Richtlinie
für den Umgang mit personenbezogenen Daten
in der Freien Demokratischen Partei

– Beschluss des Bundesvorstands vom 27. Mai 2019 –

§ 1 - Grundsatz 1
§ 2 - Geltungsbereich 1
§ 3 - Verpflichtung auf den Datenschutz, Verantwortlichkeiten 2
§ 4 - Datenschutzbeauftragte/r 2
§ 5 - Erhebung und Verarbeitung 3
§ 6 - Informationspflichten 4
§ 7 - Datenzugriff 4
§ 8 - Speicherung, Löschung 5
§ 9 - Elektronische Kommunikation 5
§ 10 - Datensicherheit 6
§ 11 - Meldung von Datenschutzverstößen 7
§ 12 - Betroffenenrechte 7
§ 13 - Rechenschaftspflicht 7
§ 14 - Informationspflicht, Verstoß 8
Anhang: Definitionen 9

§ 1 - Grundsatz

(1) Diese Richtlinie regelt den Umgang mit personenbezogenen Daten in der Freien Demokratischen Partei (FDP). Sie setzt die Anforderungen der Datenschutz-Grundverordnung (DSGVO) in die Parteiarbeit um.

(2) Als Partei der Bürgerrechte misst die FDP dem Datenschutz und der Vertraulichkeit der ihr anvertrauten Informationen einen hohen Stellenwert bei. Bei der Verarbeitung personenbezogener Daten für Zwecke der FDP sind die Grundrechte und Grundfreiheiten der Betroffenen, insbesondere ihr Recht auf Schutz personenbezogener Daten, zu wahren und zu schützen.

§ 2 - Geltungsbereich

(1) Diese Richtlinie gilt für ehrenamtlich in der FDP Tätige (Mitglieder, Funktionsträgerinnen und Funktionsträger, Freiwillige), bei der FDP Beschäftigte (Mitarbeiterinnen und Mitarbeiter, Praktikantinnen und Praktikanten, Werksstudierende) sowie für alle, die im Auftrag für die FDP personenbezogene Daten verarbeiten (Honorarkräfte, Auftragsverarbeitung).

(2) Diese Richtlinie ist für sämtliche Gliederungen der FDP auf allen Organisationsebenen verbindlich und kann nicht durch eigene Richtlinien von Gliederungen oder auf sonstige Weise außer Kraft gesetzt oder eingeschränkt werden.

(3) Diese Richtline ist beim Umgang mit sämtlichen personenbezogenen Daten zu beachten.

§ 3 - Verpflichtung auf den Datenschutz, Verantwortlichkeiten

(1) Alle Personen, die in der FDP mit personenbezogenen Daten umgehen, sind auf die Einhaltung des Datenschutzes zu verpflichten.

a) Funktionsträgerinnen und Funktionsträger sowie Freiwillige sind durch die jeweils zuständigen Vorsitzenden zu verpflichten. Die Verpflichtung muss vor Aufnahme der Vorstands- bzw. Freiwilligentätigkeit erfolgen. Bei Nutzung der zentralen Mitgliederverwaltung durch das Funktionsträgerportal erfolgt eine zusätzliche Verpflichtung in der Weise, dass bei der ersten Anmeldung eine Datenschutzverpflichtung aktiv bestätigt wird.

b) Beschäftigte werden durch die jeweils zuständigen Vorgesetzten auf den Datenschutz verpflichtet. Die Verpflichtung erfolgt in zeitlichem Zusammenhang mit der Unterzeichnung des Arbeitsvertrages.

c) Honorarkräfte sind durch die Auftraggeber im zeitlichen Zusammenhang mit der Begründung des Vertragsverhältnisses zu verpflichten. Bei Auftragsverarbeitung haben die Auftraggeber dafür Sorge zu tragen, dass der Datenschutz, insbesondere Art. 28 DSGVO, durch geeignete technische und organisatorische Maßnahmen des Auftragsverarbeiters eingehalten wird.

(2) Die Verpflichtung erfolgt schriftlich. Hierfür stellt die Bundespartei ein Formular (mit Merkblatt zum Datenschutz) bzw. eine Möglichkeit zur elektronischen Erfassung und Speicherung zur Verfügung. Sofern keine elektronische Erfassung und Speicherung erfolgt, sind die Erklärungen in den Geschäftsstellen bzw. – soweit eine solche nicht vorhanden ist – bei den zuständigen Vorsitzenden zu hinterlegen. Die Verpflichtungserklärungen Beschäftigter werden zu den Personalakten genommen.

(3) Die Verpflichtung auf den Datenschutz wirkt auch nach Beendigung der Tätigkeit für die FDP fort.

(4) Ehrenamtlich Tätige und Beschäftigte sind regelmäßig in der Einhaltung des Datenschutzes zu schulen.

(5) Alle in Abs. (1) genannten Personen sind in ihrem Aufgabenbereich für den Datenschutz verantwortlich. Die Einhaltung muss von ihnen regelmäßig kontrolliert werden.

§ 4 - Datenschutzbeauftragte/r

(1) Die FDP bestellt eine/einen Datenschutzbeauftragte/n. Sie/er erfüllt diese Aufgabe für den Gesamtverein FDP. Die Kontaktdaten lauten:

> Freie Demokratische Partei, Datenschutzbeauftragter, Reinhardtstraße 14, 10117 Berlin,
> Tel. 030 284958-90, datenschutz@fdp.de

Die Bundespartei und die Landesverbände teilen diese Kontaktdaten der jeweils für sie zuständigen Aufsichtsbehörde mit.

(2) Die/der Datenschutzbeauftragte nimmt die ihr/ihm kraft Gesetzes und in dieser Richtlinie zugewiesenen Aufgaben wahr. Dazu zählt insbesondere die Beratung bei der Umsetzung der datenschutzrechtlichen Vorgaben sowie die Überwachung deren Einhaltung. Insoweit sind alle vom Geltungsbereich dieser Richtlinie erfassten Personen der/dem Datenschutzbeauftragten auskunftspflichtig.

Die/der Datenschutzbeauftragte wird frühzeitig in alle Datenschutzfragen eingebunden und wird von allen ehrenamtlich Tätigen sowie allen Beschäftigten bei der Erfüllung ihrer/seiner Aufgaben unterstützt.

(3) Alle ehrenamtlich Tätigen, Beschäftigten sowie betroffene Personen können sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an die/den Datenschutzbeauftragte/n wenden. Hierbei ist auf Wunsch Vertraulichkeit zu wahren.

§ 5 - Erhebung und Verarbeitung

(1) Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen (Art. 6 und 9 DSGVO). Es dürfen grundsätzlich nur solche Informationen verarbeitet werden, die zur Aufgabenerfüllung erforderlich sind und in unmittelbaren Zusammenhang mit dem Verarbeitungszweck stehen.

(2) Personenbezogene Daten dürfen nach der DSGVO grundsätzlich verarbeitet werden

a) bei der Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen des Mitgliedschaftsverhältnisses.

b) bei sonstigen bestehenden Vertragsverhältnissen mit den Betroffenen.

c) wenn berechtigte Interessen der FDP bestehen, sofern nicht die Interessen oder Grundrechte der Betroffenen überwiegen (z.B. die Nutzung der postalischen Anschrift zur Aussendung von Werbeschreiben). Datenverarbeitungen unter Berufung auf ein berechtigtes Interesse sollen jedoch nicht ohne vorherige Beratung durch die/den Datenschutzbeauftragte/n vorgenommen werden.

d) wenn eine rechtliche Verpflichtung besteht, der die FDP unterliegt (z.B. gesetzliche Aufbewahrungsfristen nach Parteiengesetz und Handelsgesetzbuch).

e) wenn und soweit die Betroffenen eingewilligt haben (z.B. Interessenten melden sich zum Erhalt eines Newsletters an).

(3) Bei den von der FDP als politischer Partei verarbeiteten personenbezogenen Daten handelt es sich zum Teil um besondere Arten personenbezogener Daten (sensible personenbezogene Daten) gemäß Art. 9 Abs. 1 DSGVO. Diese zeichnen sich dadurch aus, dass sie Rückschlüsse insbesondere auf die politische Meinung der betroffenen Personen zulassen. Die Verarbeitung dieser personenbezogenen Daten unterliegt strengeren Anforderungen; sie ist unter anderem zulässig

a) bei Mitgliedern oder ehemaligen Mitgliedern der FDP sowie Personen, die regelmäßige Kontakte mit der FDP unterhalten, auf der Grundlage geeigneter Garantien im Rahmen der rechtmäßigen Tätigkeit der Partei. Eine Offenlegung nach außen darf nur mit Einwilligung der betroffenen Personen erfolgen (Art. 9 Abs. 2 Buchst. d DSGVO).

b) wenn die betroffene Person die personenbezogenen Daten selbst öffentlich gemacht hat.

c) wenn die betroffene Person in die Verarbeitung der besonderen personenbezogenen Daten eingewilligt hat.

(4) Es wird sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Profiling).

(5) Personenbezogene Daten sind für einen zuvor festgelegten, eindeutigen und legitimen Zweck zu verarbeiten. So dürfen z.B. zum Zweck der Übermittlung von politischen Informationen und Veranstaltungseinladungen zur Verfügung gestellte Kontaktdaten nur im Bereich des Informations- und Veranstaltungsmanagements verarbeitet werden. Eine Datenhaltung ohne Zweck, z.B. die Speicherung von Daten auf Vorrat, ist unzulässig. Die Änderung einer Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist – neben der erklärten Einwilligung durch die Betroffenen – nur zulässig, wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist.

(6) Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führen die Gliederungen ein Verzeichnis von Verarbeitungen gem. Art. 30 DSGVO. Hierfür stellt die Bundespartei ein Formular bzw. eine Möglichkeit zur elektronischen Erfassung und Speicherung zur Verfügung.

§ 6 - Informationspflichten

(1) Die Betroffenen sind bei der Erhebung ihrer personenbezogenen Daten umfassend über den Umgang mit ihren Daten zu informieren. Die Information hat die Zweckbestimmung, die Identität der verantwortlichen Stelle, die Empfänger der personenbezogenen Daten sowie alle sonstigen Informationen im Sinne des Art. 13 DSGVO zu beinhalten, um eine faire und transparente Verarbeitung zu gewährleisten. Die Information ist in einer verständlichen und leicht zugänglichen Form sowie einer möglichst einfachen Sprache zu verfassen.

(2) Werden personenbezogene Daten nicht bei den Betroffenen erhoben, sondern z.B. durch Internetrecherche erlangt, sind die Betroffenen nachträglich und umfassend gem. Art. 14 DSGVO über den Umgang mit ihren Daten zu informieren. Dies gilt auch für die Änderung einer Zweckbestimmung der Datenverarbeitung.

(3) Die Erfüllung der Informationspflichten wird von der Bundespartei durch die Zurverfügungstellung eines im Internet abrufbaren Textes unterstützt: http://fdp.de/dsgvo-informationen.

§ 7 - Datenzugriff

(1) Auf personenbezogene Daten dürfen nur solche Personen Zugriff haben, für deren Tätigkeit der Umgang mit diesen personenbezogenen Daten erforderlich ist. Vorsitzende sowie Schatzmeisterinnen und Schatzmeistern benötigen für die Ausübung ihrer Tätigkeit sämtliche Daten der Mitglieder ihrer Gliederung. Bei den übrigen Funktionsträgerinnen und Funktionsträgern, Beschäftigten und Honorarkräften ist die Zugriffsberechtigung nach Art und Umfang des jeweiligen Tätigkeitsbereiches zu begrenzen. Bei Funktionsträgerinnen und Funktionsträgern bedarf es hierfür eines Vorstandsbeschlusses.

(2) Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung der Betroffenen zulässig. Dritte sind auch Fraktionen, Abgeordnete und Stiftungen.

(3) Für die Übermittlung personenbezogener Daten an Empfängerinnen und Empfänger außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder über besondere Vertragsklauseln nicht hergestellt werden kann.

(4) Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung (Art. 28 Abs. 3 DSGVO). Hierfür stellt die Bundespartei ein Formular zur Verfügung.

§ 8 - Speicherung, Löschung

(1) Beschäftigte speichern personenbezogene Daten grundsätzlich auf den hierfür vorgesehenen Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern oder in Cloudspeichern bedarf der Genehmigung durch die Vorgesetzten. Bei Netzlaufwerken ist die jeweilige Geschäftsstelle für die Datensicherung verantwortlich.

(2) Sofern aus organisatorischen Gründen – oder bei ehrenamtlich Tätigen – ein anderer Speicherort gewählt werden muss (z.B. Notebook, Desktop-PC), tragen die Nutzerinnen und Nutzer für die Datensicherung selbst die Verantwortung. Durch regelmäßig anzufertigenden Sicherungskopien ist die Verfügbarkeit der Daten sicherzustellen. Der FDP zuzuordnende personenbezogene Daten sind getrennt von privaten Daten zu speichern.

(3) Personenbezogene Daten sind zu löschen, wenn wir sie für Zwecke der FDP nicht mehr benötigt werden und keine gesetzlichen Vorgaben entgegenstehen. Es gelten folgende Löschfristen:

a)	Bürgerinnen-/Bürgeranfrage	
	– einfach, ohne Folgekommunikation	1 Jahr
	– mit Folgekommunikation	alle 2 Jahre Prüfung, ob weitere Speicherung erforderlich
b)	Stellenbewerberinnen-/Stellenbewerberdaten	1 Jahr
c)	Handelsbriefe, Verträge	6 Jahre
d)	Buchhaltungsdaten, Spendendaten, Lohnbuchhaltung	10 Jahre
e)	Mitgliederdaten	10 Jahre

Sofern ein Interesse an einer längeren Speicherung besteht, ist diese in begründeten Fällen zulässig. Die Frist beginnt im Fall von Buchst. a) mit dem letzten Kommunikationskontakt, im Fall von Buchst. b) mit dem Erhalt der personenbezogenen Daten und im Fall der Buchst. c) bis e) mit Beginn des auf den Abschluss des Vorgangs folgenden Jahres. Jede der in § 3 Abs. (1) dieser Richtlinie genannten Personen sind in ihrem Aufgabenbereich für die Löschung verantwortlich.

§ 9 - Elektronische Kommunikation

(1) Insbesondere sensible personenbezogene (§ 5 Abs. 3 dieser Richtlinie) Daten bedürfen bei der elektronischen Übertragung besonderen Schutzes. Die FDP und ihre Gliederungen arbeiten kontinuierlich an der Verbesserung der Sicherheitsstandards. Gegenwärtig entspricht eine regelmäßige Inhaltsverschlüsselung von E-Mails bei der Kommunikation mit privaten Empfängerinnen und Empfängern noch nicht dem Stand der Technik und kann deshalb in einer ehrenamtlich organisierten Partei nicht realisiert werden. Zum Schutz vertraulicher Informationen sind folgende Vorgaben zu beachten:

a) Als Mindeststandard muss eine Transportverschlüsselung erfolgen, wie sie u.a. die in der Initiative „E-Mail made in Germany“ zusammengeschlossenen Provider bieten (https://www.e-mail-made-in-germany.de).

b) Es ist der Grundsatz der Datensparsamkeit zu beachten und der Umfang der im E-Mail-Text mitgeteilten sensible personenbezogene Daten auf das erforderliche Mindestmaß zu beschränken.

c) Wenn immer möglich, sollen sensible personenbezogene Daten in passwortgeschützten Anhängen (z.B. PDF-Dokument) versendet werden. Dabei muss das Passwort ausreichend komplex sein und es darf nicht gleichfalls per E-Mail mitgeteilt werden (z.B. persönlich, telefonisch, SMS, Messenger).

d) Für die Übermittlung vertraulicher Informationen durch Beschäftigte an Funktionsträgerinnen und Funktionsträger sind vorrangig die Funktionsträgerpostfächer zu nutzen.

(2) Zur Vermeidung fehlerhafter Zustellungen sind E-Mails eindeutig zu adressieren. Aussendungen an eine größere Zahl von Empfängerinnen und Empfängern müssen unter Verwendung der „BCC-Funktion“ versendet werden. Ehrenamtlich Tätige sollen für die parteiinterne Kommunikation keine beruflichen E-Mail-Postfächer nutzen.

§ 10 - Datensicherheit

(1) Personenbezogene Daten sind vor unberechtigtem Zugriff, unberechtigter Verwendung, unberechtigter Weitergabe und Verlust zu schützen. Hierzu sind geeignete technisch-organisatorische Maßnahmen zu ergreifen. In diesem Zusammenhang sind u.a.

a) der Zugang zu Systemen durch Passwörter zu sichern, die ausreichend komplex sind und stets unter Verschluss gehalten werden. Hierfür erlässt die Bundespartei eine Passwort-Richtlinie.

b) Türen unbesetzter Räume zu verschließen, Zugangskontrollen an Geräten zu aktivieren, Systemzugänge in Abwesenheit zu sperren.

c) Zugriffsberechtigungen genau und vollständig festzulegen.

(2) Den Beschäftigten ist zur Datenverarbeitung Hard- und Software zur Verfügung zu stellen, die den Anforderungen von Abs. (1) entspricht. Bereits bei der Auswahl von Hard- und Software ist das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen zu beachten. Speichermedien (z.B. mobile Endgeräte, Daten-Sticks, externe Festplatten) sind zu verschlüsseln. Die Nutzung privater Hard- und Software durch Beschäftigte bedarf der Genehmigung der jeweils zuständigen Vorgesetzten; für die Datensicherheit gilt Abs. (3).

(3) Sofern ehrenamtlich Tätige, Beschäftigte und Honorarkräfte eigene Hard- und Software zur Datenverarbeitung nutzen, sind sie verpflichtet, technische (u.a. aktuelles Antivirenprogramm, Firewall, Software-Updates, höchstmögliche Sicherheitseinstellungen, WLAN-Verschlüsselung) und organisatorische (u.a. Zugangsbeschränkung, Passwortschutz) Maßnahmen zu ergreifen.

(4) Sofern bei einer Verarbeitung ein hohes Risiko für Betroffene besteht – was insbesondere bei umfangreicher Verarbeitung sensibler personenbezogener Daten der Fall ist –, ist bei der Einführung neuer bzw. der Veränderung bestehender Verfahren und Systeme eine Datenschutz-Folgenabschätzung durchzuführen (Art. 35 DSGVO). Die/der Datenschutzbeauftragte berät die Gliederungen bei der Durchführung der Datenschutz-Folgenabschätzung sowie bezüglich der Frage, wann Verarbeitungen ein hohes Risiko für Betroffene beinhalten können.

(5) Die Gliederungen sind verpflichtet, in Abhängigkeit der konkreten Schutzbedarfsfeststellung und Risikoanalyse ein Sicherheitskonzept mit den erforderlichen technisch-organisatorischen Maßnahmen zu erstellen, das Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie die Belastbarkeit der verarbeitenden Systeme wahrt. Neben dieser Richtlinie sind die Vorgaben des Art. 32 DSGVO zu beachten.

§ 11 - Meldung von Datenschutzverstößen

(1) Sollten personenbezogene Daten unrechtmäßig Dritten offenbart worden sein, ist darüber unverzüglich die/der Datenschutzbeauftragte zu informieren. Die Mitteilung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

(2) Die Erfüllung einer etwaigen Informationspflicht gegenüber der Aufsichtsbehörde erfolgt ausschließlich durch die/den Datenschutzbeauftragte/n. Betroffene werden durch die zuständige Gliederung informiert, wobei die/der Datenschutzbeauftragte beratend hinzugezogen wird.

§ 12 - Betroffenenrechte

(1) Betroffene haben zahlreiche Rechte, u.a. das Recht auf Auskunft über die von der FDP über ihre Person gespeicherten personenbezogenen Daten sowie das Recht auf Berichtigung, auf Löschung und auf Einschränkung der Verarbeitung dieser Daten. Zudem können sie der Verarbeitung ihrer Daten widersprechen.

(2) Die Gliederungen müssen sicherstellen, dass bei ihnen eingehende Anträge auf Ausübung von Betroffenenrechten, insbesondere Auskunftsbegehren, unverzüglich bearbeitet werden. Betroffenen ist grundsätzlich innerhalb eines Monats nach Eingang des Antrags zu antworten (Art. 11 Abs. 3 DSGVO). Die/der Datenschutzbeauftragte steht bei der Wahrung der Betroffenenrechte beratend zur Verfügung.

(3) Die Auskunftserteilung an Betroffene erfolgt grundsätzlich schriftlich.

§ 13 - Rechenschaftspflicht

(1) Die Einhaltung der Vorgaben der DSGVO sowie dieser Richtlinie muss von jeder Gliederung jederzeit nachgewiesen werden können. Hierzu sind getroffene Maßnahmen nachvollziehbar und transparent zu dokumentieren.

(2) Die Dokumentation hat insbesondere zu umfassen:

a) Verzeichnis von Verarbeitungstätigkeiten (§ 5 Abs. 6 dieser Richtlinie)

b) Verträge zur Auftragsverarbeitung (§ 7 Abs. 4 dieser Richtlinie)

c) Sicherheitskonzept mit technisch-organisatorischen Maßnahmen (§ 10 Abs. 5 dieser Richtlinie)

d) Berechtigungskonzept, das Zuständigkeiten, Aufgaben und Befugnisse regelt (§ 10 Abs. 1 Buchst. c dieser Richtlinie)

e) Informationen über durchgeführte interne und externe Prüfungen

§ 14 - Informationspflicht, Verstoß

(1) Bei Verletzungen von sich aus dieser Richtlinie ergebenden Verpflichtungen ist umgehend die/der Datenschutzbeauftragte zu unterrichten.

(2) Wer Regelungen dieser Richtlinie missachtet oder verletzt, verstößt gegen Pflichten aus seinem Arbeits- bzw. Honorarvertrag bzw. gegen Pflichten, die mit der Ausübung des Amtes oder der Beauftragung übernommen wurden und muss mit arbeitsrechtlichen, vertraglichen oder sonstigen zivilrechtlichen Konsequenzen rechnen. Sofern zudem die Vorgaben der DSGVO verletzt werden, können zusätzlich die dort vorgesehenen Rechtsfolgen ausgelöst werden.

Berlin, den 27. Mai 2019

Anhang: Definitionen

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Betroffene/r). Mitgliederdaten gehören dabei ebenso zu den personenbezogenen Daten wie Personaldaten von Beschäftigten. Beispielsweise lässt der Name einer Ansprechpartnerin bzw. eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie die E-Mail-Adresse. Es genügt, wenn die jeweilige Information mit den Namen der Betroffenen verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z. B. bei der Mitgliedsnummer. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.

Besondere Arten personenbezogener Daten (sensible personenbezogene Daten) sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Gewerkschaftszugehörigkeit hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.

Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter 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, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Einschränkung der Verarbeitung ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

Profiling bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

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

Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Empfänger ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

Dritter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Eine **Einwilligung** des Betroffenen ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der der Betroffene zu verstehen gibt, dass er mit der Verarbeitung der ihn betreffenden personenbezogenen Daten einverstanden ist.