Verletzungsverhalten ist belegt. Ob es zu einem ein Verletzungserfolg gekommen ist, bleibt aber unklar, weil es dem Verantwortlichen nicht gelingt, sich ein Bild von der Lage zu verschaffen.

  Beispiel: Eine gemeindliche IT-Stelle stellt fest, dass ein Account eines ausgeschiedenen Beschäftigten „auf einmal" wieder aktiv ist. Welche Rolle dieser nun im internen Netzwerk der Gemeinde spielt, kann nicht festgestellt werden. Jedenfalls ist nicht ausgeschlossen, dass über den Account personenbezogene Daten eingesehen, verändert oder gar gelöscht werden.

  Reaktion: Der Verantwortliche legt seiner weiteren Beurteilung des Vorfalls zugrunde, dass eine Datenschutzverletzung eingetreten ist und erfüllt seine Pflichten nach Art. 33 und 34 DSGVO, soweit die weiteren Voraussetzungen gegeben sind (vorläufige Meldung).

  Die Gleichbehandlung einer nur angenommenen Datenschutzverletzung mit einer nachweisbaren ist jedenfalls dann gerechtfertigt, wenn ein Verletzungserfolg mutmaßlich realisiert ist. Der Verantwortliche muss rechtskonforme Verarbeitungen gewährleisten (vgl. Art. 24 Abs. 1 DSGVO). Hinsichtlich einer Einhaltung der Verarbeitungsgrundsätze ist er nachweispflichtig (Art. 5 DSGVO). Vor diesem Hintergrund kann er sich nicht durch den Vortrag entlasten, eine Datenschutzverletzung sei nicht feststellbar, weil das eigene System eine „black box" darstelle.

19 Die Konstellationen einer unklaren Tatsachengrundlage bei der Beurteilung der Datenschutzverletzung dürfen nicht mit den Unsicherheiten verwechselt werden, die im Rahmen der Risikobeurteilung zu bewältigen sind. Die dort zu prüfenden Nachteile sind mit dem Verletzungserfolg bei der Datenschutzverletzung nicht identisch und haben sich im Übrigen regelmäßig noch nicht realisiert.

III. Risikobeurteilung bei Meldepflicht und Benachrichtigungspflicht

Nicht jede Datenschutzverletzung löst die Meldepflicht nach Art. 33 DSGVO oder die Benachrichtigungspflicht nach Art. 34 DSGVO aus. Beide Pflichten sind Reaktionen auf das Entstehen von Risiken für die Rechte und Freiheiten natürlicher Personen, und zwar in erster Linie der von einer Verletzung des Schutzes ihrer personenbezogenen Daten betroffenen Personen. Die Meldepflicht gegenüber der Datenschutz-Aufsichtsbehörde greift bereits bei einem niedrigen Risikoniveau ein, während die Benachrichtigungspflicht gegenüber betroffenen Personen ein hohes Risikoniveau voraussetzt. **20**

Die Meldepflicht nach Art. 33 Abs. 1 Satz 1 DSGVO entsteht nicht, wenn die Verletzung **21**

> „voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt".

Demgegenüber sind betroffene Personen nach Art. 34 Abs. 1 DSGVO (nur dann) zu benachrichtigen, wenn die Verletzung **22**

> „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge [hat]".

Zu unterscheiden sind danach **drei Risikostufen**: **23**

- Tritt voraussichtlich kein Risiko auf – in der Sache handelt es sich um ein vernachlässigbar **geringes** (datenschutzrechtlich nicht relevantes) **Risiko** –, unterbleiben sowohl die Meldung einer Datenschutzverletzung an die Datenschutz-Aufsichtsbehörde wie auch die Benachrichtigung der betroffenen Personen.
- Entsteht voraussichtlich ein (datenschutzrechtlich relevantes) **Risiko**, ist nach Art. 33 Abs. 1 DSGVO zu melden, aber nicht nach Art. 34 Abs. 1 DSGVO zu benachrichtigen.
- Nur wenn die Datenschutzverletzung voraussichtlich ein **hohes Risiko** zur Folge hat, muss eine Meldung an die Datenschutz-Aufsichtsbehörde abgegeben werden und es müssen auch die betroffenen Personen benachrichtigt werden.

III. Risikobeurteilung bei Meldepflicht und Benachrichtigungspflicht

24 In Anbetracht der unübersehbaren Vielfalt der Gestalt möglicher Verletzungen des Schutzes personenbezogener Daten im Sinne von Art. 4 Nr. 12 DSGVO kommt der **Risikobeurteilung** eine **wesentliche Bedeutung** für die Reichweite der Meldepflicht wie auch der Benachrichtigungspflicht zu. Die Risikobeurteilung ist grundsätzlich **Sache des Verantwortlichen**, nicht des behördlichen Datenschutzbeauftragten.

25 Prüfungsgegenstand ist im Fall von **Art. 33 Abs. 1 DSGVO**, ob ein Risiko (vgl. Erwägungsgrund 89 Satz 3 DSGVO) als voraussichtliche Folge der Datenschutzverletzung ausgeschlossen werden kann (**Negativprüfung**), und im Fall von **Art. 34 Abs. 1 DSGVO**, ob ein hohes Risiko voraussichtliche Folge der Datenschutzverletzung ist (**Positivprüfung**).

26 Bei der Anwendung von Art. 33 Abs. 1 und Art. 34 Abs. 1 DSGVO ist eine **einzelfallbezogene Risikobeurteilung** erforderlich. Darin liegt ein Unterschied zu der von Art. 35 Abs. 1 Satz 1 DSGVO für die Datenschutz-Folgenabschätzung geforderten generalisierenden Risikobetrachtung. Im Zusammenhang mit der Melde- und der Benachrichtigungspflicht wird die Risikobeurteilung regelmäßig (erheblich) einfacher ausfallen. Zu empfehlen ist ein **Vorgehen in drei Schritten**, wie es nachfolgend dargestellt ist.

1. Erster Schritt: Gewinnung der Beurteilungsgrundlage

27 In einem **ersten Schritt** werden die für das Risiko erheblichen **tatsächlichen Umstände** erfasst. Diese Umstände bilden die **Beurteilungsgrundlage** für die in einem zweiten Schritt zu leistende Risikoanalyse. Zu erfassen sind alle Umstände, die entweder für die Eintrittswahrscheinlichkeit oder für die Schwere möglicher Nachteile von Bedeutung sein können. Die Risikoanalyse wird nämlich anschließend in diesen beiden Dimensionen durchgeführt.

28 Bei der Suche nach den für das Risiko erheblichen tatsächlichen Umständen helfen die im Folgenden dargestellten Kategorien.[7] Die Aufzählung wird in einer Vielzahl von Fällen den Weg zu den wesentlichen Umständen weisen, kann jedoch nicht jede denkbare Konstellation abdecken. Daher sollte stets bedacht werden, dass im Einzelfall weitere Aspekte in die Risikoanalyse einzubeziehen sein können.

a) Datenschutzverletzung und Umgebungsbedingungen

29 Den Ausgangspunkt für die Ermittlung der Beurteilungsgrundlage bilden immer die erreichbaren **Informationen über die Datenschutzverletzung**. Dabei sollte zunächst klar werden, ob es sich der **Art** nach um eine Datenschutzverletzung handelt,

- in welcher sich Fehler einer eingesetzten Soft- oder Hardware manifestieren, die auch ein sorgfältiger Verantwortlicher nie vollständig ausschließen kann,

[7] Siehe dazu auch die Ausführungen in WP 250 (Fn. 6), S. 28 ff.

- die aus fahrlässigen Bedienfehlern von Anwenderinnen und Anwendern oder fahrlässigen Fehlsteuerungen durch die für die Administration zuständigen Personen folgt oder
- die auf einem vorsätzlichen internen oder einem vorsätzlichen externen Angriff auf ein System beruht.

Weiterhin sollte der Verantwortliche feststellen, **wer** die Datenschutzverletzung **auf welchem Weg** bewirkt hat. Soweit die Datenschutzverletzung durch Einsatz von IT zustandegekommen ist, sollten die entsprechenden Operationen innerhalb des Systems erhoben und auch dokumentiert werden. Dazu gehört insbesondere die Sicherung entsprechend aussagekräftiger **Protokolldateien**. 30

Für die Risikoanalyse relevant sind auch die Umgebungsbedingungen, unter welchen die Datenschutzverletzung eintrat. Dazu gehört eine fallbezogene Analyse der Schwachstellen betroffener Prozesse. Ferner sollte auch ermittelt werden, ob **risikomindernde Routinen** der Datenschutzverletzung entgegengewirkt haben und inwieweit diese Routinen effektiv waren, insbesondere welche Rolle **Eingriffe systemverwaltender Personen** gespielt haben und ob diese Eingriffe standardmäßig stattfanden oder bei einer vergleichbaren Datenschutzverletzung nicht ohne Weiteres wieder erwartet werden könnten. 31

b) Art, Sensibilität und Umfang der betroffenen personenbezogenen Daten

Die Datenschutz-Grundverordnung begründet für besonders sensible Daten einen verstärkten Schutz (Art. 9 DSGVO). Personenbezogene Daten können aber auch abgesehen von dieser formalen Hervorhebung mehr oder weniger schutzbedürftig sein. 32

Eher geringeren **Schutzbedarf** haben regelmäßig die Grunddaten einer Person, die im Rahmen einer einfachen Melderegisterauskunft zu erhalten, manchmal sogar frei verfügbar im Internet bereitgestellt sind. Einen vergleichbaren Schutzbedarf mögen auch manche Daten haben, die das Verhältnis einer Person zu einer Sache betreffen, wie etwa die Lage des eigenen Grundstücks in einem Überschwemmungsgebiet oder die Denkmaleigenschaft des darauf errichteten Hauses. Der Schutzbedarf steigt, wenn die personenbezogenen Daten bei der öffentlichen Stelle zwar von Außenstehenden in Erfahrung gebracht werden können, vor der Kenntnisnahme jedoch eine behördliche Entscheidung steht, die Vertraulichkeits- und Zugangsinteresse untereinander ausgleicht. Noch stärkeren Schutz erfahren personenbezogene Daten, die gegen einen Zugang Außenstehender grundsätzlich abgeschirmt sind. Der Schutz kann durch Geheimhaltungspflichten, oft mit strafrechtlicher Bewehrung, weiter ausgebaut werden. 33

Alle diese rechtlichen Vorkehrungen beschreiben nur einen typisierten **Standard** von Schutz, den der Gesetzgeber für die betreffenden personenbezogenen Daten bereitstellt. Stets sind auch die Umstände des **Einzelfalls** zu betrachten. So können selbst die Grunddaten einer Person – wie sie im Melderegister dokumentiert sind – eines (atypisch) gesteigerten Schutzes bedürfen, so etwa unter den Voraussetzungen, bei deren Vorliegen das Melderecht eine Auskunftssperre zulässt. Die Empfindlichkeit für sich genommen nicht besonders schutzwürdiger Daten kann dadurch eine Steigerung erfahren, dass die Daten untereinander verknüpft und gleichsam im Verbund verarbeitet werden: Die Daten werden so Bestand- 34

teile eines „Profils“ der betroffenen Person, das die öffentliche Stelle zur Erfüllung ihrer Aufgaben anlegt und das wiederum zu vergleichbaren „Profilen“ anderer Stellen in Bezug gesetzt werden kann – mit der Folge, dass ein immer genaueres virtuelles Bild der betroffenen Person entsteht.

c) Identifizierbarkeit betroffener Personen

35 Gerade wenn personenbezogene Daten Unbefugten zur Kenntnis gelangen, ist für die Risikoanalyse bedeutsam, ob diese „mit den Daten etwas anfangen können“. Das ist immer dann der Fall, wenn im Zuge der Datenschutzverletzung bei Dritten aussagekräftige „**Identitätsmarker**“ anfallen oder zumindest anfallen können. Dazu zählen nicht nur Klarnamen und zugehörige Anschriften, sondern auch Kennzeichen, die ohne weiteres durch einen Dritten selbst oder mit einer erreichbaren Unterstützung „entschlüsselt“ werden können.

Beispiel: Die Flurnummern von Grundstücken oder die amtlichen Kennzeichen von Kraftfahrzeugen können mittels der hierüber geführten Register konkreten Personen (Grundeigentümern, Fahrzeughalterinnen) zugeordnet werden. Gelangen Datensätze mit solchen „Identitätsmarkern“ an Unbefugte, kommt es für die Risikoanalyse auch darauf an, ob diese auf die Hilfsmittel einer Entschlüsselung (nur) wie Jedermann zugreifen können (Eigentümerdaten von Grundstücken im Liegenschaftskataster: Beschränkung auf berechtigtes Interesse, vgl. Art. 11 Abs. 1 Satz 1, 3 Vermessungs- und Katastergesetz – VermKatG, ebenso beim Grundbuch, vgl. § 12 Abs. 1 Satz 1 Grundbuchordnung; Halterdaten von Kraftfahrzeugen: Beschränkung auf Verfolgung von Rechtsansprüchen, vgl. § 39 Abs. 1 Straßenverkehrsgesetz – StVG), oder ob ihnen ein bevorrechtigter Zugang zur Verfügung steht (Eigentümerdaten von Grundstücken: z. B. Art. 11 Abs. 1 Satz 5 VermKatG; Halterdaten von Kraftfahrzeugen: z. B. § 35 Abs. 1 StVG).

36 Auch bei einer **Pseudonymisierung** bleiben die betroffenen Personen grundsätzlich noch identifizierbar. Nach Art. 4 Nr. 5 DSGVO handelt es sich dabei um

> „die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“.

37 Im Fall einer Pseudonymisierung sind für die Risikoanalyse Informationen darüber erforderlich, welchen Grad an Sicherheit das eingesetzte Pseudonymisierungsverfahren vermittelt, ferner insbesondere, ob ein Unbefugter, der Kenntnis von pseudonymisierten Daten erlangt hat, der Verschlüsselung wie Jedermann gegenübertritt oder wie eine Person mit Sonderwissen.

d) Besondere Eigenschaften betroffener Personen

Die Eintrittswahrscheinlichkeit sowie die Schwere möglicher Nachteile können auch von Eigenschaften abhängen, welche die betroffenen Personen aus der Allgemeinheit herausheben. So können Angehörige insbesondere ethnischer, politischer oder religiöser Minderheiten (vgl. Art. 9 Abs. 1 DSGVO) einem größeren Risiko gesellschaftlicher Ausgrenzung oder Zurücksetzung ausgesetzt sein, wenn über sie bestimmte personenbezogene Daten – und sei es die Zugehörigkeit zu der jeweiligen Minderheit – einem größeren Personenkreis oder gar der Öffentlichkeit bekannt werden. Die Datenschutz-Grundverordnung hebt zudem die besondere persönliche Schutzbedürftigkeit von Personen hervor, die in der Wahrnehmung ihrer Datenschutzrechte eingeschränkt sind (Erwägungsgrund 75 a. E. DSGVO: Kinder). 38

e) Besondere Eigenschaften des Verantwortlichen

Das Maß eines Risikos ist zwar grundsätzlich unabhängig davon, bei welchem Verantwortlichen sich die zugrunde liegende Datenschutzverletzung ereignet hat. Allerdings lassen sich einzelne Verantwortliche danach unterscheiden, in welche Kontexte sie ihre Verarbeitungen stellen. 39

Beispiel: Eine öffentliche Stelle, die lediglich eine Kundendatenbank verwaltet, agiert in einem anderen Kontext als ein Zweckverband, der im Einzelfall IT-gestützt unterschiedliche Aufgaben für eine Vielzahl von Mitgliedern wahrnimmt. Im ersten Fall betreffen mögliche Risiken die Kundendatenbank, im zweiten Fall auch mögliche Verknüpfungen zwischen Fachverfahren und/oder zwischen Datenbeständen einzelner Mitglieder.

Daher darf bei der Risikoanalyse auch nicht außer Betracht bleiben, ob der konkrete Verarbeitungskontext eines Verantwortlichen (weitere) mögliche Nachteile entstehen lässt und auf ihre Eintrittswahrscheinlichkeit oder ihre Schwere Einfluss hat. 40

f) Zahl betroffener Personen

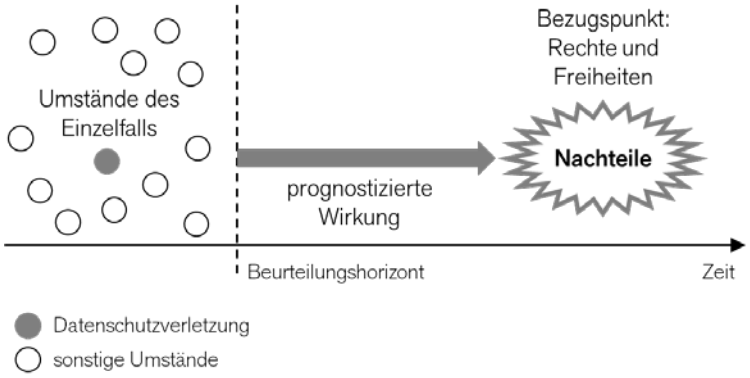
Schließlich ist für die Risikoanalyse von Belang, wie viele Datensätze von wie vielen natürlichen Personen von einer Datenschutzverletzung – möglicherweise – betroffen sind. Bei der Erfassung dieses Parameters sollte zwischen der bereits feststellbaren und einer möglichen Betroffenheit differenziert werden. 41

2. Zweiter Schritt: Risikoanalyse

Die in einem **zweiten Schritt** der Risikobeurteilung durchzuführende **Risikoanalyse** zielt auf die **rechtliche Bewertung eines tatsächlich entstandenen Risikos**. Eine exakte Quantifizierung ist nicht erforderlich. Risiken müssen den drei Stufen „geringes Risiko“, „Ri- 42

siko“ und „hohes Risiko“ zugeordnet werden. Eine feinere Differenzierung wird für die Anwendung von Art. 33 und Art. 34 DSGVO nicht benötigt.

43 Nach dem hier zugrunde gelegten Modell wird der ermittelte Sachverhalt, welcher die Datenschutzverletzung, die vorgefundenen Umgebungsbedingungen sowie einige für die Quantifizierung des Risikos bedeutsame Parameter umfasst, aus der Perspektive eines Beurteilungshorizonts betrachtet, wenn der Verantwortliche von der Datenschutzverletzung Kenntnis erlangt hat. Aus dieser Perspektive werden **mögliche Nachteile** in den Blick genommen (a), die in der Zukunft eintreten können oder bereits eingetreten sind. Diese Nachteile müssen für die Rechte und Freiheiten natürlicher Personen von Bedeutung sein. Ob ein Risiko als „geringes Risiko“, „Risiko“ oder „hohes Risiko“ einzustufen ist, hängt im Fall zukünftiger Nachteile von deren **Eintrittswahrscheinlichkeit** und **Schwere** ab (vgl. Erwägungsgrund 76 Satz 1 DSGVO) (b).



44 Sind bereits **eingetretene Nachteile** festzustellen, beschränkt sich die Risikobeurteilung insofern auf eine Bewertung der Schwere. Stets sollte aber geprüft werden, ob sich diese Nachteile noch weiterentwickeln oder ob andere Nachteile hinzutreten können. In solchen Fällen ist für die noch nicht realisierten Aspekte des „Gesamtpakets“ an Nachteilen auch eine Bewertung der Eintrittswahrscheinlichkeit erforderlich.

a) Mögliche Nachteile

45 Die Datenschutz-Grundverordnung unterscheidet bei den Folgen einer Datenschutzverletzung mögliche physische, materielle und immaterielle Schäden (Erwägungsgrund 85 Satz 1 DSGVO). Sie hebt damit hervor, dass **Vermögensschäden** wie auch **Nichtvermögensschäden** in Betracht gezogen werden sollen.

46 In der Regel stehen mögliche Nachteile für **Personen** im Vordergrund, deren personenbezogene Daten von der Datenschutzverletzung **betroffen** sind. In die Risikoanalyse sind allerdings auch Nachteile einzubeziehen, die bei **anderen Personen** eintreten können. Art. 33 Abs. 1 DSGVO spricht im Zusammenhang mit dem Ausschluss eines Risikos, Art. 34 Abs. 1 DSGVO im Kontext des hohen Risikos jeweils von den „Rechte[n] und Freiheiten natürlicher Personen“. Dieser auch in der englischen Fassung anzutreffende Sprachgebrauch hebt sich von dem in Art. 4 Nr. 1 DSGVO legal definierten Begriff „betroffene Person“ ab, der in Art. 34 Abs. 1 DSGVO daneben Verwendung findet. Den Terminus „natürliche Person“ gebraucht

Art. 4 Nr. 10 DSGVO (gerade) auch zur Bestimmung, wer „Dritter" ist. Art. 6 Abs. 1 UAbs. 1 Buchst. d und Art. 12 Abs. 6 DSGVO weisen ebenfalls in Richtung einer bewusst eingeführten und normativ genutzten Bedeutungsdifferenz.

Die möglichen Nachteile müssen **Rechte und Freiheiten** betreffen. Dabei kann es sich um Positionen handeln, die abwehrrechtlich oder leistungsrechtlich geprägt sind, um Positionen, die das Unionsrecht oder das nationale Recht gewährt. Häufig werden in erster Linie Nachteile in Rede stehen, die das unionsrechtliche Datenschutzgrundrecht oder das nationale Recht auf informationelle Selbstbestimmung betreffen. Die Vorgabe, welche die Folge einer Datenschutzverletzung als Nachteil erscheinen lässt, kann aber auch in einer anderen Grundrechtsposition oder in einer einfachgesetzlich gewährleisteten Position liegen. 47

Beispiele: Eine als Datenschutzverletzung zu wertende Offenlegung von personenbezogenen Daten kann nach deren Kenntnisnahme durch Außenstehende eine Rufschädigung bewirken; betroffen ist das allgemeine Persönlichkeitsrecht. – Bei einem Angriff auf das Liegenschaftskataster verschiebt ein Hacker eine Grundstücksgrenze zu eigenen Gunsten; betroffen ist das Eigentumsgrundrecht des Nachbarn.

Art. 33 Abs. 1 und Art. 34 Abs. 1 DSGVO unterscheiden für die Risikoanalyse weiterhin nicht zwischen **unmittelbar** und **mittelbar** eintretenden **Nachteilen**. Daher sind stets beide Typen in Ansatz zu bringen. Unmittelbare Nachteile gehen ohne weitere Zwischenakte – insbesondere ohne weiteres menschliches Eingreifen – aus der Datenschutzverletzung hervor. Diese Nachteile haben sich im Zeitpunkt der durch eine Datenschutzverletzung veranlassten Risikoanalyse häufig bereits realisiert. Mittelbare Nachteile sind noch von hinzutretenden Ereignissen abhängig, insbesondere vom Verhalten des Verantwortlichen, betroffener Personen oder Dritter. 48

Bei Ermittlung möglicher Nachteile darf schließlich nicht die **Art der Datenschutzverletzung** außer Betracht bleiben: Für eine Beeinträchtigung der Datenverfügbarkeit sind andere Schadensbilder typisch als für eine Beeinträchtigung der Datenintegrität oder der Datenvertraulichkeit. 49

Ist eine **Beeinträchtigung der Datenverfügbarkeit oder der Datenintegrität** eingetreten, sollten bei der Prognose im Rahmen der Risikoanalyse insbesondere die folgenden Verläufe und aus ihnen resultierende Nachteile in Betracht gezogen werden: 50

- Der Verantwortliche kann die (richtigen) Daten in eine Entscheidung nicht einbeziehen, die betroffene Person erhält infolgedessen eine Leistung nicht oder erfährt Rechtsnachteile.
- Zur Nutzung der Daten berechtigte Dritte können die (richtigen) Daten in ihre Entscheidungen nicht einbeziehen, die betroffene Person oder ein Dritter hat daraus einen Nachteil.
- Die betroffene Person kann Nachweise gegenüber dem Verantwortlichen oder einem Dritten nicht (richtig) führen, die für den Bezug von Leistungen oder die Abwehr von Rechtsnachteilen von Bedeutung sind.

– [Nur im Fall einer Beeinträchtigung der Datenverfügbarkeit:] Der Verantwortliche kann mit den Daten nicht arbeiten und deshalb bestimmte Produkte in seinem Aufgabenbereich nicht anbieten; die betroffene Person kann auf das Produkt nicht zugreifen und nach Maßgabe der Umstände auch nicht auf einen anderen Anbieter ausweichen.

Beispiel: Ein Verschlüsselungstrojaner befällt die elektronische Patientenverwaltung eines Kreiskrankenhauses, das vorübergehend im „Analogbetrieb" arbeiten muss. Medizinische Maßnahmen werden verschoben, und Patienten müssen auf eine benachbarte Klinik ausweichen.

51 Im Fall einer **Beeinträchtigung der Datenvertraulichkeit** sollten für die Prognose im Rahmen der Risikoanalyse insbesondere folgende Verläufe und ihre Folgen bedacht werden:

– Ein Dritter nutzt eine durch Datenschutzverletzung entstandene Zugangsmöglichkeit und verschafft sich personenbezogene Daten. In einem nächsten Schritt kann der Dritte die Daten etwa mit anderen Daten verknüpfen, sie an ausgewählte Personen übermitteln, verkaufen oder im Internet bereitstellen.

– Der Dritte oder ein weiteres Glied in einer Kette von Weiterverarbeitungen nutzt die ihm infolge der Datenschutzverletzung zur Kenntnis gelangten Daten gezielt für einen Angriff auf rechtlich geschützte Positionen der betroffenen Person.

Beispiele: Jemand erfährt auf Grund einer Datenschutzverletzung sozial inkriminierende Daten über einen Kollegen und macht diese an der Arbeitsstelle bekannt. – Ein Arbeitgeber gelangt auf vergleichbare Weise an gesundheitsbezogene Informationen über eine Mitarbeiterin und kündigt dieser während der Probezeit.

b) Bewertung der möglichen Nachteile

52 Die als möglich in Betracht gezogenen Nachteile sind sodann grundsätzlich in den Dimensionen **„Schwere"** (1) und **„Eintrittswahrscheinlichkeit"** (2) zu bewerten (zum Sonderfall des bereits realisierten Nachteils →Rn. 44). Die Bewertung zielt darauf, die Schwere und die Eintrittswahrscheinlichkeit jeweils den Graden „geringfügig", „überschaubar", „substanziell" und „groß" zuzuordnen.[8] Schließlich werden die in den beiden Dimensionen gefundenen (Einzel-)Bewertungen in einer **Gesamtbewertung** verbunden (3). Diese Gesamtbewertung bildet das Ergebnis der Risikobeurteilung.

53 Bestehen bei der Quantifizierung der Schwere oder der Eintrittswahrscheinlichkeit von Nachteilen Unsicherheiten, sollte grundsätzlich der jeweils höhere Grad gewählt werden.

[8] Zur Abstufung der Grade siehe Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Risiko für die Rechte und Freiheiten natürlicher Personen, Kurzpapier Nr. 18, Stand 4/2018, S. 4, im Internet abrufbar auf https://www.datenschutzkonferenz-online.de in der Rubrik „Infothek – Kurzpapiere".

aa) Bewertung der möglichen Nachteile nach ihrer Schwere

Die Bewertung der möglichen Nachteile nach ihrer Schwere hängt maßgeblich **zum einen** davon ab, in welchem **Maß** eine Person, die Nachteile erleidet, in ihrer **Lebensführung beeinträchtigt** wird, und **zum anderen, wie viele Personen** Nachteile treffen. Worin sich die Wirkung der Nachteile zeigt, ist von den Rechten und Freiheiten abhängig, auf welche sich die Nachteile beziehen. Verantwortliche sollten insbesondere auf die folgenden Aspekte achten: 54

- Wird der bestehende **soziale Status** spürbar beeinträchtigt? – Insbesondere: Kann die Datenschutzverletzung eine Rufschädigung bewirken? Wie intensiv und nachhaltig fällt sie aus?
- Wird der bestehende **ökonomische Status** spürbar beeinträchtigt? – Insbesondere: Kann die Datenschutzverletzung Vermögensschäden verursachen? (Zu würdigen sind auch Kosten, die einer betroffenen Person für die Verteidigung ihres ökonomischen Status entstehen.) – Können einer betroffenen Person infolge der Datenschutzverletzung Vermögensvorteile entgehen?
- Können die Nachteile in **zeitlicher Dimension** nur punktuell wirken oder ist eine langfristige Beeinträchtigung möglich? – Insbesondere: Sind die Folgen einer Vertraulichkeitsverletzung durch Bereitstellung personenbezogener Daten im Internet noch revidierbar oder muss eine betroffene Person auf Dauer mit den Folgen der Datenschutzverletzung leben?
- [Bei Vertraulichkeitsverletzung:] Geraten Daten an einen **Empfänger**, bei dem kraft einer öffentlichen Aufgabe (Polizei, Strafverfolgungsbehörde, Nachrichtendienst) oder seiner gesellschaftlichen Funktion (Medien, Journalisten, wirkmächtige Blogger) mit einer nachteilsvertiefenden Weiterverbreitung oder Neukontextualisierung zu rechnen ist? Gelangt eine Stelle an die Daten, welche erkennbar geneigt sein wird, die personenbezogenen Daten gegen die betroffene Person zu verwenden (Dienstherr/Arbeitgeber, Versicherung, Bank)?

Betrifft die Datenschutzverletzung die Vertraulichkeit **besonderer Kategorien personenbezogener Daten**, so ist für den Nachteil, der in einem empfängerbezogen nicht weiter qualifizierten Bekanntwerden der Daten läge, regelmäßig mindestens eine datenschutzrechtlich substanzielle Schwere anzunehmen. 55

In jedem Fall einer Datenschutzverletzung ist aber eine **Einzelfallbetrachtung** erforderlich. Die folgenden Beispiele sollen verdeutlichen, wie eine solche Einzelfallbetrachtung aussehen kann: 56

Beispiel 1: Hotelier H. hat das erste Haus am Platz. Er hat wieder einmal im Halteverbot vor seiner Haustür geparkt. Der gemeindliche Verkehrsüberwachungsbeamte hat ihm deshalb eine gebührenpflichtige Verwarnung an die Scheibe geheftet. H. will nichts bezahlen und wendet sich in einer E-Mail an die erste Bürgermeisterin B. Da müsse doch etwas zu machen sein. B. hat es wie immer sehr eilig, tippt hastig ein „Bitte mit Augenmaß erledigen“ in die Betreffzeile, der Empfänger ergänzt sich selbst – leider war es nicht die Leiterin des Ordnungsamts Jutta O., sondern die örtliche Journalistin Jutta P. Diese macht einen kleinen Arti-

kel draus. Das Ordnungsamt besteht auf dem Verwarnungsgeld; gleichwohl muss sich B. im Gemeinderat kritische Fragen gefallen lassen. H. wird in der Folge zweimal aus der Bürgerschaft angesprochen, was ihm eigentlich einfalle, falsch zu parken und dann auch noch nicht zahlen zu wollen. Mehr passiert nicht.

Die Nachteile sind geringfügig. Infolge des „Büroversehens" von B. ist die Eingabe von H. zwar der Ortsöffentlichkeit bekannt geworden. Der eingetretene Rufschaden beschränkt sich aber auf vereinzelte moderat-negative Reaktionen aus der Bürgerschaft. Weiterungen sind nicht zu erwarten. Vielmehr wird alsbald „Gras über die Sache wachsen". Eine Prüfung der Eintrittswahrscheinlichkeit kann unterbleiben, weil die Nachteile schon eingetreten sind. Folge: Nur Meldepflicht nach Art. 2 Satz 1 BayDSG, Art. 28 Abs. 2 Satz 2 BayDSG i. V. m. Art. 33 DSGVO.

Beispiel 2: Die Meldestelle einer kreisangehörigen Gemeinde hat die Unterlagen über die von ihr nach § 51 Abs. 1 Bundesmeldegesetz in das Melderegister eingetragenen Auskunftssperren in einem Aktenordner gesammelt, der sich im Büro des Leiters der Meldestelle in einem verschlossenen Schrank befindet. Der Auszubildende A. hat erfahren, dass ihn die Stadt nach der Abschlussprüfung nicht übernehmen wird. Da er weiß, wo sich der Schlüssel zu dem fraglichen Schrank befindet, verschafft er sich während einer Mittagspause Zugang und scannt den Inhalt des Aktenordners zu den Auskunftssperren ein. In den folgenden Tagen veröffentlicht er jeweils eines der gescannten Dokumente anonym in einem rathauskritischen Blog. Ein Bürger erhält daraufhin ernstzunehmende Morddrohungen von einer ehemaligen Partnerin, während eine Rockergruppe das Motorrad der sie hartnäckig verfolgenden Staatsanwältin in die Luft jagt.

Nachteilen hinsichtlich des von Art. 16 Abs. 1 Vertrag über die Arbeitsweise der Europäischen Union (AEUV) und Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz (GG) geschützten Vertraulichkeitsinteresses lagern sich hier weitere, von einer Mitwirkung Dritter abhängende Nachteile an, die insbesondere die Rechtsgüter Leben und Gesundheit (Art. 2 Abs. 2 Satz 1 GG) sowie Eigentum (Art. 14 Abs. 1 GG) betreffen. Die Nachteile wiegen schwer; zu berücksichtigen sind nicht nur die bereits eingetretenen Beeinträchtigungen, sondern auch solche, die in Aussicht stehen. Eine Auskunftssperre knüpft (ebenfalls) an eine Prognose hinsichtlich gewichtiger Nachteile, sodass bei Bekanntwerden geschützter Anschriften stets auf die Möglichkeit des Eintritts solcher Nachteile (und im Übrigen auf eine hohe Eintrittswahrscheinlichkeit) geschlossen werden darf. Folge: Meldepflicht nach Art. 33 DSGVO und Benachrichtigungspflicht nach Art. 34 DSGVO.

Beispiel 3: Bei einer kreisangehörigen Stadt wird die Stelle eines berufsmäßigen Stadtratsmitglieds (Besoldungsgruppe A14/15) neu besetzt. Beworben hat sich auch die bei einem Landratsamt als Regierungsrätin (Besoldungsgruppe A13) beschäftigte R. Das Personalratsmitglied P. erfährt davon im Rahmen der Personalratsbeteiligung. Er zieht durch den ihm privat bekannten B., einen Beschäftigten des Landratsamts, Erkundigungen über den Ruf von R. ein, die wegen ihrer (großen) Fachkunde und ihrer (hohen) Einsatzbereitschaft im Kollegenkreis nicht sonderlich beliebt ist. P. „streut" seine „Erkenntnisse" unter den Stadtratsmitgliedern. Die Entscheidung des Gremiums fällt zugunsten eines Konkurrenten aus. R. beschwert sich bei der behördlichen Datenschutzbeauftragten der Stadt. Diese stellt

fest, dass die Aktivitäten des P. zu einem Stimmungsumschwung unter den Stadtratsmitgliedern geführt haben; R. verlor ihre Stellung als Favoritin.

Nachteile hat die R. nicht nur hinsichtlich ihres durch Art. 16 Abs. 1 AEUV und Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützten Vertraulichkeitsinteresses erlitten, sondern auch in ihrem Interesse an einer von sachlichen Gesichtspunkten geleiteten Auswahlentscheidung, für das Art. 116 Verfassung des Freistaates Bayern streitet. Die Nachteile wiegen bereits schwer. Zum einen hat P. ein empfindliches personenbezogenes Datum (Tatsache der Bewerbung von R. bei der Stadt) gerade an eine Stelle (den B.) weitergegeben, welche dieses zum Nachteil der R. einsetzen konnte und auch eingesetzt hat. Zum anderen wurde die Chancen der R., eine attraktivere Stelle zu erhalten, durch die von P. ins Werk gesetzte Datenschutzverletzung verschlechtert und im Ergebnis vereitelt. Da die Nachteile bereits eingetreten sind, ist eine Prüfung der Eintrittswahrscheinlichkeit entbehrlich. Folge: Meldepflicht nach Art. 33 DSGVO und Benachrichtigungspflicht nach Art. 34 DSGVO.

bb) Bewertung der möglichen Nachteile nach ihrer Eintrittswahrscheinlichkeit

Die Bewertung der als möglich ermittelten, noch nicht realisierten (→Rn. 44) Nachteile bezüglich ihrer Eintrittswahrscheinlichkeit kann sich auf eine Nutzung **verwaltungspragmatischen Erfahrungswissens** beschränken. Dabei können die nachfolgenden Leitbeschreibungen verwendet werden. 57

Leitbeschreibung	Eintrittswahrscheinlichkeit
Eintritt des Nachteils ist denkmöglich, er widerspricht aber jeder Erfahrung/ist eine rein theoretische Möglichkeit	hinsichtlich des Nachteils besteht eine **geringfügige Eintrittswahrscheinlichkeit**
Eintritt des Nachteils ist möglich, die konkreten Umstände sprechen aber gegen eine solche Entwicklung und es ist nicht zu erwarten, dass sich daran etwas ändert Eintritt des Nachteils ist möglich, er hängt von einem Verhalten Dritter ab, die konkreten Umstände sprechen dafür, dass der Dritte dem Eintritt des Nachteils entgegenwirkt, und es ist nicht zu erwarten, dass sich daran etwas ändert	hinsichtlich des Nachteils besteht eine **überschaubare Eintrittswahrscheinlichkeit**
Eintritt des Nachteils ist möglich, er hängt von Unwägbarkeiten ab, die sich nicht quantifizieren lassen Eintritt des Nachteils ist möglich, er hängt von einem Verhalten Dritter ab, das sich nicht vorhersagen lässt Eintritt des Nachteils ist möglich; niemand kann sagen, was weiter passieren wird	hinsichtlich des Nachteils besteht eine **substanzielle Eintrittswahrscheinlichkeit**
Eintritt des Nachteils ist wahrscheinlich/überwiegend wahrscheinlich/sehr wahrscheinlich Eintritt des Nachteils ist möglich; es ist zu erwarten, dass Umstände eintreten, die den Nachteil herbeiführen Eintritt des Nachteils ist möglich, er hängt vom Verhalten Dritter ab, das sich bereits abzeichnet/das naheliegt/für das eine wirksame Anreizsituation besteht	hinsichtlich des Nachteils besteht eine **hohe Eintrittswahrscheinlichkeit**

3. Dritter Schritt: Gesamtbewertung, Ergebnis der Risikobeurteilung

58 In der abschließenden **Gesamtbewertung** werden die Einzelbewertungen zur Schwere sowie zur Eintrittswahrscheinlichkeit möglicher Nachteile miteinander verknüpft. Dies führt zum **Ergebnis der Risikobeurteilung**. Das Risiko kann nun einer der drei **Risikostufen** (→Rn. 23) zugeordnet werden:

59 **Risikostufe 1:** Ein **geringes Risiko** tritt ein, wenn lediglich Nachteile von geringfügiger Schwere eine geringfügige oder überschaubare Eintrittswahrscheinlichkeit haben (Fälle I-1 und I-2), oder wenn Nachteile von überschaubarer Schwere eine geringfügige Eintrittswahrscheinlichkeit haben(Fall II-1). In diesen Fällen ist weder eine Meldung nach Art. 33 DSGVO noch eine Benachrichtigung nach Art. 34 DSGVO erforderlich.

60 **Risikostufe 2:** Ein **Risiko** liegt vor, wenn für Nachteile von geringfügiger Schwere eine mindestens substanzielle Eintrittswahrscheinlichkeit besteht (Fälle I-3 und I-4), wenn für Nachteile von überschaubarer Schwere eine überschaubare oder substanzielle Eintrittswahrscheinlichkeit besteht (Fälle II-2 und II-3), wenn für Nachteile von substanzieller Schwere eine geringfügige oder überschaubare Eintrittswahrscheinlichkeit besteht, oder wenn für Nachteile von großer Schwere eine geringfügige Eintrittswahrscheinlichkeit besteht (Fall IV-1). In diesen Fällen greift die Meldepflicht nach Art. 33 DSGVO, nicht jedoch die Benachrichtigungspflicht nach Art. 34 DSGVO.

61 **Risikostufe 3:** Demgegenüber zeichnet sich ein **hohes Risiko** dadurch aus, dass Nachteile von überschaubarer Schwere eine große Eintrittswahrscheinlichkeit haben (Fall II-4), dass Nachteile von substanzieller Schwere eine mindestens substanzielle Eintrittswahrscheinlichkeit haben (Fälle III-3 und III-4), oder dass Nachteile von großer Schwere eine mindestens überschaubare Eintrittswahrscheinlichkeit haben (Fälle IV-2, IV-3 und IV-4). Gleichgestellt sind bereits eingetretene Nachteile mit mindestens überschaubarer Schwere. In allen diesen Fällen ist sowohl eine Meldung nach Art. 33 DSGVO als auch eine Benachrichtigung nach Art. 34 DSGVO geboten.

Schwere des Nachteils						
	groß	**Grad IV**	2	3	3	3
	substanziell	**Grad III**	2	2	3	3
	überschaubar	**Grad II**	1	2	2	3
	geringfügig	**Grad I**	1	1	2	2
			Grad 1	**Grad 2**	**Grad 3**	**Grad 4**
			geringfügig	überschaubar	substanziell	groß
			Eintrittswahrscheinlichkeit des Nachteils			

IV. Meldepflicht des Verantwortlichen gegenüber der Datenschutz-Aufsichtsbehörde (Art. 33 DSGVO)

62 Ergibt die Risikobeurteilung, dass eine Datenschutzverletzung ein datenschutzrechtlich relevantes, wenn nicht gar ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, so muss der Verantwortliche die Meldepflicht nach Art. 33 DSGVO erfüllen. Der nachfolgende Abschnitt erläutert, wen eine Meldepflicht gegenüber dem Bayerischen Landesbeauftragten für den Datenschutz trifft (1.), zu welchem Zeitpunkt sie genau entsteht (2.), wie sie erfüllt wird (3.) und welche organisatorischen Vorkehrungen im Hinblick auf eine effektive Umsetzung der gesetzlichen Vorgaben zu treffen sind (4.).

1. Verantwortlicher, zuständige Aufsichtsbehörde

63 Die Meldepflicht nach Art. 33 Abs. 1 DSGVO trifft den „Verantwortlichen". Das ist nach Art. 4 Nr. 7 DSGVO

> „die […] juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet".

64 Art. 3 Abs. 2 BayDSG bestimmt, dass **Verantwortlicher** für die Verarbeitung personenbezogener Daten im Sinne der Datenschutz-Grundverordnung die für die Verarbeitung zuständige öffentliche Stelle ist, soweit nichts anderes bestimmt ist. Zu den öffentlichen Stellen zählen nach Art. 1 Abs. 1 BayDSG Behörden und sonstige öffentliche Stellen des Freistaates Bayern, der Gemeinden, Gemeindeverbände und der sonstigen der Aufsicht des Freistaates Bayern unterstehenden juristischen Personen des öffentlichen Rechts, nach Art. 1 Abs. 3 BayDSG darüber hinaus grundsätzlich auch Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen – ungeachtet der Beteiligung nicht öffentlicher Stellen – eine oder mehrere der in Art. 1 Abs. 1 BayDSG genannten juristischen Personen des öffentlichen Rechts unmittelbar oder durch eine solche Vereinigung beteiligt sind. Eine Pflicht, Datenschutzverletzungen zu melden, kann danach **insbesondere** treffen:

- Staatsbehörden;
- Gemeinden, Landkreise, Bezirke, Verwaltungsgemeinschaften und Zweckverbände;
- verselbstständigte Regiebetriebe und Eigenbetriebe kommunaler Träger;
- Kommunalunternehmen und gemeinsame Kommunalunternehmen;
- Kammern in den Bereichen der freien Berufe und des Handwerks, Handwerksinnungen;

- öffentlich-rechtliche Stiftungen unter staatlicher Aufsicht;
- in privater Rechtsform betriebene Stadtwerke, soweit sie die Aufgaben der öffentlichen Verwaltung wahrnehmen (etwa die Aufgabe „öffentliche Wasserversorgung“, vgl. Art. 57 Abs. 2 Satz 1 Gemeindeordnung);
- in privater Rechtsform betriebene kommunale Akutkrankenhäuser;
- Wirtschaftsförderungs- und Tourismusgesellschaften der Gemeinden und Landkreise.

Bayerische öffentliche Stellen melden Datenschutzverletzungen an den **Bayerischen Landesbeauftragten für den Datenschutz**. Dies gilt auch dann, wenn auf sie nach Art. 1 Abs. 3 Satz 1 BayDSG die Vorschriften für nicht öffentliche Stellen anzuwenden sind (vgl. Art. 1 Abs. 3 Satz 2 BayDSG). Öffentlich-rechtliche Finanzdienstleistungsunternehmen sowie ihre Zusammenschlüsse und Verbände richten ihre Meldungen dagegen an das Bayerische Landesamt für Datenschutzaufsicht (vgl. Art. 1 Abs. 2 Satz 2 BayDSG). **65**

2. Entstehen der Meldepflicht

Die Meldepflicht entsteht zu dem Zeitpunkt (a), zu welchem der Verantwortliche von dem meldepflichtigen Ereignis Kenntnis erlangt hat (b). Während einer notwendigen „Aufklärungsphase“ besteht noch keine Meldepflicht. **66**

Die Meldepflicht bezieht sich immer auf eine konkrete Datenschutzverletzung. Mehrere Datenschutzverletzungen „zusammenkommen“ zu lassen und (erst) dann eine „Sammelmeldung“ zu erstatten, ist nicht zulässig. Dies gilt auch dann, wenn sich eine Datenschutzverletzung voraussichtlich wiederholen wird. Andernfalls würde das Ziel verfehlt, der Datenschutz-Aufsichtsbehörde ein Eingreifen zu ermöglichen (vgl. Erwägungsgrund 87 Satz 3 DSGVO). Tritt eine gleichartige Datenschutzverletzung ein weiteres Mal auf, sollte auf eine bereits erstattete Meldung (unter Angabe von Datum und Uhrzeit dieser früheren Meldung) hingewiesen werden; auf bereits dort gemachte, weiterhin zutreffende Angaben kann Bezug genommen werden. **67**

a) Zeitpunkt

Eine Datenschutzverletzung ist nicht stets ein punktuelles Ereignis, das sich auf den ersten Blick in seiner Qualität zu erkennen geben. Nicht selten treten zunächst einmal Anhaltspunkte ans Licht, die darauf hindeuten, dass etwas „schiefgegangen“ ist. Der Verantwortliche muss dann erst den Sachverhalt aufklären, herausfinden, was genau passiert ist, um was für ein Ereignis es sich überhaupt handelt. Außerdem kann zu ermitteln sein, ob das Ereignis Einfluss auf Verarbeitungen personenbezogener Daten nehmen kann oder genommen hat. Diese Aufklärungsmaßnahmen nehmen Zeit in Anspruch. **68**

Ein Ereignis ist als Datenschutzverletzung zu behandeln, sobald es nach den unter Rn. 4 ff. dargestellten Maßstäben als eine solche identifiziert werden kann. Vor diesem Zeitpunkt kann die Datenschutzverletzung dem Verantwortlichen grundsätzlich nicht bekannt werden. Verfügt der Verantwortliche zunächst nur über Anhaltspunkte, dass eine Datenschutzverlet- **69**

zung vorliegen könnte, hat er im Hinblick auf Art. 32 Abs. 1 DSGVO die Obliegenheit, sich Gewissheit, zumindest aber belastbare Informationen zu verschaffen.

70 Aus aufsichtsbehördlicher Sicht kann bei Datenschutzverletzungen, die nicht auf den ersten Blick – und sei es auch nur vorläufig – einzuordnen sind, eine Aufklärungsphase von höchstens 24 Stunden ab dem Auftreten hinreichender Anhaltspunkte in Anspruch genommen werden. Die Dauer hängt von den erforderlichen Aufklärungsmaßnahmen ab. Wird mehr Zeit benötigt, ist dies in der Meldung zu erläutern (→Rn. 127).

b) Kenntniszurechnung

71 Da die Meldung durch den Verantwortlichen abzugeben ist, muss ihm das meldepflichtige Ereignis bekannt werden. Bei institutionellen Verantwortlichen wie Staatsbehörden oder Kommunen stellt sich hier die Frage nach einer **Kenntniszurechnung**, danach also, auf wessen Kenntnisstand es ankommt, wenn eine Meldepflicht zulasten des Verantwortlichen begründet werden soll. Aus aufsichtsbehördlicher Sicht wird das meldepflichtige Ereignis einer verantwortlichen bayerischen öffentlichen Stelle jedenfalls dann bekannt, wenn eine der folgenden Funktionseinheiten oder einer der folgenden Funktionsträger Kenntnis erlangt:

Funktionseinheit oder Funktionsträger[9]	**Kenntniszurechnung**
Behördenleitung	für **alle** Datenschutzverletzungen im Zuständigkeitsbereich der öffentlichen Stelle
Organisationssachgebiet	für **alle** Datenschutzverletzungen im Zuständigkeitsbereich der öffentlichen Stelle
IT-Sachgebiet	für Datenschutzverletzungen, die **betreute IT-Systeme** betreffen
Fachsachgebiete	für Datenschutzverletzungen **im eigenen Zuständigkeitsbereich**, ansonsten innerbehördliche Meldepflicht
Beschäftigte mit Vorgesetztenfunktion	für Datenschutzverletzungen, die **im eigenen Zuständigkeitsbereich durch eigene Mitarbeiter** („Untergebene") bewirkt sind, ansonsten innerbehördliche Meldepflicht

Erläuterungen:

Behördenleitung ist bei einer Staatsbehörde der Behördenleiter, wenn die Behörde (nur) eine öffentliche Stelle bildet. Umfasst die Behörde (im Sinn von Art. 1 Abs. 2 Bayerisches Verwaltungsverfahrensgesetz) ausnahmsweise mehrere öffentliche Stellen, können diese eigene Leiter haben. – **Beispiel:** Eine kreisfreie Stadt – grundsätzlich eine Einheitsbehörde – betreibt eine Fachschule als eigene Einrichtung mit eigenem Personal. Die Fachschule ist trotz ihrer Eingliederung in die Stadtverwaltung datenschutzrechtlich als gesonderte öffentliche Stelle zu bewerten. Kommt es dort zu einer Datenschutzverletzung, löst (bereits) die Kenntnis des Schulleiters die Meldepflicht aus.

Bei **kommunalen Trägern** ist Leitung der öffentlichen Stelle das zur Vertretung berufene Organ (hauptamtlicher erster Bürgermeister/Oberbürgermeister, Landrat), soweit dieses ehrenamtlich tätig ist, daneben die für die Leitung der Geschäfte zuständige Führungskraft (also neben dem ehrenamtlichen ersten Bürgermeister der ge-

[9] Die Bezeichnungen berücksichtigt das Muster einer Datenschutz-Geschäftsordnung in Bayerisches Staatsministerium des Innern, für Sport und Integration, Arbeitshilfen zur praktischen Umsetzung der Datenschutz-Grundverordnung, der Richtlinie (EU) 2016/680 (Richtlinie zum Datenschutz bei Polizei und Justiz) und des neuen Bayerischen Datenschutzgesetzes für bayerische öffentliche Stellen, Stand 3/2019, S. 22 ff., im Internet abrufbar unter http://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen.

schäftsleitende Beamte, neben dem Gemeinschaftsvorsitzenden einer Verwaltungsgemeinschaft der Leiter der Geschäftsstelle oder neben dem Bezirkstagspräsidenten der Direktor der Bezirksverwaltung).

Das **Organisationssachgebiet** – das selbstverständlich auch anders heißen kann – ist in der Behörde die Funktionseinheit, die für die Organisation des Datenschutzes in der Behörde zuständig ist.

Viele Behörden ordnen den in ihnen gebündelten Funktionseinheiten – den **Fachsachgebieten** – durch innerdienstliche Regelungen Aufgaben des Verantwortlichen zu. Mitunter werden solche Aufgaben im Übrigen ohne besondere Regelung rein faktisch wahrgenommen.

Beispiel: Erhalten für ein Fachverfahren im Steueramt einer Gemeinde durch einen unbeabsichtigten Fehler bei der Administration zu viele Beschäftigte Berechtigungen, wird die Meldepflicht ausgelöst, wenn dies innerhalb des Steueramts, im Organisationssachgebiet oder beim ersten Bürgermeister bekannt wird. Die Kenntniserlangung durch eine Mitarbeiterin im Bauamt genügt dagegen grundsätzlich nicht. Allerdings dürfte diese Mitarbeiterin dienst- oder arbeitsrechtlich gehalten sein, das erlangte Wissen an eine intern zuständige Stelle – insbesondere den behördlichen Datenschutzbeauftragten oder die erste Bürgermeisterin – weiterzugeben.

Dem Verantwortlichen nicht zuzurechnen ist das Wissen des **behördlichen Datenschutzbeauftragten**. Dieser ist nach Art. 38 Abs. 3 Satz 1 DSGVO nicht weisungsgebunden und nach Art. 38 Abs. 5 DSGVO i. V. m. Art. 12 Abs. 2 BayDSG auch hinsichtlich ihm anvertrauter Tatsachen zur Verschwiegenheit verpflichtet. Beides ist mit einer Kenntniszurechnung nicht vereinbar. Erfährt der behördliche Datenschutzbeauftragte (als erster) vertraulich von einer Datenschutzverletzung, wird er gleichwohl auf eine Risikominimierung hinwirken. Dabei kann er insbesondere **72**

- Beschäftigte, die ihm vertraulich Informationen über Datenschutzverletzungen mitteilen, hinsichtlich – häufig bestehender – innerbehördlicher Regelungen zur Meldung solcher Ereignisse an den Verantwortlichen aufklären;
- eine vertrauliche Mitteilung zum Anlass für Überwachungsmaßnahmen (Art. 39 Abs. 1 Buchst. b DSGVO) nehmen, soweit er diese ohne Offenlegung seiner Informationsquelle ergreifen kann;
- eine vertrauliche Mitteilung zum Anlass für präventive Maßnahmen nehmen, die darauf zielen, eine Verletzung gleicher Art jedenfalls für die Zukunft auszuschließen.

Auch wenn dem Verantwortlichen das Wissen des behördlichen Datenschutzbeauftragten von einer Datenschutzverletzung nicht zuzurechnen ist, darf dieser gleichwohl in den Meldeprozess einbezogen werden (vgl. für den Bereich der Datenschutz-Richtlinie für Polizei und Strafjustiz Rn. 120). Dies gilt auch für die Mitwirkung beim Ausfüllen des Meldeformulars sowie bei einer diese ergänzenden Dokumentation. **73**

3. Erfüllung der Meldepflicht

a) Grundsatz

Die Meldung ist nach Art. 33 Abs. 1 Satz 1 DSGVO **unverzüglich**, mithin **ohne schuldhaftes Zögern**, zu erstatten. Dies gilt insbesondere für leicht zu erkennende und leicht zu beschreibende sowie für besonders gewichtige meldepflichtige Ereignisse. **74**

75 Die in Art. 33 Abs. 1 Satz 1 DSGVO enthaltene **72-Stunden-Frist** ist eine Richtgröße, an deren Überschreitung eine Begründungspflicht (Art. 33 Abs. 1 Satz 2 DSGVO) anknüpft (die etwa dann zu erfüllen sein kann, wenn sich die 72-Stunden-Frist einmal gerade über die Weihnachtstage erstreckt).

b) Insbesondere: Berechnung der 72-Stunden-Frist

76 Die europarechtlich angeordnete Frist wird nach **Art. 2 ff. Fristen-VO**[10] berechnet. Diese Verordnung gilt für Rechtsakte, die der Rat und die Kommission auf Grund des Vertrages zur Gründung der Europäischen Wirtschaftsgemeinschaft erlassen (Art. 1 Fristen-VO). Dieser Vertrag ist ein Vorgängernormbestand des Vertrags über die Arbeitsweise der Europäischen Union, auf den die Datenschutz-Grundverordnung – eine Verordnung des Europäischen Parlaments und des Rates – gestützt ist. Die Vorschriften des Bürgerlichen Gesetzbuchs (BGB) zu Fristen sind nicht heranzuziehen.

77 Für den **Fristbeginn** ist bei der 72-Stunden-Frist Art. 3 Abs. 1 UAbs. 1 Fristen-VO maßgeblich. Dort heißt es:

> „Ist für den Anfang einer nach Stunden bemessenen Frist der Zeitpunkt maßgebend, in welchem ein Ereignis eintritt oder eine Handlung vorgenommen wird, so wird bei der Berechnung dieser Frist die Stunde nicht mitgerechnet, in die das Ereignis oder die Handlung fällt."

78 Das für den Anfang der Frist **maßgebliche Ereignis** ist das **Bekanntwerden der Datenschutzverletzung**. Die Frist tritt dann nicht sofort, sondern mit Anfang der nächsten Stunde in Lauf. Wird also eine Datenschutzverletzung um 16.20 Uhr bekannt, beginnt die 72-Stunden-Frist um 17.00 Uhr.

79 Das **Ende der Frist** richtet sich nach Art. 3 Abs. 2 Buchst. a Fristen-VO:

> „Eine nach Stunden bemessene Frist beginnt am Anfang der ersten Stunde und endet mit Ablauf der letzten Stunde der Frist."

80 Die Frist läuft an einem **Feiertag, Sonntag** oder **Samstag** (Normtext: Sonnabend) weiter, weil weder in der Datenschutz-Grundverordnung noch anderer Stelle etwas Abweichendes bestimmt ist (vgl. Art. 3 Abs. 3 Fristen-VO). Endet die 72-Stunden-Frist an einem Feiertag, Sonntag oder Samstag, verlängert sie sich nicht bis zum nächsten Arbeitstag (das ist nach Art. 2 Abs. 2 Fristen-VO ein Tag, der nicht Feiertag, Sonntag oder Samstag ist). Art. 3 Abs. 4 UAbs. 1 Fristen-VO, der eine solche Verlängerung bewirken könnte, ist nämlich nicht auf Fristen anwendbar, die nach Stunden bemessen sind.

81 Auch die Regelung in Art. 3 Abs. 5 Fristen-VO kann nicht zu einer Verlängerung führen; sie setzt eine „Frist von zwei oder mehr Tagen", mithin eine nach Tagen – nicht nach Stunden – bemessene Frist voraus.

[10] Nichtamtlicher Kurztitel der Verordnung (EWG, Euratom) Nr. 1182/71 des Rates vom 3. Juni 1971 zur Festlegung der Regeln für die Fristen, Daten und Termine (ABl. L 124 vom 8. Juni 1971, S. 1).

„Jede Frist von zwei oder mehr Tagen umfasst mindestens zwei Arbeitstage."

Die Norm bietet eine klare Regelung nur in den Fällen von Art. 3 Abs. 2 Buchst b Fristen-VO. Die gesetzliche Option, Stundenfristen festzulegen, ist im Übrigen – wie Art. 3 Abs. 4 UAbs. 1 Fristen-VO zeigt – als eine Option gedacht, punktgenaue, von der Lage der Feiertage, Sonntage oder Samstage unabhängige Handlungsprogramme festlegen zu können. **82**

Den Ablauf und die Berechnung der 72-Stunden-Frist veranschaulicht das nachfolgende **Beispiel**: **83**

	01:00	02:00	03:00	04:00	05:00	06:00	07:00	08:00	09:00	10:00	11:00	12:00	13:00	14:00	15:00	16:00	17:00	18:00	19:00	20:00	21:00	22:00	23:00	24:00
01.11.2018														V										
02.11.2018								F										K	1	2	3	4	5	6
03.11.2018	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
04.11.2018	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
05.11.2018	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72						
06.11.2018																								

Am Donnerstag, den 1. November 2018 (Allerheiligen) um 14.30 Uhr ereignete sich ein Außenangriff auf eine interne Datenbank. Der Vorfall (V) wurde in einem Fachsachgebiet am Freitag, den 2. November 2018 um 8.00 Uhr bemerkt (F) und der Behördenleitung gemeldet. Weil die Qualität des Vorfalls nicht „auf den ersten Blick" einzuschätzen war, ließ die Behördenleitung den Sachverhalt durch das IT-Sachgebiet näher aufklären. Um 18.50 Uhr waren dort Umstände bekannt, die den Vorfall als meldepflichtige Datenschutzverletzung erscheinen ließen. Zu diesem Zeitpunkt hatte der Verantwortliche die nötige Kenntnis (K). Der Vorfall war daher unverzüglich zu melden. Die 72-Stunden-Frist begann „zur nächsten vollen Stunde", also um 19.00 Uhr und endete am Montag, den 5. November 2018 um 19.00 Uhr. Würde die Meldung bei der Datenschutz-Aufsichtsbehörde zu einem späteren Zeitpunkt eingehen, müsste ihr eine Begründung für die Verzögerung beigegeben sein.

c) Umfang der Meldung

Die Meldung enthält mindestens die in Art. 33 Abs. 3 DSGVO aufgeführten Informationen. Der Bayerische Landesbeauftragte für den Datenschutz hat ein Online-Meldeformular bereitgestellt, das die nötigen Angaben enthält und dessen Benutzung den bayerischen öffentlichen Stellen daher empfohlen wird (Erläuterungen dazu →Rn. 121 ff.). **84**

Bei **komplexeren Datenschutzverletzungen** stehen mitunter nicht alle Informationen sogleich zur Verfügung. So kann ein von außen auf ein System geführter Angriff zunächst nur anhand bestimmter Unregelmäßigkeiten zu erkennen sein, ohne dass bereits das Angriffsmittel und/oder seine Wirkungsweise bekannt wären. Oder es wird deutlich, dass personenbezogene Daten unbefugt offengelegt worden sind, jedoch erst einmal nicht, in welchem Umfang die Vertraulichkeit beeinträchtigt ist. In Fällen dieser Art erstattet der Verantwortliche gegenüber der Datenschutz-Aufsichtsbehörde eine (Erst-)Meldung, sobald die Meldepflicht eingreift. Er ergänzt die Meldung „ohne unangemessene weitere Verzögerung" (Art. 33 Abs. 4 DSGVO), wenn ihm die noch fehlenden Angaben möglich sind, oder wenn ihm sonst Informationen bekannt werden, welche für die Beurteilung der Datenschutzverletzung von Bedeutung sind. Das gilt insbesondere für Informationen, welche die der Erstmeldung zugrunde liegenden Annahmen zu Eintrittswahrscheinlichkeit und Schwere möglicher **85**

Nachteile für betroffene Personen in einem anderen Licht erscheinen lassen (insbesondere: Aufstufung des Risikos auf Grund nachträglich gewonnener Erkenntnisse).

4. Organisatorische Vorkehrungen

86 Vor diesem Hintergrund sollte der Verantwortliche klare **Regelungen** zur Feststellung und zur Kommunikation von meldepflichtigen Ereignissen treffen. In einer Datenschutz-Dienstanweisung sowie erforderlichenfalls in ergänzenden innerdienstlichen Regelungen für das Verhalten bei solchen Ereignissen sollte nicht nur festgelegt werden, welche Funktionseinheit allfällige Meldungen gegenüber der Datenschutz-Aufsichtsbehörde regulär abgibt und welche Funktionseinheiten ausnahmsweise – etwa während Feiertagen – dafür zuständig sind. Geregelt werden sollte insbesondere auch, was beim Bekanntwerden von Anhaltspunkten für ein meldepflichtiges Ereignis zu tun ist, wie die „Meldeketten" beschaffen sind, wer erforderlichenfalls den Sachverhalt aufklärt und wer ihn in meldefähiger Form aufbereitet. Soweit es um die Meldung von Datenschutzverletzungen geht, die von Beschäftigten (selbst) verursacht sind, kann die Umsetzung der Pflicht nach Art. 33 DSGVO nur gelingen, wenn der Verantwortliche eine Fehlerkultur etabliert, welche die Risikoprävention vor die „Suche nach Schuldigen" stellt. Zudem sollte der Verantwortliche auch Ereignisse dokumentieren, die auf organisatorisches Fehlverhalten hindeuten (dazu →Rn. 10), und diesen Informationsbestand regelmäßig auswerten.

87 Davon abgesehen sollten die Beschäftigten durch geeignete **Schulungsangebote** befähigt werden, die Verursachung meldepflichtiger Ereignisse zu vermeiden und Anhaltspunkte für – insbesondere extern ins Werk gesetzte – Angriffe auf die Datensicherheit zu erkennen.

V. Meldepflicht des Auftragsverarbeiters

Art. 33 Abs. 2 DSGVO bestimmt für den Fall der Auftragsverarbeitung, dass der Auftragsverarbeiter Datenschutzverletzungen unverzüglich, also ohne schuldhaftes Zögern (→Rn. 74), an den Verantwortlichen meldet. Im „Außenverhältnis" zur Datenschutz-Aufsichtsbehörde ist der Auftragsverarbeiter nicht meldepflichtig. Wird die im „Innenverhältnis" zum Verantwortlichen bestehende Meldepflicht erfüllt, so ist damit jedoch nicht „alles erledigt". Vielmehr muss der Verantwortliche die Datenschutzverletzung nach Maßgabe von Art. 33 Abs. 1 DSGVO prüfen und erforderlichenfalls an die Datenschutz-Aufsichtsbehörde melden. Auch die zeitliche Vorgabe – unverzüglich und möglichst binnen 72 Stunden – ist dabei zu beachten. Sie wird in Lauf gesetzt, sobald der Verantwortliche die erforderlichen Informationen vom Auftragsverarbeiter erhalten hat. **88**

Vor diesem Hintergrund sollte eine Auftragsverarbeitungs-Vereinbarung für den Fall einer Datenschutzverletzung beim Auftragsverarbeiter mindestens regeln: **89**

- den **Meldeweg** zum Verantwortlichen einschließlich Benennung der jeweiligen Ansprechpersonen und ihrer Erreichbarkeit;
- den **Inhalt der** vom Auftragsverarbeiter zu erstattenden **Meldung**; zu empfehlen ist insofern eine Anlehnung an den Inhalt der Meldung, wie sie (anschließend) vom Verantwortlichen abzugeben ist (→Rn. 121 ff.).

In einer Auftragsverarbeitungs-Vereinbarung kann auch geregelt werden, dass der Auftragsverarbeiter zugleich mit der Meldung an den Verantwortlichen oder nach Einholung einer Zustimmung des Verantwortlichen in dessen Namen die Meldung an die Datenschutz-Aufsichtsbehörde erstattet. Diese Meldung muss dann den gemäß Art. 33 DSGVO für eine Meldung des Verantwortlichen geltenden Anforderungen entsprechen. Datenschutzaufsichtliche Maßnahmen wegen unterlassener, unvollständiger oder verzögerter Meldungen treffen auch in diesem Fall aber den Verantwortlichen, der sich durch eine Bevollmächtigung des Auftragsverarbeiters also nicht „freizeichnen" kann. **90**

VI. Benachrichtigungspflicht des Verantwortlichen gegenüber der betroffenen Person (Art. 34 DSGVO)

91 Kommt es zu einer Datenschutzverletzung, kann neben der Meldung an die zuständige Datenschutz-Aufsichtsbehörde auch eine Benachrichtigung von betroffenen Personen erforderlich sein. Unter welchen Voraussetzungen diese Pflicht eingreift, wann sie ausnahmsweise entfällt und wie sie zu erfüllen ist, regelt Art. 34 DSGVO. Die Vorschrift greift auf Regelungselemente zurück, die auch in Art. 33 DSGVO verwendet sind. Dies gilt insbesondere für das Merkmal der Datenschutzverletzung sowie die Risikobeurteilung.

1. Verantwortlicher, betroffene Personen

92 Die Benachrichtigungspflicht trifft den **Verantwortlichen** (Art. 4 Nr. 7 DSGVO, →Rn. 64) gegenüber einer **betroffenen Person** (Art. 4 Nr. 1 DSGVO). Das ist im Kontext der Benachrichtigungspflicht diejenige natürliche Person, für deren Rechte und Freiheiten die Datenschutzverletzung ein hohes Risiko zur Folge hat. Ein Risiko für das Datenschutzgrundrecht (Art. 16 Abs. 1 AEUV) oder das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) muss nicht im Vordergrund stehen (→Rn. 56, Beispiel 2).

93 Die Benachrichtigungspflicht trifft den Verantwortlichen nicht gegenüber **sonstigen** Interessenten, insbesondere nicht gegenüber Personen, die dem Verantwortlichen – ohne selbst an Rechten und Freiheiten berührt zu sein – Anhaltspunkte für eine Datenschutzverletzung mitgeteilt haben.

2. Entstehen der Benachrichtigungspflicht

94 Die Benachrichtigungspflicht nach Art. 34 Abs. 1 DSGVO ist mit der Meldepflicht nach Art. 33 Abs. 1 DSGVO im Entstehungstatbestand verknüpft. Sie setzt zum einen eine **Verletzung des Schutzes personenbezogener Daten** voraus (zur Prüfung dieses Merkmals →Rn. 4 ff.). Diese Datenschutzverletzung muss „voraussichtlich ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge“ haben. Dieses Risiko ist in einer Risikobeurteilung festzustellen (zur Risikobeurteilung →Rn. 20 ff.). Hat der Verantwortliche geprüft, ob eine **Datenschutzverletzung** vorliegt, und hat er weiterhin eine **Risikobeurteilung** durchgeführt, so weiß er einerseits, ob ihn eine Meldepflicht nach Art. 33 DSGVO trifft, und andererseits auch, ob er außerdem noch die Benachrichtigungspflicht nach Art. 34 DSGVO erfüllen muss.

3. Ausschluss der Benachrichtigungspflicht

Anders als die Meldepflicht kann die Benachrichtigungspflicht nach Maßgabe differenzierter **Ausschlusstatbestände** entfallen. Eine Benachrichtigung betroffener Personen ist nämlich nicht in jeder Konstellation einer Datenschutzverletzung mit der Folge eines hohen Risikos für die Rechte und Freiheiten natürlicher Personen sinnvoll. Der Unionsgesetzgeber hat solche Ausschlusstatbestände für Fälle einer **vorsorglichen Risikoabschirmung** (a), einer **nachträglichen Risikominimierung** (b) und eines **unverhältnismäßigen Aufwands** (c) vorgesehen. Der bayerische Landesgesetzgeber hat zudem die auf Art. 34 DSGVO anwendbare Ermächtigung in Art. 23 Abs. 1 DSGVO genutzt, um die Benachrichtigungspflicht auch dann auszuschließen, wenn dies zum **Schutz bestimmter rechtlich geschützter Belange** erforderlich ist (d). 95

a) Ausschluss bei vorsorglicher Risikoabschirmung

Nach Art. 34 Abs. 3 Buchst. a DSGVO ist die Benachrichtigung betroffener Personen nicht erforderlich, wenn der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden. Die Vorschrift nimmt Maßnahmen nach Art. 25 Abs. 1, 2 und Art. 32 Abs. 1 DSGVO in Bezug und nennt beispielhaft die Verschlüsselung. Dass solche Maßnahmen auch bei der Risikobeurteilung zu berücksichtigen sind und häufig zum Ausschluss eines hohen Risikos führen werden (→Rn. 57), dürfte die praktische Bedeutung von Art. 34 Abs. 3 Buchst. a DSGVO wohl relativieren. 96

b) Ausschluss bei nachträglicher Risikominimierung

Eine Benachrichtigung betroffener Personen ist nach Art. 34 Abs. 3 Buchst. b DSGVO weiterhin nicht erforderlich, wenn der Verantwortliche durch der Datenschutzverletzung nachfolgende Maßnahmen sichergestellt hat, dass ein hohes Risiko für die Rechte und Freiheiten betroffener Personen aller Wahrscheinlichkeit nach nicht mehr besteht. Eine Anwendung dieses Ausschlusstatbestands setzt zum einen voraus, dass ein hohes Risiko jedenfalls anfänglich bestand, und zum anderen, dass sich das hohe Risiko nicht bereits in einem Schaden manifestiert hat. 97

Die „Abwendungsmaßnahme“ muss so wirken, dass mit einem Schadenseintritt aus Sicht eines verständigen Beurteilers nicht mehr zu rechnen ist (Niveau des geringen Risikos, →Rn. Fehler! Verweisquelle konnte nicht gefunden werden.). Der Verantwortliche muss in solchen Fällen eine klare Vorstellung von der Datenschutzverletzung, von möglichen Folgen sowie von den Verletzung und Folge verknüpfenden Wirkungszusammenhängen haben. Dieses Wissen ist zu dokumentieren; der Verantwortliche hat – im Rahmen seiner Rechenschaftspflicht auch gegenüber der Datenschutz-Aufsichtsbehörde – nachzuweisen, dass die gewählten Abwendungsmaßnahmen eine sachgerechte und hinreichend risikominimierende Reaktion auf die Datenschutzverletzung darstellen. 98

Beispiele: Ein interner Angreifer verschafft sich Zugangspasswörter von Kollegen, um auf Daten aus deren jeweiligem Zuständigkeitsbereich zugreifen zu können. Der Verantwortli-

che bemerkt dies, bevor es zu einem Zugriff kommt und ändert die Passwörter. – Einem Verantwortlichen fällt auf, dass ein externer Angreifer in ein System eindringt. Bevor er personenbezogene Daten herunterladen kann, gelingt es dem Verantwortlichen, den Hacker zu enttarnen, der im weiteren Verlauf auf Veranlassung der vom Verantwortlichen verständigten Strafverfolgungsbehörde festgenommen wird.

c) Ausschluss bei unverhältnismäßigem Aufwand

99 Nicht erforderlich ist eine Benachrichtigung betroffener Personen zudem, wenn dies mit einem unverhältnismäßigen Aufwand verbunden wäre (Art. 34 Abs. 3 Buchst. c Satz 1 DSGVO). Für die Anwendung dieses Ausnahmetatbestandes genügt es nicht, dass die Erfüllung der Benachrichtigungspflicht lästige Mehrarbeit und/oder Kosten verursacht. Im Fall einer Datenschutzverletzung, die mit einem hohen Risiko verbunden ist, kommt dem Transparenzgedanken besondere Bedeutung zu (vgl. Art. 5 Abs. 1 Buchst. a DSGVO). Dem entspricht am ehesten eine individuell adressierte Information.

100 Allerdings sind Fälle denkbar, in welchen der Verantwortliche nicht über die für eine Benachrichtigung erforderlichen Kontaktdaten verfügt oder genaue Betroffenheiten (noch) nicht bekannt sind. In solchen Fällen muss sich der Verantwortliche nicht darauf konzentrieren, die fehlenden Informationen zu beschaffen. Er kann den in Art. 34 Abs. 3 Buchst. c Satz 2 DSGVO gewiesenen Weg einer öffentlichen Bekanntmachung wählen. So ist auch eine zeitnahe Information sichergestellt. Die öffentliche Bekanntmachung muss (zumindest) die in Art. 34 Abs. 2 DSGVO genannten Informationen enthalten. In der Regel dürfte es ratsam sein, die Information durch aufklärende Öffentlichkeitsarbeit zu begleiten. Dies gilt insbesondere dann, wenn eine individuell adressierte Information gerade auch im Hinblick auf die Unübersehbarkeit des Kreises von der Datenschutzverletzung betroffener Personen unterbleibt.

d) Ausschluss zum Schutz bestimmter rechtlich geschützter Belange

101 Nach Art. 13 BayDSG kann die Benachrichtigung betroffener Personen auch unter den Voraussetzungen des Art. 6 Abs. 2 Nr. 3 Buchst. a, b oder d BayDSG unterbleiben. Die Vorschrift greift – bei abweichender Formulierung – die Struktur von Art. 34 Abs. 3 DSGVO auf. Sind die Voraussetzungen des Ausschlusstatbestandes erfüllt, darf eine öffentliche Stelle auf die Benachrichtigung verzichten. Möchte sie dennoch informieren, müssen die Interessen, die der jeweilige Ausschlusstatbestand in Bezug nimmt, zur Disposition der öffentlichen Stelle stehen. Daran fehlt es jedenfalls dann, wenn die Ausschlusstatbestände dem Schutz privater Rechte dienen.

aa) Abwehr von Nachteilen zulasten der Allgemeinheit

102 Eine Benachrichtigung kann nach Art. 13, Art. 6 Abs. 2 Nr. 3 Buchst. a BayDSG unterbleiben, wenn dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und Ordnung erforderlich ist. Diese Intention einer Nicht-Benachrichtigung liegt regelmäßig vor, wenn die personenbezogenen Daten, auf die sich die Datenschutzverletzung bezieht, vom Verantwortlichen zum Zweck der Abwehr erheblicher Nach-

teile für das Gemeinwohl oder von Gefahren für die öffentliche Sicherheit und Ordnung verarbeitet werden. Der Ausschlusstatbestand in Art. 13, Art. 6 Abs. 2 Nr. 3 Buchst. a BayDSG soll auf der in Art. 23 Abs. 1 DSGVO erteilten Ermächtigung zur Beschränkung von Betroffenenrechten beruhen[11]. Die Begriffe „erhebliche Nachteile für das Gemeinwohl" und „Gefahren für die öffentliche Sicherheit und Ordnung" sind vor diesem Hintergrund unionsrechtlich zu verstehen. Die Bedeutungen, die sie im nationalen Polizei- und Sicherheitsrecht haben, können nicht unbesehen übernommen werden.[12]

bb) Verfolgung von Straftaten und Ordnungswidrigkeiten

Eine Benachrichtigung kann gemäß Art. 13, Art. 6 Abs. 2 Nr. 3 Buchst. b BayDSG weiterhin unterbleiben, wenn dies zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 Strafgesetzbuch oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist. **103**

Dieser Ausschlusstatbestand betrifft den Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz (→Rn. 115). Er zielt darauf, die Effektivität der entsprechenden Verfolgungs- und Vollstreckungsmaßnahmen zu gewährleisten. Strafverfolgungsbehörden sind oftmals darauf angewiesen, personenbezogene Daten zunächst ohne Kenntnis betroffener Personen zu erheben und weiterzuverarbeiten. **104**

Zahleiche Befugnisse zu Datenerhebungen sind bereits durch den Gesetzgeber so konzipiert, dass sie auf verfassungsrechtliche Anforderungen an heimliche Grundrechtseingriffe reagieren, indem etwa qualifizierte Verdachts- oder Gefahrentatbestände gefordert werden (siehe etwa § 100c Abs. 1 Strafprozeßordnung – StPO – oder Art. 41 Abs. 1 Polizeiaufgabengesetz – PAG), Richtervorbehalte eingreifen (siehe etwa Art. 100e Abs. 2 Satz 1 StPO oder Art. 41 Abs. 4 Satz 1 PAG) oder eine Protokollierungspflicht mit Kontrollpflicht einer unabhängigen Stelle vorgesehen wird (siehe etwa Art. 51 PAG). In solchen Fällen ist typischerweise auch eine Pflicht einer nachträglichen Benachrichtigung angeordnet, sobald diese ohne Gefährdung des Maßnahmezwecks erteilt werden kann (siehe etwa § 101 Abs. 4 Satz 1 Nr. 5, Abs. 5 Satz 1 StPO, Art. 50 Abs. 1 Satz 1 Nr. 6 PAG). **105**

cc) Abwehr von Nachteilen zulasten Dritter

Eine Benachrichtigung kann gemäß Art. 13, Art. 6 Abs. 2 Nr. 3 Buchst. c BayDSG schließlich unterbleiben, wenn dies zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist. Der pauschal formulierte Ausschlusstatbestand zum Schutz privater Drittinteressen verweist darauf, dass eine Benachrichtigung Empfänger im Einzelfall zu einer drittschädigenden Reaktion auf eine Datenschutzverletzung veranlassen **106**

[11] Vgl. die Entwurfsbegründung, Landtags-Drucksache 17/19628; S. 38.

[12] Siehe dazu im Einzelnen Bayerischer Landesbeauftragter für den Datenschutz, Datenschutzverletzungen: Melde- und Benachrichtigungspflicht unter der Datenschutz-Richtlinie für Polizei und Strafjustiz, Aktuelle Kurz-Information 9, Stand 10/2018, im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen".

kann. Dies gilt insbesondere dann, wenn durch die Benachrichtigung eine für die Datenschutzverletzung verantwortliche Person namhaft gemacht wird oder der Empfänger Rückschlüsse hinsichtlich der Identität einer solchen Person ziehen kann. Allerdings lässt Art. 34 Abs. 2 DSGVO eine insofern zurückhaltende Gestaltung der Benachrichtigung zu. Eine situationsadäquate Anpassung des Inhalts einer Benachrichtigung ist deren Unterlassung stets vorzugswürdig. Im Übrigen kommt eine Anwendung von Art. 13, Art. 6 Abs. 2 Nr. 3 Buchst. c BayDSG wohl in erster Linie dann in Frage, wenn eine „Überreaktion" des Empfängers konkret zu befürchten ist.

3. Erfüllung der Benachrichtigungspflicht

107 Die Benachrichtigung ist grundsätzlich an die betroffenen Personen zu richten. Ausnahmsweise kann eine öffentliche Bekanntmachung in Betracht kommen (→Rn. 100). Den Übermittlungsweg kann der Verantwortliche nach Maßgabe der bei ihm vorhandenen Kontaktdaten wählen (regelmäßig verschlüsselte E-Mail oder Brief). Die Benachrichtigung sollte kurz und verständlich sein (Art. 34 Abs. 2 DSGVO: „in klarer und einfacher Sprache"). Sie zielt darauf, dass der Adressat erfährt, was passiert ist und mit welchen Nachteilen er rechnen muss. Soweit der Adressat (noch) die Möglichkeit hat, selbst zu einer Abwendung oder Verringerung von Nachteilen beizutragen, sollte er auf Grund der Benachrichtigung auch erkennen können, was insofern sinnvollerweise zu tun ist. Vor diesem Hintergrund schreibt Art. 34 Abs. 2 DSGVO vor, dass mindestens die in Art. 33 Abs. 3 Buchst. b, Buchst. c (→Rn. 45 ff., 159 ff.) und Buchst. d DSGVO (→Rn. 31, 57, 97 f., 165 ff.) genannten Informationen und Maßnahmen mitzuteilen sind.

VII. Meldepflicht und Benachrichtigungspflicht im Bereich der Datenschutz-Richtlinie für Polizei und Strafjustiz

Neben der Datenschutz-Grundverordnung haben das Europäische Parlament und der Rat auch die Datenschutz-Richtlinie für Polizei und Strafjustiz erlassen. Diese Richtlinie enthält besondere Regelungen für die Verarbeitung personenbezogener Daten in den Bereichen der Strafverfolgung und -vollstreckung sowie der polizeilichen Gefahrenabwehr. Im Unterschied zur Datenschutz-Grundverordnung musste die Richtlinie in nationales Recht umgesetzt werden; unmittelbare Wirkungen im Verhältnis zwischen den betroffenen Personen und den öffentlichen Stellen kann sie grundsätzlich nicht entfalten. **108**

Die Datenschutz-Richtlinie für Polizei und Strafjustiz macht in Art. 30 RLDSJ zur Meldepflicht des Verantwortlichen gegenüber der Datenschutz-Aufsichtsbehörde und in Art. 31 RLDSJ zur Benachrichtigungspflicht gegenüber betroffenen Personen umfangreiche Vorgaben. Die Vorschriften beschreiben eine herzustellende Rechtslage. Art. 30 RLDSJ lehnt sich dabei an Art. 33 DSGVO, Art. 31 RLDSJ an Art. 34 DSGVO an. **109**

1. Grundgedanken der Umsetzung

Der bayerische Gesetzgeber hat für die Umsetzung der Datenschutz-Richtlinie für Polizei und Strafjustiz insgesamt eine Regelungslösung gewählt, die ein möglichst einheitliches Datenschutzregime sicherstellen möchte: Er hat (in einem ersten Schritt) die Geltung der Datenschutz-Grundverordnung auch für den Bereich der Datenschutz-Richtlinie für Polizei und Strafjustiz angeordnet (Art. 2 Satz 1 BayDSG). In Teil 2 Kapitel 8 des Bayerischen Datenschutzgesetzes (Art. 28 ff. BayDSG) hat er dessen Regelungsgefüge dann (in einem zweiten Schritt) für die Strafverfolgung und -vollstreckung sowie für die polizeiliche Gefahrenabwehr näher angepasst. **110**

Art. 28 Abs. 1 Satz 1 BayDSG nennt die Behörden, für welche die Vorschriften der Art. 28 ff. BayDSG gelten: Polizei, Gerichte in Strafsachen, Staatsanwaltschaften, Strafvollstreckungs- und Justizvollzugsbehörden sowie Behörden des Maßregelvollzugs. Darüber hinaus sind nach Art. 28 Abs. 1 Satz 2 BayDSG Behörden erfasst, die personenbezogene Daten verarbeiten, um Straftaten oder Ordnungswidrigkeiten zu verfolgen oder zu ahnden. Das können auch Kommunen sein, so im Bereich der Verkehrsüberwachung. **111**

Art. 28 Abs. 2 BayDSG regelt näher, welche Vorschriften der Datenschutz-Grundverordnung anzuwenden sind, während Art. 28 Abs. 3 BayDSG einzelne Bestimmungen in Teil 2 Kapitel 1 bis 7 des Bayerischen Datenschutzgesetzes von einer Anwendung ausschließt, also Ausnahmen zum Grundsatz des Art. 2 Satz 1 BayDSG festlegt. In Art. 29 bis 37 BayDSG fin- **112**

den sich dann ergänzende oder modifizierende Vorschriften zu einzelnen Regelungsgegenständen.

113 In diesem Rahmen ist Art. 30 RLDSJ durch Verweis auf Art. 33 DSGVO und Art. 31 RLDSJ durch Verweis auf Art. 34 DSGVO umgesetzt.

2. Regelungen im Einzelnen

114 Allerdings bestehen hinsichtlich der einzelnen von der Datenschutz-Richtlinie für Polizei und Strafjustiz erfassten Verwaltungsbereiche noch fachgesetzliche Regelungen (in der nachfolgenden Tabelle durch Fettdruck hervorgehoben):

Verantwortlicher	Regelungen zur Meldepflicht	Regelungen zur Benachrichtigungspflicht
Staatsanwaltschaften in den Bereichen der Strafverfolgung und der Strafvollstreckung, Polizeidienststellen im Bereich der Strafverfolgung sowie Behörden bei der Verfolgung und Ahndung von Ordnungswidrigkeiten	Art. 2 Satz 1 BayDSG, Art. 28 Abs. 2 Satz 2 BayDSG i. V. m. Art. 33 DSGVO	Art. 2 Satz 1 BayDSG, Art. 28 Abs. 2 Satz 1 Nr. 3 BayDSG i. V. m. Art. 34 DSGVO
Polizeidienststellen im Bereich der Gefahrenabwehr	**Art. 66 Satz 1 PAG**, Art. 2 Satz 1 BayDSG, Art. 28 Abs. 2 Satz 2 BayDSG i. V. m. Art. 33 DSGVO	**Art. 66 Satz 1 PAG**, Art. 2 Satz 1 BayDSG, Art. 28 Abs. 2 Satz 1 Nr. 3 BayDSG i. V. m. Art. 34 DSGVO
Justizvollzugsbehörden, insbesondere Justizvollzugsanstalten und Jugendarrestanstalten	**Art. 205 Abs. 3 Bayerisches Strafvollzugsgesetz (BayStVollzG)**, Art. 2 Satz 1 BayDSG, Art. 28 Abs. 2 Satz 2 BayDSG i. V. m. Art. 33 DSGVO	**Art. 205 Abs. 3 BayStVollzG**, Art. 2 Satz 1 BayDSG, Art. 28 Abs. 2 Satz 1 Nr. 3 BayDSG i. V. m. Art. 34 DSGVO
Einrichtungen des Maßregelvollzugs	**Art. 34 Bayerisches Maßregelvollzugsgesetz (BayMRVG)**, Art. 205 Abs. 3 BayStVollzG, Art. 2 Satz 1 BayDSG, Art. 28 Abs. 2 Satz 2 BayDSG i. V. m. Art. 33 DSGVO	**Art. 34 BayMRVG**, Art. 205 Abs. 3 BayStVollzG, Art. 2 Satz 1 BayDSG, Art. 28 Abs. 2 Satz 1 Nr. 3 BayDSG i. V. m. Art. 34 DSGVO

115 Im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz ist die Meldepflicht nach Art. 33 DSGVO im Übrigen um eine **Nachberichtspflicht** ergänzt. In Art. 33 BayDSG heißt es:

> „Wenn Daten von oder an den Verantwortlichen eines anderen Mitgliedstaates übermittelt wurden, sind die Informationen nach Art. 33 Abs. 3 DSGVO unverzüglich auch an diesen zu melden."

Die nach Art. 30 Abs. 6 RLDSJ umzusetzende Nachberichtspflicht gegenüber dem Verantwortlichen in einem anderen Mitgliedstaat (in der Regel eine im Bereich der Strafverfolgung oder Strafvollstreckung tätige Justiz- oder Polizeibehörde) greift ein, wenn (kumulativ) **116**

- die bayerische öffentliche Stelle im Anwendungsbereich der Datenschutz-Richtlinie für Polizei und Strafjustiz personenbezogene Daten von dem Verantwortlichen aus einem anderen Mitgliedstaat erhalten oder an einen solchen Verantwortlichen übermittelt hat,
- bei der bayerischen öffentlichen Stelle hinsichtlich dieser Daten eine meldepflichtige Datenschutzverletzung eintritt.

Eine andere Funktion hat die in Art. 36 BayDSG geregelte Möglichkeit einer **vertraulichen Meldung von Datenschutzverstößen**, die Art. 48 RLDSJ umsetzt: **117**

> „[1]Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstöße gegen Datenschutzvorschriften zugeleitet werden können. [2]Art. 12 Abs. 2 gilt für die zur Entgegennahme dieser Meldungen betraute Stelle entsprechend."

„Meldbare" Ereignisse sind hier „Verstöße gegen Datenschutzvorschriften"; um eine Verletzung des Schutzes personenbezogener Daten (→Rn. 4 ff.) muss es sich dabei nicht handeln. Die Vorschrift zielt auf eine Fehlerkultur, bei welcher Hinweise auf Defizite nicht „auf dem Dienstweg hängen bleiben." Beschäftigte sollen über Missstände informieren können, ohne Sanktionen durch „Zwischenvorgesetzte" fürchten zu müssen. Außer der meldenden Person und dem Verantwortlichen soll niemand von der Tatsache der Meldung und ihrem Inhalt erfahren. Die mit der Entgegennahme der Meldungen betraute Stelle ist daher grundsätzlich wie der behördliche Datenschutzbeauftragte zur Verschwiegenheit verpflichtet (Art. 36 Satz 2 BayDSG). **118**

Auch wenn in einem Einzelfall ein mitgeteilter Datenschutzverstoß einmal zugleich eine Datenschutzverletzung darstellen sollte, kann die Verschwiegenheitspflicht nur auf den ersten Blick in eine Spannungslage mit der Meldepflicht geraten: Zwar können bei der Meldung gerade Tatsachen mitzuteilen sein, die vertraulich erlangt sind. Doch wirkt die Verschwiegenheitspflicht nach Art. 36 Satz 2 BayDSG trotz der Bezugnahme auf Art. 12 Abs. 2 BayDSG gerade nicht gegenüber dem Verantwortlichen. Sie schottet nur die „zwischengeschaltete" betraute Stelle gegen die übrige Behördenorganisation ab. **119**

Betraute Stelle kann auch der behördliche Datenschutzbeauftragte sein. § 14 Muster einer Datenschutz-Geschäftsordnung (→Fn. 9) enthält einen entsprechenden Regelungsvorschlag. Der behördliche Datenschutzbeauftragte wird im Fall einer ihm vertraulich zur Kenntnis gebrachten Datenschutzverletzung individuell prüfen, wie er ohne Missachtung seiner Verschwiegenheitspflicht auf eine Risikominimierung hinwirken kann (→Rn. 72). Hier kann allerdings der Fall eintreten, dass der Meldende auch die Vertraulichkeit gegenüber dem Verantwortlichen wünscht. In diesem Fall hat die auch gegenüber dem Verantwortlichen wirkende Verschwiegenheitspflicht des Datenschutzbeauftragten nach Art. 12 Abs. 2 BayDSG Vorrang. Eine Zuleitung an den Verantwortlichen muss dann unterbleiben. **120**

VIII. Dokumentation

1. Allgemeines

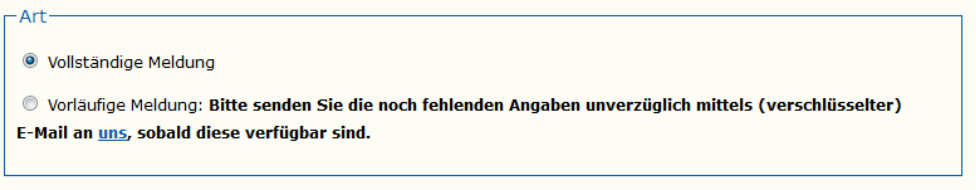
121 Für die Erfüllung der Meldepflicht nach Art. 33 Abs. 1 DSGVO hat der Bayerische Landesbeauftragte für den Datenschutz das **Online-Meldeformular** „Meldung von Verletzungen des Schutzes personenbezogener Daten (Art. 33 DSGVO)“ bereitgestellt. Dieses Formular ist unter https://www.datenschutz-bayern.de/service aufzurufen. Der sachgerechte Gebrauch ist nachstehend erläutert.

122 Die im Rahmen der Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO) gebotene Dokumentation ist mit dem Ausfüllen des Online-Meldeformulars regelmäßig nur teilweise bewirkt. Der Verantwortliche muss insbesondere die **Risikobeurteilung** (→Rn. 27 ff.) in einer nachvollziehbaren Form festhalten, von der das Online-Meldeformular nur einzelne Aspekte abfragt.

2. Hinweise zur Nutzung des Online-Meldeformulars

a) Art der Meldung

123 Was die Art der Meldung betrifft, kann zwischen einer **vollständigen** und einer **vorläufigen Meldung** gewählt werden:



124 Die **vollständige Meldung** ist der **Regelfall**. Wird eine vorläufige Meldung erstattet, sind die noch fehlenden Angaben per (verschlüsselter) E-Mail nachzuliefern. Diese E-Mail sollte die Angaben zum Verantwortlichen wiederholen (im Online-Meldeformular als „Behörde/öffentliche Stelle“ bezeichnet) sowie Datum und Uhrzeit der vorläufigen Meldung nennen. So ist eine eindeutige Zuordnung möglich. Die in der vorläufigen Meldung noch fehlenden Angaben sollten nach den Kategorien aufgeschlüsselt werden, die das Online-Meldeformular zur Verfügung stellt.

Beispiel: Bei Abgabe der vorläufigen Meldung konnte noch gar nicht abgesehen werden, wie viele Datensätze oder wie viele Personen betroffen sein würden. In diesem Fall ließen sich die mit der Nachmeldung mitzuteilenden Angaben etwa so formulieren:

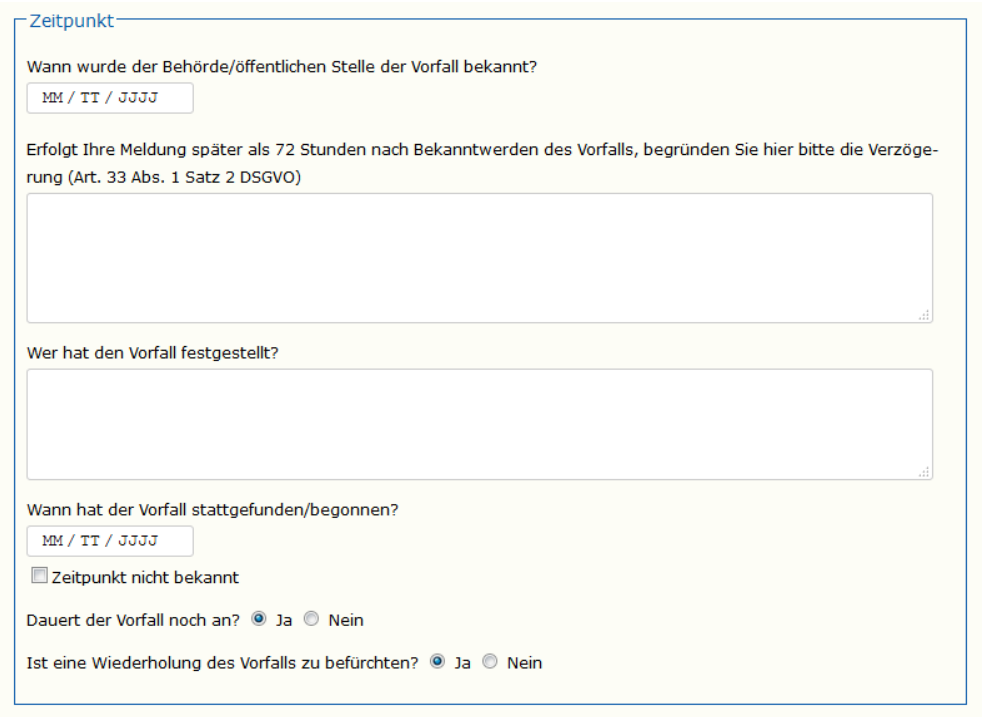
„Betroffene personenbezogene Daten:
Anzahl der Datensätze:
Minimal geschätzte Anzahl der betroffenen Datensätze: 8500

Maximal geschätzte Anzahl der betroffenen Datensätze: 9000
Angaben über die betroffenen Personen:
Minimal geschätzte Anzahl der betroffenen Personen: 3000
Maximal geschätzte Anzahl der betroffenen Personen: 3200".

Das Online-Meldeformular sollte nicht zur **„Nachmeldung"** verwendet werden. Andernfalls würde eine neue Meldung erfasst. 125

b) Zeitpunkt der Meldung

In der Rubrik „Zeitpunkt" ist anzugeben, **wann** der Vorfall **stattgefunden oder begonnen** hat, außerdem, **wann** er dem Verantwortlichen **bekannt** wurde. Das Online-Meldeformular fragt derzeit nur das Datum ab. Dies ändert nichts daran, dass die Dokumentationspflicht des Verantwortlichen insofern weiter reicht (→Rn. 76 ff.). 126



Die Überschreitung der **72-Stunden-Frist** löst eine Begründungspflicht aus (→Rn. 75). Hierfür ist ein eigenes Freitextfeld vorgesehen. Eine Angabe von Stichwörtern (etwa „Wochenende" oder „Krankheit") genügt nicht. In diesem Freitextfeld können auch die Dauer und die Art von **Maßnahmen der Sachverhaltsaufklärung** angegeben werden, wenn diese den Zeitpunkt des Bekanntwerdens hinausgeschoben haben (→Rn. 68 ff.). Als **Personen**, die den **Vorfall festgestellt** haben, werden diejenigen angeführt, die ihn erstmals bemerkt, nicht diejenigen, die ihn bewertet oder gemeldet haben. Ein **Vorfall dauert** noch an, wenn die Datenschutzverletzung eine Folge nach sich gezogen hat, die mit dem Datenschutzrecht nicht in Einklang steht und noch nicht beseitigt ist, oder wenn eine Kette von Datenschutzverletzungen noch nicht unterbrochen ist. 127

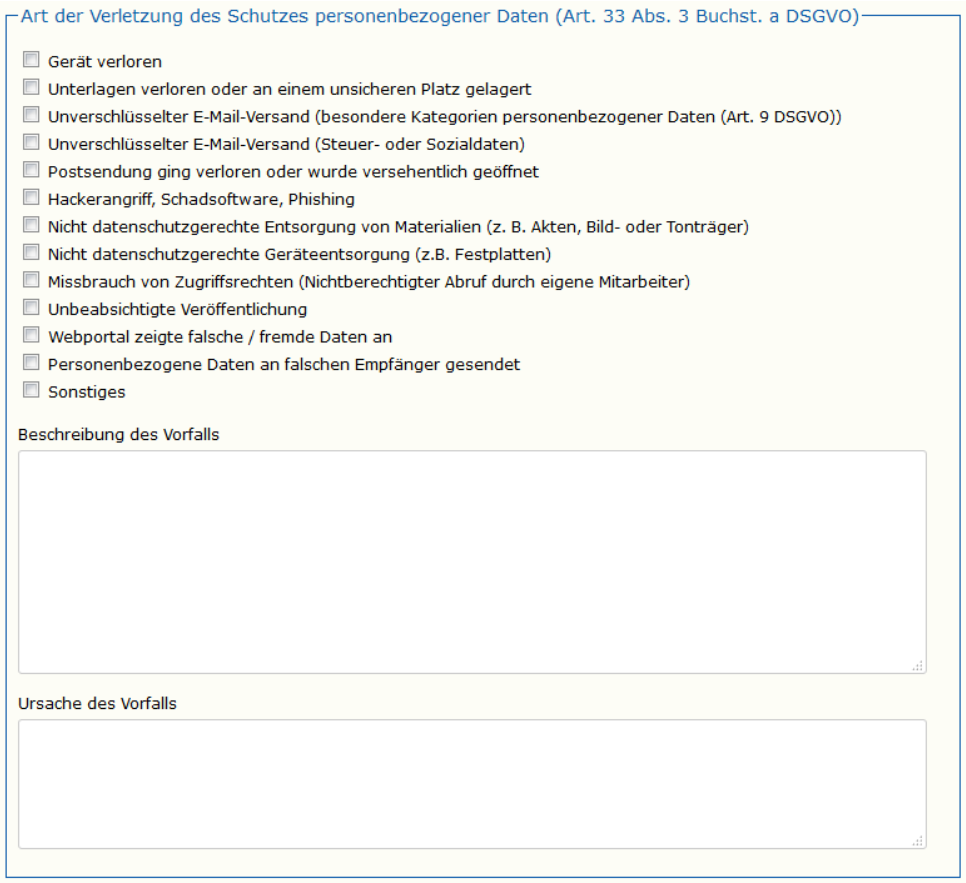
Beispiel: Eine Datenschutzverletzung durch rechtswidrige Bereitstellung personenbezogener Daten im Internet währt jedenfalls so lange, wie diese Daten von der Seite, auf der sie abgerufen werden können, noch nicht entfernt sind. Dies gilt auch dann, wenn sie dort zwar nicht mehr verlinkt sind, jedoch mittels einer Suchmaschine aufgefunden werden können.– Eine Datenschutzverletzung durch eine jeweils um Mitternacht „zuschlagende" Schadsoftware dauert so lange an, wie sie nicht erfolgreich neutralisiert ist.

128 Die **Wiederholung eines Vorfalls** ist zu befürchten, wenn aktuell wieder „alles in Ordnung ist", jedoch konkrete Anhaltspunkte dafür sprechen, dass der Vorfall mindestens ein weiteres Mal eintreten wird.

Beispiel: Zu der Datenschutzverletzung hat eine vorsätzliche Einwirkung von außerhalb eines Systems geführt, der Schädiger ist noch „aktiv", und vorbeugende Maßnahmen konnten seinem Handeln noch nicht oder nicht mit Gewissheit zuverlässig entgegenwirken.

c) Art der Verletzung des Schutzes personenbezogener Daten

129 In der Rubrik „Art der Verletzung des Schutzes personenbezogener Daten" stehen einige tatsächlich häufig vorkommende **Typen eines Verletzungsverhaltens** (→Rn. 6 ff.) zur Auswahl:



Ein **Gerät** ist **verloren**, wenn ein Nutzer nicht mehr weiß, wo er seine Hardware finden kann. Entsprechendes gilt für Unterlagen. 130

Beispiel: Das Vergessen eines Notebooks in einem öffentlichen Verkehrsmittel, das „Davonfliegen" eines versehentlich auf dem Autodach abgelegten Smartphones oder das „Verbummeln" eines USB-Sticks führt zu einem Verlust des Geräts, auch wenn es wieder „auftaucht".

Unterlagen sind an einem **unsicheren Platz** gelagert, wenn sie personenbezogene Daten enthalten und – insbesondere für Bürgerinnen und Bürger – frei zugänglich sind, im Übrigen, wenn für sie besondere technische und organisatorische Schutzmaßnahmen zu treffen sind und diese versäumt wurden. 131

Beispiel: Eine Sozialbehörde unterhält einen großen Arbeitsgruppendrucker, der auch aus den Home-Offices angesteuert werden kann. Er steht in einem Raum, der meistens nicht abgeschlossen ist, und druckt, sobald ein Auftrag eingeht. Wer den Drucker aufsucht, legt die letzten Ausdrucke auf einen Tisch neben dem Drucker. Das meiste wird schnell abgeholt, bei einigen Dokumenten ist das weitere Schicksal unklar.

Der Versand von **E-Mails** mit personenbezogenen Daten **ohne Verschlüsselung** ist datenschutzrechtlich nicht zulässig; als Datenschutzverletzung ist er (jedenfalls) dann zu werden, wenn besondere Kategorien personenbezogener Daten im Sinne von Art. 9 Abs. 1 DSGVO betroffen sind.[13] 132

Eine **Postsendung** ist **verloren**, wenn sie ihren Empfänger nicht erreicht hat. Sie ist **versehentlich geöffnet**, wenn ein Dokument durch eine andere Person als diejenige, für die es bestimmt ist, dem zum Versand dienenden Umschlag oder Behältnis entnommen worden ist. Das ist auch dann der Fall, wenn eine behördliche Poststelle eine verschlossen weiterzuleitende Sendung geöffnet hat. Entsprechende Vorgaben finden sich insbesondere in § 12 Abs. 4 Allgemeine Geschäftsordnung für die Behörden des Freistaates Bayern. 133

Ein meldepflichtiger **Hackerangriff** wird häufig das Ziel verfolgen, einem Dritten die Möglichkeit der Kenntnisnahme personenbezogener Daten zu verschaffen. Allerdings muss nicht notwendig die Datenvertraulichkeit betroffen sein. Auch wenn der Hackerangriff darauf gerichtet ist, die Zugriffsmöglichkeit der öffentlichen Stelle zu beeinträchtigen oder Änderungen in dem vorhandenen Datenbestand vorzunehmen, wird die Meldepflicht eingreifen. Zur **Schadsoftware** zählen insbesondere Computerviren und -würmer, Trojaner, Spyware, Ransomware sowie Dialer. **Phishing**-Angriffe haben regelmäßig den Zweck, Zugangsdaten von Nutzern zu verschaffen. 134

Interne Regelungen zum Umgang von Anwenderinnen und Anwendern mit dem Verdacht auf einen Hackerangriff, mit der Annahme, dass eine Schadsoftware in das System eingeschleust werden soll oder bereits erfolgreich eingeschleust worden ist, sowie mit dem Erhalt phishingsuspekter Nachrichten sollten berücksichtigen, dass technische Laien eine beste- 135

[13] Vgl. etwa Bayerischer Landesbeauftragter für den Datenschutz, 26. Tätigkeitsbericht 2014, Beitrag Nr. 3.6.6 „Verwendung unverschlüsselter E-Mails", im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Tätigkeitsberichte".

hende Bedrohung oftmals nicht adäquat einschätzen können. Solche Regelungen sollten daher stets eine Meldung an die für den IT-Betrieb zuständige Stelle des Verantwortlichen vorsehen. Dieser Stelle sollte dann die Aufgabe zugewiesen sein, die im Rahmen von Art. 33 und 34 DSGVO erforderliche Risikobeurteilung vorzunehmen.

136 Für die **datenschutzgerechte Entsorgung** von Materialien und Geräten bestehen fachliche Standards.[14] Eine Datenschutzverletzung liegt vor, wenn diese fachlichen Standards nicht beachtet werden. Nicht datenschutzgerecht entsorgt sind **beispielsweise**

- ausgesonderte Patientenakten eines Klinikums bei Einwurf in einen Altpapiercontainer (richtig: Einordnung nach DIN 66399 in Schutzklasse 3, mindestens Sicherheitsstufe 4, grundsätzlich Behandlung mit Aktenvernichter ab Anforderung P-4 unter Aufsicht zuständigen Personals des Klinikums);
- ausgesonderte Personalakten, die einem Entsorgungsbetrieb mitgegeben werden, selbst wenn dieser eine „datenschutzgerechte Vernichtung" bescheinigt (richtig: Einordnung nach DIN 66399 in Schutzklasse 2, Sicherheitsstufe 4, grundsätzlich Behandlung mit Aktenvernichter nach Anforderung P-4 unter Aufsicht einer zuständigen Kraft der Personalstelle);
- eine Festplatte, die veräußert wird, nachdem die auf ihr gesicherte Kundendatei eines gemeindlichen Wasserwerks gelöscht wurde (richtig: Einordnung nach DIN 66399 in Schutzklasse 1, Sicherheitsstufe 3, grundsätzlich Verformung der Festplatte nach Anforderung H-3 unter Aufsicht zuständigen Personals der Gemeinde).

137 Ein **Missbrauch von Zugriffsrechten** (nichtberechtigter Abruf durch eigene Beschäftigte) kommt als für Art. 33 DSGVO relevantes Verletzungsverhalten nur dann in Frage, wenn eine Anwenderin oder ein Anwender tatsächlich eine ihr oder ihm für das System nicht erteilte Berechtigung, personenbezogene Daten zur Kenntnis zu nehmen oder mit ihnen zu arbeiten (→Rn. 6 ff.), einsetzt, um einen Verletzungserfolg (→Rn. 11) herbeizuführen.

138 Bei der **unbeabsichtigten Veröffentlichung** gelangen personenbezogene Daten potenziell zur Kenntnis einer unbestimmten Zahl von Personen; die Daten dürften dabei nach dem materiellen Datenschutzrecht entweder gar nicht, jedenfalls aber nicht zu dem betreffenden Zeitpunkt publiziert werden. Unbeabsichtigt veröffentlicht sind **beispielsweise**

- Vorlagen für eine Gemeinderatssitzung, die Einzelangelegenheiten von Bürgerinnen und Bürgern betreffen, wenn sie entgegen den gesetzlichen Vorgaben oder innerbehördlichen Anweisungen in das Bürgerinformationssystem anstatt in das Ratsinformationssystem der Gemeinde eingestellt worden sind,
- der gesamte Inhalt eines Ratsinformationssystems, wenn ein Gemeinderatsmitglied versehentlich seine Benutzerkennung und sein Zugangspasswort offenlegt,

[14] Insbesondere DIN 66399-1, Büro- und Datentechnik – Vernichten von Datenträgern – Teil 1: Grundlagen und Begriffe, Stand 2012, und DIN 66399-2, Büro- und Datentechnik – Vernichten von Datenträgern – Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern, Stand 2012, im Internet beziehbar über https://www.beuth.de.

– Unterlagen für den nichtöffentlichen Teil einer Gemeinderatssitzung, die infolge Fehlbedienung bereits während des öffentlichen Teils mittels Beamer „an die Wand geworfen“ werden.

Ein **Webportal zeigt falsche oder fremde Daten** an, wenn eine Anwenderin oder ein Anwender nach einem ordnungsgemäßen Login Zugang zu einem anderen als dem „eigenen“ Datensatz erhält. Werden unzutreffende Daten angezeigt, kann dies darauf hinweisen, dass es bei dem Verantwortlichen zu einer Beeinträchtigung der Datenintegrität gekommen ist. Vor der Meldung einer Datenschutzverletzung wird der Verantwortliche allerdings prüfen, ob nicht bei einer Bearbeitung des Datensatzes eine Falscheingabe stattgefunden hat. Diese führt zwar zu unrichtigen Daten im Sinne von Art. 16 Satz 1 DSGVO, grundsätzlich jedoch nicht zu einer Datenschutzverletzung. 139

Personenbezogene Daten werden **an den falschen Empfänger** gesendet, wenn sie nicht an denjenigen adressiert sind, der bestimmungsgemäß Kenntnis erlangen soll. Typische Fälle sind die Fehladressierung von Briefen – insbesondere im Bereich der Krankenhäuser die Fehladressierung von Arztbriefen – sowie der Versand von E-Mails an eine andere Person als den vorgesehenen Empfänger oder an einen falschen Verteiler. Häufig ist die Fehladressierung bereits daran zu erkennen, dass – bei einem Brief – die Anrede und die Angaben im Adressfeld oder – bei einer E-Mail – Anrede und Adresse voneinander abweichen. Kann der Empfänger lediglich erkennen, dass das ihm zugegangenen Dokument „einen anderen betreffen muss“, nicht jedoch, um wen es sich handelt, wird regelmäßig keine Datenschutzverletzung vorliegen. Anderes gilt, wenn der Empfänger rekonstruieren kann, wer „eigentlich“ gemeint ist. 140

Lässt sich die Datenschutzverletzung keinem der angegebenen häufigen Typen zuordnen, wird ein Haken vor „Sonstiges“ gesetzt. 141

In einem Freitextfeld ist der als Datenschutzverletzung gewertete **Vorfall** zu **beschreiben**. Dies gilt unabhängig davon, wie die Datenschutzverletzung zuvor klassifiziert worden ist. Die Angaben sollen knapp, aber präzise sein. 142

Beispiel 1 (Fallgruppe „Gerät verloren“): „Der Beschäftigte […] fuhr vom Landratsamt […] mit einem Dienstwagen nach […]. Er gibt an, er müsse gegen 12:00 Uhr das ihm dienstlich überlassene Smartphone beim Einsteigen auf dem Wagendach abgelegt haben. Das Smartphone wurde von Schulkindern um 12:30 Uhr in beschädigtem Zustand am Fußgängerüberweg […] aufgefunden, anhand eines Aufklebers als Eigentum des Landratsamts identifiziert und dort um 12:45 Uhr abgegeben.“

Beispiel 2 (Fallgruppe „Hackerangriff, Schadsoftware, Phishing“): „Der Personalsachbearbeiter […] arbeitet teilweise an einem häuslichen Arbeitsplatz. Für diesen Zweck ist er mit einem Notebook ausgestattet, das sich im Rahmen einer VPN-Lösung mit dem Netzwerk des Landratsamts […] verbindet. Der Beschäftigte gibt an, er habe am Vorfallstag gegen 10:00 Uhr während der Auswertung von Bewerbungen für die Stelle eines Sachbearbeiters Bauverwaltung an seine dienstliche E-Mail-Adresse eine Nachricht von service@itdlz[…].de erhalten. In dieser Nachricht sei er aufgefordert worden, eine angehängte Datei mit dem Namen ‚Win95.exe‘ auszuführen. Wie in der E-Mail angegeben, habe er sein Administratoren-Passwort eingegeben und die erscheinenden Warnmeldungen weggeklickt. Der Bildschirm

sei dann schwarz geworden. Nach einigen Minuten sei die Windows-Eingabeaufforderung erschienen. Die Domain „itdlz[...].de“ wird von dem IT-Dienstleistungszentrum [...] verwendet, welches auch das Landratsamt [...] betreut. Allerdings ist dort die Benutzerkennung ‚service‘ nicht vergeben. Der Beschäftigte brachte das Notebook unverzüglich beim Helpdesk des IT-Dienstleistungszentrums vorbei. Wiederherstellungsversuche blieben erfolglos.“

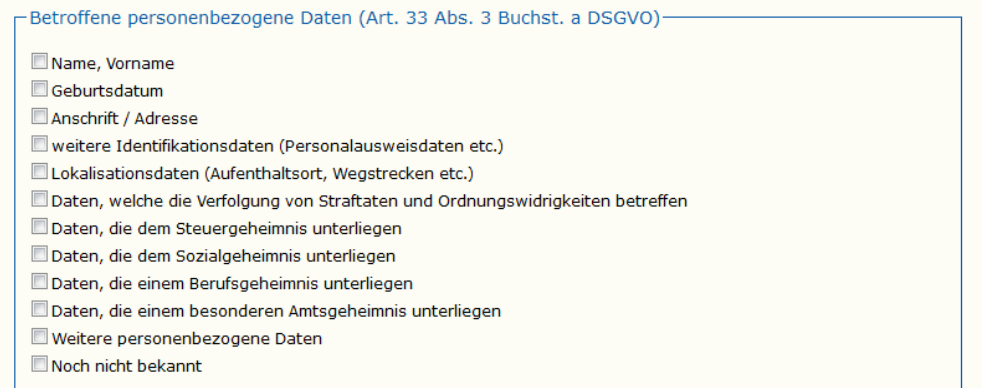
143 In einem weiteren Volltextfeld werden die **Ursachen des Vorfalls** angegeben, die bereits ermittelt werden konnten. Soweit die Ursachen noch nicht oder noch nicht vollständig bekannt sind, genügen vorläufige Angaben. Ist die Sachverhaltsaufklärung abgeschlossen, werden die Ergebnisse im Rahmen einer Nachmeldung mitgeteilt (→Rn. 124 f.).

Beispiel 1 (Fallgruppe „Gerät verloren“): „Ursächlich für den Vorfall war eine Unaufmerksamkeit des Beschäftigten, der wegen eines Termins um 12:15 Uhr rechtzeitig in [...] sein wollte.“

Beispiel 2 (Fallgruppe „Hackerangriff, Schadsoftware, Phishing“): „Ursächlich für den Vorfall war ein unter der Bezeichnung ‚Win95.exe‘ firmierendes Programm, das eine Neuformatierung der Festplatte des betroffenen Notebooks bewirkte. Mitursächlich war, dass dem Benutzer eine Kennung mit Administratorenrechten zur Verfügung stand, und dass dieser einer ungewöhnlichen Situation nicht mit dem nötigen Misstrauen begegnete. Die verwendete E-Mail-Adresse wich vom Üblichen ab, außerdem verschickt das IT-Dienstleistungszentrum [...] keine Dateien mit der Endung ‚.exe‘ an einzelne Benutzer. Die Identität des Angreifers konnte bisher nicht ermittelt werden.“

d) Betroffene personenbezogene Daten

144 In der Rubrik „betroffene personenbezogene Daten“ beschreibt die meldende öffentliche Stelle, worauf sich die Datenschutzverletzung bezieht.



145 Als Auswahlfelder für die Datenkategorien stehen zunächst **„Name, Vorname“**, **„Geburtsdatum“** sowie **„Anschrift/Adresse“** zur Verfügung. Dazu zählen neben einer Haus- oder Postfach-Anschrift auch die persönliche E-Mail-Adresse.

146 In die Rubrik **„weitere Identifikationsdaten“** gehören alle Merkmale, die einer natürlichen Person individuell zugeordnet sind, wie etwa die Personalausweisnummer, die Steueridentifikationsnummer oder die Sozialversicherungsnummer. Die Rubrik erfasst weiterhin Merk-

male, die Dritten unter Zuhilfenahme öffentlicher Register den Rückschluss auf bestimmte natürliche Personen ermöglichen, wie dies etwa bei Flurnummern von Grundstücken oder bei Kraftfahrzeugkennzeichen der Fall ist. Das ist insbesondere bei einer Beeinträchtigungen der Datenvertraulichkeit von Bedeutung.

„Lokalisationsdaten“ geben Auskunft über die Frage des „Wer – Wann – Wo?“ Dabei kann es sich um die Ortungsdaten eines GPS-Systems handeln, sei dies nun in einem Dienstfahrzeug eines kommunalen Bauhofs oder in einer elektronischen Fußfessel verbaut. Lokalisationsdaten fallen an, wenn eine Polizeibehörde die Videokameras einer U-Bahn-Station in Bezug auf eine bestimmte verdächtige Person ausgewertet und dabei dokumentiert hat, zu welcher Zeit sich diese Person an welcher Stelle in dem Bauwerk aufhielt. Gleiches gilt, wenn eine Gesichtserkennungssoftware diese Aufgabe hinsichtlich einer Vielzahl – regelmäßig überwiegend unverdächtiger – Personen übernimmt. Lokalisationsdaten enthält aber auch das klassische Fahrtenbuch. **147**

Personenbezogene **„Daten, welche die Verfolgung von Straftaten und Ordnungswidrigkeiten betreffen“**, sind von einer dafür zuständigen Behörde (Staatsanwaltschaft, Polizei, Behörde mit einer Zuständigkeit nach §§ 87 ff. Zuständigkeitsverordnung) für den Zweck der Durchführung entsprechender Verfahren bestimmt. Daten dieser Art enthalten insbesondere die Ermittlungsakten, das staatsanwaltschaftliche Verfahrensregister sowie der polizeiliche Kriminalaktennachweis. **148**

Zu den **„Daten, die dem Steuergeheimnis unterliegen“** zählen nicht nur die von § 30 Abs. 2 Abgabenordnung (AO), sondern auch die von Art. 13 Abs. 1 Nr. 1 Buchst. c Kommunalabgabengesetz i. V. m. § 30 Abs. 2 AO erfassten Daten. **149**

Hinweis: Sind Daten betroffen, die dem Steuergeheimnis unterliegen, sollte eingehend geprüft werden, an welche Datenschutz-Aufsichtsbehörde eine Meldung nach Art. 33 DSGVO zu richten ist. Die Datenschutzaufsicht ist hier zwischen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und den Landesbeauftragten – sowie im Fall der Kirchensteuer den kirchlichen Datenschutz-Aufsichtsbehörden – geteilt (näher § 32h AO).

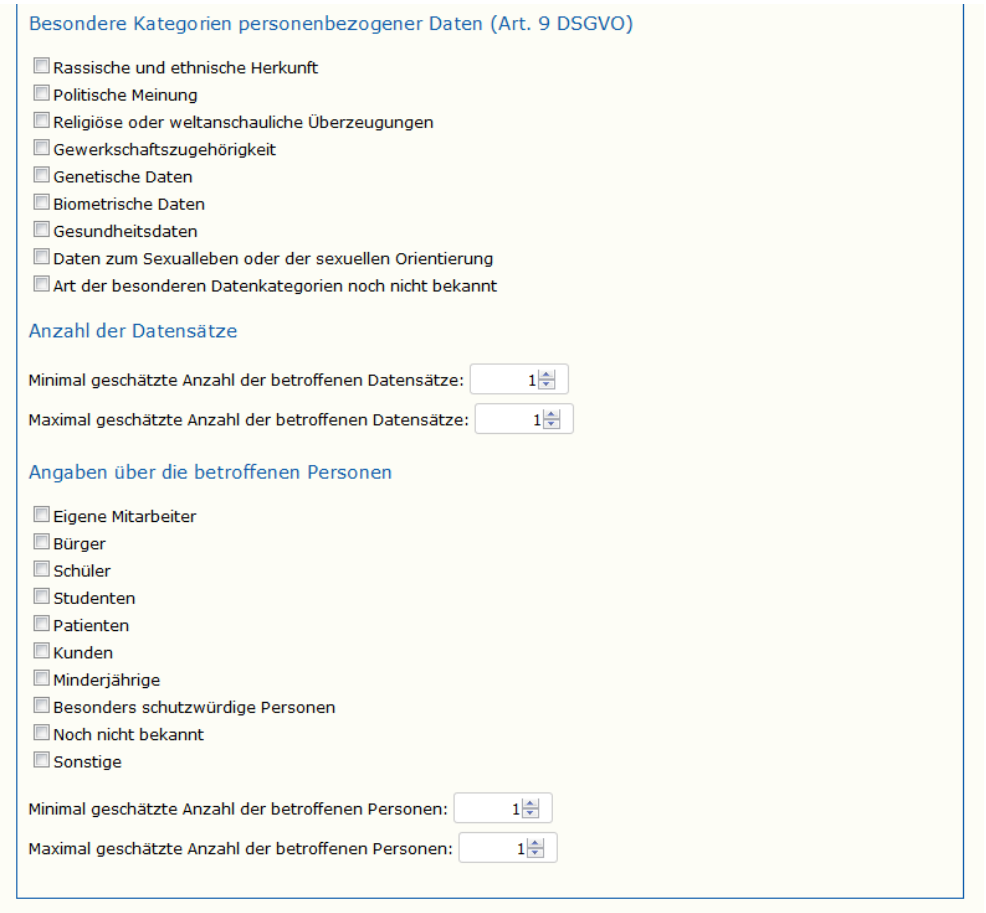
Demgegenüber regeln § 35 Abs. 1 und 4 Erstes Buch Sozialgesetzbuch – Allgemeiner Teil – i. V. m. § 67 Abs. 2 Zehntes Buch Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – (SGB X) den Umfang der **„Daten, die dem Sozialgeheimnis unterliegen“**. **150**

Das Auswahlfeld **„Daten, die dem Berufsgeheimnis unterliegen“**, erfasst eine Vielzahl von Fällen. Berufsgeheimnisse werden berufsrechtlich begründet, so durch § 43a Abs. 2 Satz 1, 2 Bundesrechtsanwaltsordnung oder durch § 9 Abs. 1 Berufsordnung für die Ärzte Bayerns. Auch das Postgeheimnis (§ 39 Abs. 1 Postgesetz) und das Fernmeldegeheimnis (§ 88 Abs. 1 Telekommunikationsgesetz) begründen Berufsgeheimnisse. **151**

Das Auswahlfeld **„Daten die einen besonderen Amtsgeheimnis unterliegen“** fasst verschiedene Fälle zusammen. Neben dem jeweils besonders ausgewiesenen (→Rn. 149) Steuer- sowie Sozialgeheimnis gehören das Statistikgeheimnis (§ 16 Abs. 1 Satz 1 Bundesstatistikgesetz, Art. 17 Abs. 1 Satz 1 Bayerisches Statistikgesetz), das Wahlgeheimnis (z. B. § 33 Abs. 1 Satz 1 Bundeswahlgesetz, Art. 13 Abs. 1 Satz 1 Landeswahlgesetz, Art. 18 Satz 1 **152**

Gemeinde- und Landkreiswahlgesetz), das Meldegeheimnis (§ 7 Abs. 1 Bundesmeldegesetz) sowie die Amtsärzte und Amtsveterinäre treffende Geheimhaltungspflicht nach Art. 30 Abs. 1 Satz 1, 2 Gesundheitsdienst- und Verbraucherschutzgesetz zu den besonderen Amtsgeheimnissen.

153 Betrifft eine Verletzung den Schutz personenbezogener Daten, die in den Auswahlfeldern nicht benannt sind, ist ein Häkchen bei der Rubrik **„Weitere personenbezogene Daten“** zu setzen. In diesem Fall ist es zweckmäßig, bei der Beschreibung des Vorfalls auch anzugeben, um welche Kategorien von Daten es sich handelt.



154 Besonders zu kennzeichnen ist eine Verletzung des Schutzes personenbezogener Daten, wenn **besondere Kategorien** im Sinne von Art. 9 DSGVO betroffen sind. Die Typenbildung im Online-Meldeformular greift Art. 9 Abs. 1 DSGVO auf. Die Begriffe der genetischen Daten, der biometrischen Daten und der Gesundheitsdaten sind in Art. 4 Nr. 13 bis 15 DSGVO legal definiert.

155 Sind personenbezogene Daten einer Mehrzahl von Personen strukturiert erfasst, beispielsweise in Akten formularmäßig festgehalten oder in eine Datenbank der vorgegebenen Kategorien eingepflegt, muss die von einer Datenschutzverletzung betroffene **„Anzahl der Datensätze“** festgestellt oder zumindest geschätzt werden. Der Mindestwert und ein Höchstwert sind anzugeben (→Rn. 124).

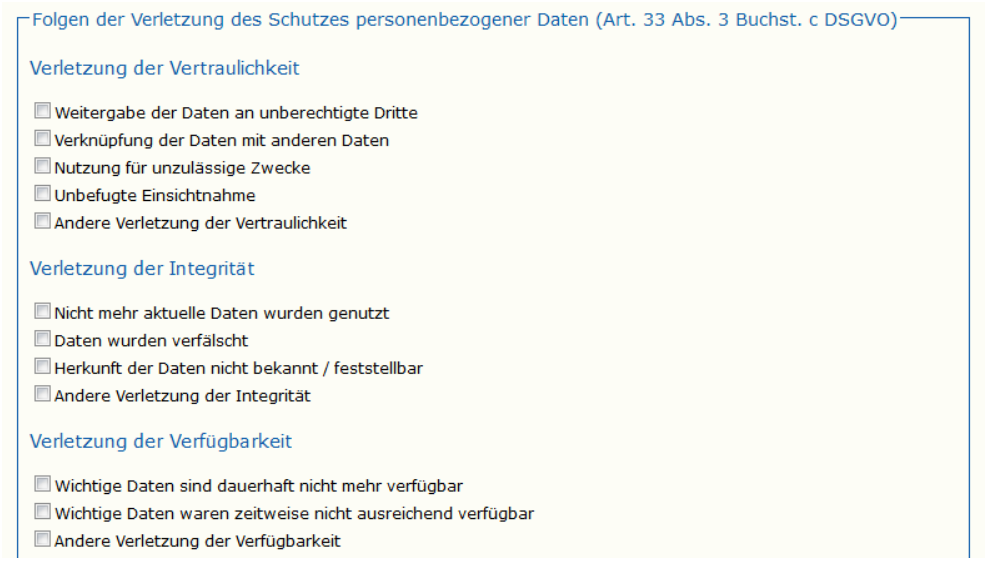
Was die **betroffenen Personen** betrifft, sind zunächst Angaben zu dem Verhältnis gefordert, in welchem diese zu der öffentlichen Stelle stehen. 156

Eigene Mitarbeiter sind die Beamtinnen und Beamten, die Tarifbeschäftigten und alle übrigen in einem öffentlich-rechtlichen oder privatrechtlichen Dienst- oder Anstellungsverhältnis für die öffentliche Stelle tätigen Personen. **Bürgerinnen** und **Bürger** stehen dieser Stelle im Bereich der Hoheitsverwaltung (zum Beispiel: Ordnungs- oder Sozialverwaltung), **Kundinnen** und **Kunden** im Bereich einer wettbewerblichen Tätigkeit (zum Beispiel: Energieversorgung) gegenüber. **Schülerinnen** und **Schüler** befinden sich in einem Schulverhältnis zu einer öffentlichen Schule (Art. 56 Abs. 1 Satz 1 Bayerisches Gesetz über das Erziehungs- und Unterrichtswesen), **Studentinnen** und **Studenten** sind an einer öffentlichen Hochschule immatrikuliert (Art. 42 Abs. 2 Satz 2, 3 Bayerisches Hochschulgesetz). **Patientinnen** und **Patienten** nehmen Dienstleistungen öffentlicher Krankenhäuser in Anspruch (vgl. Art. 27 Bayerisches Krankenhausgesetz). **Minderjährige** sind unter 18 Jahre alte Personen (vgl. § 2 BGB), also Kinder im datenschutzrechtlichen Sinn (vgl. Art. 8 Abs. 1 UAbs. 1 DSGVO). Sie zählen ebenso zu den **besonders schutzbedürftigen Personen** (Erwägungsgrund 75 a. E. DSGVO) wie etwa Betreute (§ 1896 Abs. 1 BGB). 157

Auch für die betroffenen Personen ist eine – zumindest geschätzte – **Anzahl** nach Mindest- und Höchstwert anzugeben. 158

e) Folgen der Verletzung des Schutzes personenbezogener Daten

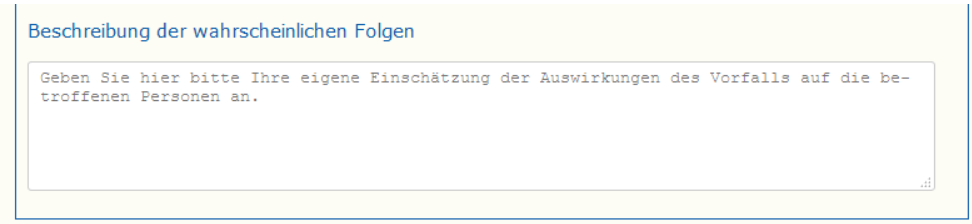
In der Rubrik „Folgen der Verletzung des Schutzes personenbezogener Daten“ dokumentiert die meldende öffentliche Stelle den im Rahmen der Risikobeurteilung prognostizierten Geschehensablauf. Beruht die Datenschutzverletzung auf menschlichem Handeln, geht es hier nicht mehr um die „Angriffsart“, sondern um die näheren und weiteren Auswirkungen, die der Angriff haben kann. 159



160 Wurde in der Rubrik „Art der Verletzung des Schutzes personenbezogener Daten“ ein Vorfall festgehalten, der die **Vertraulichkeit** personenbezogener Daten beeinträchtigt (→Rn. 16), liegen relevante **Folgen** insbesondere in einer Weiterverbreitung an Dritte und einer Verknüpfung durch Dritte. Eine Vertraulichkeitsbeeinträchtigung in der Form der unbefugten Offenlegung wird sich häufig zuerst als „unbefugte Einsichtnahme“ – nämlich durch an sich nicht zugriffsberechtigte Dritte –, sodann in einer „Nutzung für unzulässige Zwecke“ oder in einer „Verknüpfung der Daten mit anderen Daten“ fortsetzen. Liegt die Vertraulichkeitsbeeinträchtigung in einem unbefugten Zugang, steht neben den beiden zuletzt genannten Folgen die „Weitergabe der Daten an unberechtigte Dritte“ – durch die Person, die sich den unbefugten Zugang verschafft hat – im Vordergrund.

161 Betraf der Vorfall, welcher in der Rubrik „Art der Verletzung des Schutzes personenbezogener Daten“ dokumentiert wurde, dagegen die **Integrität** dieser personenbezogenen Daten (→Rn. 14), werden **Folgen** oft darin bestehen, dass bei anstehenden Verarbeitungen nicht mehr alle vor der Datenschutzverletzung vorhandenen Daten bereitstünden („nicht mehr aktuelle Daten werden genutzt“), oder dass gar am aktuellen Sachstand gemessen unzutreffende Daten zu Grunde gelegt würden („Daten wurden verfälscht“). Eine Integritätsverletzung kann im Übrigen auch dazu führen, dass die Daten ihrer Quelle nicht mehr zugeordnet werden können („Herkunft der Daten nicht bekannt/feststellbar“).

162 Ist in der Rubrik „Art der Verletzung des Schutzes personenbezogener Daten“ ein Vorfall dargestellt, der sich auf die **Verfügbarkeit** personenbezogener Daten bezieht (→Rn. 11), so liegt die **Folge** darin, dass ein Zugang zu diesen Daten entweder dauerhaft nicht mehr möglich („wichtige Daten sind dauerhaft nicht mehr verfügbar“) oder aber für einen erheblichen Zeitraum nicht eröffnet ist („wichtige Daten waren zeitweise nicht ausreichend verfügbar“).



163 Das anschließende Freitextfeld „Beschreibung der wahrscheinlichen Folgen“ sollte die meldende öffentliche Stelle insbesondere dazu nutzen, die im ersten Schritt der Risikobeurteilung herauszuarbeitenden **Nachteile** für die Rechte und Freiheiten natürlicher Personen komprimiert zu beschrieben, auch wenn diese im Einzelfall erst durch das Verhalten Dritter eintreten (→Rn. 51, 57).

f) Beschreibung der ergriffenen oder geplanten Maßnahmen

164 Schließlich sieht das Online-Meldeformular noch Angaben zu den Maßnahmen vor, welche die meldende öffentliche Stelle bereits ergriffen oder geplant hat. Dies gilt zum einen für die risikomindernden Maßnahmen, zum anderen für Benachrichtigungen in Erfüllung einer etwa eingreifenden Benachrichtigungspflicht nach Art. 34 DSGVO.

aa) Maßnahmen zur Behebung des Vorfalls und zur Abmilderung von nachteiligen Auswirkungen

In der Rubrik „Maßnahmen zur Behebung des Vorfalls und zur Abmilderung von nachteiligen Auswirkungen“ werden die bereits umgesetzten und die geplanten Maßnahmen unter jeweils zwei Gesichtspunkten abgefragt: 165

(1.1) Welche Maßnahmen sind zur Behebung des Vorfalls getroffen worden?

(1.2) Welche Maßnahmen sind zur Behebung des Vorfalls geplant?

(2.1) Welche Maßnahmen sind zur Abmilderung von nachteiligen Auswirkungen getroffen worden?

(2.2) Welche Maßnahmen sind zur Abmilderung von nachteiligen Auswirkungen geplant?

Die Antworten sollten in den beiden verfügbaren Freitextfeldern entsprechend gegliedert werden. Die öffentliche Stelle legt im ersten Freitextfeld ihre Antworten auf die Fragen (1.1) und (2.1), im zweiten Freitextfeld ihre Antworten auf die Fragen (1.2) und (2.2) dar. Die Maßnahmen sind jeweils knapp, aber präzise zu beschreiben. 166

Bei den **Maßnahmen zur Behebung des Vorfalls** beschreibt die öffentliche Stelle, mit welchen Instrumenten sie 167

- eine fortwirkende Datenschutzverletzung unterbunden hat;
- eine Wiederholung der Datenschutzverletzung ausschließen will.

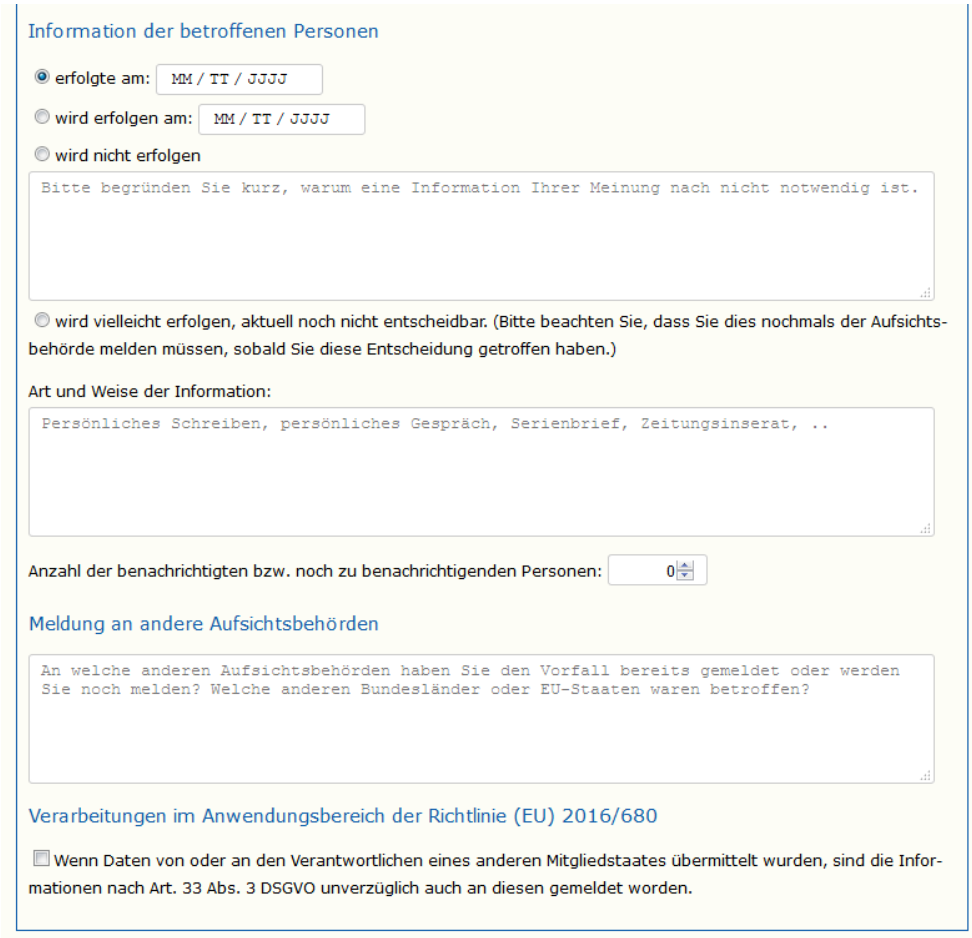
Demgegenüber legt die öffentliche Stelle bei den **Maßnahmen zur Abmilderung von nachteiligen Auswirkungen** dar, 168

- wie sie auf bereits eingetretene Auswirkungen reagiert hat;
- wie sie noch nicht eingetretenen Auswirkungen gegensteuern will.

169 Die Erläuterungen müssen so weit spezifiziert sein, dass die Datenschutz-Aufsichtsbehörde einschätzen kann, ob die Maßnahmen das verfolgte Ziel voraussichtlich erreichen werden, in welchem Grad dies der Fall ist und inwieweit nachteilige Folgen der Datenschutzverletzung nicht ausgeglichen werden können und/oder ein Restrisiko für die Wiederholung einer gleichartigen Datenschutzverletzung verbleibt.

170 Ist die meldende öffentliche Stelle der Auffassung, dass **keine Maßnahmen** zu treffen sind, muss dies eingehend begründet werden. Erscheinen die Maßnahmen als unmöglich, ist darzulegen, welche Maßnahmen erwogen wurden, aus welchen Gründen sie aber nicht zur Anwendung kommen können.

bb) Information der betroffenen Personen



171 In einem letzten Abschnitt des Online-Meldeformulars nimmt die öffentliche Stelle zur Erfüllung der Benachrichtigungspflicht nach Art. 34 DSGVO Stellung. Mitzuteilen ist das Datum, an welchem eine Benachrichtigung durchgeführt wurde oder noch durchgeführt wird. Unterbleibt eine Benachrichtigung, ist zu erläutern, warum sie für nicht notwendig gehalten wird. Ist die öffentliche Stelle der Ansicht, dass die Datenschutzverletzung kein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, muss sie das Ergebnis ihrer Risikobeurteilung (→Rn. 58 ff.) in dem entsprechenden Freitextfeld kurz darlegen. Zur

Art und Weise der Information teilt sie das ausgewählte Medium mit; wird eine Benachrichtigungspflicht durch öffentliche Bekanntmachung erfüllt (→Rn. 99, 107), sind die maßgeblichen Gründe mitzuteilen. In diesem Fall darf die Anzahl der benachrichtigten oder noch zu benachrichtigenden Personen auch geschätzt werden.

172 Meldungen an andere Aufsichtsbehörden kommen insbesondere dann in Betracht, wenn sie gesetzlich vorgeschrieben sind. Es muss sich bei den anderen Aufsichtsbehörden nicht um Datenschutz-Aufsichtsbehörden handeln. Zusätzliche Meldepflichten finden sich etwa in § 83a SGB X.[15] Das den Bereich der Datenschutz-Richtlinie für Polizei und Strafjustiz betreffende Ankreuzfeld setzt die Vorgabe in Art. 33 BayDSG um.

[15] Siehe dazu im Einzelnen Bayerischer Landesbeauftragter für den Datenschutz, „Meldung von Datenschutzverletzungen durch Sozialbehörden an die zuständigen Rechts- oder Fachaufsichtsbehörden“, Aktuelle Kurz-Information 18, Stand 2/2019, im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen“.

IX. Folgen von Pflichtverstößen

173 Eine Missachtung der Meldepflicht nach Art. 33 DSGVO sowie eine Missachtung der Benachrichtigungspflicht nach Art. 34 DSGVO können datenschutzaufsichtliche Maßnahmen nach sich ziehen. In Betracht kommen insbesondere

- die Beanstandung nach Art. 16 Abs. 4 Satz 1 BayDSG;
- die Verwarnung nach Art. 58 Abs. 2 Buchst. b DSGVO;
- die Anordnung, betroffene Personen von einer Datenschutzverletzung zu benachrichtigen (Art. 58 Abs. 2 Buchst. e, Art. 34 Abs. 4 DSGVO);
- die Anordnung einer Verarbeitungsbeschränkung oder eines Verarbeitungsverbots (Art. 58 Abs. 2 Buchst. f DSGVO), jedenfalls dann, wenn wiederholte Datenschutzverletzungen belegen, dass der Verantwortliche nicht in der Lage ist, eine sichere Verarbeitung der betroffenen personenbezogenen Daten zu gewährleisten;
- die Verhängung einer Geldbuße nach Art. 83 Abs. 4 Buchst. a DSGVO, wenn sich die Pflichtverletzung auf eine Tätigkeit bezieht, mit welcher eine bayerische öffentliche Stelle am Wettbewerb teilnimmt (vgl. Art. 22 BayDSG)[16].

[16] Siehe dazu im Einzelnen Bayerischer Landesbeauftragter für den Datenschutz, Geldbußen nach Art. 83 Datenschutz-Grundverordnung gegen bayerische öffentliche Stellen, Aktuelle Kurz-Information 17, Stand 1/2019, im Internet abrufbar auf https://www.datenschutz-bayern.de in der Rubrik „Datenschutzreform 2018 – Aktuelle Kurz-Informationen".