



Anmerkung

Dieses Dokument ist nur teilweise barrierefrei, da in dem Briefkopf Elemente des BMUKN vorgegeben sind. Das Inhaltsverzeichnis dient nur als Sprungpunkt für Screen Reader.

Inhalt

Verpflichtung zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach Datenschutzgrundverordnung sowie auf das Fernmeldegeheimnis.....	2
Anlage zur Verpflichtung auf die Vertraulichkeit.....	5
Begrifflichkeiten und Grundsätze der Verarbeitung.....	5
Artikel 4 Nummer 1 DSGVO	5
Artikel 4 Nummer 2 DSGVO	5
Artikel 5 Absatz 1 Buchstabe. a DSGVO	5
Artikel 5 Absatz 1 Buchstabe f DSGVO	5
Artikel 29 DSGVO.....	6
Artikel 32 Absatz 2 DSGVO	6
Artikel 33 Absatz 1 Satz 1 DSGVO	6
Haftung und Schadensersatz.....	6
Artikel 82 Absatz 1 DSGVO	6
Art. 83 Abs. 1 DSGVO	6
§ 42 BDSG - Strafvorschriften.....	6
§ 202a StGB - Ausspähen von Daten.....	7
§ 202b StGB – Abfangen von Daten	7
§ 275 StGB - Vorbereitung der Fälschung von amtlichen Ausweisen; Vorbereitung der Herstellung von unrichtigen Impfausweisen	7
§ 303a Abs. 1 StGB - Datenveränderung.....	8
§ 303b - Computersabotage.....	8
§ 3 TTDSG- Vertraulichkeit der Kommunikation - Fernmeldegeheimnis	9



**Verpflichtung zur Vertraulichkeit und zur Einhaltung der
datenschutzrechtlichen Anforderungen nach
Datenschutzgrundverordnung sowie auf das Fernmeldegeheimnis**

Aktenzeichen: DSB - 0130/004-2024.0001

Bonn/Berlin, _____ 2025

Sehr geehrte/r _____,

aufgrund Ihrer vorgesehenen Tätigkeit für das Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit (BMUKN) weise ich Sie auf die Einhaltung folgender Vorschriften zur Vertraulichkeit personenbezogener Daten hin.

Dies gilt sowohl für Ihre Tätigkeit innerhalb wie auch außerhalb der Behörde und gilt auch nach Beendigung Ihrer Tätigkeit weiter.

Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daher ist es Ihnen auch nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist.





Seite 3

Ferner müssen Sie beachten, dass personenbezogene Daten

- auf rechtmäßige und faire Weise, und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- für festgelegte, eindeutige und legitime Zwecke erhoben werden. Sie dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sind („Datenminimierung“);
- sachlich richtig und erforderlichenfalls auf dem neuesten Stand gebracht werden; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
- in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung“);
- in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Personenbezogene Daten dürfen daher nur nach Weisung Ihres/Ihrer Vorgesetzten im Rahmen eines Praktikums oder Referendariats bzw. durch den Auftraggeber im Rahmen ihres Werkvertrags verarbeitet werden.



Seite 4

Neben Einzelweisungen der zuvor genannten Personen gelten als Weisung auch Prozessbeschreibungen, Ablaufpläne, Dienstanweisungen sowie das Datenschutzkonzept des BMKNV soweit für ihre Aufgabe anwendbar. Sollten Sie diese Anweisungen und das Datenschutzkonzept nicht über das Intranet abrufen können, so können Sie dies in Papierform anfordern.

Verstöße gegen die Datenschutzvorschriften können ggf. mit Geldbuße oder Freiheitsstrafe geahndet werden. Entsteht der betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein (zivilrechtlicher) Schadenersatzanspruch entstehen.

Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt einen Verstoß gegen vertragliche Pflichten dar, der entsprechend geahndet werden kann.

Sollten Sie im Zusammenhang mit Ihrer Tätigkeit für das BMUKN Kenntnis von Fernmeldedaten oder Daten aus dem Intranet erhalten, so dürfen Sie sich nicht über das erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation verschaffen. Sie dürfen derartige Kenntnisse grundsätzlich nicht an Dritte weitergeben.

Für Fragen zum Datenschutz im BMUKN im Rahmen Ihrer Tätigkeit für das BMUV können Sie sich jederzeit an den Datenschutzbeauftragten des BMUK wenden. Dieser ist zur Vertraulichkeit Ihrer Anfrage gesetzlich verpflichtet.

Ich weiß darauf hin, dass diese Erklärung beim Datenschutzbeauftragten des BMUV digital gespeichert wird. Die Erklärung wird nach Ablauf der Speicherfrist (10 Jahre nach Beendigung der Aufgabe im BMUKN) dem Bundesarchiv angeboten.

Mit Ihrer Unterschrift bestätigen Sie diese Verpflichtung. Ein Exemplar dieser Verpflichtung nebst Anlage wurde ausgehändigt.

_____, _____
Ort Datum Unterschrift Verpflichtete(r)



Anlage zur Verpflichtung auf die Vertraulichkeit

Stand Januar 2024

Begrifflichkeiten und Grundsätze der Verarbeitung

Artikel 4 Nummer 1 DSGVO

„Personenbezogene Daten“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Artikel 4 Nummer 2 DSGVO

„Verarbeitung“ [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Artikel 5 Absatz 1 Buchstabe. a DSGVO

Personenbezogene Daten müssen [...] auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“).

Artikel 5 Absatz 1 Buchstabe f DSGVO

Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Artikel 29 DSGVO

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Artikel 32 Absatz 2 DSGVO

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung - insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Artikel 33 Absatz 1 Satz 1 DSGVO

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

Haftung und Schadensersatz

Artikel 82 Absatz 1 DSGVO

Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DSGVO

Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung [...] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 42 BDSG - Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

§ 202a StGB - Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b StGB – Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 275 StGB - Vorbereitung der Fälschung von amtlichen Ausweisen; Vorbereitung der Herstellung von unrichtigen Impfausweisen

(1) Wer eine Fälschung von amtlichen Ausweisen vorbereitet, indem er

1. Platten, Formen, Drucksätze, Druckstöcke, Negative, Matrizen oder ähnliche Vorrichtungen, die ihrer Art nach zur Begehung der Tat geeignet sind,
2. Papier, das einer solchen Papierart gleicht oder zum Verwechseln ähnlich ist, die zur Herstellung von amtlichen Ausweisen bestimmt und gegen Nachahmung besonders gesichert ist, oder

3. Vordrucke für amtliche Ausweise

herstellt, sich oder einem anderen verschafft, feilhält, verwahrt, einem anderen überlässt oder einzuführen oder auszuführen unternimmt, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(1a) Wer die Herstellung eines unrichtigen Impfausweises vorbereitet, indem er in einem Blankett-Impfausweis eine nicht durchgeführte Schutzimpfung dokumentiert oder einen auf derartige Weise ergänzten Blankett-Impfausweis sich oder einem anderen verschafft, feilhält, verwahrt, einem anderen überlässt oder einzuführen oder auszuführen unternimmt, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Handelt der Täter gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach Absatz 1 oder Absatz 1a verbunden hat, so ist die Strafe Freiheitsstrafe von drei Monaten bis zu fünf Jahren.

(3) § 149 Abs. 2 und 3 gilt entsprechend.

§ 303a Abs. 1 StGB - Datenveränderung

(1) Wer rechtswidrig Daten [...] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar. [...]

§ 303b - Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar. [...]

§ 3 TTDSG- Vertraulichkeit der Kommunikation - Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

(2) Zur Wahrung des Fernmeldegeheimnisses sind verpflichtet

1. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
2. Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
3. Betreiber öffentlicher Telekommunikationsnetze und
4. Betreiber von Telekommunikationsanlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden.

Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.

(3) Den nach Absatz 2 Satz 1 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang. [...]