Baden-Württemberg
DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE INFORMATIONSFREIHEIT

Zur Informationspflicht nach § 42a Bundesdatenschutzgesetz (BDSG)

(einschließlich einer Checkliste für die Mitteilung an die Aufsichtsbehörde)

- Stand: 26. April 2017 -

Der Landesbeauftragte für den Datenschutz Baden-Württemberg
Königstraße 10a
70173 Stuttgart
Telefon 0711/615541-0
Telefax 0711/615541-15
E-Mail: *poststelle@lfd.bwl.de*
(Schutzbedürftige Daten sollten nicht unverschlüsselt per E-Mail oder via Telefax übertragen werden.)
PGP-Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962
Homepage: www.baden-wuerttemberg.datenschutz.de

Inhaltsübersicht

1. Über die Informationspflicht bei unrechtmäßiger Kenntniserlangung und Datenverlust („Datenpanne“, „Datenleck“, „Datendiebstahl“)

§ 42a des Bundesdatenschutzgesetzes (BDSG) (*http://www.gesetze-im-internet.de/bdsg_1990/__42a.html*) enthält beim Vorliegen sog. „Datenpannen“, „Datenlecks“ oder bei einem „Datendiebstahl“ eine Informationspflicht für nicht-öffentliche Stellen und ihnen datenschutzrechtlich gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen gegenüber der Datenschutzaufsichtsbehörde und im Regelfall gegenüber dem/den Betroffenen; sonstige öffentliche Stellen sind nicht meldepflichtig. Die Informationspflicht besteht, wenn Dritte von besonders sensiblen personenbezogenen Daten aus dem Verfügungsbereich der verantwortlichen Stelle unrechtmäßig Kenntnis erlangen und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Entsprechende Informationspflichten gelten - teils in analoger Anwendung - auch für Diensteanbieter im Telemedienbereich (§ 15a TMG), im Telekommunikationsbereich (§§ 93 Absatz 3, 109a TKG) sowie für verantwortliche Stellen im Sozialbereich (§ 83a SGB X).

Meldepflichtig ist stets die verantwortliche Stelle, auch dann, wenn die Datenpanne bei einem von ihr gemäß § 11 BDSG beauftragten Unternehmen eintritt.

2. In welchen Fällen besteht die Informationspflicht nach § 42a BDSG?

a) Die verantwortliche Stelle muss feststellen, dass Dritte von besonders sensiblen Daten unrechtmäßig Kenntnis erlangt haben

Voraussetzung für das Entstehen der Informationspflicht ist zunächst, dass die verantwortliche Stelle anhand von tatsächlichen Anhaltspunkten, z. B. aus dem eigenen Sicherheitsmanagement, im Wege der Benachrichtigung durch den Auftragsdatenverarbeiter, durch Hinweise Betroffener oder durch Hinweise von Strafverfolgungsorganen, feststellt, dass bei ihr gespeicherte, besonders sensible personenbezogene Daten (siehe hierzu unter 2.b) unrechtmäßig übermittelt wurden oder auf sonstige Weise Dritten im Sinne von § 3 Absatz 8 Satz 2 BDSG zur Kenntnis gelangt sind.

Die Kenntniserlangung nach § 42a BDSG tritt beim Abhandenkommen z.B. eines Datenträgers (USB-Stick geht verloren; Paket mit Lohnabrechnungen kommt nicht an) im Regelfalle immer ein, da hier bereits die bloße Möglichkeit eines unbefugten Zugriffs sozusagen als „sehr wahrscheinliche Kenntniserlangung“ ausreicht.

b) Die „Datenpanne“ muss besonders sensible Daten betreffen

Die Informationspflicht ist nach § 42a Satz 1 Nummer 1 bis 4 BDSG auf besonders sensible personenbezogene Daten aus dem Verfügungsbereich der verantwortlichen Stelle begrenzt. Diese sind:

1. besondere Arten personenbezogener Daten nach § 3 Absatz 9 BDSG, (Angaben über rassische/ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheitsdaten, Angaben über das Sexualleben)

2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,

3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, und

4. personenbezogene Daten zu Bank- oder Kreditkartenkonten.

c) Es müssen schwerwiegende Beeinträchtigungen für die Betroffenen drohen (hohes Gefahrenpotential)

Für die Rechte oder schutzwürdigen Interessen der Betroffenen müssen schwerwiegende Beeinträchtigungen drohen.

Letzteres bestimmt sich unter anderem nach der Art der betroffenen Daten und den potenziellen Auswirkungen der unrechtmäßigen Kenntniserlangung durch Dritte auf die Betroffenen (z. B. materielle Schäden bei Kreditkarteninformationen oder soziale Nachteile einschließlich des Identitätsbetrugs). An dieser Stelle ist eine Prognose anzustellen, in die sämtliche tatsächlichen Anhaltspunkte, Tatsachen und Erfahrungswerte einfließen sollten.

Weitere Informationen über die Voraussetzungen der Informationspflicht nach § 42a BDSG finden Sie im Internet u.a.

- beim Berliner Beauftragten für Datenschutz und Informationsfreiheit *http://www.datenschutz-berlin.de/attachments/1040/535.4.10_Stand_Mai_2014.pdf?1402585372* sowie
- beim Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen *https://www.ldi.nrw.de/mainmenu_Service/submenu_Newsarchiv/Inhalt/Informationspflicht_bei_Datenpannen_____42a_BDSG__-_Wer_muss_wann_was_unternehmen_/Vorlage_FAQs_zur_Informationspflicht1.pdf*
-

3. Der Informationspflicht ist unverzüglich nachzukommen

Die Benachrichtigung muss nach § 42a Satz 1 BDSG sowohl gegenüber der Aufsichtsbehörde als auch gegenüber den Betroffenen unverzüglich, d. h. nach der Legaldefinition des § 121 Absatz 1 Satz 1 des Bürgerlichen Gesetzbuchs „ohne schuldhaftes Zögern“, erfolgen.

Bei nicht-öffentlichen Stellen ist die zuständige Datenschutzaufsichtsbehörde grundsätzlich die Aufsichtsbehörde nach § 38 BDSG - bei nicht-öffentlichen Stellen mit (Haupt-)Sitz in Baden-Württemberg folglich der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg -, bei Post- und Telekommunikationsunternehmen die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nach § 24 BDSG.

§ 42a Satz 2 BDSG sieht im Hinblick auf die Unverzüglichkeit der Informationspflicht eine Differenzierung vor: Die Benachrichtigung der Datenschutzaufsichtsbehörde hat aufgrund ihrer Verschwiegenheitspflicht auch vor der Beseitigung von Datensicherheitslücken und im Falle laufender Strafverfolgungsmaßnahmen immer unverzüglich - also ab dem Zeitpunkt der Kenntniserlangung von der „Datenpanne“ - zu erfolgen. Bei der Informationspflicht gegenüber dem/den Betroffenen wird klargestellt, dass ein schuldhaftes Zögern insbesondere dann nicht gegeben ist, soweit die Datensicherungspflichten des § 9 BDSG oder Interessen der Strafverfolgung einer Veröffentlichung der Datenschutzverletzung vorläufig noch entgegenstehen. Diese Regelung

zielt darauf ab, der verantwortlichen Stelle die Möglichkeit zu geben, etwaige technische Sicherheitslücken, unter deren Ausnutzung die Datenschutzverletzung erfolgte, zu analysieren und so weit wie möglich zu beheben, bevor breitere Kreise von der Lücke Kenntnis erhalten. Andernfalls bestünde die Gefahr, dass Dritte von dieser Kenntnis profitieren, um selbst die fragliche Sicherheitslücke auszunutzen. Im zweiten Fall dürfen Ermittlungen der Strafverfolgungsorgane bei einem kriminellen Hintergrund durch die Offenlegung nicht gefährdet werden.

4. Inhalt und Umsetzung der Informationspflicht

a) Informationspflicht gegenüber der Aufsichtsbehörde

Die Benachrichtigung der Aufsichtsbehörde muss nach § 42a Satz 4 BDSG eine Darlegung möglicher nachteiliger Folgen der Verletzung und der vom Betreiber nach der Verletzung ergriffenen (Gegen-)Maßnahmen enthalten. Dies soll die Aufsichtsbehörde in den Stand versetzen, sicherzustellen, dass der datenschutzrechtliche Verstoß beseitigt wurde.

Um der verantwortlichen Stelle die Abfassung der Meldung an die Aufsichtsbehörde zu erleichtern, haben wir im Anhang eine Checkliste beigefügt. Wir empfehlen, für eine vollständige Meldung nach § 42a BDSG die dort erfragten Angaben vollständig darzulegen und zu erläutern.

b) Informationspflicht gegenüber dem/den Betroffenen

Der Inhalt der Benachrichtigung variiert je nach Empfänger. Die Benachrichtigung der Betroffenen muss nach § 42a Satz 3 BDSG in allgemein verständlicher Form eine Darlegung der Art der Verletzung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten.

Eine Benachrichtigung der einzelnen Betroffenen kann für die verantwortliche Stelle einen unverhältnismäßigen Aufwand an Kosten und Zeit verursachen, z. B. bei einer vorherigen Ermittlung der Adressdaten der Betroffenen, sofern diese der verantwortlichen Stelle nicht bekannt sind. An Stelle der direkten Benachrichtigung der Betroffenen tritt mit deren Inhalt nach § 42a Satz 5 BDSG eine Information der Öffent-

lichkeit. Dies wird durch entweder durch Anzeigen, die mindestens eine halbe Zeitungsseite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder auf eine andere geeignete Weise sichergestellt.

5. Verstoß gegen die Informationspflicht ist bußgeldbewehrt

Nach § 43 Absatz 2 Nummer 7 BDSG handelt ordnungswidrig, wer vorsätzlich oder fahrlässig entgegen § 42a Satz 1 BDSG eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht. Diese Ordnungswidrigkeit kann mit einer Geldbuße bis zu 300.000 Euro geahndet werden.

6. Strafrechtliches Verwertungsverbot

§ 42a Satz 6 BDSG enthält ein flankierendes strafrechtliches Verwertungsverbot, wie es auch in anderen Vorschriften, z. B. § 97 Absatz 1 Sätze 2, 3 der Insolvenzordnung, vorgesehen ist. Danach dürfen die Benachrichtigung bzw. die darin enthaltenen Informationen in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Benachrichtigungspflichtigen oder einen seiner Angehörigen nach § 52 Absatz 1 der Strafprozessordnung nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden. Dabei ist zu berücksichtigen, dass eine Selbstbezichtigung bei juristischen Personen nicht der Regelfall ist, für einen Teil der betroffenen Unternehmen (z. B. Ein-Mann-GmbH) aber jedenfalls tatbestandlich in Betracht kommt.

Anhang: Checkliste für die Informationspflicht nach § 42a BDSG gegenüber der Aufsichtsbehörde

Checkliste für die Informationspflicht nach § 42a BDSG gegenüber der Aufsichtsbehörde		
	Notwendige Angabe	**Ergänzender Hinweis**
1.	**Name und Anschrift der verantwortlichen Stelle sowie Benennung des zuständigen Ansprechpartners**	*Falls der Vorfall im Rahmen einer Auftragsdatenverarbeitung nach § 11 BDSG beim Auftragnehmer stattfand, bitten wir Sie, uns eine Kopie des Vertrags für diese Auftragsdatenverarbeitung zu übersenden.*
2.	**Datum/Zeitraum des Vorfalls**	*Bitte teilen Sie uns den genauen Zeitpunkt mit, ab dem die bei Ihnen gespeicherten Daten im Sinne des § 42a Satz 1 BDSG unrechtmäßig übermittelt wurden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind.* *In manchen Fällen ist der genaue Zeitpunkt, an dem der Vorfall (Datenverlust) zum ersten Mal eingetreten ist, nicht bekannt. Dann ist der früheste Zeitpunkt anzugeben, an dem die verantwortliche Stelle von dem Vorfall Kenntnis erlangt hat, indem z. B. ein Betroffener (Geschädigter) sich bei ihr gemeldet hat.*

Checkliste für die Informationspflicht nach § 42a BDSG gegenüber der Aufsichtsbehörde		
	Notwendige Angabe	**Ergänzender Hinweis**
3.	**Welche Form einer sog. „Datenpanne“ liegt vor?**	*Mögliche „Datenpannen“ sind z.B.:* *1. Fehlversendung/Sendung an falschen Adressaten* *2. Unberechtigte Weitergabe/unberechtigter Zugriff Dritter* *3. Datenverlust durch verloren gegangenes Medium* *4. Datenverlust durch Hacking* *5. Datenverlust durch Ausspähen (z. B. Skimming)* *6. Datenverlust durch Diebstahl* *7. Datenverlust durch sonstige Umstände (bitte erläutern)*
4.	**Wie konnte es zu dieser „Datenpanne“ kommen (wie konnten Dritte unrechtmäßig von den Daten Kenntnis erlangen)?**	*Beschreiben Sie bitte genau und ausführlich die Umstände des Vorfalls, unter denen der Datenverlust eingetreten ist.*
5.	**Welche Datenarten sind betroffen?**	*Bitte führen Sie detailliert die Datenarten im Sinne des § 42a Satz 1 Nrn. 1 - 4 BDSG auf, die von der „Datenpanne“ betroffen sind.*
6.	**Wie viele Personen sind von der „Datenpanne“ betroffen?**	*Falls die Zahl der Betroffenen nicht genau ermittelt werden kann oder konnte, geben Sie bitte eine geschätzte Obergrenze an.*

Checkliste für die Informationspflicht nach § 42a BDSG gegenüber der Aufsichtsbehörde		
	Notwendige Angabe	**Ergänzender Hinweis**
7.	**Waren die betroffenen Daten - oder einzelne Datenarten - verschlüsselt?**	*Falls ein Verschlüsselungsverfahren angewendet wurde, bitten wir um nähere Angaben, z. B. „Verschlüsselung mit einem Passwort aus acht Zeichen“ oder „Verschlüsselung mit dem AES-Algorithmus und einer Schlüssellänge von 256 Bit."*
8.	**Welche schwerwiegenden Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen bzw. sind bereits eingetreten?**	*Die möglichen oder bereits eingetretenen nachteiligen Folgen für die Betroffenen (z.B. unberechtigte Kontoabbuchungen, Identitätsdiebstahl) sind aufzuführen.*
9.	**Von welchem Schadensrisiko gehen Sie aus (voraussichtliche Schadenshöhe / Eintrittswahrscheinlichkeit“)?**	*Wir bitten um eine Einstufung in eine der Kategorien - gering, mittel, hoch - und eine Begründung für Ihre Einstufung.*
10.	**Wie und wann wurden (werden) die Betroffenen benachrichtigt und welche Gegenmaßnahmen haben Sie ihnen empfohlen?**	*Geben Sie bitte hier an:* ➢ *Wann wurden oder werden die Betroffenen über den Vorfall informiert?* ➢ *Auf welche Weise wurden oder werden die Betroffenen informiert?* ➢ *Welche konkreten Gegenmaßnahmen haben Sie den Betroffenen empfohlen?* *Bitte übersenden Sie uns eine Kopie der Mitteilung an die Betroffenen.*

Checkliste für die Informationspflicht nach § 42a BDSG gegenüber der Aufsichtsbehörde		
	Notwendige Angabe	**Ergänzender Hinweis**
11.	**Welche Gegenmaßnahmen haben Sie bereits eingeleitet, welche weiteren Gegenmaßnahmen sind geplant?**	*Bitte erläutern Sie ausführlich die ergriffenen Gegenmaßnahmen im Hinblick auf den konkreten Vorfall sowie auf das Ziel, derartige Vorfälle zukünftig zu verhindern.*
12.	**Wurde Strafanzeige erstattet?**	*Wurde Strafanzeige gestellt? Falls ja, teilen Sie uns bitte die betreffende Dienststelle und das Aktenzeichen mit.*
13.	**Sonstige Anmerkungen**	