Freie Demokraten
FDP

Richtlinie für den Umgang mit personenbezogenen Daten

in der Freien Demokratischen Partei

– Fassung vom 16. Januar 2023 –

Die Richtlinie für den Umgang mit personenbezogenen Daten in der Freien Demokratischen Partei hat der Bundesvorstand erstmals am 15. Juni 2011 beschlossen. Am 27. Mai 2019 wurde vom Bundesvorstand eine grundlegend überarbeitete Neufassung verabschiedet; diese wurde mit Beschluss des Bundesvorstands vom 16. Januar 2023 aktualisiert.

INHALTSVERZEICHNIS

RICHTLINIE FÜR DEN UMGANG MIT PERSONENBEZOGENEN DATEN IN DER FREIEN DEMOKRATISCHEN PARTEI

§ 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) und der nationalen Datenschutzgesetze in die Parteiarbeit um. Sie wurde vom Bundesvorstand der FDP auf Grundlage von § 25a Abs. 3 Bundessatzung erlassen.

(2) Die FDP wirkt als politische Partei im Sinne von § 2 Abs. 1 Parteiengesetz an der politischen Willensbildung des Volkes mit (Art. 21 Abs. 1 Satz 1 Grundgesetz). Zur Erfüllung der ihr durch Verfassung, Gesetze und Satzungszwecke zugewiesenen Aufgaben verarbeitet die FDP personenbezogene Daten ihrer Mitglieder und ihr nahestehender Personen (§ 6 dieser Richtlinie) sowie von Bürgerinnen und Bürgern im Rahmen von Öffentlichkeitsarbeit und Wahlkampf (§ 7 dieser Richtlinie).

(3) Als Partei der Bürgerrechte misst die FDP dem Datenschutz und der Vertraulichkeit einen hohen Stellenwert bei. Bei der Verarbeitung personenbezogener Daten für Zwecke und Aufgaben 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 im Rahmen der gesetzlichen Regelungen für ehrenamtlich in der FDP Tätige (Mitglieder, Funktionsträgerinnen und Funktionsträger, Freiwillige), die der Partei angehörenden Inhaberinnen und Inhaber eines öffentlichen Wahlamtes (Mandatsträgerinnen und Mandatsträger), 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 Richtlinie ist beim Umgang mit sämtlichen personenbezogenen Daten zu beachten (für die Erklärung datenschutzrechtlicher Fachbegriffe wird auf Anlage 1 zu dieser Richtlinie verwiesen).

§ 3 - Verpflichtung auf den Datenschutz, Verantwortlichkeiten

(1) Alle Personen, die in der FDP mit personenbezogenen Daten umgehen, sind zur Wahrung des Datengeheimnisses und einer sorgfältigen Verarbeitung solcher Daten verpflichtet.

a) Funktionsträgerinnen und Funktionsträger sowie Freiwillige sind bei Aufnahme der Vorstands- bzw. Freiwilligentätigkeit auf diese Pflichten hinzuweisen. 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 schriftlich auf den Datenschutz verpflichtet. Die Verpflichtung erfolgt in zeitlichem Zusammenhang mit der Unterzeichnung des Arbeitsvertrages. Die Verpflichtungserklärungen Beschäftigter werden zu den Personalakten genommen.

c) Honorarkräfte sind durch die Auftraggeber im zeitlichen Zusammenhang mit der Begründung des Vertragsverhältnisses schriftlich 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.

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

(2) Ehrenamtlich Tätige und Beschäftigte sind regelmäßig in der Einhaltung des Datenschutzes zu schulen. Hierfür stellt die Bundespartei ein Online-Schulungstool zur Verfügung (https://elearning.lips-fdp.de/dsgvo), das die Grundlagen des Datenschutzes in der FDP vermittelt. Bei Bestehen eines abschließenden Tests erhalten die Teilnehmenden ein Zertifikat zum Nachweis der erworbenen Kenntnisse. Das Zertifikat dient der Dokumentation nach § 16 dieser Richtlinie.

(3) Alle in Abs. (1) genannten Personen sind in ihrem Aufgabenbereich für den Datenschutz verantwortlich. Die Einhaltung muss von ihnen regelmäßig kontrolliert werden. Die Einhaltung des Datenschutzes zählt zu den Geschäftsführungspflichten des Vorstands. Der Vorstand soll eine/n Ansprechpartner/in für den Datenschutz bestimmen und diese Person mit deren Kontaktdaten dem bzw. der Datenschutzbeauftragten der FDP mitteilen.

§ 4 - Datenschutzbeauftragte/r

(1) Alle Gliederungen der FDP, die personenbezogene Daten verarbeiten, trifft die gesetzliche Pflicht, eine/n Datenschutzbeauftragte/n zu haben. Diese/n benennt der Bundesvorstand gem. § 19 Abs. 1 Bundessatzung als gemeinsame/n Datenschutzbeauftragte/n der FDP (Art. 37 Abs. 2 DSGVO). Die Kontaktdaten lauten:

> Freie Demokratische Partei, Datenschutzbeauftragte/r, Reinhardtstraße 14, 10117 Berlin, Tel. 030 284958-84, 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 - Rechtsgrundlagen und Grundsätze der Datenverarbeitung

(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 insbesondere verarbeitet werden

a) zur Durchführung der rechtmäßigen Tätigkeiten der FDP nach § 25a Abs. 1 Satz 2 Bundessatzung in Bezug auf ihre Mitglieder, ehemaligen Mitglieder, und auf weitere Personen, die regelmäßige Kontakte mit ihr unterhalten – Art. 9 Abs. 2 Buchst. d DSGVO (z.B. Mitgliederbetreuung, Beitrags-/Spendenverwaltung).

b) wenn und soweit die Betroffenen eingewilligt haben – Art. 9 Abs. 2 Buchst. a bzw. Art. 6 Abs. 1 Buchst. a DSGVO (z.B. Newsletter-Anmeldung durch Interessierte, werbliche Abbildung von Personen in Flyern oder auf Plakaten).

c) zur Erbringung vertraglich geschuldeter oder zur Durchführung vorvertraglicher Maßnahmen – Art. 6 Abs. 1 Buchst. b DSGVO (z.B. Veranstaltungsmanagement, Stellenbewerbungen).

d) wenn eine rechtliche Verpflichtung besteht, der die FDP unterliegt, oder eine Aufgabe im öffentlichen Interesse liegt – Art. 6 Abs. 1 Buchst. c und e DSGVO (z.B. gesetzliche Aufbewahrungsfristen nach Parteiengesetz oder Handelsgesetzbuch).

e) wenn berechtigte Interessen der FDP bestehen, sofern nicht die Interessen oder Grundrechte der Betroffenen überwiegen – Art. 6 Abs. 1 Buchst. f DSGVO (z.B. Fotoberichterstattung von Parteiveranstaltungen, Kontaktaufnahme zu Personen des öffentlichen Lebens, postalische Wahlwerbung mit Adressen aus Melderegisterauskünften gem. § 50 Bundesmeldegesetz oder von Adressdienstleistern).

(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 (z.B. Parteimitgliedschaft, Status als Spender/in). Eine Verarbeitung setzt insbesondere voraus, dass sie im Rahmen der rechtmäßigen Tätigkeiten der FDP (Abs. 1 Buchst. a) erfolgt, auf einer Einwilligung (Abs. 1 Buchst. b) basiert, die sich ausdrücklich auf die sensiblen Daten bezieht, oder dass die betroffene Person die Information selbst öffentlich gemacht (z.B. öffentliche Postings in Sozialen Netzwerken) oder die Veröffentlichung ersichtlich veranlasst hat (z.B. Mitteilung der Vorstandsmitglieder auf Gliederungs-Webseite).

(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 zulässigen 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 - Datenverarbeitung in der Parteiorganisation

(1) Im Rahmen ihrer organisatorischen Arbeit verarbeitet die FDP personenbezogene Daten von Mitgliedern, Spenderinnen und Spendern, Interessierten sowie weiteren Dritten. Zu Letzteren zählen neben Dienstleisterinnen und -leistern sowie Kooperationspartnerinnen und -partnern u.a. Personen des öffentlichen Lebens, gesellschaftlich Aktive, Medienvertreterinnen und -vertreter sowie ehemalige Mitglieder der FDP.

(2) Die Verarbeitung erfolgt gem. § 25a Abs. 1 Bundessatzung, soweit dies für die Erreichung der Zwecke und Ziele der Partei erforderlich ist, insbesondere zur Teilnahme an Wahlen und Abstimmungen, zur Kommunikation – auch auf elektronischem Weg – mit den in Abs. 1 genannten Personen, zu deren Beteiligung an der politischen und organisatorischen Arbeit der Partei, zur Betreuung, Bindung und Rückgewinnung von Mitgliedern sowie zur Finanz-, Beitrags- und Spendenverwaltung.

(3) Folgende Kategorien von Daten sind von der Verarbeitung umfasst:

a) Personenstammdaten (z.B. Name, Namenszusätze, Geburtsdatum, Staatsangehörigkeit)

b) Kontaktdaten (z.B. Anschriften, E-Mail-Adressen, Telefonnummern)

c) Zahlungsdaten (z.B. IBAN, Einkommensstaffel, Beiträge, Spenden)

d) Mitgliedschaftsdaten (z.B. Ein-/Austrittsdatum, Gliederungen, Parteifunktionen, Mandate, Verteiler)

e) Korrespondenz (z.B. Schrift-/E-Mail-Verkehr)

f) Auftrags- und Rechnungsdaten (z.B. Auftragsbeschreibung, Rechnungsnummer)

Die Daten werden direkt bei den in Abs. 1 genannten Personen im Rahmen der Kontaktaufnahme sowie der laufenden Kontaktbeziehung erhoben. Die Bereitstellung der Daten ist für die Begründung des Mitgliedschaftsverhältnisses erforderlich. Die Daten sind von der zuständigen Gliederung unverzüglich in der zentralen Mitgliederdatei zu speichern und grundsätzlich nur über diese zu verarbeiten; werden ausnahmsweise Kopien – in Papier- oder digitaler Form – gefertigt, sind diese sorgfältig zu verwahren und nach der Nutzung zu vernichten bzw. zu

löschen. Daten Interessierter und weiterer Dritter können auch in eigenen Datenverarbeitungssystemen der Gliederungen verarbeitet werden, die diese in eigener Verantwortung entsprechend der Regelungen dieser Richtlinie betreiben.

(3) Zur leichteren Verwaltung und der eindeutigen Identifizierung erhält jedes Mitglied der FDP eine Mitgliedsnummer.

§ 7 - Datenverarbeitung in Öffentlichkeitsarbeit und Wahlkampf

(1) In Wahrnehmung ihrer verfassungsmäßigen Rolle (§ 1 Abs. 2 dieser Richtlinie) verarbeitet die FDP personenbezogene Daten von Bürgerinnen und Bürger, um diese über ihre politischen Ziele zu informieren und um für die Wahl der FDP zu werben. Die Gliederungen der FDP, ihre Funktionsträgerinnen und Funktionsträger, Mandatsträgerinnen und Mandatsträger, ihre Beschäftigten sowie ihre Wahlbewerberinnen und Wahlbewerber berichten der Öffentlichkeit und den Medien über ihre politische Arbeit und laden zu Veranstaltungen ein. Die Information erfolgt u.a. durch Texte und Fotos auf Webseiten, Profilen in Sozialen Netzwerken, Newslettern sowie in Printprodukten (z.B. Mitgliedermagazine, Flyer) sowie in Pressemitteilungen und postalischer Wahlwerbung.

(2) In diesem Zusammenhang werden insbesondere Namen, Funktionsbezeichnungen, Kontaktdaten und Personenfotos – auch von an die Öffentlichkeit gerichteten Veranstaltungen (z.B. Parteitage, Mitglieder-/Wahlversammlungen, Wahlkampfveranstaltungen) – veröffentlicht. Zudem werden im Einzelfall Namen und Kontaktdaten von Bürgerinnen und Bürgern verarbeitet (z.B. postalische Wahlwerbung). Diese Verarbeitungen erfolgen zur Wahrung der berechtigten Interessen der FDP nach Abs. 1, ohne dass eine Einwilligung der Betroffenen vorliegen muss. Soweit möglich, werden die Betroffenen nach § 9 dieser Richtlinie informiert, insbesondere über ein ggf. bestehendes Recht zum Widerspruch nach § 15 dieser Richtlinie. E-Mail-Adressen von Bürgerinnen und Bürgern dürfen nur auf Grundlage einer Einwilligung der Betroffenen verarbeitet werden.

§ 8 - Datenverarbeitung in gemeinsamer Verantwortung

(1) Die Bundespartei und die Landesverbände arbeiten bei der Mitgliederverwaltung, bei der Unterhaltung von E-Mail- und Speichersystemen, beim Betrieb von Mitgliederportal/-App und Mitglieder-Netzwerk „Meine Freiheit“ sowie bei der Finanz-, Beitrags- und Spendenverwaltung eng zusammen. Die Datenverarbeitung in diesem Zusammenhang erfolgt ganz bzw. teilweise in gemeinsamer Verantwortung (Art. 26 DSGVO).

(2) Zur Gewährleistung der Rechte der Betroffenen und unter Berücksichtigung der Vorgaben der DSGVO haben die Beteiligten eine Vereinbarung über die gemeinsame Verantwortung nach Art. 26 DSGVO geschlossen, die Regeln über die Datenverarbeitung aufstellt. Sie hat im Wesentlichen folgenden Inhalt:

a) Die zentralen Prozesse der in für die in Abs. 1 genannten Datenverarbeitungen eingesetzten Systeme, Software und Datenbanken werden von den Beteiligten gemeinsam verantwortet. Daneben ergeben sich – dem tatsächlichen Einfluss der Beteiligten entsprechend – unterschiedliche Wirkungskreise. Insbesondere sind die Landesverbände für die Pflege der Daten der ihnen zugeordneten Mitglieder verantwortlich. Dabei sind alle Beteiligten an diese Richtlinie gebunden.

b) Die Betroffenenrechte (§ 15 dieser Richtlinie) können gegenüber jedem Beteiligten geltend gemacht werden. Die Beteiligten unterrichten sich über die Geltendmachung von Betroffenenrechten unverzüglich, sofern Daten auch von oder für andere/n Beteiligte/n verarbeitet werden

c) Die Informationspflichten gem. Art. 13 und 14 DSGVO (§ 9 dieser Richtlinie) werden von jedem Beteiligten für seinen Wirkungskreis erfüllt. Die hierfür erforderlichen Informationen werden von der Bundespartei zur Verfügung gestellt.

§ 9 - Informationspflichten

(1) Die Betroffenen sind vor der Erhebung ihrer personenbezogenen Daten umfassend über den Umgang mit ihren Daten zu informieren (z.B. durch die Datenschutzerklärung zu einer Website über die dort eingebundenen Dienste Dritter, wie beispielsweise Google, oder durch die Datenschutzerklärung zu einer Facebook-Seite, die Erklärung zum Verwendungszweck bei Online-Formularen, die Fotohinweise bei öffentlichen Veranstaltungen). Die Information hat die Identität der verantwortlichen Stelle, die Zweckbestimmung, 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 Adressdienstleister oder Internetrecherche erlangt, sind die Betroffenen nachträglich gem. Art. 14 DSGVO über die Datenverarbeitung zu informieren. Dies gilt insbesondere für die Kategorien der verarbeiteten Daten sowie für deren Herkunft. Bei Verwendung der Daten zur Kommunikation (z.B. zur postalischen Wahlwerbung) sind die Informationen spätestens bei der ersten Kontaktaufnahme zu erteilen.

(3) Die Erfüllung der Informationspflichten wird von der Bundespartei durch die Zurverfügungstellung eines im Internet abrufbaren Textes unterstützt: http://fdp.de/dsgvo-informationen. Durch entsprechend angepasste Texte können die Gliederungen ihre Informationspflichten situationsgerecht auch in abgestufter Form erfüllen (z.B. Verlinkung auf Wahlwerbung bei knappem Platzangebot).

§ 10 - Datenzugriff und -übermittlung

(1) Auf personenbezogene Daten dürfen nur solche Personen zugreifen bzw. diese verarbeiten, für deren Tätigkeit der Umgang mit diesen personenbezogenen Daten erforderlich ist:

a) Vorsitzende, Stellvertreterinnen und Stellvertreter sowie Schatzmeisterinnen und Schatzmeistern benötigen für die Ausübung ihrer Tätigkeit sämtliche Daten der Mitglieder ihrer Gliederung. Bei den übrigen Funktionsträgerinnen und Funktionsträgern sowie bei Freiwilligen ist die Zugriffsberechtigung nach Art und Umfang des jeweiligen Tätigkeitsbereiches zu begrenzen (z.B. auf die Kontaktdaten der Neumitglieder für deren Betreuung); hierfür bedarf es eines Vorstandsbeschlusses. Bei kleinen Vorständen (vier/fünf Mitglieder) kann auch die gemeinschaftliche Datennutzung beschlossen werden.

b) Beschäftige und Honorarkräfte verarbeiten personenbezogene Daten in dem Umfang und in der Weise, wie es zur Erfüllung der übertragenen Aufgaben erforderlich ist.

c) Mandatsträgerinnen und Mandatsträger sowie deren Zusammenschlüsse (Fraktionen, Gruppen) dürfen Kontaktdaten der Mitglieder verarbeiten, um über ihre politische Arbeit in der jeweiligen Vertretung zu informieren und zu Veranstaltungen einzuladen, es sei denn das Mitglied widerspricht dieser Verarbeitung im Einzelfall.

d) Vertreter der Fachausschüsse und anderer beratender Gremien dürfen die Kontaktdaten ihrer Mitglieder verarbeiten, um ihre politische Arbeit zu organisieren. Auf den mit einfacher Mehrheit zu fassenden Beschluss des Gremiums werden die Kontaktdaten auch den Mitgliedern zum fachlichen Austausch untereinander zur Verfügung gestellt, es sei denn das Mitglied widerspricht dieser Verarbeitung im Einzelfall.

e) Vertrauens- und Ombudspersonen verarbeiten personenbezogene Daten der Mitglieder, soweit dies zur Erfüllung ihrer Aufgaben, insbesondere zur Gewährleistung eines respektvollen Umgangs der Mitglieder miteinander erforderlich ist.

f) Mitglieder ohne Parteifunktion oder Mandat erhalten Kontaktdaten anderer Mitglieder nur, wenn diese eine entsprechende Einwilligung erteilt haben. Ist eine Kontaktaufnahme zur Wahrnehmung von Mitwirkungsrechten bei der parteiinternen Willensbildung (z.B. Einberufung einer Mitgliederversammlung durch eine Minderheit oder Wahlwerbung für die Kandidatur um ein Parteiamt) erforderlich, ist der zuständige Vorstand verpflichtet, das Begehren zeitnah und in neutraler Weise an die Mitglieder zu verteilen. Wird dies verweigert, kann sich das Mitglied an eine übergeordnete Parteigliederung wenden. Eine Offenlegung der Mitgliedschaft ohne oder gegen den Willen der betroffenen Mitglieder erfolgt nicht.

g) Im Rahmen der Zusammenarbeit mit der Allianz Liberaler und Demokraten für Europa (ALDE Partei) und der Liberalen Internationale (LI) dürfen diesen die hierfür erforderlichen personenbezogenen Daten übermittelt werden.

(2) Die Übermittlung von personenbezogenen Daten an andere als die in Abs. 1 Buchst. c, f und g genannten Dritte sowie die Offenlegung diesen gegenüber ist nur aufgrund gesetzlicher Erlaubnis (z.B. Veröffentlichung von Spenderinnen und Spendern) oder der Einwilligung der Betroffenen (z.B. bei Medienanfragen in Bezug auf Mitglieder ohne Parteifunktion/Mandat) zulässig. Dritte im Sinne von Satz 1 sind auch rechtlich selbständige Vorfeldorganisationen der Partei sowie ihr nahestehende Stiftungen.

(3) Die Übermittlung personenbezogener Daten an Empfängerinnen und Empfänger außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, darf – vorbehaltlich gesetzlicher oder vertraglicher Erlaubnisse – nur beim Vorliegen der besonderen Voraussetzungen der Art. 44 ff. DSGVO erfolgen. D.h., die Verarbeitung erfolgt z.B. auf Grundlage besonderer Garantien, wie der offiziell anerkannten Feststellung eines der EU entsprechenden Datenschutzniveaus oder Beachtung offiziell anerkannter spezieller vertraglicher Verpflichtungen (so genannte „EU-Standardvertragsklauseln“).

(4) In Protokolle, Teilnahmelisten und andere Dokumente parteiinterner Versammlungen und Sitzungen, die in Erfüllung gesetzlicher oder satzungsmäßiger Aufgaben erstellt werden, dürfen die erforderlichen personenbezogenen Daten aufgenommen werden, auch wenn eine Einsicht durch Mitglieder möglich ist.

(5) 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 gem. Art. 28 Abs. 3 DSGVO (z.B. Lettershop, Druckerei, Newsletter-Dienst). Hierfür stellt die Bundespartei ein Formular zur Verfügung.

§ 11 - Speicherung, Löschung

(1) Beschäftigte speichern personenbezogene Daten grundsätzlich an den hierfür vorgesehenen sicheren Speicherorten, insbesondere auf Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern oder in Cloudspeichern bedarf der Genehmigung durch die Vorgesetzten. Bei Netzlaufwerken ist die jeweilige Gliederung 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 Aufbewahrungspflichten entgegenstehen. Die Löschfristen im Einzelnen sind im Löschkonzept geregelt (z.B. Stellenbewerberinnen-/Stellenbewerberdaten 6 Monate; Buchhaltungs- und Finanzdaten, 10 Jahre). Sofern ein Interesse an einer längeren Speicherung besteht, ist diese in begründeten Fällen zulässig. Jede der in § 3 Abs. (1) dieser Richtlinie genannten Personen sind in ihrem Aufgabenbereich für die Löschung verantwortlich.

(4) Personenbezogene Daten in der Mitgliederverwaltung werden nach dem Ende der Mitgliedschaft gesperrt bzw. archiviert. Einzelheiten sind im Löschkonzept geregelt.

(5) Begehren Betroffene die Löschung ihrer Daten (vgl. § 15 Abs. 1 dieser Richtlinie), ist dem unverzüglich zu entsprechen, es sei denn, dem stehen gesetzliche Aufbewahrungspflichten entgegen (z.B. bei Mitgliederdaten). Löschungen aus der Mitgliederverwaltung erfolgen durch die Landesverbände bzw. die Bundespartei. Dezentral bei den Gliederungen gespeicherte Daten (z.B. Newsletter- oder Einladungsverteiler, Kontaktlisten) werden von diesen gelöscht; die das Löschbegehren bearbeitende Stelle weist die betroffenen Gliederungen auf diese Pflicht hin.

§ 12 - Elektronische Kommunikation

(1) Insbesondere sensible personenbezogene Daten (§ 5 Abs. 3 dieser Richtlinie) 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 sollte nicht gleichfalls per E-Mail mitgeteilt werden (z.B. persönlich, telefonisch, SMS, Messenger).

Für die Übermittlung vertraulicher Informationen durch Beschäftigte an Funktionsträgerinnen und Funktionsträger ist vorrangig die Digitale Postbox im Funktionsträgerportal zu nutzen. Gliederungen und Fachausschüsse sind angehalten, die Angebote „Digitaler Verband“ und „Digitaler Fachausschuss“ zu nutzen und personenbezogene Daten hierüber zu teilen.

(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.

§ 13 - Datensicherheit

(1) Personenbezogene Daten sind vor unberechtigtem Zugriff, unberechtigter Verwendung, unberechtigter Weitergabe und Verlust zu schützen. Hierzu müssen geeignete technisch-organisatorische Maßnahmen ergriffen werden, die für ein angemessenes Schutzniveau sorgen und als geeignete Garantien im Sinne von Art. 9 Abs. 2 Buchst. d DSGVO die Voraussetzung für die Verarbeitung sensibler personenbezogener Daten sind. 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.

Weitere geeignete technisch-organisatorische Maßnahmen sind in der Anlage 2 zu dieser Richtlinie enthalten.

(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). Die Genehmigung ist schriftlich zu dokumentieren und muss die Vorgaben für die zu gewährleistende Datensicherheit enthalten.

(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.

§ 14 - Datenschutzverletzungen

(1) Im Fall einer Datenschutzverletzung ist unverzüglich die/der Datenschutzbeauftragte zu informieren. Eine Datenschutzverletzung ist gem. Art. 4 Nr. 12 DSGVO eine Verletzung der Sicherheit die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (z.B. Verlust eines USB Datensticks mit Mitgliederdaten, Vertauschen von Briefeinlagen, offene E-Mail-Rundsendung statt mit „BCC-Funktion“).

(2) Die Mitteilung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die Art der Verletzung, deren Zeitpunkt und Bekanntwerden, die Kategorien und die (ungefähre) Zahl der betroffenen Personen, die betroffenen Kategorien und die (ungefähre) Zahl der betroffenen personenbezogenen Datensätze.

(3) Die/der Datenschutzbeauftragte nimmt auf dieser Grundlage eine Risikobewertung vor. Sofern eine Meldung an die Aufsichtsbehörde erforderlich ist, nimmt diese ausschließlich die/der Datenschutzbeauftragte vor. Die Meldung muss unverzüglich und möglichst binnen 72 Stunden erfolgen, nachdem der Gliederung die Verletzung bekannt wurde (Art. 33 Abs. 1 DSGVO).

(4) Betroffene werden – soweit erforderlich – durch die zuständige Gliederung informiert (Art. 34 DSGVO), wobei die/der Datenschutzbeauftragte beratend hinzugezogen wird.

§ 15 - 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 deren Berichtigung. Unter bestimmten Bedingungen besteht zudem das Recht auf Löschung und auf Einschränkung der Verarbeitung dieser Daten sowie das Recht auf Datenübertragbarkeit. Zudem können sie erteilte Einwilligungen jederzeit widerrufen und der Datenverarbeitung – wenn diese zur Wahrung berechtigter Interessen erfolgt – widersprechen. Im Fall eines Widerspruchs verarbeitet die FDP personenbezogenen Daten nicht mehr, es sei denn, sie kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der be-

troffenen Person überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Richtet sich der Widerspruch gegen Direktwerbung (z.B. postalische Wahlwerbung) ist dem Folge zu leisten.

(2) Die Gliederungen müssen sicherstellen, dass bei ihnen eingehende Anträge auf Ausübung von Betroffenenrechten, insbesondere Auskunftsbegehren, unverzüglich bearbeitet werden. Bei den Gliederungen direkt eingehende und sich ausschließlich auf diese und/oder deren Untergliederungen beziehende Auskunftsbegehren werden von der Gliederung beantwortet. Auskunftsbegehren, die auf sämtliche, von der FDP als Gesamtpartei verarbeitete Daten gerichtet sind, werden von der Bundespartei beantwortet; gehen diese bei Gliederungen ein, sind sie an den Datenschutzbeauftragten weiterzuleiten. 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) Soweit eine Auskunft besondere Arten personenbezogener Daten (§ 5 Abs. 3 dieser Richtlinie) enthält, wird diese aus Sicherheitsgründen schriftlich erteilt. Vor einer Auskunft ist sicherzustellen, dass diese auch dem tatsächlich Betroffenen erteilt wird. Dazu kann der Betroffene auch um weitere Angaben gebeten werden (z.B. bei welcher Gelegenheit möglicherweise Daten von Ihm gespeichert bzw. verarbeitet worden sein könnten).

(4) Alle von einer Datenverarbeitung durch die FDP Betroffenen haben zudem das Recht, sich nach Art. 77 DSGVO bei einer Aufsichtsbehörde zu beschweren, wenn sie der Ansicht sind, dass die Verarbeitung ihrer personenbezogenen Daten nicht rechtmäßig erfolgt (Übersicht: https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html). Die Kontaktdaten der für die Bundespartei zuständigen Aufsichtsbehörde lauten:

> Berliner Beauftragte für Datenschutz und Informationsfreiheit, Alt-Moabit 59-61, 10555 Berlin, Tel. 030 13889-0, mailbox@datenschutz-berlin.de

§ 16 - 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) Einwilligungen (z.B. Double-Opt-In-Verfahren beim Newsletter-Abonnement)

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

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

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

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

f) Informationen über durchgeführte interne und externe Prüfungen

§ 17 - 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.

Anlage 1: Definitionen

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person – Betroffene/r) – beziehen (z.B. Name, E-Mail-Adresse, Bankverbindung). 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, Unternehmen, 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.

Anlage 2: Liste technisch-organisatorischer Maßnahmen gem. Art 32 DSGVO

Geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines dem Risiko angemessenes Schutzniveaus sind u.a.:

1. **Zutrittskontrolle** (Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren): z.B. Sicherheitsschlösser, elektrische Türöffner, Chipkartensysteme, Pforten-/Sicherheitspersonal, Alarmanlagen, Videoüberwachung der Eingänge

2. **Zugangskontrolle** (Maßnahmen, die Unbefugten die Nutzung von Datenverarbeitungsanlagen verwehren): z.B. Login mit Benutzername und Passwort, Passwortrichtlinie, automatische Desktopsperre, Anti-Viren-Software, Firewall, Zwei-Faktor-Authentifizierung, Verschlüsselung von Notebooks und Datenträgern, sichere Plattformen zum Informationsaustausch (z.B. „Meine Freiheit“, Digitale Postbox des Funktionsträgerportals)

3. **Zugriffskontrolle** (Maßnahmen, die unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei der Verarbeitung verhindern): z.B. Berechtigungskonzepte (Zugriffgewährung nur im erforderlichen Umfang), Rechteverwaltung durch Systemadministrator, regelmäßige Kontrolle der Berechtigungen, Protokollierung von Zugriffen, Aktenvernichtung

4. **Pseudonymisierung** (Maßnahme, bei der personenbezogenen Daten entfernt, durch ein Kennzeichen ersetzt und gesondert aufbewahrt werden): sofern möglich, Ersetzung von Namen und anderer Identifikationsmerkmale durch ein Kennzeichen (z.B. Mitgliedsnummer) zur Erschwerung der Identifizierung

5. **Weitergabekontrolle** (Maßnahmen, die unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei der Weitergabe/Übermittlung verhindern): z.B. E-Mail-Verschlüsselung (mind. Transportverschlüsselung), VPN-Verbindungen, verschlüsselte Verbindungen (z.B. https)

6. **Eingabekontrolle** (Maßnahmen zur nachträglichen Überprüfung, ob und von wem personenbezogene Daten in Datenverarbeitungsanlagen eingegeben, verändert oder entfernt wurden): Protokollierung der Eingabe, Änderung und Löschung von Daten, Dokumentenmanagement

7. **Auftragskontrolle** (Maßnahmen, damit personenbezogene Daten bei Auftragsverarbeitung nur entsprechend den Weisungen des Auftraggebers verarbeitet werden): z.B. Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln, Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten, vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen, regelmäßige Kontrollen

8. **Verfügbarkeitskontrolle** (Maßnahmen zum Schutz gegen zufällige Zerstörung oder Verlust und zur Wiederherstellung im Störfall): z.B. Backup- und Recovery-Konzepte, unterbrechungsfreie Stromversorgung, Kontrolle der Server (Feuer-/Rauchmelder, Temperatur-/Feuchtigkeitskontrolle), getrennte Aufbewahrung der Sicherungsmedien, Notfallpläne

9. **Datenschutzmanagement** (Maßnahmen zur Etablierung eines datenschutzsensiblen Verhaltens): z.B. Sensibilisierung der an Datenverarbeitungen Beteiligten, Schulungen, Schaffung von Strukturen zur Beratung/Lösung datenschutzrechtlicher Fragen, Umsetzung von Behördenentscheidungen und Gerichtsurteilen, datenschutzfreundliche Voreinstellungen bei Entwicklung neuer Systeme, ständige Kontrolle und Weiterentwicklung der technisch-organisatorischen Maßnahmen, Vorfallreaktionspläne

Impressum:
Freie Demokratische Partei (e.V.)
vertreten durch den Bundesgeschäftsführer Michael Zimmermann (V.i.S.d.P.)
Reinhardtstr. 14, 10117 Berlin
info@fdp.de, Tel. 030 284958-0
(Vereinsreg.-Nr.: 139996NzA5, AG Charlottenburg)