DER PARITÄTISCHE
GESAMTVERBAND

Handreichung

Datenschutz in Paritätischen Mitgliedsorganisationen

Ausgewählte Fragen zum Umgang mit personenbezogenen Daten und Geheimnisschutz

DEUTSCHER PARITÄTISCHER WOHLFAHRTSVERBAND GESAMTVERBAND e. V. | www.paritaet.org

DER PARITÄTISCHE GESAMTVERBAND

Inhalt

Impressum

Herausgeber:
Der Paritätische Gesamtverband e.V.
Oranienburger Straße 13-14
D-10178 Berlin
Telefon: +49 (0)30 24636-0
Telefax: +49 (0)30 24636-110

www.paritaet.org
info@paritaet.org

Verantwortlich im Sinne des Presserechts:
Dr. Ulrich Schneider

Bearbeitet von
Rechtsanwalt Michael Goetz, Stadtaltendorf
Rechtsanwältin Anuschka Novakovic
Rechtsanwältin Gertrud Tacke

Redaktion
Rechtsanwältin Gertrud Tacke

Titelbild:
© Alex – Fotolia.com

1. Auflage, April 2018

Vorwort

Die vorliegende **Handreichung „Datenschutz in Paritätischen Mitgliedsorganisationen“** widmet sich den häufigsten Fragen, die an uns herangetragen wurden, und praktischen Beispielen aus sozialen Organisationen rund um die Umsetzung aktueller Datenschutzverpflichtungen. Sie enthält unter anderem Informationen z. B. zum Beschäftigtendatenschutz, zum Sozialdatenschutz und zu Geheimhaltungsvorschriften, deren Verletzung nach § 203 Strafgesetzbuch (StGB) strafbar ist. Die Informationen im Text werden durch Mustertexte im Anhang ergänzt. Aufgenommen haben wir in den Anhang zudem eine ausführliche DS- und IT-Checkliste, die viele Ansatzpunkte gibt, am Daten-Sicherheitsniveau in der eigenen Organisation zu arbeiten.

Wir danken den Kolleg/-innen aus unseren Landesverbänden Niedersachsen, Rheinland-Pfalz, Saarland, Hessen, Sachsen, Baden-Württemberg, sowie unserem Datenschutzbeauftragten Dr. Thomas Pudelko für ihre wertvollen Anregungen bei der Erstellung dieser Handreichung.

Für eine grundsätzliche Einführung in die allgemeinen Grundlagen des Datenschutzes empfehlen wir Ihnen in Ergänzung zu dieser Handreichung die **Broschüre „Erste Hilfe zur Datenschutzgrundverordnung für Unternehmen und Vereine – Das Sofortmaßnahmen – Paket“, herausgegeben vom C.H. Beck-Verlag als Sonderdruck für den Paritätischen.** Sie ist für Paritätische Mitgliedsorganisationen über ihren Landesverband oder über den Gesamtverband zu beziehen, solange der Vorrat reicht. Im übrigen ist die Broschüre auch im Buchhandel erhältlich, auch als eBook. Die Broschüre bietet Hilfestellung für die schrittweise Umsetzung aktueller Datenschutzverpflichtungen. Sie richtet sich an kleine Unternehmen und Vereine und führt Sie sehr praxis- und handlungsorientiert durch Ihre anstehende Prüfung und zeigt auf, in welchen Bereichen Sie bereits ausreichend vorbereitet sind und wo es noch Handlungsbedarfe gibt.

Die rasanten technischen Entwicklungen und noch folgenden rechtlichen Entwicklungen werden auch in Zukunft weitere datenschutzrelevante Fragen aufwerfen. Aktualisierungen zum Thema finden Sie in absehbarer Zeit auf der Homepage des Paritätischen Gesamtverbands im Bereich Digitalisierung.

1. Einleitung

Ab dem 25.05.2018 findet in Deutschland und der gesamten Europäischen Union die EU-Datenschutz-Grundverordnung (**DS-GVO**) unmittelbare Anwendung. Ergänzt wird sie durch das neu gefasste Bundesdatenschutzgesetz **(BDSG)** sowie weitere Anpassungen z. B. im Sozialdatenschutz. Diese Vorschriften sind von **jeder** sozialen Organisation – egal welcher Rechtsform, ob gemeinnützig oder nicht – bei der Verarbeitung personenbezogener Daten zu beachten. Sondervorschriften speziell für Vereine gibt es nicht.

Die Veränderungen haben viele Mitgliedsorganisationen verunsichert, was verständlich ist angesichts einer Vielzahl der Regelungen, die europäischer als auch nationaler Herkunft sind. Die Leserinnen und Leser werden jedoch erkennen, dass sie viele Anforderungen an den Datenschutz bereits kennen. So gelten die wesentlichen bisherigen datenschutzrechtlichen Grundprinzipien fort (Datenerhebungsverbot mit Erlaubnisvorbehalt, Datenvermeidung und Datensparsamkeit, Zweckbindung und Transparenz, siehe Kasten 1, Seite 3). Teilweise werden sie weiterentwickelt durch erhöhte Anforderungen an Transparenz und durch Stärkung der Rechte der Betroffenen auf Information, Zugang und Löschung von Daten (Recht auf Vergessenwerden). Damit werden zukünftig erhöhte Anforderungen an die Dokumentation und

den Nachweis gestellt, dass geeignete und technisch ausreichende Maßnahmen zur Sicherstellung des Datenschutzes ergriffen wurden. Sorge bereitet vielen Organisationen die deutliche Ausweitung des Sanktionsrahmens bei Verstößen gegen den Datenschutz. Bußgelder sollen künftig „in jedem Einzelfall wirksam, angemessen und empfindlich" sein. Dabei spielen bei der Bestimmung der Höhe sowohl die Größe des Unternehmens und die Schwere des Verstoßes, das Ausmaß des Schadens, aber auch sonstige Umstände z. B. der Verantwortlichkeit eine Rolle. Immer hat die sanktionierende Behörde den Einzelfall und die Verhältnismäßigkeit zu prüfen.

Soziale Organisationen, die schon bislang ein tragfähiges Datenschutzkonzept hatten, sind gut gerüstet für die EU-Datenschutz-Grundverordnung. Sie müssen aber ihr Konzept an die Neuregelungen anpassen. Für Organisationen, die sich in der Vergangenheit noch kaum mit dem Thema Datenschutz befassten, bietet das neue Recht die Chance, gleich mit einem die aktuelle Rechtslage berücksichtigenden Datenschutzmanagement und -konzept zu starten.

Kasten 1 – Die Grundprinzipien des Datenschutzes

Transparenz

Datenverarbeitung hat nachvollziehbar zu sein. Betroffene Personen müssen die Rechtmäßigkeit der Verarbeitung ihrer Daten prüfen können. Damit korrespondiert das Auskunftsrecht des Betroffenen.

Zweckbindung und Erforderlichkeit

Ausgangspunkt der Verarbeitung ist der vorab festgelegte Zweck. Nur für diesen dürfen sie erhoben und verwendet werden und nur dann, wenn dies zur Aufgabenerfüllung erforderlich ist. Daten dürfen nicht auf Vorrat gesammelt werden.

Datenminimierung / Datensparsamkeit

Nur das für den beabsichtigten Zweck erforderliche Minimum an Daten – auf das notwendige Maß beschränkt – darf verlangt und verarbeitet werden.

Verhältnismäßigkeitsgrundsatz

Personenbezogene Daten müssen dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung darf nicht außer Verhältnis zu diesem Zweck stehen. (§ 47 BDSG)

Richtigkeit

Personenbezogene Daten müssen sachlich richtig und ggf. korrigiert, gesperrt oder auch gelöscht werden. Dieser Grundsatz korrespondiert mit dem Anspruch auf Information und Auskunft des Betroffenen.

Integrität und Vertraulichkeit

Der Grundsatz der Integrität und Vertraulichkeit beschreibt die Verpflichtung, personenbezogene Daten durch geeignete Maßnahmen zu sichern, um Datenschutzverstöße zu vermeiden. Es geht somit darum, geeignete organisatorische und technische Maßnahmen zur Datensicherung zu treffen.

2. Datenschutz – Strukturfragen

Der überwiegende Teil der Paritätischen Mitgliedsorganisationen sind eingetragene Vereine. Sie verarbeiten in verschieden Kontexten, z. B. Mitgliederverwaltung, Personalverwaltung und Abrechnung regelmäßig personenbezogene Daten von Vereinsmitgliedern, Organmitgliedern und Beschäftigten, aber auch von ehrenamtlich für den Verein Tätigen und Freiwilligen.

Im Kontext der Erfüllung ihrer satzungsrechtlichen Aufgaben verarbeiten sie in vielen Fällen außerdem personenbezogene Daten der von ihnen betreuten, beratenen und unterstützten Menschen, oft auch besondere Kategorien personenbezogener Daten, die als besonders schützenswert gelten. Eine große Rolle im Sozialbereich spielen dabei „sensible Daten" wie beispielsweise Gesundheitsdaten (siehe Kasten 2, unten). Die Organisationen müssen daher auch die strengeren Anforderungen für diese besondere Kategorie von Daten beachten.

Kasten 2 – Sensible Daten

Besonders schutzbedürftige Kategorien von Daten, Art. 9 Abs. 1 DS-GVO sind

„(…) personenbezogene[r] Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person…"

2.1 Wer ist für was verantwortlich?

Verantwortlich für die Rechtmäßigkeit der Datenverarbeitung ist die Organisation, also der Verein, gGmbH oder die Stiftung. Die Verantwortung für die Umsetzung und damit für Einhaltung des Datenschutzes im Verein trägt die **Leitung des Vereins**, der Vereinsvorstand oder die Geschäftsführung. **Datenschutz ist Managementaufgabe**. Die Leitung muss die Einhaltung des Datenschutzes im Zweifelsfalle nachweisen können. Organisationsintern werden regelmäßig Zuständigkeiten zur Umsetzung delegiert, z. B. auf IT-Verantwortliche und andere Mitarbeitende. Auch diese haben sich an die datenschutzrechtlichen Vorgaben zu halten.

Im Rahmen des Datenschutzmanagements ist die Erstellung eines **Datenschutzkonzepts** sinnvoll. Bei kleineren und ehrenamtlich strukturierten Vereinen haben oftmals verschiedene Funktionsträger die Möglichkeit, auf Mitgliederdaten und andere Daten zuzugreifen. Die Zuständigkeit für die Mitgliederverwaltung kann im ehrenamtlichen Vorstand häufiger wechseln. Auch arbeiten nicht selten ehrenamtliche Vorstandsmitglieder mit personenbezogenen Daten auf ihren privaten Computern.

Mit einem auf ihre konkrete Situation ausgerichtetes Datenschutzkonzept können Vereine für Transparenz und mehr Datensicherheit in ihrer Organisation sorgen. Ziel eines Konzeptes ist es, die Datensicherheit im Verein zu gewährleisten und Datenschutzverstöße möglichst auszuschließen. Teilweise werden auch Begriffe benutzt wie z. B. „Datenschutzordnung" oder „Datenschutzrichtlinie".

Siehe als Beispiel, Anhang A1, Seite 30: „Kodex zur Nutzung von digitalen Medien und insbesondere Messenger-Diensten bei Fröbel inkl. Bestätigungserklärung"

2.2 Müssen Beschäftigte auf den Datenschutz verpflichtet werden?

Teil eines tragfähigen Datenschutzkonzeptes ist auch die Information der Beschäftigten über die Bedeutung des Datenschutzes bei ihrem Arbeitgeber. Als Beschäftigte im Sinne von § 26 BDSG gelten neben den Arbeitnehmer/-innen u.a. auch Beschäftigte in Leiharbeit, Auszubildende, Freiwillige im FSJ und BFD sowie arbeitnehmerähnliche Personen. Eine gesetzliche Verpflichtung, diese auf den Datenschutz zu verpflichten, gibt es nicht. Das bedeutet aber nicht, dass damit die Mitarbeitenden nicht an den Datenschutz gebunden wären. Auch sie haben alle Regeln zu beachten, wenn sie mit der Verarbeitung personenbezogener Daten beauftragt sind.

Eine schriftliche Verpflichtung auf den Datenschutz ist sehr anzuraten! Sie sollte mit der Information über die Schutzpflichten verbunden werden und bei Veränderung von Aufgaben gegebenenfalls angepasst werden. Die gleiche Verpflichtung sollte beim Einsatz von Ehrenamtlichen, ggf. auch von Funktionsträgern bei der Verarbeitung personenbezogener Daten erfolgen. Im Übrigen ist die Hinweispflicht beim Umgang mit Sozialdaten im Sozialdatenschutz auch für soziale Organisationen vorgesehen (§ 78 SGB X), siehe hierzu Exkurs, Punkt 15.6, Seite 22.

Ein Muster für eine Verpflichtungserklärung findet sich im Anhang A2, Seite 35 (38)

2.3 Wann ist ein Verzeichnis von Verarbeitungstätigkeiten nötig?

Dieses Verzeichnis betrifft sämtliche automatisierten und teil-automatisierten Verarbeitungen und zumindest strukturierte Sammlungen von Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Das wesentliche Instrument, um Rechenschaft über die rechtmäßige Datenverarbeitung geben zu können, ist das **Verzeichnis von Verarbeitungstätigkeiten** gemäß Art. 30 DS-GVO. Es ist deshalb der Kern eines organisationsinternen **Datenschutzmanagements.** Die Aufstellung des Verzeichnisses von Verarbeitungstätigkeiten ist verpflichtend. Hierzu gibt es zwar eine Ausnahme: Die Pflicht zur Aufstellung eines Verzeichnisses entfällt, wenn in dem betreffenden Unternehmen oder der betreffenden Einrichtung weniger als 250 Mitarbeiter beschäftigt sind (Art. 30 Absatz 5 DS-GVO). Diese Ausnahme kommt jedoch für soziale Organisationen praktisch nicht in Betracht.

Sie müssen unabhängig von der Zahl ihrer Beschäftigten ein Verzeichnis der Verbeitungstätigkeiten aufstellen,

- wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen und **die Verarbeitung nicht nur gelegentlich erfolgt** oder
- wenn es um besonders geschützte Kategorien von Daten geht (Art. 9 Absatz 1 bzw. Art. 10 DS-GVO), siehe Kasten 2, Seite 4.

Da in jedem Verein die Erfassung und Verarbeitung personenbezogener Daten **nicht gelegentlich** erfolgt, ist bereits aus diesem Grund in der Regel in jeder Organisation ein Verzeichnis aller Verarbeitungstätigkeiten zu führen.

Siehe weitere Einzelheiten im Sonderdruck „Erste Hilfe“, S.12–20 mit Muster

Ein alternatives Muster finden Sie im Anhang A3, Seite 40: https://www.bfdi.bund.de/DE/Datenschutz/DatenschutzGVO/Aktuelles/Aktuelles_Artikel/Muster_Verzeichnis_Verarbeitungstaetigkeiten.html, Abruf 13.04.2018)

2.4 Wann muss ein Datenschutzbeauftragter im Verein benannt werden?

Oft werden soziale Vereine auch zur Bestellung eines Datenschutzbeauftragten verpflichtet sein. Dies ist zum einen der Fall,

- wenn ein Verein mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

- wenn die Kerntätigkeit des Vereins in der umfangreichen Verarbeitung besonders schutzbedürftiger Kategorien von Daten im Sinne des Art. 9 Abs. 1 DS-GVO (siehe Kasten 2, Seite 4) besteht.

Das führt dazu, dass bei den meisten unserer Mitgliedsorganisationen eine Pflicht zur Benennung eines/er Datenschutzbeauftragen besteht.

Seine/ ihre Aufgabe besteht darin, die Verantwortlichen bei Fragen des Datenschutzes fachlich zu unterstützen. Benannt werden kann eine interne Person aus dem Verein, aber auch eine externe Person.

Die Kontaktdaten des Datenschutzbeauftragten müssen veröffentlicht werden, **es genügt eine E-Mail-Funktionsadresse**, praktischerweise im Internet. Sie soll ermöglichen, dass sich Betroffene an den Datenschutzbeauftragten wenden können.

Siehe weitere Einzelheiten im Sonderdruck „Erste Hilfe", S.33–37 mit Prüfraster und Muster zur Benennung

3. Wann ist die Verarbeitung der personenbezogenen Daten erlaubt?

Wie bisher ist die Verarbeitung personenbezogener Daten grundsätzlich verboten außer in den Fällen, in denen das Gesetz sie ausdrücklich erlaubt (Verbot mit Erlaubnisvorbehalt). Die Erlaubnistatbestände sind in Art. 6 DS-GVO geregelt. Sie kann aus verschiedenen Gründen erlaubt sein, z. B. wenn eine Einwilligung vorliegt, aber auch zur Anbahnung und Durchführung eines Vertragsverhältnisses, einem der häufigsten Anwendungsfälle. Es reicht, wenn eine der nachstehend aufgeführten Voraussetzungen erfüllt ist.

Das ist nach Art. 6 DS-GVO der Fall, wenn

(1) ein Gesetz sie ausdrücklich erlaubt

(2) die betroffene Person **eingewilligt** hat,

(3) sie für die **Durchführung eines Vertrages oder dessen Anbahnung** erforderlich ist ,

(4) sie zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich ist, z. B. aufgrund gesetzlicher Vorschriften,

(5) sie erforderlich ist, um **lebenswichtige Interessen der betroffenen Person** oder einer anderen natürlichen Person zu schützen,

(6) sie für die Wahrnehmung einer **Aufgabe** erforderlich ist, die **im öffentlichen Interesse** liegt ,

(7) sie zur **Wahrung berechtigter Interessen des Verantwortlichen** erforderlich ist, sofern nicht die Interessen (…) der betroffenen Person (…) überwiegen.

4. Grundsätzliches zur Einwilligung in die Datenverarbeitung

4.1 Wie muss eine Einwilligungserklärung aussehen?

Die Einwilligung gilt gemeinhin als der sicherste Weg für eine rechtmäßige Datenverarbeitung. Deshalb ist es für soziale Organisationen immer sinnvoll, mit Einwilligungen zu arbeiten. Sie wird oft auch als der **Königsweg der rechtmäßigen Datenverarbeitung** bezeichnet. Die Einwilligung ist in Art. 4 DS-GVO definiert (siehe Kasten 3, unten). Näheres zur Einwilligung regelt Art. 7 DS-GVO.

Die Einwilligung sollte schriftlich vorliegen, damit sie als Nachweis für eine rechtmäßig erfolgte Datenverarbeitung dienen kann. Sie ist jederzeit widerrufbar.

Kasten 3 – Einwilligung

Eine Einwilligung des Betroffenen ist jede freiwillig für einen bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

siehe auch Sonderdruck „Erste Hilfe“, Seite 21

Wie nach altem Recht muss die **Einwilligung** auch nach den neuen Rechtsvorschriften

- **freiwillig**
- **in informierter Weise,** d.h. die betroffene Person muss klar und verständlich informiert werden, für wen die Einwilligung ist, zu welchem Zweck die Verarbeitung erfolgen soll und für welchen bestimmten Fall sie abgegeben wird und dass die Erklärung jederzeit widerrufen werden kann
- **eindeutig bestätigend,** also durch eine zustimmende Handlung wie z. B. schriftlich, online auch durch ein aktiv gesetztes Häkchen im Internet (sog. opt–in)

abgegeben worden sein.

Die Einwilligung bedarf nicht zwingend der Schriftform, sie kann auch mündlich, elektronisch oder in Textform erfolgen. Wegen der erforderlichen Nachweisbarkeit bleibt aber die Empfehlung, hierfür wenigstens die Text- oder Schriftform einzuhalten.

Ein Muster einer Einwilligung mit Schweigepflichtsentbindung findet sich im Anhang A4, Seite 43

4.2 Ist eine Einwilligung noch freiwillig, wenn die Gewährung von Leistungen davon abhängt?

Beispiel
Für die Aufnahme in eine Wohneinrichtung wird ein Wohn- und Betreuungsvertrag geschlossen. Separater Teil des Vertrages ist auch eine Einwilligung in die für das Vertragsverhältnis erforderliche Datenverarbeitung. Ohne diese Einwilligung nimmt die Einrichtung die anfragende Person nicht auf. Trotz dieser „Koppelung" bleibt die Einwilligung freiwillig, da es dem Betroffenen freisteht, keinen Vertrag zu schließen. Außerdem ist sie für die Betreuung und Versorgung und somit zur Vertragsdurchführung personenbezogener Daten betreffend Gesundheitszustand, Behinderung, Familienstand, rechtliche Betreuung, Kostenzusagen usw. erforderlich. Wird die Einwilligung zur Datenverarbeitung verweigert, kann der Vertrag nicht zustande kommen.

Eine Einwilligung bleibt also freiwillig, auch wenn sie Bedingung für die Erbringung einer Leistung ist.

4.3 Einwilligung von Kindern und Jugendlichen

Für die Einwilligung von Kindern und Jugendlichen sind Art. 8 DS-GVO sowie die deutschen Regelungen zur Einwilligungsfähigkeit zu beachten.

Neu ist, dass auch schon **Minderjährige ab 16 Jahren** in einzelnen Bereichen in die Verarbeitung ihrer Daten einwilligen können. Dies zielt vor allem auf den Internethandel. Die deutschen Regelungen zur Geschäftsfähigkeit bleiben allerdings davon unberührt.

Beispiel
Bestellt eine 17-jährige junge Frau online Waren, so kann sie nach dem neuen Recht in die Verarbeitung ihrer Daten einwilligen. Trotzdem kann das Rechtsgeschäft, je nach Umfang, (schwebend) unwirksam sein, weil sie noch nicht voll geschäftsfähig ist. Wird es von den Sorgeberechtigten nicht genehmigt, bleibt es unwirksam.

Anders im Bereich des Rechts am eigenen Bild. Da es hier um ein höchstpersönliches Recht des/der Minderjährigen geht, ist seine/ihre persönliche Einwilligung erforderlich, sobald von einer „natürlichen" Einsichtsfähigkeit ausgegangen werden kann. Es ist allerdings rechtlich umstritten, ab wann sicher von einer solchen Einsichtsfähigkeit ausgegangen werden kann.

Grundsätzlich empfiehlt sich, bei Minderjährigen nicht auf die vorab erteilte Einwilligung der Sorgeberechtigten zu verzichten.


siehe Sonderdruck „Erste Hilfe", Kapitel 13.3. „Bilder auf Internetseiten", Seite 52–54.

5. Mitgliederdaten

5.1 Erlaubnis der Verarbeitung

Nach Art. 6 DS-GVO ist die Verarbeitung zulässig für die **Erfüllung des Mitgliedschaftsverhältnisses** zwischen dem Verein und seinem Mitglied. Das Mitgliedschaftsverhältnis ist ein vertragsähnliches Verhältnis. Der Verein darf deshalb beim Vereinsbeitritt (Aufnahmeantrag oder Beitrittserklärung) und während der Mitgliedschaft die hierfür erforderlichen Daten erheben und verarbeiten, **die zur Verfolgung der Vereinsziele und der Betreuung und Verwaltung der Mitglieder** erforderlich sind. Dafür muss keine Einwilligung der Mitglieder oder der aufnahmewilligen Mitglieder vorliegen. Die Verarbeitung darüberhinausgehender personenbezogener Informationen bedarf der Einwilligung (siehe Punkt 3).

Nur ausnahmsweise dürfen diese Daten zu einem anderen Zweck als die soeben genannten verarbeitet werden, wenn berechtigte Interessen des Vereins vorliegen und keine schutzwürdigen Interessen der betroffenen Personen überwiegen. (Wegen der relativ schwer zu fassenden Rechtsgrundlage empfehlen wir, in diesen Fällen die Einwilligung der betroffenen Personen einzuholen.)

Die Nutzung der Vereinsdaten für Spendenaufrufe an die Vereinsmitglieder oder Werbung zur Erreichung der eigenen Ziele des Vereins ist erlaubt, keinesfalls aber die Weitergabe an Dritte zu deren Werbezwecken oder andere Außenstehende ohne Einwilligung.

Die Weitergabe von Mitgliederdaten an Außenstehende ist ohne Einwilligung des betreffenden Vereinsmitglieds grundsätzlich verboten.

5.2 Wann können Mitgliederdaten an andere Vereinsmitglieder herausgegeben werden?

Der Zugriff verschiedener Funktionsträger des Vereins auf die Mitgliederdaten ist eine innerorganisatorische Datenverarbeitung. Vereinsmitglieder haben in der Regel keinen Zugriff auf die Daten anderer Vereinsmitglieder. Eine Datenweitergabe an andere Vereinsmitglieder bedarf einer besonderen Rechtfertigung. Besteht der Vereinszweck darin, die persönlichen Kontakte zu stärken, z. B. im Bereich der Selbsthilfe, kann die Herausgabe einer Mitgliederliste zur Erreichung des Vereinsziels zulässig sein. Allerdings sind immer die schutzwürdigen Interessen und Belange der Mitglieder zu berücksichtigen.

Eine Bekanntgabe kann unter Umständen im Vereinsinteresse erforderlich sein, um die Ausübung satzungsrechtlicher Rechte zu ermöglichen, z. B. für die Einberufung außerordentlicher Mitgliederversammlungen. Um nicht entgegenstehende Interessen oder Schutzbedarfe zu verletzen, sollte der Verein eine Lösung suchen, die alle Mitglieder über das Begehren informiert, ohne deren Daten bekanntzugeben. Die Möglichkeit kann z. B. durch Veröffentlichung des beabsichtigten Antrags mit Gründen und Antragsteller in einem Vereinsorgan, z. B. Zeitschrift, Newsletter o. ä. geschehen, sodass interessierte Mitglieder die Möglichkeit der Kontaktaufnahme bekommen.

Die Mitglieder müssen sich grundsätzlich darauf verlassen können, dass ihre Mitgliederdaten ausschließlich für die Förderung der Vereinszwecke und die Verwaltung und Betreuung ihrer Mitgliedschaft verwendet werden.

5.3 Wie ist die Beitrittserklärung im Hinblick auf den Datenschutz zu gestalten?

Auch Vereinsmitglieder haben hinsichtlich ihrer persönlichen Daten das Recht auf Auskunft, Berichtigung, Löschung und Widerspruch sowie das neue Recht auf Datenübertragbarkeit.

siehe Sonderdruck „Erste Hilfe", Seite 40, 41

Um dem Datenschutz-Grundsatz der Transparenz zu genügen, sollte damit im Verein offen umgegangen werden. Schon auf der Beitrittserklärung sollte der Hinweis erfolgen, dass die personenbezogenen Daten der Mitglieder in dem Verein erhoben und verarbeitet werden.

Kasten 4 – Muster einer Beitrittserklärung

Beitrittserklärung

Ich…, Anschrift…trete dem Verein xy e. V. bei. Meine Bankverbindung lautet: …..

Datum und Unterschrift

Mir ist bekannt, dass die mich betreffenden Daten in dem Verein erhoben, gespeichert und verarbeitet werden, soweit sie für das Mitgliedschaftsverhältnis, die Betreuung und der Verwaltung der Mitglieder und die Verfolgung der Vereinsziele erforderlich sind.

Datum und Unterschrift

5.4 Wann sind Daten der Mitglieder zu löschen?

Die Organisation muss sicherstellen, dass personenbezogene Daten gelöscht werden, wenn die Notwendigkeit der Verarbeitung zur Zweckerreichung entfallen ist. Dies ist in der Regel bei dem Austritt eines Mitglieds aus dem Verein der Fall.

5.5 Datenschutzhinweis für die Mitglieder in der Vereinssatzung

Eine Datenschutzregelung in der Vereinssatzung dient ebenfalls der Transparenz des Datenschutzes im Verein. Es bedarf nicht zwingend einer Regelung in der Satzung. Übersichtlich bleibt die Vereinssatzung, wenn die Regelung knapp gehalten wird. Wir empfehlen eher, die Grundsätze der Datenerhebung, -verarbeitung und -nutzung schriftlich z. B. in einem Datenschutzkonzept, -ordnung oder -richtlinie niederzulegen, die der Vorstand erlässt. So kann sie jederzeit rechtlichen Änderungen angepasst werden.

Kasten 5 – Muster Satzungsbestimmung

§… Datenschutz

Der Verein benötigt zur Erfüllung seiner Zwecke die personenbezogenen Daten seiner Mitglieder. Unter Beachtung der Regelungen der EU-Datenschutzgrundverordnung sowie des Bundesdatenschutzgesetzes werden personenbezogene Daten der Mitglieder im Verein verarbeitet. Jedes Vereinsmitglied hat das Recht auf:

- *Auskunft über die zu seiner Person gespeicherten Daten,*
- *Berichtigung der Daten, sofern diese unrichtig sind,*
- *Sperrung der Daten, wenn deren Richtigkeit nicht feststeht,*
- *Löschung der Daten, wenn die Speicherung unzulässig war oder wird, z. B. bei Austritt aus dem Verein (Recht auf Vergessenwerden)*
- *Bereitstellung dieser Daten in einem gängigen Format (Recht auf Datenübertragung), Art. 20 DS-GVO.*

6. Spenderdaten

Viele Vereine sind auf Spenden angewiesen. Aber auch personenbezogene Daten von Spendern und Förderern (insbesondere deren Name, Adresse und Kontonummer) dürfen nur erhoben und verarbeitet und gespeichert werden, um die Spende abzuwickeln.

Beispiel

Eine gemeinnützige Organisation erhält Spenden und speichert die Spenderdaten. Für einen neuen Spendenaufruf nutzt sie die gespeicherten Daten. Diese Verarbeitung ist erlaubt, weil es in ihrem „berechtigten Interesse" liegt, Spenden zu erhalten (siehe Punkt 3). Bei den erneut angeschriebenen Spendern sind keine vorrangigen Interessen erkennbar, nicht erneut um eine Spende gebeten zu werden. Sie können aber die Löschung ihrer Daten aus der Spenderdatei verlangen. Diesem Verlangen ist nachzukommen, wenn nicht die Spenderdaten aus steuerrechtlichen Gründen noch aufgehoben werden müssen. Es handelt sich dann um eine Speicherung aufgrund einer rechtlichen Verpflichtung. (Siehe Punkt 3).

7. Klientendaten

7.1 Was ist zu beachten bei der Verarbeitung der personenbezogenen Daten von Nutzern der Dienste der Vereine, von Betreuten oder Personen, die beraten und unterstützt werden?

Auch hier gelten zunächst die allgemeinen Grundsätze der DS-GVO und des BDSG. (vgl. Punkt 3)

Sind diese Daten z. B. für die finanztechnische Abwicklung mit den Kostenträgern, die Abwicklung der angebotenen Dienstleistungen oder z. B. des Veranstaltungsgeschäftes erforderlich, handelt es sich meist um eine erlaubte Verarbeitung etwa im Rahmen der Erfüllung oder Anbahnung eines Vertrags, Erfüllung einer rechtlichen Verpflichtung, die keiner besonderen Einwilligung der betroffenen Personen bedarf. Dazu können auch Informationen über die konkreten Situationen und Probleme der Betroffenen gehören, wenn das für die zielgerichtete Erfüllung der Aufgaben des Vereins erforderlich ist.

Aber Achtung:

Die Erlaubnis kann eingeschränkt sein durch eine besondere Geheimhaltungspflicht des Vereins oder einer Einrichtung, die sich aus dem Zweck ihrer Arbeit ergibt, meist niedergelegt in zugrundeliegenden Vereinbarungen (Aufnahmevertrag, Leistungsvertrag). Das **prägnanteste Beispiel** hierfür ist die Arbeit der Frauenhäuser, die von Gewalt betroffenen Frauen einen anonymen Aufenthalt gewähren. Die Kontaktdaten sind streng zu schützen. **Erforderlich ist deshalb in solchen Fällen eine Einwilligungserklärung der Betroffenen für die notwendige Verarbeitung der personenbezogenen Daten, die sich auch auf notwendige Weitergaben bezieht.**

Sie kann weiter eingeschränkt sein, wenn es um die **besonders schutzbedürftigen Kategorien von Daten,** z. B. Gesundheitsdaten, Daten zum Sexualleben aber auch Daten, aus denen die „rassische und ethnische Herkunft" hervorgeht (Siehe Kasten 2). Auch Daten über die Erbringung von Gesundheitsdienstleistungen gelten als besonders schutzwürdig.

Nach Art. 9 Abs. 1 DS-GVO ist für die Verarbeitung dieser Daten **in der Regel eine Einwilligung der betroffenen Person erforderlich**.

§ 22 Abs. 1 BDSG enthält jedoch **Lockerungen für die rechtmäßige Verarbeitung von sensiblen Daten im Gesundheits- und Sozialbereich**,

„wenn sie

1. erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen,

2. zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden, oder

aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, (…)".

Gleichwohl ist sozialen Organisationen bei der Verarbeitung von besonders sensiblen Daten die Einholung einer möglichst schriftlichen **Einwilligung** als dem „sichersten Weg" anzuraten. Das gilt z. B. besonders für Beratungsstellen im Bereich der Unterstützung von Opfern von Gewalt und ähnlichen Institutionen.

siehe Anhang A5, Seite 44, Muster einer Einwilligung für den Bereich Frauenunterstützungseinrichtungen

8. Beschäftigtendaten

Auch im Bereich des Schutzes der Beschäftigtendaten gelten die „Grundprinzipien" des Datenschutzes (siehe Kasten 1) und die sonstigen allgemeinen Regeln, die für jedes Rechtsverhältnis gelten. Der **Beschäftigtenbegriff** im Datenschutzrecht umfasst neben den Arbeitnehmer/-innen unter anderem auch Freiwillige im **FSJ und BFD** sowie Beschäftigte in **Werkstätten für behinderte Menschen**. Auch auf Ehrenamtliche und Organschaftsverhältnisse sind die Regeln ergänzend anzuwenden.

Der neue § 26 BDSG entspricht weitgehend dem bisherigen Recht. Danach darf der Arbeitgeber z. B. personenbezogene Daten verarbeiten, wenn dies für die Begründung (Bewerberdaten), die Durchführung oder die Beendigung erforderlich ist. Das gilt auch für die Verarbeitung personenbezogener Daten durch Arbeitgeber und Betriebsräte **bei der Verwirklichung der Rechte und Pflichten von Interessenvertretungen** der Beschäftigten.

Im neuen BDSG wird klargestellt, dass auch sogenannte „Kollektivvereinbarungen", also Tarifverträge, Betriebs- oder Dienstvereinbarungen „Rechtsvorschriften" im Sinne des BDSG sind und demnach geeignete Rechtsgrundlagen für eine zulässige Datenverarbeitung schaffen können.

Es fallen **alle Formen der Verarbeitung** von personenbezogenen Daten unter die datenschutzrechtlichen Bestimmungen, also auch wenn die Daten nicht in einem Dateisystem gespeichert sind oder werden sollen. Auch die papiernen Personalakten oder mündliche Formen (z. B. bei Weitergabe von Daten) gehören dazu.

Arbeitnehmerdaten können auch **besonders zu schützende Kategorien von Daten sein (**siehe Kasten 2, Seite 4), z. B. gesundheitliche Angaben zu einem/er Arbeitnehmer/-in. So werden in der Personalverwaltung z.B. auch Krankheitszeiten und die Schwerbehinderteneigenschaft erfasst. Während im Grundsatz bei **besonders zu schützenden Kategorien von Daten** aufgrund der strengeren Anforderungen eine Einwilligung der betroffenen Person in die Verarbeitung notwendig ist, **macht § 26 Absatz 3 und 4 BDSG hier eine Ausnahme**.

Die Verarbeitung solcher sensibler Daten für Zwecke des Beschäftigungsverhältnisses ist immer zulässig, wenn sich entsprechende Verarbeitungspflichten aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit ergeben. Dazu gehören z. B. Meldungen zu dem Beschäftigungsverhältnis an die Sozialversicherung.

Möglich ist die Verarbeitung darüberhinausgehender besonders schützenswerter Daten und sonstiger personenbezogener Daten, wenn eine **freiwillige, schriftliche Einwilligung** vorliegt, die den in § 26 Abs. 2 BDSG formulierten Anforderungen entspricht:

„Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. **Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Absatz 3 der Verordnung (EU) 2016/679 in Textform aufzuklären."**

In der Praxis kann dies z. B. im Kontext der Durchführung des betrieblichen Eingliederungsmanagements oder bei der Gestattung privater Nutzung von dienstlichen Fahrzeugen, Telefonen, EDV-Geräten erforderlich sein.

Die Arbeitnehmer/-innen haben Anspruch auf Auskunft über die gespeicherten Daten (siehe zu „Betroffenenrechte" Punkt 11, Seite 17). Der Arbeitgeber hat außerdem über den Zweck der Datenverarbeitung und die jederzeitige Widerrufsmöglichkeit zu informieren.

9. Der Verein und das Internet

9.1 Veröffentlichungen von personenbezogenen Daten auf Internetseiten

Fast jede Organisation hat eine Internetseite, auf der sie sich darstellt. Eine Veröffentlichung personenbezogener Daten von Mitgliedern oder anderen Menschen im Internet ist jedoch grundsätzlich nur mit ausdrücklicher Einwilligung der Personen zulässig. (zur Einwilligungserklärung siehe Punkt 4, Seite 7) Sie stellt ohne Einwilligung eine unzulässige Übermittlung an jedermann dar.

Funktionsbezogene Daten wie beispielsweise Vor- und Nachnamen oder vereinsbezogene E-Mail-Adressen von Vereinsfunktionären und -organen dürfen auch ohne deren Einwilligung im Internet veröffentlicht werden. Die Angabe privater Adressen (E-Mail wie postalisch) bedarf hingegen wiederum einer Einwilligung des Funktionsträgers.

9.2 Online-Anmeldungen zu Veranstaltungen und Allgemeine Geschäftsbedingungen (AGB)

Immer häufiger ist es möglich, sich zu Veranstaltungen von Mitgliedsorganisationen online anzumelden. Die Anmeldung erfolgt regelmäßig durch Absenden der Anmeldemaske, in der die personenbezogenen Angaben eingetragen wurden.

Regelmäßig wird auch eine Zustimmung zu Allgemeinen Geschäftsbedingungen (AGB) durch Anklicken eines Kästchens erwartet.

Einwilligungen in die Datenverarbeitung der personenbezogenen Daten dürfen jedoch aus Transparenzgründen datenschutzrechtlich nicht mit den AGB´s verbunden sein. Die entsprechende Einwilligungserklärung muss gesondert auf der Anmeldeseite aufrufbar sein und durch aktives Anklicken eines Kästchens bestätigt werden.

Kasten 6 – Muster einer Datenschutzeinwilligung bei Online-Anmeldung

Der/die Teilnehmenden wird darauf hingewiesen, dass die zur Abwicklung der Veranstaltung erforderlichen persönlichen Daten (Vorname, Name, Anschrift, besondere Anforderungen zur Barrierefreiheit) vom Veranstalter … auf elektronischen Datenträgern gespeichert werden.

Der/die Teilnehmende stimmt der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten beim Veranstalter … zur Abwicklung der Veranstaltung ausdrücklich zu. Die gespeicherten persönlichen Daten werden vom Veranstalter … vertraulich behandelt. Die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten des/der Teilnehmende erfolgt unter Beachtung der DS-GVO, des Bundesdatenschutzgesetzes (BDSG) und des Telemediengesetzes (TMG).

Dem/der Teilnehmenden steht das Recht zu, die Einwilligung jederzeit mit Wirkung für die Zukunft zu widerrufen. Der Veranstalter … ist in diesem Fall zur sofortigen Löschung der persönlichen Daten des/der Teilnehmenden verpflichtet.

9.3 Onlineberatung

Im Paritätischen bietet eine ganze Reihe von Einrichtungen eine Onlineberatung zu verschiedensten Bereichen an. Die betreffenden Einrichtungen sollten sich mit ihrem Anbieter in Verbindung setzen. Nach Auskunft unseres Rahmenvertragspartners Beranet (Zone35) haben die Einrichtungen in der Regel selbst technisch nichts zu veranlassen. Notwendig wird eine Anpassung der Datenschutzerklärung sein (Information). Weitere Informationen und ggf. Anpassungsbedarf in den Nutzungsbedingungen wird Beranet (Zone35) unaufgefordert allen seinen Kunden im Laufe des Aprils 2018 zur Verfügung stellen.

9.4 Bilder / Fotos auf Internetseiten

Dieses nicht ausschließlich datenschutzrelevante Thema ist deshalb von Bedeutung, weil sich Bilder über eine öffentliche Internetseite mühelos verbreiten lassen und im Nachgang nicht mehr einzufangen sind. Nach Aussagen des Landesdatenschutzbeauftragten des Landes Bayern reichen technische Maßnahmen in keinem Fall aus, „das Persönlichkeitsrecht an Bildern auch nur halbwegs zu schützen." (siehe Sonderdruck „Erste Hilfe...", Seite 50). Auch Fotos können personenbezogene Informationen enthalten, die es ermöglichen, eine Person zu identifizieren. Es reicht, wenn dies nur wenigen Personen möglich ist.

Im Kunsturhebergesetz (KUG) ist das Recht am eigenen Bild geregelt. Nach § 22 KUG dürfen Bildnisse von Abgebildeten **nur mit Einwilligung** verbreitet oder öffentlich zur Schau gestellt werden. Auch nach dem Tod des/der Abgebildeten bedarf es noch 10 Jahre lang einer Einwilligung der Angehörigen. Hier einige Grundsätze:

- Die Einwilligung muss vor der Veröffentlichung vorliegen.
- Einwilligungen im Arbeitsleben müssen schriftlich und ausdrücklich mit dem Betroffenen abgeschlossen sein.
- Ein Widerruf wirkt nur für die Zukunft.

§ 23 KUG regelt Ausnahmen, die vor allem im Bereich Veranstaltungen relevant sein können.

„(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. Bildnisse aus dem Bereiche der Zeitgeschichte;

2. Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;

3. Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;

4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.

(2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird."

Zu weiteren Einzelheiten, insbesondere Grundregeln für Bilder auf Vereinsveranstaltungen und Ausnahmeregelungen, sowie zu Besonderheiten in Bezug auf Einwilligungen bei Minderjährigen möchten wir auf die **ausführlichen Informationen im Sonderdruck der Broschüre „Erste Hilfe" 13. Kapitel, Seite 50–57 hinweisen.** Dort ist auch ein Muster zur Einwilligung zu Fotoaufnahmen auf Veranstaltungen und zur Einwilligung zu Fotoaufnahmen mit Kindern zu finden.

Siehe im Anhang A1, Seite 30 das Beispiel des Kodex der Fröbelstiftung, der Regeln hierzu aufstellt.

10. Datensicherheit = IT- Sicherheit

Art. 32 Abs. 1 Satz 1 DS-GVO

„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen **treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;…."**

„Datensicherheit ohne IT-Sicherheit kann es praktisch nicht geben", so die Aussage der Landesdatenschutzbehörde Bayern im Sonderdruck Broschüre „Erste Hilfe" im 6. Kapitel „Sicherheit der Verarbeitung". Dort werden ab S. 25–31 die zentralen Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) erläutert und die verschiedenen Herausforderungen wie IT = Chefsache, Berechtigungsmanagement, Risiken bestimmen und begegnen, Verschlüsselung im Alltag, Aktualisierung (Patch-Management), E-Mail-Kommunikation richtig einsetzen, Schadsoftware vorbeugen: Backups, Zugang erschweren und verwehren, sowie Typische Irrtümer zur IT-Sicherheit, bearbeitet.

Siehe dazu Anhang A7 Seite 46, IT-DS Check, Dr. Thoma Pudelko

Es gilt die Empfehlung, dass selbst kleine Unternehmen in einer Sicherheitsrichtlinie oder einem Konzept die wesentlichen Aspekte für den eigenen sicheren Betrieb ihres IT-Systems umschreiben sollten. Dazu gehört auch, die eigenen Mitarbeiter/-innen und Ehrenamtlichen zu befähigen, eigenständig in ihrem Arbeitsbereich den Sicherheitsanforderungen zu genügen. Dies erfolgt durch Schulungen, Unterweisungen ggf. mit Unterstützung des betrieblichen Datenschutzbeauftragten

11. Welche Rechte haben betroffene Personen?

Mit den Neuregelungen sollen die Betroffenenrechte bei der Verarbeitung ihrer personenbezogenen Daten gestärkt werden. Die Betroffenenrechte dienen besonders der Umsetzung des oben beschriebenen Grundsatzes der Transparenz (Siehe Kasten 1, Seite 3).

So haben betroffene Personen

- einen Anspruch, bei Erhebung von personenbezogenen Daten **informiert** zu werden**.** Auch über Zweckänderungen der Datenerhebung ist zu informieren. Eine Informationspflicht besteht auch, wenn Datenverarbeitungen unrechtmäßig erfolgen, z. B. bei unsachgemäßem Umgang mit Daten oder Datendiebstahl.

- auf Anfrage **Auskunft** zu erhalten. Dieses Recht ist umfassend. Es geht darum, welche Daten erfasst wurden und zu welchem Zweck, aber auch die Herkunft der Daten, ihre Speicherdauer, Rechte auf Berichtigung und Löschung. Die Auskunftserteilung erfolgt i. d. R. unentgeltlich, auch die Herstellung von Kopien. Die Auskunft kann schriftlich, elektronisch oder auch mündlich erfolgen. Die soziale Organisation hat dafür zu sorgen, dass Auskünfte nur an berechtigte Personen erteilt werden. Bei Auskunftserteilung ist auf die Rechte anderer betroffener Personen zu achten. In einem Datenschutzkonzept können Regelungen zum Umgang mit Auskunftsersuchen aufgenommen werden.

- ein Recht auf **Berichtigung** unrichtiger Daten.

- ein Recht auf **Löschung („Recht auf Vergessenwerden“)**, z. B. wenn der Zweck der Datenverarbeitung erreicht ist oder entfällt. Das Recht besteht auch, wenn eine Einwilligung widerrufen wurde und kein anderer Rechtsgrund zur weiteren Datenverarbeitung besteht.

- ein Recht auf **Einschränkung der Verarbeitung** (früher: Sperrung)

- **nach den neuen Regelungen ein Recht auf Datenübertragung** (Art. 20 DS-GVO). Grundsätzlich kann eine betroffene Person verlangen, dass sie ihre personenbezogenen Daten in maschinenlesbarer Form erhält, damit sie diese in einer neuen Geschäftsbeziehung nutzen kann. Diese Regelung zielt besonders auf langfristige Geschäfte, z. B. mit Telekommunikationsanbietern („Handy-Verträge“). Sie kann aber auch für soziale Organisationen von Bedeutung sein, z. B. beim Wechsel zu einem anderen Leistungsanbieter.

Beispiel
Bei einem Wechsel von einem ambulanten Pflegedienst zu einem anderen kann der Patient die Herausgabe der ihn betreffenden Unterlagen verlangen, um sie dem neuen Pflegedienst weitergeben zu können.

12. Sanktionen, Haftung

Ausgeweitet wurde der **Sanktionsrahmen** für Verstöße gegen den Datenschutz. Auch nach bisherigem Recht wurden Verstöße mit Bußgeldern und Geldstrafen geahndet. Allerdings kam es bisher selten vor, dass gegen eine soziale Organisation wegen eines Verstoßes gegen den Datenschutz ermittelt wurde. Eine Prüfung erfolgte eher anlassbezogen (z. B. auf Anzeige eines Betroffenen).

Im Vergleich zu den bisherigen Regelungen wurde der Bußgeldrahmen durch die DS-GVO erheblich erweitert. Für bestimmte schwere Rechtsverstöße kann es Bußgelder in Höhe von bis zu 4 Prozent des Jahresumsatzes eines Unternehmens geben. Die Bußgelder sollen künftig „in jedem Einzelfall wirksam, angemessen und empfindlich“ sein. Dabei spielt bei Bestimmung der Höhe sowohl die Größe des Unternehmens und die Schwere des Verstoßes, das Ausmaß des Schadens, aber auch sonstige Umstände z. B. der Verantwortlichkeit eine Rolle. Immer hat die ermittelnde Behörde den Einzelfall und die Verhältnismäßigkeit zu prüfen. Nach Aussage der Landesdatenschutzbehörde Bayern kann bei kleinen Unternehmen und Vereinen bei ernsthaften Verstößen mit Geldbußen in vier- oder fünf-stelliger Höhe zu rechnen sein.

Siehe Sonderdruck „Erste Hilfe“, Seite 47.

Das BDSG sieht auch Strafvorschriften vor.

Schließlich hat die DS-GVO einen Schadensersatzanspruch gegenüber dem Verantwortlichen geschaffen, wenn einer Person aufgrund eines Verstoßes ein materieller oder immaterieller Schaden entstanden ist.

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

13. Schweigepflicht

13.1 Woraus ergeben sich Schweigepflichten?

Schließlich unterliegen auch die handelnden Personen in den sozialen Organisationen selbst in ihrer Arbeit **Schweigepflichten**, auch wenn dies nicht zum Datenschutz im engeren Sinne zählt. Dabei kann es um die Achtung der Privatsphäre von Kunden, aber auch um Betriebs- und Geschäftsgeheimnissen gehen.

Adressaten der Vorschriften zu den Schweigepflichten und den Zeugnisverweigerungsrechten sind meist die Mitarbeiter/-innen der sozialen Organisationen. Hierunter fallen die Arbeitnehmer/-innen, freie Mitarbeiter/-innen aber auch Ehrenamtliche und freiwillig Tätige und Organmitglieder (z. B. Vereinsvorstand).

Geheimhaltungspflichten sind in Deutschland außerhalb des eigentlichen Datenschutzrechts geregelt. Sie sind Ausfluss des Rechts auf informationelle Selbstbestimmung. Jeder Bürger verfügt selbst über seine Daten.

Geheimhaltungspflichten ergeben sich z. B. aus dem Arbeitsvertrag. Ein Arbeitnehmer hat gegenüber seinem Arbeitgeber eine Treuepflicht. Er hat über Dienstgeheimnisse Stillschweigen zu wahren. Verstößt er gegen diese Pflicht, so kann dieser Verstoß arbeitsrechtliche Konsequenzen haben, z. B. eine Abmahnung, je nach Schweregrad ggf. auch eine Kündigung des Arbeitsverhältnisses. Schweige- und Geheimhaltungspflichten können sich aus freien Mitarbeiterverträgen, oder aus Verpflichtungserklärungen, die im Rahmen der Übernahme von Vereinsämtern abgegeben werden, ergeben.

13.2 Die Berufliche Schweigepflicht nach § 203 StGB – Verletzung von Privatgeheimnissen ist strafbewehrt

Der wichtigste Regelungsbereich für Geheimhaltungspflichten sind die Vorschriften im Strafgesetzbuch sowie der Strafprozessordnung. Im Strafgesetzbuch (StGB) geht es hierbei um die **„Straftaten wegen der Verletzung des persönlichen Lebens- und Geheimbereichs“**, die in den §§ 201 – 206 StGB geregelt sind. Es handelt sich dabei um die Verletzung

– der Vertraulichkeit des Wortes (§ 201)

– des höchstpersönlichen Lebensbereiches durch Bildaufnahmen (§ 201a)

– des Briefgeheimnisses (§ 202)

– von Privatgeheimnissen (§ 203)

– des Post- und Fernmeldegeheimnisses

– das Ausspähen von Daten und die Verwertung fremder Geheimnisse (§§ 206, 203a und 204).

Bei diesen Straftaten handelt es sich überwiegend um Antragsdelikte. Dies bedeutet, dass ein Strafantrag des/der Betroffenen für die Strafverfolgung notwendig ist.

Aus dem Katalog der genannten Strafvorschriften ist vor allem für die soziale Praxis die **Verletzung von Privatgeheimnissen** von besonderer Bedeutung.

In § 203 StGB werden Berufsträger aus besonders hervorgehobenen sensiblen Arbeitsbereichen als Adressaten genannt. Traditionell gehören hierzu Ärzte, Berufspsychologen und Rechtsanwälte, außerdem Ehe-, Familien, Erziehungs- oder Jugendberater sowie Berater, die in einer anerkannten Suchtberatungsstelle bzw. einer anerkannten Schwangerschaftskonfliktberatungsstelle arbeiten und auch staatlich anerkannte Sozialarbeiter oder staatlich anerkannte Sozialpädagogen.

Sie alle haben ihnen anvertraute persönliche Geheimnisse zu wahren, soweit ihnen diese Geheimnisse im Zusammenhang mit ihrer Berufsausübung bekannt geworden sind. In die Schweigepflicht einbezogen sind immer auch die so genannten Gehilfen der genannten Berufsträger (Verwaltungspersonal) sowie die zur Vorbereitung auf den Beruf in den sozialen Organisationen tätigen Mitarbeiter/-innen. Das sind z. B. Jahrespraktikanten im Anerkennungsjahr der Sozialarbeit / Sozialpädagogik.

Es handelt sich dabei um eine **persönliche Pflicht** des einzelnen Berufsträgers. Die Geheimhaltungspflicht gilt auch gegenüber Kollegen und Vorgesetzten in der sozialen Organisation.

Für eine Verletzung von Privatgeheimnissen kann nur derjenige bestraft werden, der **unbefugt** gegen diese Strafvorschrift verstößt. Eine Geheimhaltungspflicht gilt nicht, wenn der Berufsträger eine **Offenbarungspflicht** oder ein **Offenbarungsrecht** hat. Die Befugnis zur Offenbarung eines Geheimnisses kann sich aus verschiedenen Vorschriften ergeben. Die betreffenden Beschäftigten sind auf diese besonderen Geheimhaltungspflicht nach § 203 StGB beii Vertragsabschluss gesondert hinzuweisen und zu verpflichten.

Siehe Beispiel in Anhang A2a, Seite 39.

Kasten 7 – Berufliche Schweigepflicht

Vorschrift

§ 203 StGB Verletzung von Privatgeheimnissen (Auszug)

„(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis (….) offenbart, das ihm als

1. Arzt, (…) oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,

2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,

3. Rechtsanwalt, (…) Steuerberater, (…)

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die (…) anerkannt ist,

5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,

6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

7. (…)

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

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

13.3 Entbindung von der Schweigepflicht

Die Offenbarung der anvertrauten Geheimnisse ist dann gerechtfertigt, wenn eine Einwilligung der Betroffenen vorliegt, beziehungsweise wenn Betroffene den/die Geheimnisträger/-in von der Schweigepflicht entbunden hat. Die Schweigepflichtsentbindungserklärung folgt den gleichen Regeln wie die weiter oben beschriebene datenschutzrechtliche Einwilligungserklärung. Auch hier ist zu empfehlen, für diese Erklärung grundsätzlich die schriftliche Form zu wählen.

Siehe Muster im Anhang A4, Seite 43; Anhang A6, Seite 45

13.4 Weitere Offenbarungsbefugnisse

Jeder ist zur **Anzeige geplanter Verbrechen gem. § 138 StGB** verpflichtet. Hierbei handelt es sich um schwerste Straftaten. Zur Strafanzeige verpflichtet ist, wer von dem Vorhaben oder der Ausführung z. B. eines Mordes oder Totschlags oder einer anderen schweren Straftat erfährt. Dies kommt im Zusammenhang mit einer Tätigkeit in einer sozialen Organisation doch eher selten vor.

§ 34 StGB regelt den so genannten **rechtfertigenden Notstand**. Der Bruch des Schweigens kann gerechtfertigt sein, wenn es um die Abwendung von ernsten Gefahren insbesondere für Leib und Leben geht.

In der Jugendhilfe wurde vor einigen Jahren im § 8a SGB VIII geschaffen, der einen **Schutzauftrag bei Kindeswohlgefährdung** vorsieht. Adressat ist in erster Linie das Jugendamt. Werden dem Jugendamt wichtige Anhaltspunkte für die Gefährdung des Wohls eines Kindes oder Jugendlichen bekannt, so ist es verpflichtet, ein Schutzverfahren einzuleiten, das in § 8a SGB VIII geregelt ist. Freie Jugendhilfeträger werden über Leistungsvereinbarungen in dieses Schutzverfahren einbezogen. Nach § 8a Abs. 4 Satz 2 SGB VIII ist in die Vereinbarung die Verpflichtung aufzunehmen, „dass die Fachkräfte der Träger (...) das Jugendamt informieren, falls eine Gefährdung nicht anders abgewendet werden kann."

14. Zeugnispflicht und Zeugnisverweigerungsrechte

Schließlich wird die berufliche Schweigepflicht dann verdrängt, wenn eine **Zeugnispflicht** vor einem deutschen Gericht besteht. Dies ist im **Strafverfahren** der Fall. Jeder Bürger ist dort verpflichtet, als Zeuge auszusagen, es sei denn, er hat ein **Zeugnisverweigerungsrecht aus persönlichen Gründen** (Angehörige, Ehepartner) oder **beruflichen Gründen**. Das Zeugnisverweigerungsrecht aus beruflichen Gründen ist geregelt in § 53 StPO und hat als Adressaten wie in § 203 StGB Berufsgruppen, in denen traditionell ein besonderes Vertrauensverhältnis geschützt werden soll. Dies sind, wie bereits zu § 203 StGB ausgeführt, u. a. Ärzte, Berufspsychologen und Rechtsanwälte. In § 53 StPO finden sich auch die Mitarbeiter/-innen einer anerkannten Schwangerschaftskonfliktberatungsstelle und die Mitarbeiter/-innen einer anerkannten Suchtberatungsstelle wieder, nicht aber **Sozialarbeiter/-innen, Sozialpädagog/-innen oder auch Diplompädagog/-innen. Sie müssen also im Strafverfahren aussagen. Der Personenkreis in § 203 StGB und § 53 StPO ist nicht deckungsgleich**.

Eine Zeugnispflicht besteht hingegen im **Zivilprozess** nicht, wenn es um Tatsachen geht, die unter die berufliche Schweigepflicht nach § 203 StGB fallen (§ 383 ZPO Zeugnisverweigerungsrecht). Das Gleiche gilt im familiengerichtlichen Verfahren und in Angelegenheiten der freiwilligen Gerichtsbarkeit. Im Unterschied zum Strafverfahren geht es in diesem Bereich um Interessen von einzelnen Personen und nicht wie im Strafprozess um den Strafanspruch des Staates.

15. Exkurs: Besonderheiten im Kontext des Sozialdatenschutzes unter Einbeziehung sozialer Organisationen

15.1 Neuregelungen durch die DS-GVO?

Auch der Sozialdatenschutz wurde an die EU-Datenschutz-Grundverordnung angepasst. Die DS-GVO regelt umfassend den Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten, egal ob die Datenverarbeitung durch öffentliche oder nicht öffentliche Träger geschieht. „Verantwortliche" im Sinne des Datenschutzes in der DS-GVO sind alle natürlichen oder juristischen Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden (Art. 4 Ziffer 7 DS-GVO). An verschiedenen Stellen wird ausdrücklich der Gesundheits- und Sozialbereich als Adressat der Datenschutzbestimmungen in der DS-GVO genannt. Wie bereits ausgeführt, sind Gesundheitsdaten als besondere Kategorie personenbezogener Daten durch Art. 9 DS-GVO nochmals stärker geschützt.

Die Anpassung der Vorschriften im Sozialdatenschutz an die DS-GVO erfolgt zeitgleich zum 25.05.2018. Anders als im BDSG ändert sich aber im Sozialdatenschutz inhaltlich im Vergleich zu den bisher geltenden Regelungen kaum etwas. In der Regel sind es nur redaktionelle Anpassungen an die DS-GVO, indem die neue Terminologie des Datenschutzrechts auch im Sozialdatenschutz eingeführt wird. Daneben werden im Sozialgeheimnis des § 35 SGB I nun auch ausdrücklich die Sozialdaten von Verstorbenen erfasst. Diese Regelung fehlte bisher in der Vorschrift. In der Rechtspraxis wurden aber auch schon länger die Daten Verstorbener geschützt.

In § 67a Abs. II SGB X wird das Gebot der Direkterhebung beim Betroffenen für den Bereich des Sozialdatenschutzes ausdrücklich und unverändert geregelt. Personenbezogene Daten sind in erster Linie bei der betroffenen Person zu erheben. Dies ist im Übrigen Ausfluss des im Datenschutzrecht geltenden Grundsatzes der Verarbeitung nach Treu und Glauben sowie des Transparenzprinzips (siehe Kasten 1, Seite 3).

15.2 Das sozialrechtliche Dreiecksverhältnis – was ist das?

Soziale Organisationen bieten Dienstleistungen für nachfragende Bürger an. Sind sie als eingetragene Vereine befasst, so ist Grundlage ihrer Arbeit der in der Vereinssatzung beschriebene Satzungszweck. In der Regel dient diese Aufgabenerfüllung der Erbringung von in den Sozialgesetzbüchern festgelegten Sozialleistungen. Träger dieser Sozialleistungen sind die im Sozialgesetzbuch I genannten Leistungsträger, z. B. der Sozial- und Jugendhilfeträger, die gesetzlichen Krankenkassen, die gesetzliche Rentenversicherung, die Agentur für Arbeit u. a.. Begehrt ein Bürger eine Sozialleistung, so stellt der zuständige Leistungsträger den Anspruch in der Regel in einem förmlichen Bescheid fest. Es entsteht ein **Sozialleistungsverhältnis**, in dem beide Seiten Rechte und Pflichten haben. Der Leistungsbescheid ist ein hoheitlicher Akt. Handelt es sich bei der begehrten Sozialleistung um eine Dienstleistung (Sachleistung), so erbringt der Leistungsträger in den meisten Fällen die Sozialleistungen nicht selbst. Er verweist den anspruchsberechtigten Bürger z. B. auf die Leistungsangebote von sozialen Organisationen der freien Wohlfahrtspflege. Zur Leistungserbringung schließen sie mit dem anspruchsberechtigten Bürger **privatrechtliche (Dienstleistungs-) Verträge** ab. Die Kostenübernahme wird zwischen dem Leistungsträger und der sozialen Organisation als Leistungserbringerin geregelt (**Leistungs- und Versorgungsvertrag**). Auch auf dieser Ebene entsteht ein Rechtsverhältnis.

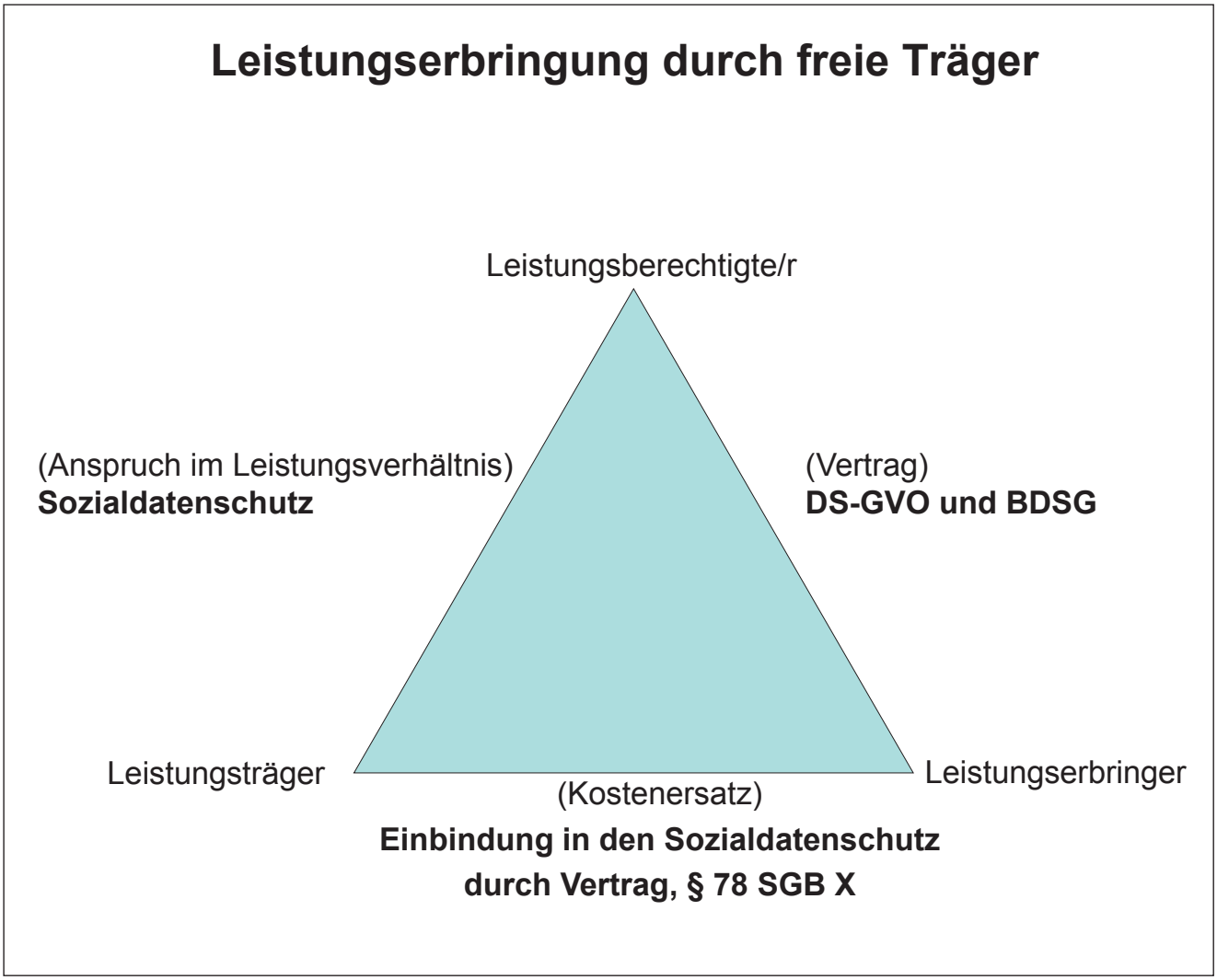
In diesen drei Rechtsverhältnissen ist auch der Datenschutz zu beachten. Aufgrund des informationellen Selbstbestimmungsrechts bleibt der/die Anspruchsberechtigte weiter Herr/Frau über seine personenbezogenen Daten.

Überwiegend dient dieses sozialrechtliche Dreieck der Gestaltung der Rechtsbeziehungen bei Leistungserbringung durch soziale Organisationen. Daneben erbringen soziale Organisationen im Rahmen ihrer satzungsgemäßen Aufgabenerfüllung auch

Leistungen in anderen rechtlichen Konstellationen. So sind z. B. die Empfänger von Pflege- und Altenhilfeleistungen oft auch (teilweise) Selbstzahler. Traditionell werden Beratungsangebote und offene Hilfen durch staatliche Zuwendungen finanziert. Im Zuwendungsbereich werden keine einzelnen Leistungen durch die Leistungsträger bezahlt. Diese unterstützen soziale Organisationen in deren Aufgabenerfüllung durch die Gewährung von Finanzhilfen. Die Aufgabenerfüllung durch die sozialen Organisationen geschieht dann nicht in dem oben beschriebenen sozialrechtlichen Dreieck der Leistungserbringung. Datenschutzfragen sind deshalb im Zuwendungsbereich und auch bei Selbstfinanzierung durch die Leistungsempfänger nochmals anders zu bewerten.

Soweit die Leistungserbringung aber in dem sozialrechtlichen Dreieck erfolgt, sind die einschlägigen Sozialgesetzbücher anwendbar. Es gilt dann das Sozialgeheimnis, das in § 35 SGB I niedergelegt ist. Es bestimmt, dass jeder Mensch Anspruch darauf hat, dass seine Sozialdaten von Leistungsträgern nicht unbefugt bearbeitet werden.

Unter Berücksichtigung des Datenschutzes stellt sich das sozialrechtliche Dreieck der Leistungserbringung wie folgt dar:



15.3 Einbindung der sozialen Organisationen in den Sozialdatenschutz

Der Sozialdatenschutz betrifft das Sozialleistungsverhältnis zwischen Sozialleistungsträger und dem anspruchsberechtigten Bürger. Adressaten des Sozialgeheimnisses sind die Leistungsträger, die im SGB I abschließend aufgezählt sind. Die privatrechtlich organisierten sozialen Organisationen gehören dazu nicht. Sie sind somit nicht primär Adressaten des Sozialdatenschutzes. Der Datenschutz bei sozialen Organisationen richtet sich vorrangig nach der DS-GVO und dem BDSG.

Aber: Soziale Organisationen als Leistungserbringer im Rahmen des oben beschriebenen sozialrechtlichen Dreiecks der Leistungserbringung werden in den Sozialdatenschutz einbezogen.

§ 78 SGB X bestimmt die **Zweckbindung und Geheimhaltungspflicht eines Dritten, an den Daten durch einen Sozialleistungsträger im Rahmen eines Sozialleistungsverhältnisses übermittelt werden.** Solche „Dritte", denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, zu dem sie ihnen befugt übermittelt worden sind.

„Dritte" in diesem Sinne sind die sozialen Organisationen.

Außerdem ist eine Übermittlung von Sozialdaten an eine nicht öffentliche Stelle (soziale Organisationen) nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle (Sozialleistungsträger) verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dem sie ihr übermittelt werden.

Diese Verpflichtung ist in der Regel vertraglich festgeschrieben in den **Leistungs- bzw. Versorgungsverträgen**, die zwischen den Sozialleistungsträgern und den privatrechtlich organisierten Sozialleistungserbringern (soziale Organisationen) abgeschlossen werden.

Im Jugendhilfebereich gelten dann nochmals strengere Anforderungen an die Einbindung nicht öffentlicher Stellen in den Sozialdatenschutz.

Ausgangspunkt des Sozialdatenschutzes ist das beschriebene **Sozialgeheimnis** des § 35 SGB I. Die wichtigsten Regelungen zum Sozialdatenschutz enthält dann das **SGB X - Sozialverwaltungsverfahren und Sozialgeheimnis**. Ergänzend sind die einzelnen Sozialleistungsgesetze heranzuziehen. Diese enthalten auch Sozialdatenschutzregelungen. Meistens geht es dabei aber um Einschränkungen im Sozialdatenschutz und erweiternde Erlaubnisse der Datenverarbeitung, z. B. auch der Datenweitergabe an andere Sozialleistungsträger.

Der Sozialdatenschutz betrifft privatrechtlich organisierte soziale Organisationen in zweierlei Hinsicht. Zum einen verstehen sich diese Organisationen immer auch als **Anwälte ihrer Klienten**. Sie beraten ihre Klienten immer umfassend in sozialen Fragen, zu denen auch Fragen des Sozialdatenschutzes gehören. Zum anderen sind sie, wie beschrieben, als Sozialleistungserbringer in den sozialen Datenschutz einbezogen.

15.4 Ausführung der Sozialleistungen und Sozialdatenschutz

In dem Sozialleistungsverhältnis zwischen (öffentlichen) Sozialleistungsträger und anspruchsberechtigten Bürger sind verschiedene **Eckpunkte** der Leistungserbringung von Bedeutung.

- Der Schutz der Sozialdaten wird durch das **Sozialgeheimnis** garantiert. Beantragen Bürger Sozialleistungen, so müssen sie der ausführenden Behörde aber auch gewisse Informationen zukommen lassen, damit diese prüfen kann, ob überhaupt ein Sozialleistungsanspruch besteht. Es gibt Informations- Auskunft- und **Mitwirkungspflichten**. Letztere sind im SGB I in den §§ 60–67 geregelt. So kann z. B. die datenschutzrechtlich notwendige **Einwilligung** der betroffenen Personen in die Datenerhebung bei Dritten Teil der Mitwirkungspflichten sein.

- Als weiterer Eckpunkt im Sozialleistungsverhältnis ist der **Grundsatz der Amtsermittlung** von Bedeutung. Der Sozialleistungsträger ermittelt den Sachverhalt von Amts wegen (§ 20 SGB X). Hierzu hat er verschiedene Instrumente, z. B. die Zeugenbefragung.

- Schließlich ist ein (öffentlicher) Sozialleistungsträger verpflichtet, **Leistungen schnell und umfassend zu gewähren**. Gemäß § 1 Abs. 2 SGB I sollen Sozialleistungen rechtzeitig und ausreichend zur Verfügung stehen.

Das Zusammenspiel dieser verschiedenen Regelungsbereiche und Eckpunkte soll am folgenden Beispiel verdeutlicht werden:

Fallbeispiel

Familie A (zwei Erwachsene, zwei Kinder) bezieht Leistungen nach dem SGB II. Die Familie bewohnt ein angemietetes Haus in L. Für die Mietkaution hatte die Familie 2.600,00 € an den Vermieter gezahlt. Ein Umzug war notwendig. Das zuständige Jobcenter stimmte dem Umzug zu. Für das neue Haus musste eine Mietkaution in Höhe von 1.700,00 € geleistet werden. Familie A beantragte beim Jobcenter ein Darlehen für diese Mietkaution. Weiterhin beantragte sie die Ausstattung mit zwei Kleiderschränken für die Kinder. Dies wurde damit begründet, dass in der alten Wohnung Einbauschränke vorhanden gewesen wären. ***Das Jobcenter erkundigte sich schriftlich und telefonisch bei dem alten Vermieter, ob die seinerzeit gezahlte Mietkaution zurückgezahlt worden wäre. Außerdem wollte es von dem alten Vermieter wissen, ob in seinem Haus tatsächlich Einbauschränke vorhanden seien. Der Vermieter bestätigte letzteres und teilte mit, dass die Mietkaution in Höhe von 2.000,00 € an die Familie zurückgezahlt worden wäre.*** *Das Darlehen für die Mietkaution wurde vom Jobcenter daraufhin abgelehnt. Leistungen zur Anschaffung von zwei Kleiderschränken wurden bewilligt.*

Dieser Beispielsfall lehnt sich an das Urteil des Bundessozialgerichts vom 25.01.2012 - B 14 AS 65/11 R.

Es ging in dem Verfahren unter anderem um die Frage, ob das Jobcenter durch seine Anfrage an den früheren Vermieter das Sozialgeheimnis verletzte. Dies bejahte das Bundessozialgericht: Informationen seien bei den Leistungsberechtigten zu erheben. Der Amtsermittlungsgrundsatz rechtfertige in der Regel nicht, dass ohne Einwilligung der betroffenen Person Dritte befragt werden. Hierdurch werde das informationelle Selbstbestimmungsrecht der Betroffenen Person verletzt. Der Dritte (hier: früherer Vermieter) erfahre von dem Sozialleistungsbezug der betroffenen Person. Allerdings hätte das Jobcenter von dem Leistungsempfänger verlangen können, dass dieser seine Einwilligung in die Befragung des alten Vermieters erteilt. Eine Verweigerung dieser Einwilligung wäre möglicherweise ein Verstoß gegen die Mitwirkungspflichten gewesen. Ein solcher Verstoß könnte zum Entzug der Sozialleistungen führen.

15.5 Weitergabe von Sozialdaten – Übermittlungsbefugnisse der Sozialbehörden

Grundsätzlich geht das Sozialrecht davon aus, dass es für einen Bürger, der eine Sozialleistung begehrt, nicht von Bedeutung ist, von welchem Sozialleistungsträger er die Sozialleistungen letztlich bekommt. So kennt das Sozialleistungsrecht sehr weitgehende Übermittlungsbefugnisse zwischen den einzelnen Sozialbehörden – mit dem Ziel, die notwendigen Sozialleistungen umfassend und zeitnah zur Verfügung zu stellen. Weitere Übermittlungsbefugnisse ergeben sich z. B. bei der Verletzung von Unterhaltspflichten und beim Versorgungsausgleich oder für die Durchführung eines Strafverfahrens.

In den einzelnen Sozialleistungsgesetzen werden diese datenschutzrechtlichen Übermittlungsbefugnisse dann verfahrensrechtlich ausgestaltet. So sind z. B. Sozialleistungsanträge, die bei einem unzuständigen Leistungsträger oder bei einer nicht zuständigen Kommunalen Stelle eingehen, unverzüglich an den zuständigen Leistungsträger weiterzuleiten. Im Rehabilitationsrecht gilt § 14 SGB IX. Werden Leistungen zur Teilhabe beantragt, so hat der Rehabilitationsträger grundsätzlich innerhalb von zwei bis drei Wochen seine Zuständigkeit zu klären. Sieht er seine Zuständigkeit nicht als gegeben an, so muss er innerhalb der genannten Frist den Antrag an den zuständigen Rehabilitationsträger weiterleiten. Tut er dies nicht, so wird er formal zuständig.

Bei all diesen Regelungen wird das Recht der antragstellenden Bürger, selbst über ihre personenbezogene Daten (Sozialdaten) zu verfügen, eingeschränkt. Diese Einschränkung findet aber ihre Rechtfertigung darin, dass Sozialleistungen umfassend und rechtzeitig zur Verfügung gestellt werden sollen. Wichtig sei, dass im Bedarfsfall die Leistung sofort zur Verfügung stünde. Die hieraus resultierenden Einschränkungen im Sozialdatenschutz nimmt der Gesetzgeber in der Abwägung hin.

15.6 Datenweitergabe zwischen öffentlichen Sozialleistungsträgern und sozialen Organisationen als Leistungserbringer

Für die Einbindung sozialer Organisationen in den Sozialdatenschutz gilt § 78 SGB X. Die Datenverarbeitung von Sozialdaten, die ein öffentlicher Leistungsträger der sozialen Organisation zur Verfügung stellt, ist zweckgebunden. Der öffentliche Leistungsträger hat den nicht öffentlichen Leistungserbringer (soziale Organisation) durch Vertragsgestaltung auf diese Zweckbindung zu verpflichten.

Außerdem bestimmt § 78 SGB X, dass die soziale Organisation ihre Beschäftigten, die in der Datenverarbeitung tätig sind, auf die Einhaltung der Pflichten aus dem Sozialdatenschutz hinzuweisen hat. Anders als in der DS-GVO und dem neuen BDSG bleibt somit die bisher im Datenschutz allgemein geregelte Pflicht der sozialen Organisation, ihre **Beschäftigten auf das Sozialgeheimnis zu verpflichten**, im Sozialdatenschutz erhalten.

Im Übrigen werden privatrechtlich gefasste soziale Organisationen durch die Einbeziehung in das sozialrechtliche Dreieck der Leistungserbringung nicht Teil des Sozialleistungsverhältnisses. Ausnahmsweise ist dies der Fall, wenn die soziale Organisation mit einer öffentlichen Aufgabe beliehen wird und somit auch hoheitlich im Auftrag des Leistungsträgers handelt. Ein Beispiel hierfür ist die Inobhutnahme im Bereich der Jugendhilfe.

Grundsätzlich werden soziale Organisationen aber nicht in das Sozialleistungsverhältnis einbezogen. Dies bedeutet, dass für sie auch nicht die sehr weitreichenden Befugnisse zur Übermittlung von personenbezogenen Daten, die im Sozialdatenschutz bestehen, gelten.

Aus dem Sozialleistungsverhältnis ergeben sich keine Pflichten zur Datenweitergabe für soziale Organisationen an den öffentlichen Leistungsträger.

Sollen Daten zwischen einer sozialen Organisation und einem öffentlichen Leistungsträger ausgetauscht werden, so ist dies nur zulässig, wenn die betroffene Person diesem Datenaustausch zustimmt. Erforderlich ist deshalb eine wirksame **Einwilligung** speziell für diesen Datenaustausch.

Siehe Beispiel im Anhang A5, Seite 44

15.7 Schutzpflichten des Staates vs. Informationelles Selbstbestimmungsrecht

Im Zusammenhang mit dem Sozialdatenschutz sind weitere Schutz- und Eingriffsrechte öffentlicher Träger von Bedeutung. Der Sozialdatenschutz steht nicht isoliert in der Rechtsordnung, sondern ist immer im Zusammenspiel mit anderen, ihn zum Teil verdrängenden Eingriffsrechten zu betrachten. In sozialen Organisationen können Schutzaufgaben öffentlicher Stellen von Bedeutung sein. So hat die staatliche **Heimaufsicht** oder auch der **Medizinische Dienst der Krankenkassen** Prüfrechte bei sozialen Organisationen. Diese Prüfrechte schränken im Interesse der betroffenen Personen deren Rechte ein z. B. das Informationelle Selbstbestimmungsrecht. In Wohneinrichtungen kann z. B. auch das Recht auf Unverletzlichkeit der Wohnung eingeschränkt sein.

Anhang

Abkürzungen

Abs.	Absatz
AGB	Allgemeine Geschäftsbedingungen
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BFD	Bundesfreiwilligendienst
DS-GVO	Datenschutz - Grundverordnung
DSK	Datenschutzkonferenz der Länder
FSJ	Freiwilliges Soziales Jahr
KUG	Kunsturhebergesetz
SGB	Sozialgesetzbuch
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
ZPO	Zivilprozessordnung

Literaturempfehlungen

Folgende Broschüre wird im Text an verschiedenen Stellen in der Handreichung zitiert:

Sonderdruck „Erste Hilfe", Seite …

– Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine, Das Sofortmaßnahmen-Paket; 63 Seiten, Geheftet C.H.BECK ISBN 978-3-406-71662-1, **seit kurzem auch als ebook erhältlich.**

– J. M. Leuchtner, Datenschutz in der Pflege, Ein Praxishandbuch, mit Mustertexten und Arbeitshilfen., 2018. Buch. XVII, 177 S. Mit Mustertexten und Arbeitshilfen online; medhochzwei Verlag ISBN 978-3-86216-343-4

– Dr. Grit Reimann, Betrieblicher Datenschutz Schritt für Schritt – gemäß EU-Datenschutzgrundverordnung, Lösungen zur praktischen Umsetzung, Textbeispiele, Musterformulare, Checklisten; DIN e.V. (Herausgeber), Beuth (Verlag) 2. Auflage erscheint ca. im Mai 2018, 166 Seiten ISBN 978-3-410-27981-5

– Eugen Ehmann / Silvia C. Bauer / Andreas Grimme; Datenschutzlexikon von A-Z, Das praktische Datenschutz Lexikon im handlichen Taschenformat; WEKA MEDIA (Verlag), 03/2017 – **Neuauflage abwarten!**

Links

– www.bfdi.bund.de – Bundesbeauftragter für den Datenschutz und Informationsfreiheit

Auf dieser Seite befinden sich die sog. Kurzpapiere der Datenschutzkonferenz der Länder (DSK, die in komprimierter Form Informationen zu zentralen Themen zur Verfügung stellen.

– https://dsgvo-gesetz.de/bdsg-neu/
Hier sind die beiden wesentlichen Rechtsgrundlagen DS-GVO und das neue BDSG zu finden.

– www.lfd.niedersachsen.de
Die Broschüre „Datenschutz im Verein" der Landesbeauftragten für Datenschutz Niedersachsen (Stand 2013) mit Arbeitshilfen und Merkblättern soll demnächst aktualisiert auf den Internetseiten der Niedersächsischen Landesbeauftragten zur Verfügung stehen.

– www.baden-wuerttemberg.datenschutz.de
Der Landesbeauftrage für Datenschutz Baden Württemberg hat eine ausführliche aktuelle Orientierungshilfe für Vereine herausgegeben "Datenschutz im Verein nach der Datenschutzgrundverordnung DS-GVO".

Beispiele, Muster, Checkliste

A1 – Kodex zur Nutzung von digitalen Medien und insbesondere Messenger-Diensten bei Fröbel inkl. Bestätigungserklärung

FRÖBEL
Kompetenz für Kinder

KODEX ZUR NUTZUNG VON DIGITALEN MEDIEN UND INSBESONDERE MESSENGER-DIENSTEN BEI FRÖBEL

© Renate Alf

Die Mitarbeiterinnen und Mitarbeiter der FRÖBEL-Gruppe haben gemeinsam ein Unternehmensleitbild entwickelt, das neben anderem ausdrückt, wofür FRÖBEL heute und in Zukunft steht: „Kompetenz für Kinder".

In unserem Leitbild spielen die **Rechte der Kinder** eine zentrale Rolle, sie sind das Fundament unserer Arbeit. Für alle Familien bei FRÖBEL sind wir ein zuverlässiger Partner in der Erfüllung und Wahrung dieser Rechte.

In dem Wissen, dass ein verantwortungsbewusster und kritischer Umgang mit neuen Medien die möglichen Risiken, die im Zusammenhang mit der Mediennutzung stehen, bedenken und die einschlägigen Gesetze und Rechtsvorschriften beachten muss, soll dieser Kodex der Belegschaft, aber auch den Kindern und ihren Eltern beim täglichen Umgang mit digitalen Medien eine Handlungsgrundlage und Rechtssicherheit bieten.

Ziel ist es, einen verantwortungsbewussten und kritischen Umgang mit digitalen Medien (Fotos, Videos und andere personenbezogene Daten) **und Messenger-Diensten** (Facebook, WhatsApp etc.) **zu erreichen**. Für alltägliche Kommunikationssituationen vereinbaren wir auf der Grundlage geltender Rechtsvorschriften („Datenschutz") und der Allgemeinen Geschäftsbedingungen der Dienstanbieter eine Selbstverpflichtung zu **Möglichkeiten und Grenzen der digitalen Kommunikation in den Einrichtungen**.

Mit dieser Selbstverpflichtung beachten wir Persönlichkeitsrechte der Kinder und ihrer Familien ebenso wie die unserer Mitarbeiterinnen und Mitarbeiter. Der Kodex weist uns den Weg zwischen (emotionaler) Nähe und professioneller Distanz im Verhältnis von pädagogischen Fachkräften zu den Eltern.

Digitale Medien sind aus unserem Alltag nicht mehr wegzudenken, sie eröffnen ungeahnte Wege der modernen Kommunikation, wie die Möglichkeit, Informationen parallel mit vielen anderen teilen zu können oder auch mit Freunden in der Ferne einen intensiven Kontakt zu halten. Wie auch in den persönlichen Kontakten unterscheiden wir in der digitalen Welt zwischen dienstlicher und privater Kommunikation. Digitale Medien nicht nur zu konsumieren, sondern vor allem kreativ und innovativ im Rahmen der täglichen Bildungsarbeit mit Kindern einzusetzen, eröffnet neue Wege des Lernens, die wir gezielt und verantwortungsvoll beschreiten wollen.

Dem Kodex liegt ein Arbeitspapier mit Praxisbeispielen bei. Es gibt Hinweise auf konkrete Fragestellungen in Ihrem beruflichen Alltag und die entsprechende Lösung im Sinne unseres digitalen Kodex. Die Regelungen zur Nutzung digitaler Medien werden darüber hinaus in der Betriebsvereinbarung „Gesamtbetriebsvereinbarung über die Nutzung Internet, Intranet und E-Mail – elektronische Kommunikation" festgehalten.

UNSERE REGELN ZUM UMGANG MIT DIGITALEN MEDIEN

1 Aktive Nutzung von digitalen Medien – auch im pädagogischen Alltag

Uns ist es wichtig, dass Kinder einen sinnvollen und bereichernden Umgang mit digitalen Medien lernen. Die aktive Nutzung von digitalen Medien sehen wir als Bereicherung unserer Kommunikation an, die uns neue Zugänge zu Informationen eröffnet und zum Teil noch ungeahnte Möglichkeiten des Forschens und der Kreativität schafft.

- Wir setzen digitale Medien nur dann ein, wenn damit ein pädagogischer Mehrwert für das Kind (oder eine Gruppe von Kindern) verbunden ist und es dabei aktiv tätig wird.
- Damit grenzen wir uns bewusst von einem passiven Medienkonsum ab. Der reine Konsum von Medien (z. B. im Fall von Computerspielen) findet bei FRÖBEL nicht statt.
- Uns ist es wichtig, über unser Verständnis eines pädagogisch wertvollen Einsatzes der digitalen Medien auch mit den Eltern ins Gespräch zu kommen und sie in an diesem Prozess zu beteiligen.

2 Nutzung privater Mobiltelefone im Dienst

- Wir nutzen während der Betreuung der Kinder grundsätzlich keine privaten Handys für persönliche Angelegenheiten, ebenso erledigen wir keine privaten Anliegen während der Dienstzeiten.
- Es gibt begründete individuelle Ausnahmefälle, in denen die Nutzung privater Mobiltelefone unerlässlich erscheint. Diese Ausnahmefälle sind im Team vereinbart und werden vorab mit der Leitung abgesprochen.
- Grundsätzlich gibt es in der Einrichtung die Möglichkeit, über das Einrichtungstelefon in absoluten Notfällen erreichbar zu sein.

3 Elternkommunikation mittels digitaler Medien

Für die Kommunikation mit Eltern nutzen wir dienstliche Kommunikationswege. Zum Schutz unserer Privatsphäre, aber auch zur Wahrung einer professionellen Distanz achten wir auf eine strikte Trennung zwischen privater und dienstlicher Kommunikation. Eltern sind trotz aller familiennahen Kontakte letztlich unsere Kunden.

- Wir nutzen zur dienstlichen Kommunikation mit Eltern ausschließlich Telefonnummern oder E-Mail-Adressen, die FRÖBEL dafür zur Verfügung stellt.
- Wir entscheiden mit Bedacht, den Eltern unsere privaten Telefonnummern und E-Mail-Adressen herauszugeben. Die privaten Kontaktdaten unserer Kolleginnen und Kollegen teilen wir nicht mit. Denn mit der Herausgabe privater Handynummern haben Eltern auch Zugriff auf etwaige Chatprofile bei Messenger-Diensten, ohne dass wir hiervon Kenntnis erlangen.
- Die privaten Telefonnummern und E-Mail-Adressen werden Eltern untereinander grundsätzlich nicht bekannt gemacht. Sollten wir mit einer E-Mail-Nachricht mehrere Empfänger erreichen wollen, stehen zur Beachtung des Datenschutzes alle Empfängeradressen im Feld Blind Carbon Copy (BCC).

FRÖBEL
Kompetenz für Kinder

4 Private Kommunikation in sozialen Netzwerken

Private Informationen (Fotos, Kommentare) sind für viele von uns selbstverständlich, aber auch für alle Menschen in einem sozialen Netzwerk sichtbar, wenn man diese Sichtbarkeit nicht bewusst einschränkt. Viele Eltern und Teammitglieder haben Zugriff auf öffentliche Internetplattformen, wie zum Beispiel Facebook.

- Deshalb gehen wir in der Kommunikation über solche Plattformen sorgfältig mit unseren personenbezogenen Daten um und nutzen gegebenenfalls vorhandene Möglichkeiten, um die Einsehbarkeit einzuschränken.
- Freundschaftseinladungen von Eltern nehmen wir nur nach gründlicher Überlegung an, zum Beispiel, wenn wir selbst Eltern eines in der Einrichtung betreuten Kindes sind oder bereits unabhängig vom Betreuungsverhältnis private Beziehungen bestanden oder bestehen. Denn es ist uns bewusst, dass wir oder auch die Eltern über diese Netzwerke womöglich Informationen erhalten, die uns aktuell oder später in Konfliktsituationen bringen könnten.
- Wie auch sonst äußern wir uns in privaten Internetplattformen über FRÖBEL und pädagogische Themen im Sinne unseres Leitbildes und nicht rufschädigend.

5 Dienstliche Nutzung von Messenger-Diensten

Messenger-Dienste (z. B. WhatsApp, Viper, Threema, Signal) erfüllen aufgrund ihrer Allgemeinen Geschäftsbedingungen nicht die Voraussetzungen für eine rechtssichere digitale Kommunikation. Eine rechtssichere Kommunikation ist für uns jedoch unter Beachtung der Persönlichkeitsrechte, des Datenschutzes sowie unseres Anspruchs an eine professionelle Kommunikation mit Eltern zwingend geboten.

- Wir beachten, dass eine Kommunikation über Messenger-Dienste kein offizieller Dienstweg für den Kontakt zu Arbeitgeber, Kollegen und Kolleginnen und Familien ist.
- Die Versendung von Informationen, personenbezogenen Daten, Fotos und Videos, insbesondere von Kindern, ist über derartige Messenger-Dienste nicht möglich, selbst wenn die Eltern dies einvernehmlich wünschen. (Andere Möglichkeiten werden derzeit geprüft.)

6 Foto-, Video- und Sprachaufnahmen

Bei allen Foto-, Video- und Sprachaufnahmen, die bei FRÖBEL entstehen, beachten wir das uneingeschränkte Persönlichkeitsrecht („Recht am eigenen Bild“) einer jeden Person, ob Kind, Angehöriger oder Angehörige, Kollege oder Kollegin. Fotos von Dritten dürfen nach der aktuellen Gesetzeslage und Rechtsprechung nur bei Vorhandensein einer schriftlichen Genehmigung der fotografierten Person, bei Kindern die der Eltern, veröffentlicht werden. Das Einstellen von Fotos, Sprachaufnahmen oder Videos in

FRÖBEL
Kompetenz für Kinder

geschlossenen Benutzergruppen von Messenger-Diensten oder in geschlossenen Gruppen in sozialen Medien wie Facebook ist nach aktueller Rechtsprechung selbst beim Vorliegen einer schriftlichen Einwilligung verboten.

- Alle benutzten Aufnahmegeräte und Speichermedien sind ausschließlich von FRÖBEL bereitgestellt worden, und keinesfalls kommt das private Handy zum Einsatz.
- Wir beachten, dass Eltern für ihre Kinder entscheiden, zu welchem Zweck Aufnahmen von ihrem Kind gemacht, verwendet und verteilt werden dürfen („Fotoerlaubnis").
- Wir beachten, dass auch unsere Mitarbeiterinnen und Mitarbeiter für Aufnahmen, die von ihnen gemacht werden, und für deren Verwendung ihr Einverständnis geben müssen.
- Bei Aufnahmen, die durch betriebsfremde Personen getätigt werden (z. B. externe Fotografen), stellen wir sicher, dass nur Bilder von Personen auf dem Speichermedium bleiben, für die eine entsprechende Genehmigung vorliegt.

7 Eltern als Nutzer von Smartphones, Handys und Kameras

In Fällen der Nutzung von Smart- oder Mobiltelefonen in den Einrichtungen durch Eltern ist es uns im Einzelnen grundsätzlich nicht möglich, das Vorliegen einer Fotoerlaubnis anderer Kinder und der Mitarbeiterinnen und Mitarbeiter im Blick zu behalten. Eltern, die in der Einrichtung fotografieren oder filmen, ohne das Einverständnis der abgebildeten Personen, geraten in Konflikt mit den allgemeinen Rechtsvorschriften. FRÖBEL macht die Eltern über verschiedene Wege auf diesen Sachverhalt aufmerksam.

- Während Kitafesten und Elternabenden müssen die Eltern bei Foto- und Videoaufnahmen darauf achten, dass sie nur ihr eigenes Kind dokumentieren. Deshalb fordern wir Eltern aktiv dazu auf, den Moment mit ihrem Kind ungetrübt und ungeteilt zu genießen und auf die Nutzung elektronischer Endgeräte möglichst zu verzichten.
- Wir appellieren an die Eltern, dass auch sie in der Bring- und Abholsituation der Kinder die Nutzung von Mobiltelefonen möglichst einschränken, um sich gut auf ihr Kind konzentrieren zu können.
- Wir sensibilisieren die Eltern, bei ihren Kindern darauf hinzuwirken, bei der Benutzung digitaler Medien die Rechte der anderen zu respektieren.

www.froebel-gruppe.de

Seite 4

FRÖBEL
Kompetenz für Kinder

BESTÄTIGUNG DER KENNTNISNAHME

Der „Kodex zu digitalen Medien und insbesondere Messenger-Diensten bei FRÖBEL“ in der Fassung vom Oktober 2017 und die „Gesamtbetriebsvereinbarung über die Nutzung Internet, Intranet und E-Mail – elektronische Kommunikation“ vom 30. November 2017 werden den Mitarbeiterinnen und Mitarbeitern ausgehändigt. Alle Mitarbeiterinnen und Mitarbeiter bestätigen mit ihrer Unterschrift, den Erhalt beider Dokumente.

Ich habe den „Kodex zur Nutzung von digitalen Medien und insbesondere Messenger-Diensten bei FRÖBEL“ (Fassung vom Oktober 2017) sowie die „Gesamtbetriebsvereinbarung über die Nutzung Internet, Intranet und E-Mail – elektronische Kommunikation“ (vom 30.11.2017) erhalten.

Name der Mitarbeiter*in

Einrichtung/Abteilung

Ort, Datum

Unterschrift

www.froebel-gruppe.de

A2 – Information und Verpflichtung von Beschäftigten auf den Datenschutz der Bayerischen Landesaufsicht für den Datenschutz

Bayerisches Landesamt für Datenschutzaufsicht

Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO

Herausgeber:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27
91522 Ansbach

Telefon: (0981) 53 - 1300
Telefax: (0981) 53 - 981300
E-Mail: poststelle@lda.bayern.de
Webseite: www.lda.bayern.de

Stand: Februar 2018

1. Was regelt die Datenschutz-Grundverordnung (DS-GVO)?

Nach Art. 29 DS-GVO dürfen Beschäftigte eines Verantwortlichen (eines Unternehmens, eines Vereins, eines Verbands, eines Selbstständigen, einer Behörde usw.) oder eines Auftragsverarbeiters personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen oder Auftragsverarbeiters verarbeiten, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor.

Ergänzend dazu regelt Art. 32 Abs. 4 DS-GVO, dass der Verantwortliche oder Auftragsverarbeiter Schritte unternehmen muss, um sicherzustellen, dass ihnen unterstellte Personen (insbesondere ihre Beschäftigten), die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten (es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor). Für den Fall der Auftragsverarbeitung bestimmt Art. 28 Abs. 3 Satz 2 lit. b DS-GVO, dass der Auftragsverarbeiter gewährleisten muss, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben (soweit sie nicht einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen; dies gilt z.B. für privatärztliche, steuerberaterliche oder anwaltliche Verrechnungsstellen).

Selbst wenn nach dem Wortlaut der DS-GVO nur die Beschäftigten eines Auftragsverarbeiters zu „verpflichten“ sind, trifft inhaltlich diese „verpflichtende Unterrichtung“ (im Folgenden: Verpflichtung) auch die Verantwortlichen und ihre Beschäftigten. Wie Verantwortliche diese gesetzliche Verpflichtung umsetzen (und ggfls. der Aufsichtsbehörde nachweisen) ist nicht verbindlich geregelt. Es wird empfohlen, dies mit einem entsprechenden Dokument zu tun. Ein Muster für eine solche Verpflichtung finden Sie in Anlage.

2. Zu was soll verpflichtet werden?

Die Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen ist ein wichtiger Bestandteil der Maßnahmen, damit ein Verantwortlicher (siehe Art. 5 Abs. 2 und Art. 24 Abs. 1 DS-GVO) oder ein Auftragsverarbeiter (siehe Art. 28 Abs. 3 Satz 1 DS-GVO) die Einhaltung der Grundsätze der DS-GVO sicherstellen und nachweisen kann („Rechenschaftspflicht“). Diese Grundsätze der DS-GVO, festgelegt in Art. 5 Abs. 1 DS-GVO, beinhalten im Wesentlichen folgende Pflichten:

Personenbezogene Daten müssen

a) auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist;

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

3. Wer muss verpflichtet werden?

Der Kreis der zu verpflichtenden Personen (die DS-GVO spricht insoweit von „unterstellten natürlichen Personen“) ist aufgrund der Bedeutung dieser Regelung weit auszulegen. Insbesondere sind ergänzend zum regulären Mitarbeiterstamm auch Auszubildende, Praktikanten, Leiharbeiter und ehrenamtlich Tätige mit einzubeziehen.

4. Wann muss die Verpflichtung erfolgen?

Die Verpflichtung muss bei der Aufnahme der Tätigkeit erfolgen. Sie sollte daher möglichst (spätestens) am ersten Arbeitstag vorgenommen werden.

5. Wie muss eine Verpflichtung erfolgen?

Zuständig für die Verpflichtung ist die Unternehmensleitung, der Inhaber einer Firma oder ein von diesen Beauftragter. Selbst wenn, wie oben ausgeführt, die DS-GVO keine bestimmte Form der Verpflichtung vorschreibt, sollte schon aus Nachweisgründen ein spezielles Formular verwendet werden, wobei die Verpflichtung schriftlich oder in einem elektronischen Format erfolgen kann.

Zur Verpflichtung gehört auch eine Belehrung über die sich ergebenden Pflichten. Die Beschäftigten müssen darüber informiert werden, was sie in datenschutzrechtlicher Hinsicht bei ihrer täglichen Arbeit beachten müssen, möglichst anhand typischer Fälle. Mit der Verpflichtung nach der DS-GVO können auch andere Geheimhaltungsvereinbarungen kombiniert werden, z. B. zum Betriebs-, Telekommunikations- oder Steuergeheimnis. Aus Nachweisgründen im Rahmen der Rechenschaftspflicht nach der DS-GVO ist es wichtig, die Verpflichtung ausreichend zu dokumentieren.

6. Reicht die einmalige datenschutzrechtliche Verpflichtung?

Zur laufenden Sensibilisierung der Beschäftigten für Fragen des Datenschutzes empfiehlt es sich, ab und zu im Rahmen von Schulungen oder in schriftlichen Hinweisen, z. B. in der Betriebszeitung, daran zu erinnern, dass die Beschäftigten verpflichtet worden sind und welche Bedeutung dieser Verpflichtung zukommt. Wenn ein Arbeitsplatzwechsel im Unternehmen erfolgt, der mit einem Aufgabenwechsel verbunden ist, sollte dies immer auch zum Anlass genommen werden, die Verpflichtung anzupassen bzw. zu erneuern.

Anlage/Musterbeispiel für eine schriftliche Verpflichtung:

Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Frau/Herr

wurde darauf verpflichtet, dass es untersagt ist, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen[1]:

Personenbezogene Daten müssen

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

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.
Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

_____	_____	_____
Ort, Datum	Unterschrift des Verpflichteten	Unterschrift des Verantwortlichen

[1] Der Inhalt der Verpflichtung ist im Einzelfall anzupassen. So können bestimmte Aufgaben und Tätigkeiten zusätzliche Unterrichtungen erfordern, etwa zum Beschäftigten- oder Sozialdatenschutz, zum Telekommunikationsgeheimnis usw.

A2a – Verpflichtung von Beschäftigen auf die Schweigepflicht nach § 203 StGB, besondere Gemeinhaltungspflichten, Sozialdatenschutz

2a - Verpflichtung auf § 203 StGB, besondere Gemeinhaltungspflichten, Sozialdatenschutz

Beispiel Frauenhaus)

Der besondere Zweck des Frauenhauses (Gewährung eines anonymen Aufenthaltes, Beratung und Unterstützung) oder der Beratungsstelle (Beratung und Unterstützung) erfordert einen besonders sorgfältigen Umgang mit den Informationen, die Sie im Rahmen Ihrer Tätigkeit von den aufgenommenen Frauen und ihren Kindern erfahren.

1. Verpflichtung auf die berufliche Schweigeplicht nach § 203 StGB

Vertrauliche Informationen, die Sie im Rahmen Ihrer Berufsausübung von den Bewohnerinnen erfahren, unterliegen der Schweigeplicht gemäß § 203 StGB. Eine Weitergabe darf nur erfolgen, wenn eine wirksame Entbindungserklärung von der Schweigeplicht vorliegt. Ein Verstoß hiergegen ist strafbar.

2. Verpflichtung auf die vertragliche Plicht zur Geheimhaltung des Aufenthaltsortes der Bewohnerinnen

Der Zweck des Frauenhauses, den Bewohnerinnen einen anonymen Aufenthalt zu gewähren, erfordert hinsichtlich der Geheimhaltung des Aufenthaltes der Frauen in der Schutzeinrichtung eine besondere Aufmerksamkeit. Diese Geheimhaltungsplicht ist besonders zu beachten. Wenn im konkreten Gefährdungsfall erforderlich, ist eine gesonderte Zustimmung zur Weitergabe des Aufenthaltsortes unter Angabe des Zwecks bei der Betroffenen einzuholen.

3. Verpflichtung zur Wahrung des Sozialgeheimnisses nach § 35 SGB I

Werden der Unterstützungseinrichtung Sozialdaten übermittelt, dürfen diese nur zu dem jeweils rechtmäßigen Zweck, zu dem sie übermittelt wurden, verarbeitet und genutzt werden, § 78 Abs. 1 SGB X. Die Plicht zur Wahrung des Sozialgeheimnisses bleibt auch nach Beendigung der Beschäftigung bestehen. Verstöße gegen das Sozialgeheimnis können mit Bußgeld, Freiheits- oder Geldstrafe geahndet werden.

_____

Datum/Ort

_____

Vorname, Name, Geburtsdatum

A3 – Verzeichnis zu Verarbeitungstätigkeiten für Verantwortliche, bereitgestellt vom Bundesbeauftragten für den Datenschutz und Informationsfreiheit

Verzeichnis von Verarbeitungstätigkeiten **Verantwortlicher** **gem. Artikel 30 Abs. 1 DSGVO**	Vorblatt

Angaben zum Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Internet-Adresse

Angaben zum ggf. gemeinsam mit diesem Verantwortlichen

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zum Vertreter des Verantwortlichen

Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc.

Name

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift)

* sofern gem. Artikel 37 DS-GVO benannt

Anrede Titel

Name, Vorname

Straße

Postleitzahl

Ort

Telefon

E-Mail-Adresse

Verarbeitungstätigkeit: Benennung: _____	**lfd. Nr.:** _____
Datum der Einführung:	Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)	
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)	
Optional: Name des eingesetzten Verfahrens	
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	☐ Beschäftigte ☐ Interessenten ☐ Lieferanten ☐ Kunden ☐ Patienten ☐ ☐ ☐
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	☐ ☐ ☐ Besondere Kategorien personenbezogener Daten (Art. 9): ☐

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	☐ intern (Zugriffsberechtigte) Abteilung/ Funktion
	☐ extern Empfängerkategorie
	☐ Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☐ Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	☐ Drittland oder internationale Organisation (Name)
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g) *Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten“, Ziff. 6.7. und 6.8*

…… …… ……
Verantwortlicher Datum Unterschrift

A4 – Einwilligung mit Schweigepflichtsentbindung – Beratungsstelle

Muster – Einwilligung mit Schweigepflichtsentbindung

Beratungsstelle … des XY e.V.

Einwilligungserklärung gemäß Art. 6 Abs. 1 a) EU-DS-GVO mit Schweigepflichtsentbindung

Name, Vorname _____Anschrift: _____geb. am: _____

Ich bin über die in der Beratungsstelle ……. verwendeten Dokumentationssysteme und die berufliche Schweigepflicht der Mitarbeiter/-innen **informiert**. Mit der elektronischen Erfassung meiner Daten und deren Verarbeitung innerhalb der Beratungsstelle für Beratungs- und Betreuungszwecke bin ich einverstanden. Innerhalb der Beratungsstelle können meine Daten ausgetauscht werden. Ich befreie die mich beratenden Mitarbeiter/-innen für diesen Zweck von der **Schweigepflicht**. Mir ist bekannt, dass ich jederzeit einen Anspruch auf **Auskunft** über die von mir erhobenen Daten habe, dass ich der Speicherung meiner Daten für die Zukunft **widersprechen** kann und diese daraufhin in personenbezogener Form gelöscht werden. Eine Weitergabe meiner Daten an Einzelpersonen, Arbeitgeber, Institutionen oder Behörden findet ohne meine Zustimmung nicht statt.

Datum, Ort, Unterschrift

A5 – Einwilligung zum Datenschutz – Frauenunterstützungseinrichtung

Einwilligungserklärung zum Datenschutz

Name, Vorname _____

Geboren am _____

Ich bin über die in der Unterstützungseinrichtung _____ in _____

verwendeten Dokumentations- und Informationssysteme informiert worden.

Hiermit willige ich in die Erfassung und Verarbeitung meiner personenbezogenen Daten und deren Nutzung, soweit diese erforderlich sind, zum Zwecke der Erfüllung der Geschäftszwecke der Unterstützungseinrichtung (insbesondere Sicherstellung der Unterkunft, Beratung und Unterstützung) ein.

Die Einwilligung bezieht sich ausdrücklich auch auf besonders schützenswerte Kategorien von Daten im Sinne des Art. 9 Abs. 1 DS-GVO, soweit sie zu den genannten Zwecken erforderlich sind.

Die Einwilligung gilt auch für eine ggf. erforderliche Weitergabe sog. „Rahmendaten“ des Unterstützungsprozesses wie Beginn, Ende, Abbruch und Fortsetzung, an einen Kostenträger zur Sicherstellung der Finanzierung der Hilfen.

Stehen der Weitergabe schutzwürdige Interessen meiner Person oder meiner Kinder entgegen, hat die Weitergabe zu unterbleiben.

Ergibt sich aus einer Übermittlung von Aufenthaltsdaten eine besondere Gefährdung für die mich und meine Familie, ist eine gesonderte Einwilligung für die beabsichtigte Weitergabe einzuholen.

In jedem Fall ist für eine etwaige Weitergabe von vertraulichen Inhalten aus dem Beratungs- und Unterstützungsprozess an Dritte eine gesonderte Zustimmung meinerseits einzuholen.

In bin darauf hingewiesen worden, dass ich die Einwilligung jederzeit widerrufen kann.

_____

Datum/Ort

_____

Unterschrift

A6 – Entbindung von der Schweigepflicht nach § 203 StGB

Entbindung von der Schweigepflicht

Name, Vorname _____

Anschrift

Geboren am _____

Ich bin informiert worden über die bestehende berufliche Schweigeplicht gemäß § 203 StGB der Beschäftigten der Unterstützungseinrichtung.

Hiermit entbinde ich die Mitarbeiter/-innen der Unterstützungseinrichtung

_____

in _____

von der Schweigeplicht gemäß § 203 StGB ausschließlich für folgende Sachverhalte

a) soweit dies im Haus/Team zur Beratung und Unterstützung der Bewohnerinnen und ihrer Kinder, erforderlich ist, gegenseitig

b) im Falle einer Supervision gegenüber dem/der Supervisor/in

c) im Falle, dass Schutz- und Unterstützungsmaßnahmen sichergestellt werden müssen, gegenüber anderen kooperierenden Einrichtungen und Stellen, die die Bewohnerin und ihre Kinder unterstützen, z. B. im Falle von Weitervermittlung

d) zur Unterstützung bei der Geltendmachung von Sozialleistungsansprüchen gegenüber dem Sozialleistungsträger, soweit es um die sog. „Rahmendaten“ der Maßnahme ……(z.B.„psychosoziale Betreuung“, bitte konkret benennen) (Beginn, Ende, Abbruch, Fortsetzung und Erläuterung des Fortsetzungsbedarfes) geht,

e) _____

f) _____

(Nicht zutreffendes bitte streichen)

Ich weiß, dass ich diese Erklärung ohne Angaben von Gründen jederzeit für die Zukunft widerrufen kann.

_____

Datum/Ort

_____

Unterschrift

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Checkliste zur Überprüfung der Informationssicherheit

Die Fragen im Fragenkatalog sind so gestellt, dass „ja“ Antworten erwartet werden. Werden Fragen mit Teilweise“ oder „Nein“ beantwortet, ist dies zu erklären. Es ist dann zu entscheiden, ob Maßnahmen eingeleitet werden müssen, um einen systemkonformen Zustand zu erreichen, oder ob zu einem späteren Zeitpunkt die Überprüfung zu wiederhole ist.

Bestellung eines Datenschutzbeauftragten
Gesetzlich erforderlich?
☐ Ja ☐ Nein Kommentar

Ist ein Datenschutzbeauftragter bestellt?
☐ Ja ☐ Nein Kommentar

Ist die erforderliche Fachkunde des Datenschutzbeauftragten nachgewiesen?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Ist die „Zuverlässigkeit“ des Datenschutzbeauftragten gewährleistet („keine Interessenskonflikte“)?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Ist der Datenschutzbeauftragte direkt der Geschäftsleitung unterstellt und in die Informationsprozesse im Unternehmen, insbesondere bei der Planung und Anschaffung von Informationstechnologie eingebunden?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Hat der Datenschutzbeauftragte die Möglichkeit, sich regelmäßig fortzubilden (Schulung, Literatur etc.)
☐ Ja ☐ Nein Kommentar

Verpflichtung auf das Datengeheimnis
Sind alle Beschäftigten auf das Datengeheimnis i.S.d. Art. 5 DSGVO, Art. 24 DSGVO verpflichtet worden?
☐ Ja ☐ Nein Kommentar

Werden auch externe Mitarbeiter (z.B. Reinigungskräfte, Werkstudenten u.ä.) auf das Datengeheimnis verpflichtet?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Gibt es ein **Verzeichnis von Verarbeitungstätigkeiten** nach Art. 30 DSGVO, mit denen personenbezogene Daten verarbeitet werden (ehemals „internes Verfahrensverzeichnis“ / Verarbeitungsübersicht)
☐ Ja ☐ Nein Kommentar

Ist gewährleistet, dass bei der Anschaffung/Änderung neuer IT, bei der Gestaltung neuer IT-Abläufe oder der Änderung im IT-Bereich eine Anpassung der Verarbeitungsübersicht erfolgt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

^

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Meldepflicht
Erfolgt die Meldung bei der geschäftsmäßigen Übermittlung von Daten oder für Zwecke der Markt- und Meinungsforschung)?
☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Falls ja, wurde die Meldepflicht eingehalten?
☐ Ja ☐ Teilweise ☐ Nein

Datenschutz-Folgenabschätzung (ehemals Vorabkontrolle**)**
Werden Datenschutz-Folgenabschätzungen (Art. 33 DSGVO) vor der Einführung von automatisierten Datenverarbeitungsvorgängen durchgeführt, wenn diese Vorgänge besondere Risiken für die Rechte der Betroffenen beinhalten?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

IT-Sicherheit
Technische und organisatorische Maßnahmen gemäß Art. 32 EU-DSGVO und § 58 Abs. 3 des deutschen Ausführungsgesetz zur Datenschutz-Grundverordnung
Gibt es schriftliche Dokumentation der technischen und organisatorischen Maßnahmen i.S.d. Art. 32 EU-DSGVO
☐ Ja ☐ Nein Anmerkung

Gibt es eine Leitlinie zur Informationssicherheit?
☐ Ja ☐ Nein Anmerkung

Gibt es eine IT-Richtlinie (o.ä.) für Beschäftigte, aus der sich ergibt, ob und wie diese IT-Systeme im Unternehmen verwenden dürfen?
☐ Ja ☐ Nein Anmerkung

Gibt es eine Risiko- und Schwachstellenanalyse im Hinblick auf Räume, IT-Systeme, IT-Applikationen und Netzwerkkomponenten?
☐ Ja ☐ Nein Anmerkung

Gibt es einen Notfallplan?
☐ Ja ☐ Nein Anmerkung

Compliance bei der Verarbeitung von Daten
Direkterhebung
Werden personenbezogene Daten grundsätzlich selbst beim Betroffenen erhoben?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Festlegung von Verantwortlichkeiten und Regelungen für den Computer- und Interneteinsatz

Sind Verantwortliche für die IT-Sicherheit und den Datenschutz in allen Untergliederungen (Abteilungen/Bereichen/Standorten etc.) benannt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind deren Befugnisse festgelegt worden?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Gibt es Regeln über:

Dokumentation von IT-Verfahren, Software, IT-Konfiguration?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Zutrittsberechtigungen (Räume)
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Zugangsberechtigungen (Computer)
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Zugriffsberechtigungen (Dateien)
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Gebrauch von Passwörtern
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Datenübertragung
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Schutz gegen Schadsoftware
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Datenträgertransport
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Datensicherung
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Datenarchivierung
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Datenschutz
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Notfallvorsorge
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wartungs- und Reparaturarbeiten
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Vorgehensweise bei Verletzung der Sicherheitspolitik (s. auch Informationspflicht bei „Datenpannen“
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Information der Mitarbeiter/-innen

Sind diese Regelungen den betroffenen Mitarbeiter/-innen in geeigneter Weise bekannt gegeben worden?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Ist die Bekanntgabe dokumentiert worden?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden alle Regelungen in der aktuellen Fassung an einer Stelle vorgehalten, so dass sie bei einem berechtigten Interesse zugänglich sind?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden die Regelungen regelmäßig aktualisiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Dokumentation von IT-Verfahren, Software, IT-Konfiguration

Einspielung neuer und freigegebener Software

Gibt es ein Software-Freigabe-Verfahren, welche Software wann von wem verwendet werden darf?
☐ Ja ☐ Nein Kommentar

Gibt es ein Verzeichnis der freigegebenen und eingesetzten Software (Software-Bestandsverzeichnis)?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Ist ein Nutzungsverbot nicht freigegebener Software schriftlich fixiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind alle Mitarbeiter/-innen über das Nutzungsverbot unterrichtet?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wurde in regelmäßigen Abständen an das Nutzungsverbot erinnert?
☐ Ja ☐ Nein Kommentar

Überprüfung des Software-Bestandes

Werden regelmäßig Überprüfungen des Software-Bestandes durchgeführt (mind. Jährlich)?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird der Software-Bestand komplett überprüft?
☐ Ja ☐ Nein Kommentar

Wird der Software-Bestand stichprobenartig überprüft?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden Verstöße angemessen geahndet?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden die Ergebnisse der Überprüfung nachvollziehbar dokumentiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden Veränderungen in den grundsätzlichen Konfigurationen des IT-Systems dokumentiert?
☐ Ja ☐ Nein Kommentar

Vergabe von Zutrittsberechtigungen

Sind die schutzbedürftigen Räume eines Gebäudes bestimmt worden?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird die Dokumentation schutzbedürftiger Räume und zutrittsberechtigter Personen regelmäßig aktualisiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Ich für jeden dieser Räume festgelegt worden, welche Person welche Zugriffsrechte hat?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird die Vergabe und Zurücknahme von Zutrittsrechten dokumentiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden alle Zutrittsberechtigungen kontrolliert (durch Personen und technisch)?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Existiert eine Regelung zur Schlüsselverwaltung?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Existiert ein Schließplan für alle Schlüssel der Gebäudeteile der Organisation?
☐ Ja ☐ Nein Kommentar

Wird die Ausgabe der Schlüssel dokumentiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird regelmäßig (mindestens jährlich) kontrolliert, ob die Dokumentation über ausgegebene Schlüssel noch aktuell ist?
☐ Ja ☐ Nein Kommentar

Vergabe von Zugangsberechtigungen

Werden die Vergabe sowie der Einzug von Zugangsberechtigungen und Zugangsmitteln dokumentiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird die Dokumentation über Vergabe sowie Einzug von Zugangsberechtigungen und Zugangsmitteln regelmäßig (mindestens einmal im Jahr) aktualisiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden personelle und aufgabenbezogene Änderungen unverzüglich berücksichtigt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden die Benutzer/-innen bei der Vergabe von Zugangsberechtigungen über die Handhabung von Zugangs- und Authentifikationsmitteln (z.B. Umgang mit Chipkarten, Passworthandhabung) informiert?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden Zugangsberechtigungen bei längerer Abwesenheit von Benutzern gespeist?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird die Nutzung von Zugangsberechtigungen protokolliert?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird dies regelmäßig ausgewertet?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Der Arbeitsplatz

Sind die Mitarbeiter/-innen dazu angehalten worden, bei längerer Abwesenheit die Arbeitsplätze „aufgeräumt" zu hinterlassen?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind die Mitrbeiter/-innen dazu angehalten worden, bei kürzerer Abwesenheit die Arbeitsräume zu schließen?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind die Mitarbeiter/-innen dazu angehalten worden, bei kürzerer Abwesenheit die Monitore „dunkel" zu schalten?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Vergabe von Zugriffsrechten

Ist für jedes IT-System bzw. jede IT-Anwendung festgelegt worden, welche Personen welches Zugriffsrecht (Schreiben, Lesen, Gesperrt, Löschen etc.) haben?

☐ Ja ☐ Nein Kommentar

Liegen aktuell Dokumentationen der vergebenen Zugriffsrechte vor?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind Zugriffsrechte für Benutzergruppen definiert worden?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Regelung des Passwortgebrauchs

Existiert eine Regelung zum Passwortgebrauch?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden darin konkrete Anforderungen an Passwörter gestellt?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

- an Erratbarkeit, Passwortgüte?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

- an die Passwortlänge (mind. 8 Zeichen?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

- an die Geheimhaltung?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

- an die Hinterlegung?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

- an die Häufigkeit des Passwortwechsel (mindestens alle drei Monate)?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind die Benutzer/-innen über diese Regelung bzw. den korrekten Umgang mit Passwörtern unterrichtet worden?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Ist sichergestellt, dass für den Zugriff auf alle IT-Systeme bzw. IT-Anwendungen ein Passwort erforderlich ist?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden sofort nach Inbetriebnahme von IT-Systemen oder Benutzerwechsel individuelle Passwörter vergeben?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Datenübertragung / Datenaustausch mit externen Partnern

Wurden Regelungen zum Austausch von Daten definiert? (Wege über das Internet, mit CD, USB-Stick, in Papierform, welche Verantworlichkeiten sind damit verbunden?)

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wurden dabei entsprechende Sicherheitsstufen der Informationssicherung vereinbart?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wurden Datenaustauschformate (DOC, RTF, TXT, PDF, HTML) mit den Partnern vereinbart?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wurden die anzuwendenden Verschlüsselungen der Daten jeweils eingerichtet, getestet und angewandt?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird sichergestellt, dass in Abwesenheit von Mitarbeitenden dieser Datenaustausch bei Bedarf weiter stattfinden kann?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird eine Sicherungskopie für auszutauschende Datenträger erstellt?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Schutz gegen Schadsoftware

Werden Schadsoftwareschutzprogramme auf allen Servern eingesetzt?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden Schadsoftwareschutzprogramme auf allen PC eingesetzt?
☐ Ja ☐ Nein Kommentar

Werden die Schadsoftwareschutzprogramme in regelmäßigen Abständen durch neue Versionen ersetzt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind die Verantwortlichkeiten zur Aktualisierung geregelt und werden die Aktualisierungen auf den jeweiligen Systemen dokumentiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wurden Verhaltensregeln des Schadsoftwareschutzes und der Reaktion im Schadensfall allen betroffenen Mitarbeiter/-innen bekannt gemacht?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind die zuständigen Personen in der Lage im Bedarfsfall angemessene Schritte durchzuführen?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Datenträgerverwaltung

Gibt es eine Datenträgerverwaltung?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Existieren Bestandsverzeichnisse für Datenträger?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Liegt ein aktuelles Ordnerverzeichnis vor?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Gibt es klare Regelungen für die Kennzeichnung der Datenträger?
☐ Ja ☐ Nein Kommentar

Werden regelmäßig (mind. halbjährlich) Vollständigkeitskontrollen des Datenträgerbestandes vorgenommen?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden alle Datenträger sachgerecht aufbewahrt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind alle Datenträger vor unbefugtem Zugriff geschützt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Ist der Umgang mit alten oder unbrauchbaren Datenträgern so geregelt, dass sie auf sicherem Wege vernichtet werden?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Datensicherung

Wird eine regelmäßige Datensicherung der Daten auf allen Systemen durchgeführt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind die entsprechenden Verantwortlichkeiten für die Durchführung der Datensicherung geregelt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird die Datensicherung protokolliert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden die Sicherungsmedien an einem sicheren Ort (z.B. Fernsicherung) aufbewahrt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden Tests für die Rücksicherung regelmäßig durchgeführt?
☐ Ja ☐ Nein Kommentar

Datenarchivierung

Wird in regelmäßigen Abständen eine Datenarchivierung der jeweiligen Arbeitsbereiche durchgeführt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Sind die Befugnisse und Verantwortlichkeiten für die Archivierung verbindlich geregelt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden die archivierten Daten an einem sicheren Ort aufbewahrt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Ist verbindlich geregelt, wer auf die ausgelagerten Daten Zugriff bekommt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Entsorgung von schützenswerten Betriebsmitteln

Existiert eine verbindliche Regelung zur Entsorgung von schützenswerten Betriebsmitteln?
☐ Ja ☐ Nein Kommentar

Werden in dieser Regelung alle schützenswerten Betriebsmittel genannt?
☐ Ja ☐ Nein Kommentar

Werden mit der Entsorgung beauftragte Unternehmen auf die Einhaltung erforderlicher Sicherheitsmaßnahmen verpflichtet?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird der Entsorgungsvorgang regelmäßig (mindestens jährlich) kontrolliert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Datenschutz

Liegen Regelungen zur Umsetzung und zur Beachtung des Datenschutzes vor?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wurden die Arbeitsbereiche mit besonderen Datenschutzbestimmungen definiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird eine Vorabkontrolle bei besonders schutzwürdigen Daten nach Art. 9 – EU-DSGVO durchgeführt?

☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird das Verzeichnis der Verfahren geführt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Gibt es ein Risikomanagement bezüglich des Datenschutzes?
☐ Ja ☐ Nein Kommentar

Gibt es ein IT- Sicherheitskonzept?
☐ Ja ☐ Nein Kommentar

Werden Änderungen an der Dateiorganisation vollständig protokolliert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird die Durchführung von Datensicherungsmaßnahmen protokolliert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werde alle Versuch des unbefugten Einloggens und Überschreitens von Befugnissen protokolliert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Kennen die Mitarbeiter/-innen die Möglichkeiten der eingesetzten Protokollierung und dessen Verwendung?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Notfallvorsorge

Ist eine Übersicht der Verfügbarkeitsanforderungen vorhanden?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Existiert eine Untersuchung interner und externer Auseichmöglichkeiten?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Gibt es Regelungen für den Notfall für ausgewählte Schadensereignisse?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Existiert ein Alarmierungsplan?
☐ Ja ☐ Nein Kommentar

Wurden entsprechende Notfallübungen bereits durchgeführt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden die Partner/Landesverbände/Mitgliedsorganisationen über entsprechende Notfallpläne informiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Regelungen für Wartungs- und Reparaturarbeiten

Sind Verantwortliche für die Beauftragung von Wartungs- und Reparaturarbeiten der IT-Architektur und Komponenten benannt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden dabei durch Externe im Haus durchgeführte Wartungs- und Reparaturarbeiten durch fachkundige Mitarbeiter/-innen beaufsichtigt?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Wird nach Abschluss der Wartungs- und Reparaturarbeiten überprüft, ob der Wartungsauftrag vollständig und erfolgreich ausgeführt wurde?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Gibt es besondere Regelungen, wenn auf von Wartungs- und Reparaturarbeiten betroffenen Speichermedien besonders sensible Daten gespeichert sind?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden nach Abschluss von Wartungs- und Reparaturarbeiten in den betroffenen Bereichen die Passwörter geändert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden die durchgeführten Wartungs- und Reparaturarbeiten dokumentiert (Umfang, Ergebnis, Zeitpunkt, etc.)?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Werden die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der erforderlichen IT- Sicherheitsmaßnahmen verpflichte?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Reaktion auf Verletzung der Sicherheitspolitik

Ist die Vorgehensweise bei Verdacht auf Verletzung der IT- Sicherheitspolitik klar definiert?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Ist festgelegt worden, welche Reaktion auf Verletzung der IT- Sicherheitspolitik erfolgen soll?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

Ist jemand in der Organisation benannt worden, der für Kontakte mit anderen Organisationen (Mitgliedsorganisationen, Partnerorganisationen) verantwortlich ist, um diese Informationen über aufgetretene Sicherheitslücken weiterzugeben?
☐ Ja ☐ Teilweise ☐ Nein Kommentar

IT+DS-Sicherheitscheck gemäß Art. 24 und 32 DS-GVO der EU-Datenschutzgrundverordnung

Rechtsgrundlage
Wird Sorge dafür getragen, dass personenbezogene Daten grundsätzlich nur dann verarbeitet werden, wenn dies zur Erbringung vertraglicher Leistungen erforderlich, im Rahmen einer Interessenabwägung zulässig ist oder eine Einwilligung des Betroffenen vorliegt?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Einwilligung
Wird bei der Verwendung von Einwilligungen darauf geachtet, dass der Betroffene über Zweck, Art und Umfang der Verwendung der von ihm freiwillig angegebenen Daten informiert wird?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Kann der Betroffene die Einwilligungserklärung auch ohne Fachkenntnisse verstehen und erkennen, dass die Einwilligung freiwillig ist und ggf. welche Konsequenzen eine Nichterteilung einer Einwilligung hat?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Ist im Falle eines Widerrufs der Einwilligung gewährleistet, dass die betroffenen personenbezogenen Daten nicht weiter verwendet werden?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Ist bei der Einholung der Einwilligung die Trennung von ggf. verschiedenen Zwecken der Datenverarbeitung gewährleistet (keine konkludierende Einwilligung)?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Auftragsdatenverarbeitung
Gibt es eine Übersicht aller Dienstleister/Lieferanten, die entweder Daten im Auftrag der Gesamtorganisation verarbeiten oder IT- Systeme warten und pflegen?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Wird Sorge dafür getragen, dass bei den Auftragnehmern/Dienstleistern ein Auftragsdatenverarbeitungsvertrag geschlossen wurde (und wird)?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Gibt es ein Muster für einen Auftragsdatenverarbeitungsvertrag im Unternehmen?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Wird Sorge dafür getragen, dass der Auftragnehmer bei einer Auftragsdatenverarbeitung vor Vertragsschluss im Hinblick auf die getroffenen IT- Sicherheitsmaßnahmen kontrolliert wird?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Ist gewährleistet, dass Auftragnehmer regelmäßig (grundsätzlich 1x jährlich) im Hinblick auf Änderungen im Bereich der IT- Sicherheit kontrolliert werden?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Informationspflicht bei „Datenpannen“ (Art. 4 Nr.12 DSGVO)
Werden Verfahren, mit denen besondere Arten personenbezogener Daten, personenbezogene Daten, die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder personenbezogene Daten zu Bank- oder Kreditkartenkonten gesondert intern gekennzeichnet bzw. überwacht?
☐ Ja ☐ Nein Anmerkung ☐ Anforderung nicht anwendbar/relevant

Wird Sorge dafür getragen, dass im Falle einer unbefugten Kenntnisnahme durch Dritte von Daten, die nach Art. 4 Nr.12 DSGVO geschützt sind, sofort der Datenschutzbeauftragte informiert wird?
☐ Ja ☐ Nein Anmerkung ☐ Anforderung nicht anwendbar/relevant

Gibt es einen Ablaufplan für den Fall einer Datenpanne?
☐ Ja ☐ Nein Anmerkung ☐ Anforderung nicht anwendbar/relevant

Betroffenenrechte
Gibt es ein „Betroffenenmanagement“ dahingehend, dass Betroffene, die ihre Betroffenenrechte i.S.d. Art. 15 EU-DSGVO geltend machen, direkten Kontakt zum Datenschutzbeauftragten erhalten?
☐ Ja ☐ Nein Anmerkung

Werden Auskunftsersuchen von Betroffenen kurzfristig und vollständig beantwortet?
☐ Ja ☐ Nein Anmerkung

Gibt es ein Löschkonzept im Unternehmen, das Regelfristen für die Löschung von Daten vorsieht?
☐ Ja ☐ Nein Anmerkung

Internet / E-Mail

Internetseite
Gibt es für die Internetseite des Unternehmens gesonderte Datenschutzhinweise, die von jeder Seite der Internetseite aus erreichbar sind (nicht nur im „Impressum“)
☐ Ja ☐ Nein Anmerkung

Wird über Webanalyse-Software informiert?
☐ Ja ☐ Nein Anmerkung ☐ Anforderung nicht anwendbar/relevant

Wird über die Verwendung und das „Blocken“ von Cookies informiert?
☐ Ja ☐ Nein Anmerkung ☐ Anforderung nicht anwendbar/relevant

Wird über Tracking-Pixel oder sonstige verwendete Methoden für Zwecke der Werbung oder des Marketings informiert und werden Möglichkeiten für ein „Opt-Out“ angezeigt?
☐ Ja ☐ Nein Anmerkung ☐ Anforderung nicht anwendbar/relevant

E-Mail-Marketing
Wird ein E-Mail-Newsletter angeboten?
☐ Ja ☐ Nein

Werden Newsletter-Abonnenten hinreichend über Zweck, Art und Umfang der Datenverarbeitung beim E-Mail-Newsletter informiert (insbes. Tracking von „Open Rates“, „Click Rates“ u.Ä.)?
☐ Ja ☐ Nein Anmerkung ☐ Anforderung nicht anwendbar/relevant

Gibt es ausreichende vertragliche Regelungen zur Verwendung der Daten durch einen externen Newsletter-Dienstleister (z.B. Auftragsdatenverarbeitungsvertrag, Einwilligung etc.)
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Private Internet-/E-Mail-Nutzung im Unternehmen
Gibt es eine unternehmensinterne Regelung zur privaten Nutzung des Internets im Unternehmen
☐ Ja ☐ Nein Anmerkung

Gibt es eine unternehmensinterne Regelung zur privaten Nutzung von E-Mail im Unternehmen
☐ Ja ☐ Nein Anmerkung

Betriebsrat
Gibt es einen Betriebsrat im Unternehmen
☐ Ja ☐ Nein

Gibt eine Übersicht der Betriebsvereinbarungen, die Regelungen zum Umgang mit personenbezogenen Daten enthalten?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Datenflüsse in der Gesamtorganisation
Gehören mehrere Organisationen zur Gesamtorganisation („Konzerngesetz der EU“)?
☐ Ja ☐ Nein

Falls ja, gibt es Regelungen zur gemeinsamen Nutzung von Daten oder IT-Infrastrukturen im Unternehmen?
☐ Ja ☐ Nein ☐ Anforderung nicht anwendbar/relevant

Grenzüberschreitender Datenverkehr
Werden Daten des Unternehmens im Ausland verarbeitet bzw. in das Ausland übermittelt?
☐ Ja ☐ Nein Anmerkung

Europäische Union / EWR
Ist im Falle einer Verarbeitung von Daten in anderen EU-Mitgliedsstaaten oder EWR-Staaten gewährleistet, dass eine Rechtsgrundlage für die Verwendung im Ausland besteht (z. B. Art. 9 Abs. 3 EU-DSGVO) und ggf. Auftragsdatenverarbeitung)?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

„Drittstaaten“
Werden Daten in „Drittstaaten“ verwendet bzw. dorthin übermittelt?
☐ Ja ☐ Nein

Ist von der Organisation geprüft worden, ob es für die Übermittlung in den Drittstaat bzw. die Verarbeitung dort eine Rechtsgrundlage in der EU-DSGVO (Art. 44ff.) gibt („erste Stufe“)?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Handelt es sich bei dem Drittstaat um einen Staat mit „angemessenen Datenschutzniveau“?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Gibt es eine Einwilligung des Betroffenen zur Übermittlung von personenbezogenen Daten an das Unternehmen in dem Drittstaat?
☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Ist mit dem Unternehmen in dem Drittstaat ein Vertrag auf Basis der EU-Standardvertragsklauseln geschlossen worden?

☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Ist bei einer Übertragung in die USA im Rahmen des EU-US Privacy Shield die Angemessenheit des Datenschutzniveaus festgestellt worden?

☐ Ja ☐ Nein Anmerkung | ☐ Anforderung nicht anwendbar/relevant

Stand: 08.02.2018