

Datenschutz

Anwaltskanzlei Baron v. Hohenhau

Beim Datenschutz stehen, anders als der Begriff zunächst vermuten lässt, nicht die Daten im Vordergrund, sondern die Personen, über die Informationen (Daten) verarbeitet werden. Rechtlicher Ausgangspunkt ist das **Grundrecht auf informationelle Selbstbestimmung**.

Informationelle Selbstbestimmung - was bedeutet das?

Kurz gesagt: jeder hat das Recht zu wissen, wer was wann über ihn weiß.

Das Bundesverfassungsgericht hat im Volkszählungsurteil 15.12.1983 den Begriff „Recht auf informationelle Selbstbestimmung“ erstmals in dem Sinne verwendet, dass es sich beim Datenschutz um ein Grundrecht handelt.

Dieses Grundrecht gewährleistet dem Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf "informationelle Selbstbestimmung" sind nur im überwiegenden Allgemeininteresse zulässig.

Gemäß dieser Entscheidung "*wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst.*" Dies bedeutet, dass das allgemeine Persönlichkeitsrecht in Zusammenhang mit der Menschenwürde die verfassungsrechtlichen Grundlagen für das Recht auf informationelle Selbstbestimmung bilden.

Wichtige Adressen zum Datenschutz:

Der Bayerische Landesbeauftragte für den Datenschutz

Dr. Thomas Petri
Wagmüllerstr. 18, 80538 München
Tel: 089 - 212672-0 - Fax: 089 - 212672-50
E-Mail: poststelle@datenschutz-bayern.de

Aufsichtsbehörde für den privaten Bereich in Bayern

Regierung von Mittelfranken
Promenade 27
91522 Ansbach
Tel.: 09 81 - 53 – 228 - Fax: 09 81 - 53 206
E-Mail: datenschutz@reg-mfr.bayern.de

Linktipps:

- www.datenschutz.de - Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder
- www.datenschutz-bayern.de - Bayerischer Landesbeauftragte für den Datenschutz
- www.datenschutz-berlin.de - gute Webseite Berliner Datenschutzbeauftragter
- www.sicherheit-im-internet.de - Bundesmin. für Wirtschaft
- www.bsi.bund.de - Bundesamt für Sicherheit in der Informationstechnologie

Wer ist für die Datenschutzkontrolle zuständig – wer hilft bei Fragen weiter?

Im deutschen Recht wird grundsätzlich unterschieden zwischen dem öffentlichen und dem privaten Bereich.

Wenn Daten von öffentlichen Stellen verarbeitet werden, sind die Datenschutzbeauftragten des Bundes oder der Länder für die Datenschutzkontrolle zuständig. Öffentliche Stellen der Länder sind z.B. die Verwaltungen von Städten, Gemeinden, Kreisen, Landesbehörden und die meisten Schulen und Universitäten. Öffentliche Stellen des Bundes sind z.B. Bundesbehörden, Arbeitsämter und die Bundeswehr.

Wenn Daten von einer privaten Stelle (nichtöffentlicher Bereich) z.B. Versandhäuser, Adresshändler, Internet-Provider, aber auch Vereine, Ärzte und Angehörige anderer freier Berufe verarbeitet werden, sind meist die sog. Aufsichtsbehörden der Länder zuständig. Für die Kontrolle der Verarbeitung personenbezogener Daten durch kirchliche Stellen sind die Datenschutzbeauftragten der evangelischen und katholischen Kirchen zuständig.

Für die Datenverarbeitung bei Unternehmen aus dem Bereich Telekommunikation ist für die Datenschutzkontrolle in jedem Fall der Bundesbeauftragte für den Datenschutz zuständig, unabhängig davon, wo das Unternehmen seinen Sitz hat.

Aufgaben der Aufsichtsbehörden:

Die Aufgaben der Aufsichtsbehörden ergeben sich direkt aus dem Bundesdatenschutzgesetz (BDSG)

§ 38 BDSG (Auszug)

(I).. Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie **befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterrichten...**

(III) Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben **erforderlichen Auskünfte unverzüglich zu erteilen**. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

(IV) Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, **während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen...**

(V) Zur Gewährleistung des Datenschutzes nach diesem Gesetz und anderen Vorschriften über den Datenschutz, ... , kann die Aufsichtsbehörde anordnen, dass im Rahmen der Anforderungen nach § 9 Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel getroffen werden. Bei schwerwiegenden Mängeln dieser Art, insbesondere, wenn sie mit besonderer Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie den Einsatz einzelner Verfahren untersagen, wenn die Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.

Wichtiges zum Datenschutz in Kürze:

Rechte der Betroffenen:

- **Recht auf Benachrichtigung über die Datenerhebung**

Der Betroffene ist bei der Erhebung seiner Daten darüber aufzuklären, welche Stelle zu welchem Zweck die Daten erhebt. In vielen Fällen muss zusätzlich darüber informiert werden, ob es eine Verpflichtung zur Angabe der Daten gibt und an welche anderen Stellen die Daten voraussichtlich übermittelt werden. Außerdem ist er auf das Recht auf Auskunft und Berichtigung hinzuweisen.

- **Recht auf Auskunft**

Die Betroffenen haben ein Recht darauf, Auskunft darüber zu erhalten, welche Informationen über sie gespeichert sind. Dabei muss auch darüber informiert werden, zu welchem Zweck die Informationen gespeichert sind, woher diese stammen und an welche Stellen sie übermittelt werden.

- **Recht auf Berichtigung, Sperrung oder Löschung**

Stellt sich heraus, dass die gespeicherten Informationen unrichtig sind, besteht ein Anspruch darauf, dass diese berichtigt werden. Der Betroffene hat ein Recht darauf, dass seine Daten gelöscht werden, wenn diese nicht mehr gespeichert werden dürfen. Dies ist meist dann der Fall, wenn die Informationen für den Zweck, zu dem sie gespeichert wurden, nicht mehr erforderlich sind. Die Daten sind zu sperren, wenn der Betroffene behauptet, die Informationen seien unrichtig und sich die Richtigkeit nicht nachweisen lässt, oder wenn die Daten nicht mehr erforderlich sind, aber nach bestimmten Rechtsvorschriften (z. B. zum steuerlichen Nachweis) noch länger gespeichert werden müssen. Gesperrte Daten müssen als solche gekennzeichnet werden; sie dürfen nicht weiter verwendet werden.

- **Anspruch auf Schadensersatz**

- **Anspruch auf Anrufung der Datenschutzkontrollinstanz (siehe oben)**

Jeder, der glaubt, durch die Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt worden zu sein, kann sich an die zuständige Kontrollstelle wenden. Diese muss der Beschwerde nachgehen und den Betroffenen über den Ausgang unterrichten.

Wichtige Grundsätze zum Datenschutz

Generell gilt der **Grundsatz der Datensparsamkeit** nach

§ 3a BDSG Datenvermeidung und Datensparsamkeit

„Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“

Daten dürfen nur mit **Einwilligung** des Betroffenen erhoben, verarbeitet oder genutzt werden

§ 4 BDSG Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der **Betroffene eingewilligt** hat.

Die Einwilligung wird in § 4a BDSG näher definiert:

§ 4a BDSG Einwilligung

- (1) Die Einwilligung ist nur wirksam, wenn sie auf der **freien Entscheidung** des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. **Die Einwilligung bedarf der Schriftform**, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie **besonders hervorzuheben**.
- (2) ...

Mitteilung der Datenverarbeitung an den Betroffenen:

(§ 4 III BDSG – Auszug)

Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,
2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss,

zu unterrichten.

Der Datenschutzbeauftragte

Generell besteht bei Unternehmen, welche automatisierte Verarbeitungen von personenbezogenen Daten verwenden, eine **Meldepflicht gegenüber der zuständigen Aufsichtsbehörde**. Bei Bestellung eines Datenschutzbeauftragten entfällt diese Meldepflicht.

§ 4d BDSG Meldepflicht

- (1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde .. nach Maßgabe von § 4e zu melden.
- (2) Die **Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat**.
- (3) ...

Unabhängig davon ist bei Unternehmen, in denen **der Regel mindestens 20 Mitarbeiter** mit der Erhebung, Verarbeitung oder Nutzung von Daten beschäftigt sind, ein Datenschutzbeauftragter schriftlich zu benennen.

Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben **erforderliche Fachkunde und Zuverlässigkeit** besitzt. Der Beauftragte für den Datenschutz ist **der Geschäftsleitung unmittelbar zu unterstellen**. Er ist in Ausübung seiner

Fachkunde auf dem Gebiet des Datenschutzes **weisungsfrei**. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Der Beauftragte für den Datenschutz ist zur **Verschwiegenheit** über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird. Der Datenschutzbeauftragte ist bei der Erfüllung seiner Aufgaben zu unterstützen. Insbesondere ist ihm, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

Betroffene können sich jederzeit an den Datenschutzbeauftragten wenden.

Aufgaben des Beauftragten für den Datenschutz (§ 4g BDSG)

Der Datenschutzbeauftragte wirkt auf die Einhaltung der Vorschriften über den Datenschutz hin. Zu diesem Zweck kann er sich in Zweifelsfällen an die für die Datenschutzkontrolle zuständige Behörde wenden. Er hat insbesondere

1. die **ordnungsgemäße Anwendung der Datenverarbeitungsprogramme**, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu **überwachen**; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten **rechtzeitig zu unterrichten**,
2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

Datengeheimnis:

§ 5 BDSG Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit **auf das Datengeheimnis zu verpflichten**. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Firewalls:

Um das interne Netz abzusichern, kann es erforderlich sein, eine Firewall zu installieren wenn personenbezogene Daten zu schützen sind. Eine solche könnte sich z.B. **Sicherungspflicht** aus **§ 9 BDSG** ergeben.

§ 9 BDSG Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, **haben die technischen und organisatorischen Maßnahmen zu treffen**, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die Anlage zu § 9 BDSG sagt hierzu weiter aus:

Anlage (zu § 9 Satz 1)

Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die ... innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (**Zutrittskontrolle**),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (**Zugangskontrolle**),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (**Zugriffskontrolle**),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (**Weitergabekontrolle**),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (**Eingabekontrolle**),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Eine Protokollierung an der Firewall ist zulässig, sofern die Daten einer Abrechnung der Telekommunikation dienen oder wenn es sich auf einen Angriff auf das System handelt. Eine Verwendung der Protokolldaten für andere Zwecke ist nicht erlaubt.

Inhaltskontrollen können einen Eingriff in das Fernmeldegeheimnis darstellen. Werden Mechanismen zum Content Filtering eingesetzt, z.B. um sicherheitskritische Inhalte wie Viren aus E-Mail Nachrichten auszusondern, sollte möglichst automatisiert kontrolliert werden, um den Eingriff gering zu halten.

Bei Firewalls können datenschutzrechtliche Informationen, insbesondere **Nutzungsdaten** anfallen, da damit mögliche Angriffe auf die Systeme protokolliert werden sollen. Nutzungsdaten dienen dazu, dem Nutzer die Teilnahme am Dienst des Anbieters überhaupt zu ermöglichen z.B. Identifikationsdaten in Kombination mit Tag und Uhrzeit der Verbindung.

Diese Nutzungsdaten müssen mit besonderer Vorsicht behandelt werden, da sie persönliche Daten enthalten. Nutzungsdaten dürfen nicht auf Dauer gespeichert werden, sondern spätestens mit Abschluss der Nutzung wieder gelöscht werden. Daher müssten diese Log-Dateien prinzipiell sofort nach Verbindungsende gelöscht werden.

Es besteht das Problem, dass weder eine gesetzliche Erlaubnis zur Speicherung der Daten noch eine Einwilligung des Nutzers besteht. Eine sofortige Löschung würde jedoch den Zweck der Sicherungsmaßnahme entgegenstehen. Daher ist zu empfehlen, die Prüfintervalle der Protokolle möglichst kurz zu halten. Eine Weitergabe der Daten ist auf jeden Fall verboten.

§ 31 BDSG Besondere Zweckbindung

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

Datenerhebung im Auftrag

Sofern von einem Daten im Auftrag für einen Anderen erhoben, verarbeitet oder genutzt werden ist folgendes zu beachten:

§ 11 BDSG Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, **ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. ...**

(2) Der **Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen.**

Haftung für Verstöße gegen das BDSG

Verstöße gegen das BDSG können eine **Ordnungswidrigkeit** oder bei vorsätzliche Handlung auch eine **Straftat** mit bis zu 2 Jahren Freiheitsstrafe darstellen. Die Ordnungswidrigkeit kann auch fahrlässig begangen werden!

§ 43 BDSG Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer **vorsätzlich oder fahrlässig**

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, **einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,**
3. entgegen § 28 Abs. 4 Satz 2 **den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet** oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,
4. – 10. (...)
10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine **Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet** oder
11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. **unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,**
2. **unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,**
3. **unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abrufen oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,**
4. – 6. (...)

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

Darüber hinaus können **Schadensersatzansprüche** nach § 7 BDSG und 823 BGB bestehen:

§ 7 BDSG Schadensersatz

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

Haftung nach Teledienstschutzgesetz (TDDSG)

§ 9 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 3 Abs. 4 die Erbringung von Telediensten von einer Einwilligung des Nutzers in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig macht,
2. entgegen § 4 Abs. 1 Satz 1 oder 2 den Nutzer nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,
3. entgegen § 4 Abs. 2 oder 4 Satz 1 Nr. 1 bis 5 einer dort genannten Pflicht zur Sicherstellung nicht oder nicht richtig nachkommt,
4. entgegen § 5 Satz 1 oder § 6 Abs. 1 Satz 1 oder Abs. 8 Satz 1 oder 2 personenbezogene Daten erhebt, verarbeitet, nutzt oder nicht oder nicht rechtzeitig löscht oder
5. entgegen § 6 Abs. 3 Satz 3 ein Nutzungsprofil mit Daten über den Träger des Pseudonyms zusammenführt.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.