Leitfaden zur Verarbeitung personenbezogener Daten in den Gliederungen der Freien Demokratischen Partei

– zur Umsetzung der Datenschutz-Grundverordnung –

(Stand: 4. Mai 2018)

Ab **25. Mai 2018** findet die **Datenschutz-Grundverordnung (DSGVO)** Anwendung. Sie ist auch von politischen Parteien und ihren Gliederungen zu beachten. Das bisher für die Parteiarbeit relevante Bundesdatenschutzgesetz (BDSG) wurde umfassend überarbeitet und enthält künftig nur noch ausführende und ergänzende Bestimmungen zur DSGVO.

Auch wenn sich an den Grundsätzen des Datenschutzrechts wenig ändert, treten doch viele neue Vorschriften in Kraft – insbesondere **strengere Transparenz- und Dokumentationspflichten, ausgeweitete Betroffenenrechte und schärfere Sanktionen**. Dies zwingt zu einem noch verantwortungsvolleren und sensibleren Umgang mit personenbezogenen Daten.

Dieser Leitfaden und die zugehörigen Muster[1] sollen Ihnen die Umsetzung der DSGVO vor Ort erleichtern. Natürlich können wir nicht jedes Problem voraussehen. Sollten Fragen offengeblieben sein, können Sie sich jederzeit an den Liberalen Parteiservice wenden. Ihre **Ansprechpartner** sind:

Rechtsanwalt **Christian Graf Dohna** Tel.: 0228 547380 christian.dohna@lips-fdp.de	Rechtsanwalt **Dr. Thomas Hahn** Tel.: 030 28495890 thomas.hahn@lips-fdp.de

Inhaltsverzeichnis

[1] Die Muster zu diesem Leitfaden finden Sie zum Download auf https://meine-freiheit.de in der Rubrik „FDP intern“ unter dem Punkt „Datenschutz-Grundverordnung“. So können wir die Dokumente jederzeit für Sie aktuell halten.

1. Verarbeitung personenbezogener Daten innerhalb der FDP

Personenbezogene Daten sind nicht nur Angaben, die zur unmittelbaren Identifizierung einer natürlichen Person erforderlich sind, wie etwa **Name, Anschrift und Geburtsdatum**. Hierunter fallen auch alle Informationen, die sich auf eine in sonstiger Weise identifizierte oder identifizierbare natürliche Personen beziehen, z.B. **Familienstand, Zahl der Kinder, Beruf, Telefonnummer, E-Mail-Adresse, Anschrift, Eigentums- oder Besitzverhältnisse, persönliche Interessen, Mitgliedschaft in einer politischen Partei oder Datum des Parteibeitritts**. Dies gilt für Informationen jedweder Art, also für Schrift, Bild oder Tonaufnahmen.

Innerhalb der FDP und ihren Gliederungen werden personenbezogene Daten zahlreicher betroffener Personengruppen verarbeitet – von **Mitgliedern, Interessentinnen und Interessenten, Journalistinnen und Journalisten sowie politischen Kontaktpersonen** in Vereinen, Verbänden und anderen Organisationen. Hinzukommen **Mitarbeiterinnen und Mitarbeiter sowie Vertragspartnerinnen und -**

partner, z.B. beim Hosting der Verbands-Homepage oder der Anmietung von Veranstaltungsräumen. In allen Fällen ist künftig die DSGVO zu beachten!

Nicht von der DSGVO geschützt werden Angaben über **Verstorbene**. Ein Nachruf für ein verstorbenes Parteimitglied auf der Homepage oder die Nennung in der Reihe der Verstorbenen auf dem Parteitag ist damit datenschutzrechtlich zulässig.

2. Datenschutz als Managementaufgabe

Die Vorgaben der DSGVO lassen sich nicht mit einer Aktion für immer erfüllen. Mit ihrem Inkrafttreten wird der Datenschutz endgültig zu einer **ernst zu nehmenden Daueraufgabe der Parteiorganisation.** Als Vorstandsmitglieder sind Sie dazu verpflichtet, die Persönlichkeitsrechte Ihrer Mitglieder zu schützen. Dies gilt umso mehr, da die von Parteien verarbeiteten personenbezogenen Daten in der Regel die **politische Meinung der betroffenen Person erkennen lassen** und somit zu den besonders **schutzbedürftigen** Daten i.S. des Art. 9 DSGVO zählen.

2.1. Datenschutz-Compliance im Vorstand

Die Einhaltung der Bestimmungen des Datenschutzes sollte nicht erst mit der Einführung der DSGVO eine Selbstverständlichkeit für jedes Vorstandsmitglied sein. Die Arbeit im Vorstand bringt in jedem Falle den Umgang mit personenbezogenen Daten mit sich. Dabei gilt:

> Die Datenverarbeitung durch ein Vorstandsmitglied ist nur dann erlaubt, wenn sie **zur Aufgabenerfüllung erforderlich** ist. Das ist grundsätzlich bei Vorsitzenden und Schatzmeisterinnen bzw. Schatzmeistern der Fall; sie haben in jedem Fall Zugang zu allen personenbezogenen Daten der Mitglieder ihres Verbandes. Weitere Vorstandsmitglieder können zur Erfüllung ihrer Vorstandsaufgaben – z.B. zur Neumitgliederbetreuung oder zur Veranstaltungsorganisation – das Recht zur Datenverarbeitung eingeräumt bekommen. Dazu bedarf es eines besonderen **Vorstandsbeschlusses**. Sofern alle Vorstandsmitglieder gemeinsam die Geschäftsführungsaufgaben wahrnehmen – wie dies gerade bei kleinen Vorstandsgremien häufig der Fall ist –, kann dieser Beschluss auch die gemeinschaftliche Datennutzung zum Inhalt haben.

Um die Bedeutung des Datenschutzes zu unterstreichen und in das Bewusstsein aller Vorstandsmitglieder zu bringen, sollen künftig alle Vorstandsmitglieder eine entsprechende Erklärung zur **Verpflichtung auf den Datenschutz** (**Muster 1a**). unterschreiben, nicht nur, wie bisher, diejenigen, die dies mit dem Zugang zur Mitgliederverwaltung in Navision ohnehin tun mussten.

2.2. Datenschutz als Vorstandsaufgabe

Auch wenn der Vorstand die Gesamtverantwortung für den Datenschutz trägt, ist es ratsam, ein Vorstandsmitglied zu bestimmen, das **für datenschutzrechtliche Belange eine koordinierende Rolle** übernimmt. Der Datenschutz wird künftig eine zentrale Vorstandsaufgabe sein; dies muss sich auch in der internen Aufgabenverteilung abbilden. Das zuständige Vorstandsmitglied sollte auf Einhaltung der datenschutzrechtlichen Bestimmungen in der Verbandsarbeit achten. Zudem hält es den Kontakt zur bzw. zum Datenschutzbeauftragten der FDP (s. unten, Ziff. 2.4).

> Das den Datenschutz koordinierende Vorstandsmitglied ist keine Datenschutzbeauftragte bzw. **kein Datenschutzbeauftragter** in Sinne von Art. 37 DSGVO!

2.3. Verfahrensverzeichnisse

Die DSGVO verpflichtet die Verantwortlichen, **Rechenschaft über ihren Umgang mit personenbezogenen Daten** ablegen zu können. Das wesentliche Instrument, um diesen Nachweis zu erbringen, ist das sog. „Verzeichnis von Verarbeitungstätigkeiten" (Art. 30 DSGVO). Darin ist zu dokumentieren, in welchem Zusammenhang mit personenbezogenen Daten gearbeitet wird.

Bei einem sog. „Gesamtverein" wie der FDP, bei dem es eine mehrstufige Vereinsorganisation, z.B. mit Kreis-, Landes- und Bundesverband gibt, muss nicht in jeder Gliederung für jede Verarbeitung ein separates Verzeichnis angelegt werden; **für die Mitglieder- und Finanzverwaltung** in Navision übernimmt diese Aufgabe die **Bundespartei**.

Für Bereiche, in denen Sie darüber hinaus personenbezogene Daten nutzen, z.B. für Einladungs- oder Informationsschreiben an **Interessentinnen und Interessenten**, die nicht zentral in Navision gespeichert sind (s. unten, Ziff. 4), müssen Sie dagegen selbst ein Verzeichnis anlegen (**Muster 2**). Hierbei leisten unsere Ansprechpartner (s. oben, Einleitung) gern Unterstützung!

2.4. Die bzw. der Datenschutzbeauftragte der FDP

Sie müssen in Ihrem Verband keine Datenschutzbeauftragte bzw. keinen Datenschutzbeauftragten benennen! Der „Gesamtverein" FDP hat einen Datenschutzbeauftragten, der von einem Stellvertreter unterstützt wird:

Datenschutzbeauftragter der FDP:	**Stellvertreter:**
Jörg van Essen	**Christian Graf Dohna**
Tel. 030 28495886 datenschutz@fdp.de	Tel.: 0228 547380 christian.dohna@lips-fdp.de

Dem Datenschutzbeauftragten und seinem Stellvertreter obliegt die Pflicht, die Partei und ihre Gliederungen über deren datenschutzrechtliche Pflichten zu unterrichten und bei deren Erfüllung zu beraten. Zudem überwachen sie die Einhaltung der Datenschutzvorschriften.

Die Angabe der Kontaktdaten der bzw. des Datenschutzbeauftragten zählt künftig zu den zentralen Informationspflichten (Art. 13, 14 DSGVO). Sie müssen diese z.B. in die **Datenschutzerklärung Ihrer Homepage** (s. unten, Ziff. 5.1), oder in Ihre Einwilligungsformulare (s. unten, Muster 4) aufnehmen.

3. Der korrekte Umgang mit Mitgliederdaten[2]

Mitgliederdaten politischer Parteien sind **besonders sensibel** (s. oben, Ziff. 2). Dementsprechend verantwortungsvoll ist damit umzugehen.

[2] Zum korrekten Umgang mit personenbezogenen Daten in der **Schatzmeisterei** informiert die Navision-Schulung.

3.1. Aufnahmeverfahren

Bei der Aufnahme von neuen Mitgliedern sind neben den grundsätzlichen Bestimmungen der Bundessatzung (§§ 2, 3 BS), die für alle Gliederungsebenen gelten, auch Grundsätze des Datenschutzes zu beachten.

Auch die neue DSGVO kennt den bisherigen Grundsatz der Datensparsamkeit und Datenvermeidung (**Datenminimierun**g – Art. 25 DSGVO), so dass nur die personenbezogenen Daten erhoben und verarbeitet werden sollen, die für den bestimmten Zweck erforderlich sind. Die betroffenen Personen sind über die Erhebung zu unterrichten (**Informationspflich**t – Art. 13 DSGVO). Deshalb verwenden Sie für die Aufnahme von Neumitgliedern nur die offiziellen, datenschutzrechtlich **geprüften Aufnahmeformulare**, gleichgültig ob online oder analog. Die Bundespartei wird hierzu neue Formulare erstellen und zur Verfügung stellen.

Hinzuweisen ist im Zusammenhang mit dem Aufnahmeverfahren auch auf die Tatsache, dass die Daten der Mitgliedschaftsbewerberin bzw. des -bewerbers **zunächst nur während der Dauer des Aufnahmeverfahrens gespeichert** werden dürfen. Sollte der Aufnahmeantrag abgelehnt werden, sind sie zu löschen.

Es ist strikt darauf zu achten, dass nur die Mitglieder der **zur Entscheidung über die Mitgliedschaft berufenen Vorstände** die personenbezogenen Daten der Bewerberinnen und Bewerber zur Kenntnis bekommen.

3.2. Die Mitgliederverwaltung in Navision

Die Mitgliederverwaltung sollte grundsätzlich **ausschließlich über das Funktionsträger-Portal** in Navision vorgenommen werden. Um eine datenschutzrechtlich nicht zulässige Weitergabe der Daten zu verhindern, sollten **Ausdrucke künftig unterbleiben** – auch im Hinblick auf die durch die DSGVO erhöhten Sanktionen bei Datenschutzverletzungen (Art. 83 DSGVO), die bis zu 20 Millionen Euro betragen können.

Dies gilt insbesondere für die sog. **„Stammblätter“**, die alle über das Mitglied in Navision gespeicherten Daten – nicht nur Adress-, sondern auch Finanzdaten – enthalten. Eine Weitergabe von Stammblättern – auch innerhalb eines Vorstandes – kann bereits den Tatbestand eines Datenschutzverstoßes bedeuten (s. oben, Ziff. 2.1).

Sofern – im Ausnahmefall! – personenbezogene Daten von Mitgliedern doch ausgedruckt und in Papierform vorgehalten werden, sind diese **sicher zu verwahren**. Sie müssen sich in einem verschlossenen Schrank befinden; die Schlüssel hierfür dürfen nur berechtigte Vorstandsmitglieder haben.

3.3. E-Mail-Verteiler

E-Mail-Adressen sind als **personenbezogene Daten** anzusehen, da sie Rückschlüsse auf den Inhaber zulassen. Die Bekanntgabe einer E-Mail-Adresse auf einer Empfängerliste stellt daher grundsätzlich eine Datenübermittlung dar, für die eine Einwilligung vorliegen muss. Dies gilt nicht (!) nur für die Fälle, in denen der Klarname des Inhabers der E-Mail-Adresse verwendet wird. Deshalb ist bei einer Versandaktion mit mehreren Empfängerinnen und Empfängern darauf zu achten, dass immer die „**BCC-Funktion**“ verwendet wird, um unzulässige Übermittlungen von E-Mail-Adressen zu verhindern.

Der häufigste Grund für Beschwerden über unzulässige Datenverarbeitung ist die Nutzung alter E-Mail-Verteiler, die noch E-Mail-Adressen **ausgetretener Mitglieder** enthalten. Sie sollten sich deshalb vor jeder Aussendung den betreffenden **Verteiler neu aus Navision** ziehen. Wenn Sie dabei in der „Schnellauswahl" das Häkchen bei „Mitglieder" setzen, ist sichergestellt, dass Sie nur den aktuellen Mitgliederbestand Ihrer Gliederung selektieren.

3.4. Geburtstagslisten

Geburtstagslisten – also Auszüge aus der Mitgliederverwaltung mit Namen und Geburtsdatum – sind selbstverständlich **personenbezogene Daten**. Hierauf haben grundsätzlich nur die bzw. der Vorsitzende sowie die Schatzmeisterin und der Schatzmeister einer Gliederung Zugriff – weitere Vorstandsmitglieder nur zur Erfüllung ihrer Aufgaben auf Grundlage eines Vorstandsbeschlusses (s. oben, Ziff. 2.1).

Die Weitergabe von Geburtstagslisten an Empfängerinnen und Empfänger außerhalb des Kreises der berechtigten Vorstandsmitglieder ist **ohne Einwilligung** der Betroffenen **nicht erlaubt** – dies gilt auch für die Übermittlung an Mandatsträgerinnen und Mandatsträger, die diese Daten zu Gratulationszwecken nutzen wollen.

3.5. Vorstandsprotokolle

Im Gegensatz zu Protokollen öffentlicher Mitgliederversammlungen enthalten Protokolle von **Vorstandssitzungen** nicht nur die Dokumentation von Beschlüssen, sondern auch häufig personenbezogene Daten und unterliegen insofern den Reglungen des Datenschutzes. Die Annahme oder Ablehnung eines Aufnahmeantrages oder der Bericht des Schatzmeisters über Beitragsangelegenheiten sind nur einige Beispiele hierfür. Aus diesem Grund gibt es auch **keine generelle Einsichtsmöglichkeit** in Vorstandsprotokolle für Mitglieder.

3.6. Datenaustausch mit Dritten

Die Übermittlung personenbezogener Daten an Dritte ist nur zulässig, wenn hierfür eine **Einwilligun**g vorliegt. Da die Vorfeldorganisationen der Partei alle „Dritte" im Sinne des Datenschutzes sind, ist deshalb eine Weitergabe von Mitgliederdaten nur dann zulässig, wenn hierfür eine Einwilligung des einzelnen Mitgliedes vorliegt. Dies gilt auch für die Weitergabe an Fraktionen, Abgeordnete und liberale Stiftungen.

Aus diesem Grund enthalten die Aufnahmeanträge besondere Einwilligungsmöglichkeiten, die von den Interessentinnen und Interessenten anzukreuzen sind. Eine Ablehnung der Datenweitergabe muss möglich sein, ohne dass das Mitgliedschaftsverhältnis hiervon betroffen ist. Nur wenn eine solche Einwilligung vorliegt, ist die Weitergabe zulässig.

3.7. Öffentliche Erklärungen zur Mitgliedschaft

Da die Mitgliedschaft in einer politischen Partei datenschutzrechtlich zu den sog. sensiblen Daten zählt (s. oben, Ziff. 2), die einem besonderen Schutz unterliegen, **muss niemand seine Mitgliedschaft öffentlich machen** – auch nicht innerhalb der Partei! Das ergibt sich aus dem durch die Rechtsprechung des Bundesverfassungsgerichts garantierten „Recht auf informationelle Selbstbestimmung".

Mit dem Aufnahmeantrag hat das Mitglied zwar seine Einwilligung zur **parteiinternen** Nutzung seiner Daten zur Mitgliederverwaltung (Beitragszahlung, Einladungen zu Mitgliederversammlungen oder Kandidatenaufstellungen) gegeben, nicht aber zur Preisgabe seiner Daten an Dritte oder auch andere Mitglieder der Partei.

Aus diesem Grund ist eine Veröffentlichung der Mitgliedschaft, z.B. auf der Homepage der Gliederung („Neumitglied des Monats“ u.ä.) oder Auskünfte über die Mitgliedschaft an die Presse nur mit der **ausdrücklichen Einwilligung** des Mitgliedes zulässig (s. unten, Ziff. 5.4.1).

3.8. Auftragsverarbeitung

Sie müssen personenbezogene Daten nicht selbst verarbeiten, sondern können damit auch einen **Dienstleister betrauen**, z.B. einen Webhoster mit der Veröffentlichung Ihrer Homepage oder einen Lettershop mit der Versendung von Einladungen. Die dazu erforderliche Datenweitergabe ist **datenschutzrechtlich privilegiert**, so dass der Auftragnehmer nicht als „Dritter“ im Sinne des Datenschutzes (Art. 4 Nr. 10 DSGVO) anzusehen ist.

Voraussetzung ist allerdings, dass für diese sog. Auftragsverarbeitung eine entsprechende **vertragliche Vereinbarung** getroffen wird, die Regelungen über die Sicherheit der übermittelten Daten, das Weisungs- und Kontrollrecht des Auftragsgebers und die Behandlung der Daten nach Abschluss des Auftrages festlegt.

Weitere Beispiele für Auftragsverarbeitungen sind Cloud-Lösungen, CRM-Systeme, Newsletter-Dienste, Aktenvernichtung oder externe Lohn- und Gehaltsabrechnung. Sofern Sie solche Dienstleistungen nutzen und noch keine **Vereinbarung** über eine Auftragsverarbeitung abgeschlossen haben, sollten Sie dies umgehend **nachholen**. Viele Dienstleister haben eigene Vertragsformulare; falls nicht, können sie auf **Muster 3** zurückgreifen.

4. Personenbezogene Daten von Interessentinnen und Interessenten

Ob Sie zu Veranstaltungen einladen, Informationen über Ihre politischen Ziele versenden oder um Spenden bitten – überall verarbeiten Sie **personenbezogene Daten interessierter Bürgerinnen und Bürger**.

Da die politische Arbeit vor Ort ohne solche Kontakte kaum denkbar ist, dürften in nahezu jedem Verband ein oder auch mehrere **Verteiler** existieren, die Namen, Postanschriften, E-Mail-Adressen oder Telefonnummern von Interessentinnen und Interessenten enthalten. Das Inkrafttreten des DSGVO macht es erforderlich, diese Verteiler zu **überprüfen**; denn künftig müssen Sie den **Nachweis** führen können, dass Sie personenbezogene Daten rechtmäßig – z.B. aufgrund einer Einwilligung – verarbeiten.

4.1. Überprüfung „alter“ Kontaktdaten

Bei der Überprüfung bestehender Verteiler ist folgende Differenzierung vorzunehmen:

4.1.1. Selbst veröffentlichte Kontaktdaten

Hat die betroffene Person ihre Kontaktdaten **selbst öffentlich gemacht** (z.B. auf der Homepage eines Unternehmens, einer Arztpraxis oder einer Rechtsanwaltskanzlei), dürfen Sie die **Postanschrift** weiterhin verwenden. Für die Nutzung von **E-Mail-Adressen** war bereits in der Vergangenheit eine ausdrückliche Einwilligung erforderlich – es sei denn, die betroffene Person nimmt ihrer Funktion nach auch die Kontaktpflege zu politischen Parteien wahr (z.B. Geschäftsführer/in der IHK oder Handelskammer); dann dürfen Sie auch die herfür bereitgestellte E-Mail-Adresse nutzen.

4.1.2. Kontaktdaten von Privatpersonen

Bei **Privatpersonen**, die ihre personenbezogenen Daten nicht selbst veröffentlicht oder einer Veröffentlichung durch Dritte (z.B. in Online-Telefonbüchern) zugestimmt haben, ist für die Datenverarbeitung regelmäßig eine **Einwilligung** erforderlich. Auf Einwilligungen, die nach dem BDSG a. F. wirksam erteilt wurden, können Sie sich weiterhin stützen. Sofern Sie jedoch **keine Einwilligung nachweisen** können, sollten Sie eine **neue Einwilligung einholen** – z.B. indem Sie einem Informationsschreiben ein entsprechendes Formular beifügen (**Muster 4**). Die Einwilligung muss aber nicht notwendigerweise schriftlich erfolgen; es reicht auch die elektronische (E-Mail) oder mündliche Erteilung aus (in letzterem Fall ist besonderer Wert auf die Dokumentation zu legen, s. unten, Ziff. 4.3). Private Empfängerinnen und Empfänger, die keine (neue) Einwilligung abgeben, müssen Sie leider aus Ihren Verteilern **streichen**.

4.1.3. Aus dem Adresshandel erworbene Daten

Sofern Sie Postadressen **rechtmäßig zur zeitweiligen Nutzung erworben** haben, dürfen Sie diese Ihrem Nutzungsvertrag entsprechend weiterverwenden. Im Zweifel ist eine Nachfrage beim Adresshändler ratsam. Unter Geltung der DSGVO ist es umso wichtiger, die Empfängerinnen und Empfänger eines Werbeanschreibens darüber zu unterrichten, aus welcher Quelle Sie deren Daten haben und dass ihnen ein **Widerspruchsrecht** zusteht. Widerspricht eine Empfängerin bzw. ein Empfänger der Nutzung seiner Daten, müssen Sie dies umgehend beachten.

4.2. Neuerhebung von Kontaktdaten

Für die Erhebung und Verarbeitung **neuer Kontaktdaten** gelten die für die Prüfung der Altbestände dargestellten Grundsätze:

4.2.1. Selbst veröffentlichte Kontaktdaten

Von der betroffenen Person selbst öffentlich gemachte personenbezogene Daten dürfen Sie verarbeiten (s. oben, Ziff. 4.1.1). Bei Neuerhebungen müssen Sie jedoch **hierüber informieren**! Dieser Pflicht müssen Sie spätestens zum Zeitpunkt der ersten Mitteilung an die die betroffene Person nachkommen (**Muster 5**).

4.2.2. Kontaktdaten von Privatpersonen

Andernfalls benötigen Sie eine **Einwilligung** (s. oben, 4.1.2). Ein Vorrat an Einwilligungserklärungen (**Muster 4**) sollte deshalb künftig zur festen Ausstattung bei allen Veranstaltungen, Infoständen und sonstigen Aktivitäten zählen – so wie bisher schon der Aufnahmeantrag.

4.3. Dokumentation

Um für Auskunftsbegehren betroffener Personen und mögliche Prüfungen durch die Aufsichtsbehörde gewappnet zu sein, sollten Sie **dokumentieren**, auf welcher rechtlichen Grundlage Sie personenbezogene Daten zu Kontaktaufnahme verarbeiten. Insbesondere das **Vorliegen einer wirksamen Einwilligung** müssen Sie nachweisen können! Es ist also eine Dokumentation erforderlich, die Ihnen die eindeutige Zuordnung von Einwilligungstext zu betroffener Person erlaubt. Schon deshalb ist die Verwendung schriftlicher bzw. elektronisch erteilter Einwilligungen zu empfehlen – die **sorgfältig aufzubewahren** sind. Eine **mündliche** Einwilligung muss unter Angabe von Ort und Zeit der Erteilung schriftlich vermerkt werden –

am besten unter Angabe eines weiteren Vorstandsmitglieds, das die Abgabe der Einwilligung bezeugen kann. Dabei ist zu beachten, dass bei einer mündlich erteilten Einwilligung auch ein mündlich erklärter Widerruf akzeptiert werden muss.

5. Die datenschutzkonforme Homepage

Selbst wenn Sie für die Erstellung Ihrer Verfahrensverzeichnisse (s. oben, Ziff. …) oder die Prüfung Ihrer Verteiler (s. oben, Ziff. 4.1) noch etwas Zeit brauchen sollten, die Homepage Ihres Verbandes sollte zum 25. Mai 2018 den neuen gesetzlichen Anforderungen entsprechen; denn hier wird auf den ersten Blick erkennbar, falls Sie die Vorgaben der DSGVO nicht umsetzen.

5.1. Datenschutzerklärung

Insbesondere die Datenschutzerklärung Ihrer Homepage bedarf einer **gründlichen Aktualisierung**. Durch die DSGVO sind künftig noch weitergehende Informationen bereitzustellen als bisher. Z.B. müssen auf jeder (!) Homepage einer Gliederung der FDP die Kontaktdaten unseres **Datenschutzbeauftragten** sowie die für die Verarbeitung personenbezogener Daten herangezogenen **Rechtsgrundlagen** zu finden sein.

Sofern Sie einen neuen **Homepage-Baukasten von Universum** nutzen, können Sie sicher sein, dass dieser datenschutzrechtlich auf dem aktuellen Stand ist. Für alle **anderen** Homepages stellen wir Ihnen eine **Muster-Datenschutzerklärung** zur Verfügung (**Muster 6**), die Sie selbstverständlich noch auf Ihre individuelle Situation anpassen müssen. Dazu wenden Sie sich am besten an Ihren Webmaster.

5.2. Impressum

Jede Homepage einer Parteigliederung benötigt ein korrektes Impressum! Auch wenn es sich hierbei nicht um ein datenschutzrechtliches Thema im engeren Sinn handelt, sollten Sie die Gelegenheit nutzen, um auch das Impressum Ihrer Verbands-Homepage zu **überprüfen**. Durch die DSGVO selbst ergibt sich hier jedoch kein Änderungsbedarf.

Glücklicherweise muss das Impressum bei einer Parteigliederung nicht viele Angaben umfassen. Häufig wird jedoch vergessen, einen **Verantwortlichen für journalistisch-redaktionelle Inhalte** zu benennen. Dies schreibt § 55 Abs. 2 des Rundfunkstaatsvertrages (RStV) zwingend vor, sobald Ihre Homepage über eine Rubrik „News“ oder „Aktuelles“ verfügt oder Sie Ihre Pressemitteilungen einstellen.

Folgende Angaben muss das Impressum Ihrer Homepage beinhalten (**Muster 7**):

- Name des Verbandes und ladungsfähige Anschrift (Postfach genügt nicht!)
- Name und Vorname der bzw. des Vorsitzenden
- Telefonnummer und E-Mail-Adresse
- Verantwortliche/r im Sinne vom § 55 RStV (Name und Anschrift)

Das Impressum muss **leicht erkennbar, unmittelbar erreichbar** und ständig verfügbar sein. Es bietet sich eine Platzierung auf der Eingangsseite der Homepage an, idealerweise in einer für die Nutzerinnen und Nutzer ständig erreichbaren Navigationsleiste.

Die Impressumspflicht besteht auch für die **Social-Media-Seiten** Ihres Verbandes bei Facebook, Twitter oder Google+.

5.3. Kontaktformular

Falls Sie auf Ihrer Homepage zur schnellen Kontaktaufnahme ein Kontaktformular bereitstellen, müssen Sie dabei folgende Punkte beachten:

- Es gilt das Gebot der Datensparsamkeit: Im Kontaktformular dürfen also nur die zum Beantworten der Anfrage erforderlichen Angaben **Pflichtfelder** sein. Dies sind die E-Mail-Adresse und der Name. Wohnanschrift und Telefonnummern dürfen dagegen nicht zwingend abgefragt werden.

- Die DSGVO bezeichnet die **Verschlüsselung** personenbezogener Daten ausdrücklich als geeignete Maßnahme, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Spätestens ab jetzt sollte also die Übertragung der im Formular eingegebenen Daten verschlüsselt sein, damit diese nicht abgegriffen werden können.

- Die über das Kontaktformular erhobenen personenbezogenen Daten dürfen **nur für die Beantwortung der Anfrage** genutzt werden. Eine Speicherung oder eine Nutzung für andere Zwecken ist nicht erlaubt. Hierfür würden Sie eine Einwilligung benötigen.

- Nutzerinnen und Nutzer müssen vor dem Ausfüllen des Kontaktformulars über Art, Umfang und Zweck von Erhebung und Verwendung ihrer personenbezogenen Daten **unterrichtet** werden. Der Vereis auf die allgemeine Datenschutzerklärung der Homepage (s. oben, Ziff. 5.1.) ist wichtig, reicht aber nicht; Sie müssen die relevanten Informationen auch **in unmittelbarem Zusammenhang mit dem Kontaktformular** angeben. Auf www.fdp.de/kontakt finden Sie z.B. folgenden Hinweis:

  „Sofern Sie über unser Kontaktformular Kontakt mit uns aufnehmen möchten, um sich über uns und/oder Veranstaltungen zu informieren und/oder allgemeine Fragen zu stellen, müssen Sie hierzu Ihren Vornamen, Ihren Namen und Ihre E-Mail-Adresse angeben. Zusätzlich können Sie auch Ihre Anschrift angeben, soweit Sie eine postalische Antwort bekommen möchten. Wir erheben, verarbeiten und nutzen Ihre Daten nur, um Ihre jeweilige Anfrage beantworten zu können; eine anderweitige Datenverwendung findet nicht statt.“ [zzgl. Link auf die allgemeine Datenschutzerklärung]

5.4. Personenfotos

Fotos, die Personen abbilden, enthalten personenbezogene Daten. Wie sich die DSGVO auf die rechtlichen Vorgaben für die Veröffentlichung und Verbreitung von Personenfotos auswirkt, ist **bislang ungeklärt**.

Bis Rechtsprechung und Behörden für Klarheit gesorgt haben, ist folgendes Vorgehen ratsam: 1) Holen Sie möglichst die **Einwilligung** der Abgebildeten ein und dokumentieren Sie diese. 2) Halten Sie ansonsten die rechtlichen **Maßstäbe** ein, **die bereits galten.** Dann ist davon auszugehen, dass damit auch die Vorgaben der DSGVO erfüllt werden.

5.4.1. Einwilligung der Abgebildeten

Grundsätzlich sollten Sie Personenfotos **nur mit Einwilligung** des bzw. der Abgebildeten auf Ihrer Homepage verwenden oder an Ihre örtliche Zeitung zur Berichterstattung weitergeben – es sei denn, es liegt eine der Ausnahmen des sog. Kunsturhebergesetzes – kurz KUG – vor (s. unten, Ziff. 5.4.2). „Einwilligung“ heißt dabei: Die Zustimmung muss **vorher eingeholt** werden! Natürlich können die Betroffenen auch

noch nachträglich die Verwendung ihres Bildes genehmigen, zunächst einmal ist jedoch eine Rechtsverletzung erfolgt.

Es mag Fälle geben, in denen eine **schriftliche** Einwilligung möglich und sinnvoll ist (**Muster 8**), z.B. wenn Fotos von Mitgliedern in einem Werbe-Flyer abgedruckt oder im Rahmen einer Aktion „Neumitglied des Monats“ auf der Homepage abgebildet werden sollen. Wesentlich praktikabler dürfte im Regelfall aber eine **elektronische** oder **mündliche** Einwilligung sein. Schicken Sie z.B. das Foto der Verbandsweihnachtsfeier, bevor Sie es auf die Homepage stellen, einfach per E-Mail an die Abgebildeten und bitten hierfür um Einverständnis. Natürlich geht das auch mündlich; eine gewissenhafte Dokumentation ist dann aber umso wichtiger (s. oben, Ziff. 4.3).

Die abgebildete Person kann eine einseitige Einwilligung **jederzeit widerrufen**. Gestaltet man die Einwilligung dagegen als **vertragliche Vereinbarung** aus, die auch die bzw. der Vorsitzende unterschreibt, ist für einen Widerruf ein **wichtiger Grund** erforderlich. Ein solcher läge z.B. vor, wenn das abgebildete Mitglied die Partei verlässt. Dieses Vorgehen ist zu empfehlen, wenn Personenfotos für Printprodukte verwendet werden sollen, die im Fall eines Widerrufs unbrauchbar würden.

Bei **Minderjährigen** ist eine Einwilligung der Eltern erforderlich. Wenn beide Elternteile die elterliche Sorge ausüben, müssen auch **beide Elternteile** einwilligen. Falls die minderjährige Person über die Fähigkeit verfügt, die Tragweite ihrer Entscheidung zu erkennen, bedarf zusätzlich ihrer Einwilligung. Von einer entsprechenden Einsichtsfähigkeit ist im Regelfall ab einem Alter von **14 Jahren** auszugehen.

5.4.2. Erlaubte Fotonutzung

Das KUG enthält seit über 100 Jahren Regelungen zum Umgang mit Bildern von Personen. Darunter sind wichtige Ausnahmen, in denen **auf eine Einwilligung** der Abgebildeten **verzichtet** werden kann:

- **Bildnisse aus dem Bereich der Zeitgeschichte**

  Das Foto einer Person im Zusammenhang mit der Berichterstattung über ein **„zeitgeschichtliches Ereignis“** darf veröffentlicht werden. Der Begriff der Zeitgeschichte ist weit zu verstehen und es kommt dabei immer auch darauf an, an wen sich die Berichterstattung wendet. Ein öffentliches Interesse an der Veröffentlichung muss aber stets vorhanden sein. Nach diesen Maßstäben ist z.B. der **Kreisparteitag für die Leser der Lokalzeitung** vor Ort ein zeitgeschichtliches Ereignis; Fotos, die Teilnehmer der Veranstaltung zeigen, dürfen in der Zeitung abgedruckt werden.

  Zusätzlich können Sie in der Einladung und auf Aushängen auf die Fotoaufnahmen und -verwendung **hinweisen**. Im Falle einer Auseinandersetzung haben Sie dann noch ein weiteres Argument, das Sie für die Zulässigkeit der Veröffentlichung ins Feld führen können. Der Hinweis könnte z.B. lauten:

  „Achtung Fotoaufnahmen! Auf der Veranstaltung macht ein Fotograf – erkennbar am Namensschild – Bilder. Diese werden in Sozialen Netzwerken, den Homepages und in den Mitgliedermagazinen der FDP veröffentlicht.“

- **Bilder einer Landschaft oder sonstigen Örtlichkeit mit Personen als Beiwerk**

  Ist nicht eine (zufällig abgebildete) Person das **Hauptmotiv** eines Fotos sondern die **Umgebung**, dürfen Sie es einwilligungsfrei verwenden. Als Kontrollüberlegung ist dabei stets die Frage zu stellen, ob sich Gegenstand und Charakter des Bildes ändern würden, wenn die Person nicht auf dem Foto wäre. Danach dürfen Sie z.B. das **Foto eines Infostandes** veröffentlichen – auch wenn im Hintergrund Passanten zu sehen sind.

- **Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen**

  Teilnehmer **öffentlicher Veranstaltungen** müssen grundsätzlich damit rechnen fotografiert zu werden. Diese Ausnahme gilt für Demonstrationen (z.B. Christopher-Street-Day) sowie für feste Veranstaltungen – egal ob unter freiem Himmel oder in geschlossenen Räumen (z.B. Wahlkundgebungen). Die Veranstaltung muss aber tatsächlich öffentlich sein und darf sich nicht nur an einen begrenzten Einladungskreis richten. Fotos müssen grundsätzlich größere Personengruppen abbilden **(„repräsentative Ausschnitte“** der Veranstaltung); einzelne Teilnehmerinnen und Teilnehmer dürfen nur dann gezielt optisch herausgehoben werden, wenn sie sich selbst exponieren (z.B. durch Schilder, Kostüme etc.).

Auch Fotos, die unter die geschilderten Ausnahmen fällen, dürfen nicht das Persönlichkeitsrecht der Abgebildeten verletzen. Dies wäre z.B. bei der Veröffentlichung **besonders unvorteilhafter Fotos** der Fall. Fotos, auf denen **Minderjährige** im Mittelpunkt stehen, sollten grundsätzlich nicht ohne Einwilligung der Sorgeberechtigten verwendet werden (s. oben, Ziff. 5.4.1).

5.5. Namen und Kontaktdaten

Die Veröffentlichung personenbezogener Daten von Mitgliedern im Internet ist **grundsätzlich unzulässig**, sofern sich die betroffene Person nicht ausdrücklich damit einverstanden erklärt hat. Dies gilt auch für die **Delegierten** zu Parteitagen! Eine Ausnahme sind die **Funktionsträger** der Partei (Vorstandsmitglieder, Mandatsträgerinnen und Mandatsträger); deren „partei-dienstliche“ Erreichbarkeit (z.B. persönliche FDP-E-Mail-Adresse – max.mustermann@fdp-musterstadt.de, Kontaktangaben der Geschäftsstelle) können Sie ohne Einwilligung auf Ihrer Homepage angeben. Für Fotos und private Kantaktdaten benötigen Sie aber auch hier die Einwilligung der Funktionsträger.

6. Geschäftsstelle

Sofern Ihr Verband über eine Geschäftsstelle verfügt, in der Mitarbeiterinnen und Mitarbeiter tätig sind, müssen Sie ferner folgende Punkte beachten:

6.1. Verpflichtung auf den Datenschutz

Die bisherige „Verpflichtung auf das Datengeheimnis“ (§ 5 BDSG a.F.) ist in der DSGVO nicht mehr enthalten. Aufgrund der strengeren Dokumentations- und Nachweispflichten ist es gleichwohl ratsam, auch künftig Mitarbeiterinnen und Mitarbeiter **vor** Aufnahme der datenverarbeitenden Tätigkeit bzw. des Arbeitsverhältnisses auf den Datenschutz zu verpflichten. Aus Beweisgründen bietet sich an, hierfür die **Schriftform nebst eigenhändiger Unterschrift**

zu wählen (**Muster 1b**). Soweit eine Verpflichtung bereits erfolgt ist, bleibt diese auch nach dem 25. Mai 2018 gültig; einer Neuverpflichtung bedarf es nicht.

6.2. Schulung der Mitarbeiterinnen und Mitarbeiter

Die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für den Datenschutz bekommt durch die DSGVO noch mehr Bedeutung. Verpflichten Sie Ihre Mitarbeiterinnen und Mitarbeiter zur Teilnahme an Schulungsmaßnahmen und dokumentieren sie diese.

Bundespartei und Liberaler Parteiservice werden deshalb in den nächsten Monaten verstärkt **Datenschutzschulunge**n anbieten. Über die Veranstaltungen **in Ihrer Nähe** werden Sie durch Ihren Landesverband informiert.

6.3. Technisch-organisatorischer Datenschutz

Die DSGVO legt ein besonderes Augenmerk auf die IT-Sicherheit. So verpflichtet Art. 32 DSGVO den Verantwortlichen, **„geeignete technische und organisatorische Maßnahmen"** zu ergreifen, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten". Schwerpunkt hierbei ist, die „Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit" der zur Datenverarbeitung verwendeten Systeme und Dienste sicherzustellen. Dies erfordert z.B. die regelmäßige Aktualisierung der verwendeten Software, ein Zugriffskonzept für unterschiedlich berechtigte Mitarbeiterinnen und Mitarbeiter aber auch vergleichsweise einfach umzusetzende Maßnahmen, wie die Anbringung von Blickschutzfolien auf Laptops.

7. Rechte der Betroffenen

Die DSGVO gewährt Personen, deren Daten verarbeitet werden, umfassende Rechte:

- Recht auf Auskunft (Art. 15 DSGVO)
- Recht auf Berichtigung (Art. 16 DSGVO)
- Recht auf Löschung (Art. 17 DSGVO)
- Recht auf Einschränkung der Verarbeitung (Art. 18 DSGVO)
- Recht auf Datenübertragbarkeit (Art. 20 DSGVO)
- Widerspruchsrecht (Art. 21 DSGVO)

7.1. Recht auf Auskunft

Jede Person hat das Recht, Auskunft darüber zu verlangen, welche sie betreffenden personenbezogenen Daten die Freien Demokraten über sie verarbeiten.

Bitte beachten Sie: Die Auskunft darf sich **nicht allein auf die in Navision gespeicherten Daten** stützen; sondern hat – sofern vorhanden – weitere Datenbanken einzubeziehen! Wenden sich Auskunftssuchende direkt an Ihren Verband, müssen Sie also auf Grundlage **aller vorhandenen Datenbestände** antworten (wir unterstützen dabei gern!). Bei Anfragen aus dem Gebiet Ihres Verbandes, die in der Bundesgeschäftsstelle eingehen, werden wir uns **umgehend an Sie wenden**, damit Sie Ihre Datenbanken überprüfen und uns das Ergebnis mitteilen; die Bundesgeschäftsstelle kann nur die Navision-Daten einsehen und würde deshalb im Zweifel nur eine unvollständige Antwort geben. Aufgrund der kurzen gesetzlichen Fristen müssen Sie sicherstellen, dass unsere **Anfrage innerhalb von zwei Wochen** beantwortet wird!

Der Antrag des bzw. der Betroffenen kann **formfrei** gestellt werden (bei einem elektronischen Auskunftsverlangen muss auch die Antwort in einem „gängigen elektronischen Format" – z.B. PDF-Format – zur Verfügung gestellt werden). Der Antrag bedarf **keiner Begründung** und muss auch nicht auf bestimmte Informationen präzisiert sein; es kann **auch pauschal** Auskunft über alle gespeicherten Daten verlangt werden.

Vor Erteilung der Auskunft müssen Sie sich **über die Identität der bzw. des Antragstellenden vergewissern**. Sie bzw. er und die betroffene Person, deren Daten gespeichert sind, müssen identisch sein. Stimmen bei einer schriftlichen Anfrage die dort angegebenen Adressdaten der betroffenen Person mit den bei der verantwortlichen Stelle gespeicherten Angaben überein, darf wie früher schon von der Berechtigung des Auskunftsersuchens ausgegangen werden. Ist eine Identifizierung nicht möglich, sind weitere Informationen anzufordern (z.B. das Geburtsdatum).

Es besteht ein **Anspruch** auf folgende Informationen:

- konkret verarbeitete personenbezogene Daten (z.B. Name, Vorname, Anschrift, Geburtsdatum, Beruf)

- Kategorien der verarbeiteten personenbezogenen Daten, also die Gruppenbezeichnungen (z.B. „Adressdaten" oder „Bonitätsdaten")

- Verarbeitungszwecke

- Empfänger bzw. Kategorien von Empfängern, die die Daten bereits erhalten haben oder künftig noch erhalten werden (bei der Beantwortung besteht ein Wahlrecht zwischen Nennung der konkreten Empfänger oder nur der Gruppenbezeichnungen)

- geplante Speicherdauer – falls möglich, andernfalls die Kriterien für die Festlegung der Speicherdauer

- Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden

Zudem müssen Sie über bestehende **Rechte** auf Berichtigung, Löschung oder Einschränkung der Verarbeitung informieren, ebenso über ein mögliches Widerspruchsrecht und das Beschwerderecht bei der Aufsichtsbehörde (**Muster 9 und 10**).

Zudem besteht Anspruch auf eine **unentgeltliche Kopie** der personenbezogenen Daten.

Sofern Sie keine personenbezogenen Daten der bzw. des Antragstellenden verarbeiten, müssen Sie dies ebenfalls mitteilen (**Anspruch auf Negativauskunft**).

Auskünfte müssen **unverzüglich** erteilt werden, spätestens **innerhalb eines Monats.**

7.2. Recht auf Löschung und auf Einschränkung der Verarbeitung

Betroffene haben das Recht, die Löschung ihrer Daten zu verlangen, wenn einer der gesetzlichen Löschungsgründe vorliegt – u.a., wenn

- die Verarbeitung der Daten für den Zweck, zu dem sie ursprünglich erhoben wurden, nicht mehr erforderlich ist

- die Daten unrechtmäßig verarbeitet wurden

- die Einwilligung, auf die sich die Einwilligung gestützt hat, widerrufen wurde

Falls **gesetzliche Aufbewahrungsfristen** bestehen, tritt an die Stelle der Löschung die Einschränkung der Verarbeitung. Bei der **Einschränkung der Verarbeitung** werden die Daten gesperrt und dürfen somit nicht mehr weiterverarbeitet werden.

Für politische Parteien normiert § 24 Abs. 2 Satz 2, 3 Parteiengesetz eine wichtige Aufbewahrungsfrist. Danach sind „Rechnungsunterlagen, Bücher, Bilanzen und Rechenschaftsberichte“ **zehn Jahre aufzubewahren**. Die Frist beginnt mit Ablauf des jeweiligen Rechnungsjahres. Deshalb dürfen die personenbezogenen Daten von **ehemaligen Mitgliedern oder Spendern** erst nach Ende der Zehn-Jahres-Frist gelöscht werden; bis dahin unterliegen sie der eingeschränkten Verarbeitung!

8. Verhalten bei Datenschutzpannen

Trotz aller Vorsicht kann es zu Datenschutzverletzungen kommen (z.B. durch Verlust eines USB-Sticks, Diebstahl eines Laptops, Aufdeckung von Passwörtern oder Hacking einer Datenbank). Sofern hierdurch **nicht nur ein geringfügiges Risiko** für die Rechte und Freiheiten natürlicher Personen besteht, ordnet die DSGVO bestimmte Maßnahmen an, u.a. die Meldung an die Aufsichtsbehörde. Das bestehende Risiko kann nur durch **Abwägung** aller relevanten Umstände ermittelt werden; in diesem Zusammenhang ist z.B. zu erwägen, ob den Betroffenen durch Bekanntwerden ihrer Daten Diskriminierung, finanzielle Verluste oder Ansehensverluste drohen.

Aufgrund der schwierigen Abwägungsentscheidung sollten Sie bei einer Datenschutzpanne in jedem Fall **Kontakt mit einem der Ansprechpartner** aufnehmen (s. oben, Einleitung)!

Für den Fall einer Datenschutzverletzung sieht die DSGVO **folgende Maßnahmen** vor:

8.1. Meldung an die Aufsichtsbehörde

Es besteht die Pflicht, eine Datenschutzverletzung „unverzüglich und möglichst **binnen 72 Stunden“**, nachdem die Verletzung **bekannt wurde**, der zuständigen Aufsichtsbehörde zu melden. Die Meldung muss enthalten:

- eine Beschreibung der Datenschutzverletzung – soweit möglich mit Angabe der Kategorien, also der Gruppenbezeichnungen, der personenbezogenen Daten, der ungefähren Betroffenenzahl sowie der ungefähren Zahl der betroffenen Datensätze

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen

- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung

- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung sowie zur Abmilderung ihrer Folgen

Zuständig für Sie ist die **Aufsichtsbehörde Ihres Bundeslandes**. Eine Übersicht finden Sie auf der Homepage des Bundesdatenschutzbeauftragten: https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html („Landesdatenschutzbeauftragte“)

8.2. Benachrichtigung der betreffenden Person/en

Gegenüber Betroffenen besteht nur dann eine Benachrichtigungspflicht, wenn die Verletzung **„ein hohes Risiko“** für ihre persönlichen Rechte und Freiheiten zur Folge hat. Allerdings greift diese Verpflichtung nicht, wenn der Zugang zu den personenbezogenen Daten „hinreichend sicher geschützt“ war, durch nachfolgende Maßnahmen das ursprünglich hohe Risiko „aller Wahrscheinlichkeit nach“ beseitigt wurde oder die Benachrichtigung „mit einem unverhältnismäßigen Aufwand verbunden wäre und statt ihrer eine Information der Öffentlichkeit mit vergleichbarem Informationswert tritt“.

8.3. Dokumentation

Außerdem müssen Sie nicht nur die Datenschutzverletzung selbst, sondern auch **alle mit ihr im Zusammenhang stehenden Fakten** dokumentieren. Hierzu gehören auch die Auswirkungen der Verletzung sowie die von Ihnen ergriffenen Abhilfemaßnahmen. Diese Dokumentation muss es der Aufsichtsbehörde ermöglichen zu überprüfen, ob Sie alle Vorgaben der DSGVO eingehalten haben. Beachten Sie: Auch Datenschutzpannen, die keine Meldepflicht auslösen, müssen dokumentiert werden.

9. Übersicht der verfügbaren Muster

Auf https://meine-freiheit.de (Rubrik „FDP intern“ unter „Datenschutz-Grundverordnung“) finden Sie folgende Muster zum Download:

Muster 1a:	Verpflichtung auf den Datenschutz (Vorstandsmitglieder)
Muster 1b:	Verpflichtung auf den Datenschutz (Mitarbeiterinnen/Mitarbeiter)
Muster 1c:	Merkblatt zur Verpflichtung auf den Datenschutz
Muster 2:	Verfahrensverzeichnis
Muster 3:	Auftragsverarbeitung
Muster 4:	Einwilligungserklärung (DSGVO)
Muster 5:	Informationen zur Datenerhebung gem. Art. 14 DSGVO
Muster 6:	Datenschutzerklärung
Muster 7:	Impressum
Muster 8:	Einwilligungserklärung (Personenfotos)
Muster 9:	Antwort auf Auskunftsbegehren (Interessent/in)
Muster 10:	Antwort auf Auskunftsbegehren (ehemaliges Mitglied)