Der Datenschutzbeauftragte, der IT-Sicherheitsbeauftragte und der Geheimschutzbeauftragte des Umweltbundesamtes

Verpflichtung auf die Vertraulichkeit

(Stand 27.06.2022)

1. Grundsätze

1.1 Gesetzliche Verpflichtungen

Die einschlägigen gesetzlichen Vorschriften verlangen, dass vertrauliche Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daten, die Ihnen im Rahmen Ihrer Tätigkeit im oder für das **Umweltbundesamt**, Wörlitzer Platz 1, 06844 Dessau-Roßlau, bekannt werden, dürfen daher auch nur in dem Umfang und in der Weise verarbeitet werden, wie es zur Erfüllung der Ihnen übertragenen Aufgaben notwendig ist.

Zu beachten sind dabei unter anderem die Europäische Datenschutzgrundverordnung, die Regelungen zur Amtsverschwiegenheit (§ 30 VwVfG) und strafrechtliche Bestimmungen zur Verletzung und Verwertung von Privatgeheimnissen oder Betriebs- und Geschäftsgeheimnissen (u. a. §§ 203 und 204 StGB).

Soweit Sie im Rahmen Ihrer Tätigkeit für das Umweltbundesamt bei der Erbringung geschäftsmäßiger Telekommunikationsdienste mitwirken, sind Sie aufgrund von § 3 TTDSG zur Wahrung des Fernmeldegeheimnisses verpflichtet.

Aufgrund von § 78 SGB X sind Sie zur Wahrung des Sozialdatengeheimnisses verpflichtet, soweit Sie im Rahmen Ihrer Tätigkeit für das Umweltbundesamt von Sozialdaten gem. § 67 SGB X Kenntnis erlangen.

1.2 Wahrung der Vertraulichkeit und Integrität

Vertraulichkeit bedeutet, dass die Daten, Informationen und deren Attribute nur berechtigten Personen zur Kenntnis gelangen dürfen. Integrität bedeutet, dass die Daten, Informationen und deren Attribute unverändert bleiben müssen und nicht durch Sie geändert werden dürfen.

Der Schutz von Integrität und Vertraulichkeit bedeutet, dass Daten, Informationen und Attribute in einer Weise zu verarbeiten sind, die eine angemessene Sicherheit gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung, vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Hierfür sind geeignete technische und organisatorische Maßnahmen zu treffen.

Im Folgenden wird zur Vereinfachung der Begriff „Daten“ als Sammelbegriff für die Begriffe Daten, Informationen und Attribute genutzt.

1.3 Weiterverwendung

Es ist untersagt, die vertraulichen Daten ohne vorherige schriftliche Vereinbarung mit dem Umweltbundesamt für eigene gewerbliche oder private Zwecke zu verwenden oder sie Dritten sonst wie zugänglich zu machen, soweit dies nicht vom Auftrag gedeckt ist.

1.4 Unterauftragnehmer

Grundsätzlich sind Unterauftragnehmer nicht zulässig, soweit der Vertrag nichts anderes bestimmt. Ist eine Einbindung von Unterauftragnehmern unvermeidbar oder erforderlich und nichts Näheres im Vertrag bestimmt, bedarf dies der schriftlichen Zustimmung des Umweltbundesamtes. Nicht als Leistungen von Unterauftragnehmern im Sinne dieser Regelung gelten Dienstleistungen, die der Auftragsverarbeiter bei Dritten als Nebenleistung zur Unterstützung der Auftragsdurchführung in Anspruch nimmt, beispielsweise Telekommunikationsdienstleistungen.

Werden im Rahmen der Zusammenarbeit mit dem Umweltbundesamt weitere Personen durch Auftragnehmer beauftragt, müssen diese dritten Personen vom Auftragnehmer über alle relevanten Aspekte der Vertraulichkeit und Integrität informiert und ebenfalls auf die Vertraulichkeit verpflichtet werden.

1.5 Folgen der Missachtung

Verstöße gegen Vorschriften zum Schutz der Vertraulichkeit können ggf. mit Geldbuße, Geldstrafe oder Freiheitsstrafe geahndet werden. Entsteht durch die unzulässige Verarbeitung von Daten ein materieller oder immaterieller Schaden, kann ein Schadensersatzanspruch entstehen.

2. Schutzbedarfsfeststellung der Daten

2.1 Einstufung der Daten

Gibt das UBA eine Einstufung der Daten hinsichtlich ihres Schutzbedarfes vor, so ist diese zu beachten und darf nicht geändert werden. Entstehen während des Auftrages weitere Daten, sind diese angemessen einzustufen und zu schützen.

2.2 Verschlusssachen

Werden bzw. wurden Daten als Verschlusssachen (VS) eingestuft, sind die Bestimmungen der Verschlusssachenanweisung (VSA) zu beachten.
So ist z. B. gem. § 4 Abs. 1 der VSA eine Person auf das VS-NfD-Merkblatt (Anlage V der VSA) zu verpflichten, bevor sie Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) erhält. Dabei ist ihr gegen Empfangsbestätigung ein Exemplar der Anlage V zugänglich zu machen.

3. Besondere Regelungen für IT-Systeme

3.1 Grundsätze

Fachvorgesetzte Behörde in Fragen der Informationssicherheit für Bundesbehörden ist das Bundesamt für Sicherheit in der Informationstechnik (BSI[1]). Das BSI gibt mit seinen Standards

200-1 Managementsysteme für Informationssicherheit[2]
200-2 IT-Grundschutz Methodik[3]
200-3 Risikomanagement[4]

und den entsprechenden Mindeststandards und technischen Richtlinien Vorgaben, die für den IT-Betrieb von Bundesbehörden verbindlich sind. Im Vertrag werden externe Auftragnehmer, die vertrauliche Daten des Bundes verarbeiten, dazu verpflichtet, ebenfalls diese Regelungen einzuhalten.

Haben die verarbeiteten Daten den Schutzbedarf „normal“, sind die Standards 200-1 und 200-2 einzuhalten. Ist der Schutzbedarf der Daten „hoch“, ist zusätzlich der Standard 200-3 anzuwenden.

Die Regelungen für IT-Systeme und die Maßgaben zur Kommunikation der Daten unterscheiden hierbei nach der Nutzung hausinterner IT des Umweltbundesamtes oder der externen IT des Dienstleisters bzw. einer hausinternen Kommunikation innerhalb des UBA und einer Kommunikation mit externen Stellen.

3.2 Regelung für UBA-interne IT-Systeme

Für externe IT-Dienstleister, die **nicht direkt** im Rechenzentrum (Z 2.2) angestellt sind oder unmittelbar für das Rechenzentrum arbeiten, gilt folgender Absatz:

> An Hard-, Software, Netzwerken, Dateien oder Daten des UBA oder Dateien und Daten, die dem UBA von Dritten zur Verfügung gestellt wurden, dürfen keine Änderungen vorgenommen werden, es sei denn, das UBA hat dem zuvor schriftlich zugestimmt.

Für externe IT-Dienstleister, die **direkt** im Rechenzentrum (Z 2.2) angestellt sind oder unmittelbar für das Rechenzentrum arbeiten, gilt folgender Absatz:

> An Hard-, Software, Netzwerken, Dateien oder Daten des UBA oder Dateien und Daten, die dem UBA von Dritten zur Verfügung gestellt wurden, dürfen nur Änderungen vorgenommen werden, die der Aufgabe, die im Arbeitsvertrag festgelegt ist, entsprechen.

Die folgenden Absätze des Abschnittes 3.2 gelten vollumfänglich für externe IT-Dienstleister, die **nicht direkt** im Rechenzentrum (Z 2.2) angestellt sind, wie beschrieben. Sollten die im Folgenden beschriebenen Maßgaben dem Arbeitsauftrag externer IT-Dienstleister, die **direkt** im Rechenzentrum (Z 2.2) angestellt sind, widersprechen, ist das Rechenzentrum (Z 2.2) darüber in Kenntnis zu setzen; das Rechenzentrum kann dann eine Ausnahme von den hier beschriebenen Maßgaben genehmigen.

[1] https://www.bsi.bund.de/DE/Home/home_node.html
[2] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard201/ITGStandard201_node.html
[3] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html
[4] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard203/ITGStandard203_node.html

Ohne vorherige Zustimmung des UBA ist Dritten kein Zugang zu den IT-Systemen des UBA oder IT-Systemen der Kunden des UBA zu gewähren. Wird Dritten nach Zustimmung des UBA ein solcher Zugang gewährt, müssen die Dritten ebenfalls entsprechend diesem Dokument auf die Vertraulichkeit verpflichtet werden und ist dies gegenüber dem UBA zu belegen.. Es sind eigene angemessene technische und organisatorische Maßnahmen zu treffen, welche die Einhaltung dieser Pflichten sicherstellen.

Mit dem Hausnetz (Intranet) des UBA darf nur IT verbunden werden, die der administrativen Hoheit des UBA unterliegt. Ist es für den Auftragnehmer erforderlich, eigene IT zu verwenden und mit dem Hausnetz des UBA zu verbinden, sind zuvor der Informationssicherheitsbeauftragte (ISB) und das Referat Z 2.2 - IT-Strategie, -Steuerung und -Service zu unterrichten und um Zustimmung zu bitten.

Das UBA betreibt Schutzmechanismen zum Schutz seiner IT. Dies sind insbesondere ein Scan auf Schadsoftware, automatische Updates der IT und ein Intrusion Prevention System. Der Auftragnehmer akzeptiert diese Schutzmechanismen und wird sie nicht unterbinden oder stören.

Sofern im Rahmen der Zusammenarbeit der Parteien Fernwartungen durch den Auftragnehmer erforderlich sind, wird der Auftragnehmer folgende Maßgaben einhalten:

- Wird die Fernwartung in den Anlagen des UBA oder auf deren Daten durchgeführt oder besteht die Möglichkeit durch entsprechende Konfigurationen eine solche Fernwartung durchzuführen, wird das UBA hierüber informiert. Der Auftragnehmer wird besonderen angemessenen und zumutbaren Anforderungen des UBA an die Durchführung der Fernwartung unverzüglich nachkommen. Das UBA setzt aktuell zur Fernwartung die genubox[5] ein. Damit wird eine BSI-konforme Fernwartung praktiziert.
- Der Auftragnehmer wird die der Fernwartung dienenden IT-Systeme umfassend gegen unberechtigten Zutritt, Zugang und Zugriff schützen, so dass Missbrauch angemessen verhindert wird.
- Die im Rahmen der Fernwartung online übermittelten Informationen gelten als vertraulich im Sinne dieser Datenschutz- und Vertraulichkeitsvereinbarung. Dasselbe gilt für die Tatsache der Fernwartung selber und die näheren Regelungen der Parteien hierzu.

3.3 Regelung für die IT-Systeme des Auftragnehmers

Der Auftragnehmer muss das in der Leistungsbeschreibung und dieser Datenschutz- und Vertraulichkeitserklärung aufgeführte Mindestniveau an IT-Sicherheit für seine IT-Systeme gewährleisten und für das Projekt nur Beschäftigte einsetzen, die auf die Vertraulichkeit entsprechend dem hier vorliegenden Dokument verpflichtet wurden.

[5] https://www.genua.de/it-sicherheitsloesungen/fernwartungs-appliance-genubox

4. Kontrollrecht des Datenschutzbeauftragten und IT-Sicherheitsbeauftragten des Umweltbundesamtes

Das Umweltbundesamt ist berechtigt, die Einhaltung der vorgenannten Vereinbarungen zu kontrollieren. Soweit ein*e für das Unternehmen Zeichnungsberechtigte*r diese Erklärung unterzeichnet, erklärt sie/er damit auch, dem Datenschutzbeauftragten des Umweltbundesamtes, dem Informationssicherheitsbeauftragten des Umweltbundesamtes und/oder von ihnen namentlich benannten unterstützenden Personen nach schriftlicher Voranmeldung zu den üblichen Geschäftszeiten Zutritt zum Betrieb des Unternehmens zu gewähren, soweit der Geschäftsbetrieb hierdurch nicht unverhältnismäßig gestört wird. Der Datenschutzbeauftragte des UBA, der Informationssicherheitsbeauftragte des UBA und/oder die von ihnen namentlich benannten unterstützenden Personen werden bei der Kontrolle durch Mitarbeitende des Unternehmens angemessen unterstützt. Die vorgenannte Kontrolle erstreckt sich auf den Umgang mit Daten sowie technische und organisatorische Maßnahmen, die im Zusammenhang mit der Tätigkeit für das Umweltbundesamt stehen.

Sie sind verpflichtet, von den zuständigen Datenschutzaufsichtsbehörden, dem Datenschutzbeauftragten oder Informationssicherheitsbeauftragten des Umweltbundesamtes festgestellte Mängel in der Datensicherheit umgehend zu beseitigen.

5. Kommunikation

5.1 UBA-intern

Die hausinterne Kommunikation innerhalb des UBA kann persönlich, per Telefon oder per E-Mail erfolgen. Werden vertrauliche Inhalte besprochen, ist darauf zu achten, dass Dritte keine Kenntnis der kommunizierten Inhalte erhalten. Alle drei Kommunikationsformen sind hausintern zulässig bis zur Schutzstufe Verschlusssachen – nur für den Dienstgebrauch (VS-NfD).

5.2 externe Kommunikation

Eine Kommunikation mit externen Stellen ist fernmündlich, per E-Mail oder per Netzzugriff möglich. Werden dabei vertrauliche Inhalte kommuniziert, ist Folgendes zu beachten:

5.2.1 fernmündlich

Es ist darauf zu achten, dass keine Dritten die kommunizierte Information mithören können.

5.2.2 E-Mail

Werden vertrauliche Daten kommuniziert, sind diese angemessen zu verschlüsseln. Empfohlen werden folgende Verschlüsselungsprogramme (Erläuterungen s. im Glossar):

- PGP4WIN
- Zip mit dem Verschlüsselungsverfahren AES-256
- Bitlocker

Werden Verschlusssachen (VS) kommuniziert, ist das Programm GnuPG VS-Desktop vom Hersteller g10 code GmbH zur Verschlüsselung zu verwenden.

Werden vertrauliche Inhalte kommuniziert und verarbeitet, die nicht als Verschlusssache eingestuft sind, wird eine Einstufung der Daten und eine Behandlung nach dem Traffic Light Protokoll[6] (TLP) empfohlen. Dabei ist das Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP) zu beachten und die Teilnehmer sind darauf mit diesem Formular zu verpflichten.

Die Schlüssel für Zip und Bitlocker haben ausreichend sicher und komplex zu sein. Empfohlen wird eine Zeichenkette aus mindestens 12 Zeichen aus 3 Zeichenklassen. Die entsprechenden Schlüssel sind auf separatem Wege, also nicht per E-Mail oder Fax, sicher auszutauschen. Dies kann z. B. persönlich oder per Schriftpost erfolgen.

5.2.3 Netzzugriff

Für einen Austausch von Daten per Netzzugriff (z. B. auf Fileserver, Clouds, o. ä.) ist für die Datenübertragung der Mindeststandard für den Einsatz des SSL/TLS-Protokolls für Bundesbehörden[7] anzuwenden. Eine Überprüfung der Qualität der Netzwerkverbindung ist mit dem Tool https://www.ssllabs.com/ssltest/[8] möglich. Ergebnis sollte mindestens ein grünes „A“ sein.

Weiterhin ist eine Authentifizierung per Nutzernamen und Passwort erforderlich. Das entsprechende Passwort ist auf separatem Wege, also nicht per E-Mail oder Fax, sicher auszutauschen. Dies kann z. B. persönlich oder per Schriftpost erfolgen.

6. Beendigung des Vertrages

6.1 Löschung

Sobald durch die vorgenannten Regelungen geschützte Daten im Rahmen der Zusammenarbeit der Parteien nicht mehr erforderlich sind, werden sie - soweit keine anderslautende schriftliche Vereinbarung mit dem Umweltbundesamt getroffen wurde - unverzüglich und unwiederbringlich sicher nach dem aktuellen Stand der Technik gelöscht oder zurückgegeben. Auf Aufforderung des Umweltbundesamtes muss die Löschung schriftlich bestätigt werden. Zurückbehaltungsrechte bestehen insoweit nicht.

6.2 Pflicht zur Verschwiegenheit

Die Verpflichtung auf Vertraulichkeit und Integrität besteht auch nach Beendigung der Tätigkeit für das Umweltbundesamt fort. Selbiges gilt auch für Unterauftragnehmer.

[6] https://de.wikipedia.org/wiki/Traffic_Light_Protocol
[7] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_Version_2_1.html
[8] https://www.ssllabs.com/ssltest/

Von diesen Verpflichtungen habe ich Kenntnis genommen. Ich bin mir bewusst, dass ich mich bei Verletzungen dieser Verpflichtungen strafbar machen kann, insbesondere nach Art. 84 DSGVO i. V. m. § 42 BDSG, §§ 203, 204, 206 Strafgesetzbuch (StGB). Mir ist bekannt, dass auch unterhalb der Strafbarkeitsschwelle eine Ordnungswidrigkeit vorliegen kann.

Darüber hinaus kann ich bei Verstößen unter bestimmten Voraussetzungen zivilrechtlich in Anspruch genommen werden. Soweit personenbezogene Daten betroffen sind, führt Art. 82 DSGVO zu einer Beweislastumkehr. Danach ist der Verantwortliche nur von der Haftung für Schäden befreit, wenn er nachweisen kann, in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich zu sein.

Eine Kopie dieser Niederschrift nebst der Anlage „Ausgewählte Vorschriften zum Schutz der Vertraulichkeit von Daten“ mit den Abschriften der genannten und weiteren Vorschriften habe ich erhalten.

Gegebenenfalls: Mündliche Erläuterungen zu dieser Erklärung wurden amtsseitig vorgenommen durch (Hinweis: solche Erläuterungen sind nicht zwingend erforderlich):

Name	Vorname	Ort, Datum	Unterschrift

Die vorstehenden Regelungen wurden verstanden und anerkannt:

(Hinweis: Eine Kopie dieser Erklärung samt Unterschriftenliste sollte den Unterzeichnenden zur Verfügung gestellt werden. Sollten einzelne Unterzeichnende nicht damit einverstanden sein, dass bei einer Sammelunterzeichnung auch die anderen Unterzeichnenden auf diese Weise eine Kopie der Erklärung bekommen, ist für diese Personen jeweils ein einzelnes Erklärungsformular zu verwenden)

Name	Vorname	Ort, Datum	Unterschrift

Anlage „Ausgewählte Vorschriften zum Schutz der Vertraulichkeit von Daten“

Strafgesetzbuch (StGB)

§ 202a 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.

§ 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,
3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,
4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,
6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist, anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) (weggefallen)

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,
2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

§ 204 Verwertung fremder Geheimnisse

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) § 203 Absatz 5 gilt entsprechend.

§ 206 Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.
(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt
1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die
1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. 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.

§ 303a Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

EU-Datenschutzgrundverordnung (DSGVO)

Art. 4 Begriffsbestimmungen (Auszug)

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „personenbezogene Daten“ 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann;
2. „Verarbeitung“ 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;

(…)

Art. 5 Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) 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“);
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; 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“);
e) 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; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
f) 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“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 29 Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters

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.

Art. 32 Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

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

(3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

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

(1) 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 gemäß Artikel 55 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. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, 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.

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

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

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;

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.

(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.

(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.

Art. 82 Haftung und Recht auf Schadenersatz

(1) 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.

(2) Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

(3) Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

(4) Ist mehr als ein Verantwortlicher oder mehr als ein Auftragsverarbeiter bzw. sowohl ein Verantwortlicher als auch ein Auftragsverarbeiter an derselben Verarbeitung beteiligt und sind sie gemäß den Absätzen 2 und 3 für einen durch die Verarbeitung verursachten Schaden verantwortlich, so haftet jeder Verantwortliche oder jeder Auftragsverarbeiter für den gesamten Schaden, damit ein wirksamer Schadensersatz für die betroffene Person sichergestellt ist.

(5) Hat ein Verantwortlicher oder Auftragsverarbeiter gemäß Absatz 4 vollständigen Schadenersatz für den erlittenen Schaden gezahlt, so ist dieser Verantwortliche oder Auftragsverarbeiter berechtigt, von den übrigen an derselben Verarbeitung beteiligten für die Datenverarbeitung Verantwortlichen oder Auftragsverarbeitern den Teil des Schadenersatzes zurückzufordern, der unter den in Absatz 2 festgelegten Bedingungen ihrem Anteil an der Verantwortung für den Schaden entspricht.

(6) Mit Gerichtsverfahren zur Inanspruchnahme des Rechts auf Schadenersatz sind die Gerichte zu befassen, die nach den in Artikel 79 Absatz 2 genannten Rechtsvorschriften des Mitgliedstaats zuständig sind.

Artikel 83 Allgemeine Bedingungen für die Verhängung von Geldbußen (Auszug)

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. (…)

Bundesdatenschutzgesetz (BDSG)

§ 42 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.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)

§ 3 Vertraulicheit der Kommunikation - Fernmeldegeheimnis (Auszug)

(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 natürlich und juristische Personen, die an der Erbringung solcher Dienste mitwirken
2. Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie natürlich und juristische Personen, die an der Erbringung solcher Dienste mitwirken
3. Betreiber öffentlicher Telekommunikationsnetze
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 Verpflichteten ist es untersagt, sich oder anderen über das für die Erbringung der Telekommunikationsdienste oder ihrer Telekommunikationsanlagen 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.

(…)

§ 25 Schutz der Privatsphäre bei Endeinrichtungen

(1) Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer auf der Grundlage von klaren und umfassenden Informationen eingewilligt hat. Die Information des Endnutzers und die Einwilligung haben gemäß der Verordnung (EU) 2016/679 zu erfolgen.

(2) Die Einwilligung nach Absatz 1 ist nicht erforderlich,

1. wenn der alleinige Zweck der Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der alleinige Zweck des Zugriffs auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen die Durchführung der Übertragung einer Nachricht über ein öffentliches Telekommunikationsnetz ist oder
2. wenn die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf bereits in der Endeinrichtung des Endnutzers gespeicherte Informationen unbedingt erforderlich ist, damit der Anbieter eines Telemediendienstes einen vom Nutzer ausdrücklich gewünschten Telemediendienst zur Verfügung stellen kann.

Sozialgesetzbuch X (SGB X)

§ 78 Zweckbindung und Geheimhaltungspflicht eines Dritten, an den Daten übermittelt werden (Auszug)

(1) Personen oder Stellen, die nicht in § 35 des Ersten Buches genannt und denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck verarbeiten oder nutzen, zu dem sie ihnen befugt übermittelt worden sind. Eine Übermittlung von Sozialdaten nach den §§ 68 bis 77 oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch an eine nicht-öffentliche Stelle auf deren Ersuchen hin ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. Die Dritten haben die Daten in demselben Umfang geheim zu halten wie die in § 35 des Ersten Buches genannten Stellen. Sind Sozialdaten an Gerichte oder Staatsanwaltschaften übermittelt worden, dürfen diese gerichtliche Entscheidungen, die Sozialdaten enthalten, weiter übermitteln, wenn eine in § 35 des Ersten Buches genannte Stelle zur Übermittlung an den weiteren Dritten befugt wäre. Abweichend von Satz 4 ist eine Übermittlung nach § 115 des Bundesbeamtengesetzes und nach Vorschriften, die auf diese Vorschrift verweisen, zulässig. Sind Sozialdaten an Polizeibehörden, Staatsanwaltschaften, Gerichte oder Behörden der Gefahrenabwehr übermittelt worden, dürfen diese die Daten unabhängig vom Zweck der Übermittlung sowohl für Zwecke der Gefahrenabwehr als auch für Zwecke der Strafverfolgung und der Strafvollstreckung speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen.

(2) Werden Daten an eine nichtöffentliche Stelle übermittelt, so sind die dort beschäftigten Personen, welche diese Daten speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, von dieser Stelle vor, spätestens bei der Übermittlung auf die Einhaltung der Pflichten nach Absatz 1 hinzuweisen.

(…)

Verschlusssachenanweisung (VSA)

Zu den gesetzlichen Grundlagen s. folgende Links:
Verschlusssachenanweisung (VSA)

Link: http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_10082018_SII554001196.htm

Anlage V zur VS-Anweisung - VS-NfD Merkblatt

Link: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/anlage-vsa.pdf?__blob=publicationFile&v=5

Anhang - Glossar

Attribute

Siehe Daten, Informationen und Attribute

Bitlocker

Bitlocker ist ein Tool zur Festplattenverschlüsselung und standardmäßig ab Windows 7 enthalten. Das BSI empfiehlt die Verwendung von Bitlocker. Mit Bitlocker lassen sich nur Speichermedien und keine einzelnen Dateien verschlüsseln.

Chiasmus

Die Zulassung des Programmes chiasmus zur Verschlüsselung von Verschlusssachen der Stufe VS-NfD wurde vom BSI entzogen. Es darf nicht mehr zur Verschlüsselung von Verschlusssachen verwendet werden. Eine Alternative steht unter GPG zur Verfügung.

Daten, Informationen und Attribute

Datum (Singular) oder **Daten** (Plural) sind einzelne Zahlen oder Worte, die eine Eigenschaft beschreiben. Sie werden oft mit einer Einheit versehen.
Beispiel: 13 m, 42 kg , warm

Informationen ergeben sich aus Zusammenhängen. Dies können das Aufstellen von Beziehungen, das Bewerten eines Zustandes, das Beschreiben von Zusammenhängen, o. a. Information sein.
Beispiele:
- Karl ist der Bruder von Otto.
- Es war ein heißer Tag.
- Der kürzeste Weg von A nach B führt über C.

Attribute sind Eigenschaften von Daten und Informationen, die i. d. R. unsichtbar sind, jedoch für deren Auswertung von Bedeutung sein können.
Beispiele:
- Absendedatum einer E-Mail
- Korrekturdatum eines Inhaltes
- Person und Datum einer Mitzeichnung
- angewendete Messmethode

Informationen

Siehe Daten, Informationen und Attribute

Mindeststandards

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt verschiedene Mindeststandards heraus, die für die IT der Bundesbehörden verpflichtend umzusetzen und einzuhalten sind. Eine Auflistung der Mindeststandards bietet folgender Link:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Mindeststandards_Bund.html

Soll eine bestimmte IT eingesetzt werden, müssen Sie selber prüfen, ob das BSI hierzu einen Mindeststandard veröffentlicht hat.

PGP4Win

PGP4 Win[9] ist ein asymmetrisches Verschlüsselungsverfahren[10]. Das heißt, dass der Schlüssel aus einem privaten und öffentlichen Schlüssel besteht. Die Bedienung ist ungewohnt für Personen, die bislang nur symmetrische Verschlüsselungsverfahren (Bitlocker, Chiasmus, Zip, o. a.) genutzt haben, der Vorteil liegt jedoch im einfachen Schlüsseltausch. Der private Schlüssel bleibt privat und muss wie das eigene Passwort gehütet werden; der öffentliche Schlüssel kann jedoch einfach per E-Mail ausgetauscht werden. Vor der Nutzung von PGP4WIN muss sich jeder Nutzer so ein eigenes Schlüsselpaar erzeugen.

Bei symmetrischen Verschlüsselungsverfahren (Bitlocker, Chiasmus, Zip, o. a.) wird die Datei oder der Datenträger nur einmal mit dem einen Schlüssel verschlüsselt. Sollen weitere Personen die Datei oder den Datenträger lesen, muss diesen nur der Schlüssel auf sicherem Wege übermittelt werden. Bei der asymmetrischen Verschlüsselung wird die Datei nutzerspezifisch verschlüsselt. Neben dem eigenem privaten Schlüssel müssen alle öffentlichen Schlüssel der Kommunikationspartner*innen zur Verschlüsselung genommen werden und nur diese können dann auch die Datei entschlüsseln. Soll eine weitere Person Zugang zu der Datei erhalten, muss diese erneut mit ihrem öffentlichen Schlüssel verschlüsselt werden. Diesem „Mehraufwand“ steht entgegen, dass die öffentlichen Schlüssel auch auf unsicherem Wege per E-Mail ausgetauscht werden können und nicht auf separatem, vertraulichem Wege ausgetauscht werden müssen. Für kurzfristig erforderliche ad-hoc-Verschlüsselungen ist dies klar ein Vorteil.

PGP4Win ist kostenlos erhältlich. Es darf jedoch nicht zur Verschlüsselung von Verschlusssachen der Stufe VS-NfD verwendet werden. Hierzu siehe den nächsten Absatz

[9] https://www.gpg4win.de/
[10] https://de.wikipedia.org/wiki/Asymmetrisches_Kryptosystem

GnuPG VS-Desktop

Zur Verschlüsselung von Verschlusssachen der Stufe VS-NfD ist das Programm GnuPG VS-Desktop der g10code GmbH zu verwenden. Hintergrund ist, dass zum zuverlässigen Betrieb einer Sicherheitssoftware vom BSI Verträge mit dem Anbieter geschlossen werden müssen, die auch Fristen zur Beseitigung von Sicherheitsmängeln beinhalten. PGP4Win wird durch eine Kommunität angeboten und gegenüber einer Kommunität können keine entsprechenden Verträge geschlossen werden.

Schutzbedarfsfeststellung

Um Daten angemessen schützen zu können, bedarf es einer sog. Schutzbedarfsfeststellung[11]. Entscheidend ist dabei nicht der subjektiv gefühlte Schutzbedarf, sondern der gesetzlich erforderliche Schutzbedarf: Welcher Schaden entsteht, wenn diese Daten unberechtigt bekannt werden?

Die Schutzbedarfsfeststellung wird i. d. R. für die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit durchgeführt. Für besondere Zwecke können auch noch die Schutzziele Authentizität (Wer ist garantiert der Verfasser?) und Nichtabstreitbarkeit (Wer hat garantiert die Aktion (Mitzeichnung, Änderung, Kommentar, u. a.) durchgeführt.

Das UBA verwendet hausintern ein Verfahren zur Schutzbedarfsfeststellung, dass es bei Bedarf gerne zur Verfügung stellt.

Schutzstufen

Für die Informationstechnische Verarbeitung innerhalb des UBA sind die Schutzstufen

- normal
- hoch

von Bedeutung. Bei normalem Schutzbedarf muss der verarbeitende IT-Verbund die Anforderungen des IT-Gundschutz Standard 200-2[12] vollumfänglich erfüllen. Ist der Schutzbedarf hoch, muss zusätzlich die Erweitertete Risikoanalyse auf der Basis von IT-Grundschutz 200-2[13] angewendet werden, um einen angemessenen Schutz herzustellen (siehe Ausschreibungsbestimmung).

Verschlusssachen sind eine eigene Klassifizierung behördlicher Inhalte. Siehe dazu das Stichwort „Verschlusssachen“. Im Umweltbundesamt relevant ist praktisch nur die Schutzstufe VS-NfD.

Sicheres Löschen

[11] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_4_Schutzbedarfsfeststellung/4_00_Einleitung.html
[12] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard202/ITGStandard202_node.html
[13] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard203/ITGStandard203_node.html

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beschreibt das sichere Löschen in den IT-Grundschutz Maßnahmen im Baustein CON.6 Löschen und Vernichten:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/03_CON_Konzepte_und_Vorgehensweisen/CON_6_Loeschen_und_Vernichten_Edition_2022.pdf?__blob=publicationFile&v=3

Aufwand und Methode zur Datenlöschung hängen auch vom Schutzbedarf der Daten ab. Aufgrund der fortschreitenden Weiterentwicklung der Informationsverarbeitung müssen die Methoden zur sicheren Datenlöschung stets weiterentwickelt werden. Es ist stets die aktuell empfohlene Methode anzuwenden.

Technische Richtlinien

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt verschiedene technische Richtlinien heraus, die für die IT der Bundesbehörden verpflichtend umzusetzen und einzuhalten sind. Eine Auflistung konkreter technischer Richtlinien existiert leider nicht. Soll eine bestimmte IT eingesetzt werden, müssen Sie selber prüfen, ob das BSI hierzu eine technische Richtlinie veröffentlicht hat.

Traffic Light Protokoll

Da Verschlusssachen[14] eine eigene staatliche Methodik zur Einstufung und Behandlung vertraulicher Informationen sind, stößt diese an Grenzen, wo vertrauliche Informationen den Staat verlassen sollen oder müssen. Dies kann z. B. die Kommunikation vertraulicher Inhalte in kritischen Infrastrukturen[15] sein.

Hier bietet sich das Traffic Light Protokoll[16] (TLP) an. Es ist eine standardisierte Vereinbarung zum Austausch schutzwürdiger Daten. Es gibt die Schutzstufen

- **TLP:RED**: Informationen dürfen nur im Kreise der auf das TLP verpflichteten, in einer Besprechung anwesenden Personen ausgetauscht werden. Dokumente dürfen vom Empfänger nur nach Genehmigung durch den Absender weitergegeben werden.

- **TLP:AMBER**: Wenn es den Zielen der Arbeitsgruppe dient, dürfen Informationen auch an Kollegen in der eigenen Organisation oder an andere Organisationen (zum Beispiel Berater) weitergegeben werden („Need-to-know“-Prinzip).

- **TLP:GREEN**: Informationen dürfen auch an andere Organisationen weitergegeben, aber nicht veröffentlicht oder den Massenmedien zugänglich gemacht werden.

[14] https://de.wikipedia.org/wiki/Geheimhaltungsstufe
[15] https://de.wikipedia.org/wiki/Kritische_Infrastrukturen
[16] https://de.wikipedia.org/wiki/Traffic_Light_Protocol

- **TLP:WHITE** : Informationen dürfen uneingeschränkt an jeden einschließlich Massenmedien weitergegeben werden.

Je nach Schutzstufe müssen die Informationen bei der elektronischen Kommunikation angemessen verschlüsselt werden. Da bei ist das Merkblatt zum sicheren Informationsaustausch mit dem Traffic Light Protocol (TLP) zu beachten und die Teilnehmer sind darauf mit diesem Formular zu verpflichten.

Verschlusssachen (VS)

Verschlusssachen[17] sind eine eigene Methodik zur Einstufung staatlicher Informationen. Sie basieren auf der Verschlusssachenanweisung (VSA)[18]

Link: http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_10082018_SII554001196.htm

VS-NfD

Siehe Schutzstufen

Zip

Zip ist eigentlich ein Komprimierungsprogramm, um Dateien zusammenzufassen und/oder zu verkleinern. Als Option bietet Zip auch die Verschlüsselung der Ergebnisdatei an.
Gehen Sie dazu im Microsoft-Explorer oder einem anderen Dateiverwaltungsprogramm auf die Datei oder das Verzeichnis, dass Sie verschlüsseln wollen und drücken die rechte Maustaste. Wählen Sie „7-Zip“ und „Zu einem Archiv hinzufügen“:
Geben Sie dann der Datei unter „Archiv“ den gewünschten Namen, gehen zu „Verschlüsselung“, wählen Sie ein ausreichend sicheres Passwort (mindestens 12 Zeichen aus 3 Zeichenkategorien) und das Verfahren AES-256. Mit „OK“ wird die Datei dann im gewünschten Ordner verschlüsselt abgelegt.
Typ: AES-256 ist ein symmetrisches Verschlüsselungsverfahren[19].
Bitte beachten Sie, dass der Empfänger der Datei entweder 7-Zip oder ein alternatives Programm zum Entschlüsseln von AES-256-verschlüsselten Dateien installiert haben muss. Im Umweltbundesamt ist 7-Zip auf allen Clients installiert.

[17] https://de.wikipedia.org/wiki/Geheimhaltungsstufe
[18] http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_10082018_SII554001196.htm
[19] https://de.wikipedia.org/wiki/Symmetrisches_Kryptosystem