STUPS

STUDENTISCHES PROJEKT FÜR SOZIALE EINRICHTUNGEN E. V.

Datenschutz im Verein

Dieter Ruß i.A. des Vorstands

Inhaltsverzeichnis

1. Begriffsbestimmungen....3
2. Allgemein....4
3. Präambel....4
4. Datenschutz in der Vereinsverwaltung....4
Erhebung, Speicherung und Nutzung von Daten der Vereinsmitglieder....4
Datenschutzbeauftragter....5
Was muss der Verein beachten?....5
Weitergabe von Daten....6
Erhebung von Personaldaten der Beschäftigten des Vereins....7
Sperrung und Löschung von Daten....7
Weitergabe von Daten von Vereinsfunktionären (Vorstand)....8
5. Datenschutz beim Bauzug....9
6. Datenschutz in Kinderbetreuungseinrichtungen....10
Allgemeines....10
Aufnahme & Betreuungsvertrag....10
Foto-, Ton- und Viedoaufzeichnungen – Berichte über Beobachtungen....11
Elternlisten – Notfallnummern – Aushänge....12
Weitergabe von Daten an Dritte....12
Aufbewahrung der Daten....12
7. Datenschutz im Unithekle....13
Datenschutz für die Mitarbeiterschaft....13
Daten für Wochenendveranstaltungen....13
Datenschutz im Gastbetrieb....14
8. Der Verein im Internet – Online-Arbeit....14
Internet-Zugang und Email-Verkehr der Beschäftigten....14
Homepages....15

Social Media.....15
9. Betroffenen-Rechte.....16
Auskunfts- und Informationsrecht.....16
Recht auf Berichtigung.....17
Recht auf Löschung / Vergessenwerden.....17
Recht auf Einschränkung der Verarbeitung 18
Recht auf Datenübertragbarkeit 18
Widerspruchsrecht 18
10. Übersicht über Verarbeitungstätigkeiten.....18
11. Folgenabschätzung.....19

1. Begriffsbestimmungen

Personenbezogene Daten sind nicht nur die zur Identifizierung einer natürlichen Person erforderlichen Angaben, wie etwa Name, Anschrift und Geburtsdatum, sondern darüber hinaus sämtliche Informationen, die etwas über die persönlichen oder sachlichen Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener) aussagen (§ 3 Abs. 1 BDSG), wie beispielsweise Familienstand, Zahl der Kinder, Beruf, Telefonnummer, E-Mail-Adresse, Anschrift, Eigentums- oder Besitzverhältnisse, persönliche Interessen, Mitgliedschaft in Organisationen, Datum des Vereinsbeitritts, sportliche Leistungen, Platzierung bei einem Wettbewerb und dergleichen. Nicht vom Bundesdatenschutzgesetz geschützt werden Angaben über Verstorbene (beispielsweise in einem Nachruf für ein verstorbenes Vereinsmitglied im Vereinsblatt oder die Nennung auf einer Liste der Verstorbenen).

Erheben ist das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 3 BDSG), etwa mit Hilfe eines Aufnahmeformulars oder eines Anmeldeformulars für die Teilnahme an einem Wettbewerb oder einem Lehrgang oder durch den Ankauf von Adressdaten. Die Datenerhebung kann auch mündlich erfolgen (Befragung des Betroffenen).

Speichern ist das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung.

Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft.

Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken.

Löschen ist das Unkenntlichmachen gespeicherter personenbezogener Daten.

Nutzen ist jede sonstige Verwendung personenbezogener Daten (§ 3 Abs. 5 BDSG), insbesondere innerhalb des Vereins für die Verwaltung und Betreuung der Vereinsmitglieder. Darunter fällt etwa die Verwendung der postalischen Anschrift oder der E-Mail-Adresse von Vereinsmitgliedern zum Versand von Briefen oder der E-Mails durch Funktionsträger des Vereins. Eine Datennutzung liegt auch vor, wenn die Daten von einem Funktionsträger des Vereins an einen anderen desselben Vereins weitergegeben werden. Da der Empfänger hier nicht außerhalb des Vereins steht, sondern mit den anderen Funktionsträgern eine organisatorische Einheit bildet, handelt es sich nicht um eine Datenübermittlung.Eine Datennutzung ist auch dann gegeben, wenn der Verein seine Daten an eine Serviceeinrichtung weitergibt, damit diese die Daten der Vereinsmitglieder verwaltet. Dagegen stellt die Datenweitergabe an eigene Vereinsmitglieder oder einen Dachverband im Verhältnis zum Verein eine Datenübermittlung dar.

Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von digitalisierten oder in sonstiger Weise programmgesteuerten Datenverarbeitungsanlagen (§ 3 Abs. 2 Satz 1 BDSG).

Eine **nicht automatisierte** Datei ist jede nicht in einer elektronischen Datenverarbeitungsanlage erfasste Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen erschlossen und ausgewertet werden kann (§ 3 Abs. 2 Satz 2 BDSG). Umstritten ist, ob es sich bei Listen um „nicht automatisierte Dateien“ in diesem Sinne handelt. Nach dem Schutzzweck des Bundesdatenschutzgesetzes wird man im Zweifelsfall davon ausgehen müssen.

2. Allgemein

Das Bundesdatenschutzgesetz (BDSG) als zentrale Norm des Datenschutzes sieht vor, dass der Einzelne davor geschützt werden soll, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (§ 1 Absatz 1 BDSG). Personenbezogen – und damit schutzwürdig im Sinne des BDSG – sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person.
Mit der Erweiterung des Datenschutzgesetzes am 25.05.2018 wird die Datenschutzordnung von Stups e.V. erweitert. Diese Ordnung hat das Ziel in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen z.B. durch Auftraggeber im Rahmen der Auftragsverarbeitung genutzt werden. Dadurch soll die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) nicht nur gewährleistet, sondern auch der Nachweis der Einhaltung geschaffen werden.

3. Präambel

Stups e.V. ist ein gemeinnütziger Verein, der es sich zur Aufgabe gemacht hat der sozialen, kulturellen und wirtschaftlichen Betreuung von Studentinnen und Studenten der Hochschulregion Stuttgart zu dienen. Diesen Zweck erfüllt der Verein durch Schaffung und Unterhaltung von entsprechender Einrichtungen wie Kinderbetreuungseinrichtungen und die Unterhaltung einer studentischen Begegnungsstätte.
Im Zusammenhang dieser Tätigkeiten entstehen mehrere Kontaktpunkte mit sensiblen personenbezogen Daten, deren Erfassung, Verarbeitung, Nutzung, Weitergabe und Löschung im Folgenden für alle frei zugänglich eingeordnet werden soll.

4. Datenschutz in der Vereinsverwaltung

Erhebung, Speicherung und Nutzung von Daten der Vereinsmitglieder

Ein Verein darf aufgrund des § 28 Abs. 1 Satz 1 Nr. 1 BDSG beim Vereinseintritt (Aufnahmeantrag oder Beitrittserklärung) und während der Vereinsmitgliedschaft nur solche Daten von Mitgliedern erheben, die für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich sind. Damit dürfen alle Daten erhoben werden, die zur Verfolgung der Vereinsziele und für die Betreuung und Verwaltung der Mitglieder (wie etwa Name, Anschrift, in der Regel auch das Geburtsdatum, ferner Bankverbindung, Bankleitzahl und Kontonummer) erforderlich sind. Die Angabe von Telefonnummer und E-Mail-Adresse sollte dem Mitglied freigestellt werden.

Soll die Erhebung, Verarbeitung und Nutzung personenbezogener Daten aufgrund des § 28 BDSG (z.B. Übermittlung von Daten zur Wahrung berechtigter Interessen eines Dritten oder zur Abwehr von Gefahren bzw. zur Verfolgung von Straftaten) erfolgen, ist dies nur zulässig, wenn dem keine höherrangigen schutzwürdigen Interessen der Betroffenen entgegenstehen. Solche können wirtschaftliche und berufliche Belange ebenso sein, wie der Wunsch des Betroffenen, dass seine Privat-, Intim- und Vertraulichkeitssphäre gewahrt wird. Neumitglieder sollten beim Eintritt in den Verein danach gefragt werden, ob es derartige schutzwürdige Belange in ihrer Person gibt. Es ist aber durchaus auch möglich, später in einem Rundschreiben, im Vereinsblatt oder per E-Mail die Mitglieder aufzufordern, derartige Belange vorzubringen, wenn der Verein eine Datenverarbeitung aufgrund dieser Vorschriften beabsichtigt.

Für den Umgang mit Mitgliederdaten gilt, dass jeder Funktionsträger nur die für die Erfüllung seiner Aufgaben erforderlichen Mitgliederdaten kennen, verarbeiten oder nutzen darf. So darf etwa der

Vorstand auf alle Mitgliederdaten zugreifen, wenn er diese zur Aufgabenerledigung benötigt. Auch müssen der Vereinsgeschäftsstelle alle Mitgliederdaten regelmäßig für die Mitgliederverwaltung und -betreuung zur Verfügung stehen, während es in der Regel für den Kassierer genügt, wenn er die für den Einzug der Mitgliedsbeiträge relevanten Angaben (Name, Anschrift und Bankverbindung) kennt. Dabei dürfen die Daten grundsätzlich nur zur Verfolgung des Vereinszwecks bzw. zur Betreuung und Verwaltung von Mitgliedern genutzt werden (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Nur ausnahmsweise ist es möglich, diese Daten für sonstige berechtige Interessen des Vereins oder Dritter zu nutzen, vorausgesetzt, dem stehen keine schutzwürdigen Interessen der Vereinsmitglieder entgegen (§ 28 Abs. 1 Nr. 2 und Abs. 2 Nrn. 1 und 2.a) BDSG; s. o. Nr. 2.1).

Vereine haben regelmäßig ein erhebliches Interesse an der Mitglieder- und Spendenwerbung, um einen ausreichenden Mitgliederbestand und genügend finanzielle Mittel sicherzustellen. Die Daten seiner Vereinsmitglieder darf der Verein nur für Spendenaufrufe und für Werbung zur Erreichung der eigenen Ziele des Vereins nutzen (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Die Nutzung von Mitgliederdaten für die Werbung Dritter ist ohne Einwilligung der Mitglieder grundsätzlich nicht zulässig.

Datenschutzbeauftragter

Die Verpflichtung, personenbezogene Daten zu schützen, betrifft jeden Verein. Verantwortlich dafür ist der Vorstand. Wenn innerhalb eines Vereins mindestens 10 Personen ständig mit der Verarbeitung von Daten beschäftigt beschäftigt sind, muss er einen Datenschutzbeauftragten bestimmen. Dies ist bei Stups e.V. nicht zutreffend, denn in der Verwaltung für Vereins- und Abteilungsbelange sind maximal 6-8 Personen tätig (3 Personen in Verwaltung und Lohnbuchhaltung, 3-5 Personen in Verwaltung von Abteilungen). Dabei sind nur 2 Personen innerhalb der Vereinsverwaltung mit allen Daten aller Abteilungen in Kontakt, die restlichen Personen betreuen lediglich Daten der Bereiche, für die sie zuständig sind..

Da Stups e.V. keinen Datenschutzbeauftragten bestellen muss, hat der Vorstand sicherzustellen, das der Verein die Regeln des Datenschutzes einhält. Er muss dann selbst die entsprechenden Aufgaben wahrnehmen bzw. sie an Verwaltung oder Geschäftsführung delegieren und regelmäßig kontrollieren.

Unabhängig davon, ob ein Datenschutzbeauftragter zu bestellen ist oder nicht, müssen die Personen, die mit der Datenverarbeitung befasst sind, auf das Datengeheimnis verpflichtet werden (§ 5 BDSG). Für diesen Zweck dient sowohl diese Datenschutzordnung als auch eine interne Datenschutzrichtlinie, die alle Beteiligten über Rechte und Pflichten beim Umgang mit personenbezogenen Daten aufklärt und unterrichtet.

Was muss der Verein beachten?

Der Verein muss das „Datengeheimnis“ wahren. Er darf die gesammelten Daten somit nur im Rahmen des BDSG oder einer anderen Rechtsvorschrift nutzen. Die Satzung des Vereins ist keine „andere Rechtsvorschrift“ im Sinne des BDSG. Die gesetzlichen Datenschutzbestimmungen können also nicht per Satzung eingeschränkt oder außer Kraft gesetzt werden.

Die Zulässigkeit der Datenverarbeitung richtet sich nach § 28 BDSG. Danach ist ein Erheben, Speichern, Ändern oder Übermitteln personenbezogener Daten oder ihre Nutzung nur zulässig, wenn dies erforderlich ist, um den Vereinszweck zu erfüllen. Die Vereinsmitgliedschaft wird hier als „vertragsähnliches Vertrauensverhältnis“ angesehen.

Um seinen Zweck erfüllen zu können, müssen dem Verein zumindest „Korrespondenzdaten“ (Name und Anschrift) vorliegen. Sofern weitere Daten für die Vereinsarbeit erforderlich sind, dürfen auch diese erhoben werden (Beispiel: Kontodaten für den Lastschrifteinzug des Mitgliedsbeitrags). Es muss immer gewährleistet sein, dass der jeweils Betroffene über diesen Umstand unterrichtet

wird. Nach § 4 Absatz 3 BDSG ist der Betroffene über folgende Umstände zu informieren:

1. Die Identität der verantwortlichen Stelle (= der Verein).
2. Die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung.
3. Die Empfänger der Daten, soweit die Daten weitergeleitet werden und der Betroffene nicht mit einer Übermittlung zu rechnen hatte.
4. Das Recht, jederzeit Auskunft über den Umfang, die Art, die Verwendung oder die Löschung der erhobenen Daten zu erhalten.
5. Das Recht jederzeit Einspruch gegen die Erhebung personenbezogener Daten zu erheben.
6. Das Recht eine gegebene Einwilligungserklärung jederzeit widerrufen zu können.

(Näheres regelt „9. Betroffenen-Rechte“)

Bestehen eines Beschwerderechts

Bereits beim Eintritt wird eine Einverständnis vom Mitglied eingeholt. Diese unterscheidet sich optisch vom Beitrittsformular und besitzt ihre Grundlage innerhalb der Vereinssatzung.

Auszug aus der Satzung Stups e.V. (§4 Abs. 8):

(8) Im Rahmen der Mitgliederverwaltung werden von den Mitgliedern folgende Daten erhoben: Name, Vorname, Anschrift, Telefonnummer, Email-Adresse und Kontoverbindung. Diese Daten werden ausschließlich im Rahmen der Mitgliedschaft verarbeitet und gespeichert und für keine darüber hinaus gehenden Zwecke verwendet. Der Verein veröffentlicht Daten seiner Mitglieder nur, wenn der Gesamtvorstand einen entsprechenden Beschluss fasst, die Mitglieder darüber informiert wurden und diese der Veröffentlichung ihrer Daten nicht widersprochen haben.

Bei allen Formularen und Erhebungsbögen, die zur Datenerhebung eingesetzt werden, gilt die Hinweispflicht nach §4 Abs. 3 BDSG.

Beispiel:

Bei Vereinseintritt:

Ich erkläre mich hiermit einverstanden, das meine personenbezogenen Daten ausschließlich im Rahmen der Mitgliederverwaltung und Beitragserhebung gespeichert und genutzt werden. Jegliche Weitergabe, Veröffentlichung oder über die Mitgliederverwaltung hinaus gehende Nutzung meiner personenbezogenen Daten bedarf meiner schriftlichen Zustimmung.

Weitergabe von Daten

In Sonderfällen muss der Verein Daten von Mitgliedern weitergeben. Grundsätzlich richtet sich die Erlaubnis zur Weitergabe nach § 28 BDSG. Ob sie zulässig ist, hängt vom jeweiligen Empfängerkreis ab.

Bei der Weitergabe von Daten an andere Mitglieder sind die verschiedenen Interessen der Mitglieder gegeneinander abzuwägen. Ein typischer Anlass zur Weitergabe kann sich aus § 37 BGB ergeben. Danach besteht eine Verpflichtung, eine Mitgliederversammlung einzuberufen, wenn es ein bestimmter Teil der Mitglieder beantragt. Um hier ein entsprechendes (durch die Satzung vorgegebenes) Quorum erreichen zu können, werden die entsprechenden Anschriften bzw. Kontaktdaten benötigt. Gegen eine Weitergabe der Daten bestehen dabei keine Bedenken, da die Mitglieder ihre satzungsmäßigen Rechte verfolgen.

Viele Vereine verfügen über eine eigene Vereinszeitschrift oder einen Internetauftritt. Teilweise wird daneben noch ein Schaukasten oder ein schwarzes Brett genutzt. Hier stellt sich die Frage, ob personenbezogene Daten veröffentlicht werden können. Beispielsweise wird regelmäßig über Vereinsjubiläen oder Geburtstage informiert. Denkbar sind auch Leistungsergebnisse bei Wettbewerben oder ähnlichem. Um für den Vorstand Rechtssicherheit zu erlangen, empfiehlt es sich, einen entsprechenden Beschluss auf der Mitgliederversammlung herbeizuführen. Dieser

Beschluss sollte die geplante Veröffentlichung mitsamt den zu veröffentlichen Daten enthalten und auch auf die Möglichkeit hinweisen, dass jedem Mitglied ein Widerspruchsrecht zusteht.

Wird die Vereinszeitschrift auch an Nichtmitglieder versandt, empfiehlt es sich, von der Veröffentlichung der Daten Abstand zu nehmen. Das gilt erst recht für Veröffentlichungen auf der Vereinshomepage – zumindest wenn die Daten in den „öffentlichen Bereich“ eingestellt werden. Daten über Austritte aus dem Verein sollten nach Möglichkeit nicht veröffentlicht werden.

Erhebung von Personaldaten der Beschäftigten des Vereins

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses ist in § 32 BDSG gesondert geregelt. Als Beschäftigte i.S.v. § 32 BDSG sind die in § 3 Abs. 11 BDSG aufgeführten Personen, d.h. vor allem Arbeitnehmer, anzusehen. Soweit ein Verein daher Personen in einem abhängigen hauptamtlichen Beschäftigungsverhältnis beschäftigt (z.B. Mitarbeiter der Vereinsgeschäftsstelle) ist § 32 BDSG anwendbar. Danach dürfen personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses oder dessen Durchführung oder Beendigung erforderlich ist.

Sperrung und Löschung von Daten

Grundsätzlich dürfen personenbezogene Daten nur so lange gespeichert werden, wie ihre Kenntnis für die Erfüllung des Zwecks der Speicherung noch erforderlich ist (§ 35 Abs. 2 Satz 1 Nr. 3 BDSG). Der Verein muss daher festlegen, welche Arten von Daten bis zu welchem Ereignis (z.B. Austritt aus dem Verein, Tod) oder für welche Dauer gespeichert, verarbeitet und genutzt werden. Mit Erreichen des festgelegten Zeitpunkts müssen die Daten gesperrt werden (vgl. § 35 Abs. 3 Nr. 2 BDSG) und sind noch für eine angemessene Frist zu Dokumentationszwecken vorzuhalten. Danach sind sie zu löschen.

Der Verein hat die Möglichkeit, ein Vereinsarchiv zu führen und dort auch Vorgänge mit personenbezogenen Daten, die für eine aktive Nutzung nicht mehr benötigt werden, aufzubewahren. Dabei sollte jedoch sichergestellt sein, dass nur ein sehr kleiner zuverlässiger Personenkreis dazu Zugang hat. Die Nutzung des Archivguts in personenbezogener Form ist nur sehr eingeschränkt zulässig. Die Einzelheiten sollten ebenfalls geregelt werden. Wichtig ist auch, dass der Verein Unterlagen, die nicht mehr benötigt werden, so entsorgt, dass Dritte keine Kenntnis von den darin enthaltenen personenbezogenen Daten erlangen können. Insbesondere dürfen Mitglieder- und Spenderlisten nicht unzerkleinert in Müllcontainer geworfen werden.

Beim Ausscheiden oder dem Wechsel von Funktionsträgern ist sicherzustellen, dass sämtliche Mitgliederdaten entweder ordnungsgemäß gelöscht oder an den Nachfolger oder einen anderen Funktionsträger des Vereins übergeben werden und keine Kopien und Dateien mit Mitgliederdaten beim bisherigen Funktionsträger verbleiben.

Die erforderlichen Regelungen zu Speicherfristen sowie zur Sperrung und Löschung von Daten und ggf. zur Nutzung von Archivgut können entweder in der Vereinssatzung oder außerhalb der Satzung in einer Datenschutzordnung bzw. in einer gesonderten Datenlöschkonzeption getroffen werden.

Für alle Formulare bzw. Datenträger mit personenbezogen Daten als Inhalt gilt grundsätzlich zu prüfen, ob es auch gesetzliche Aufbewahrungsfristen gibt. So müssen beispielsweise Verträge oder Daten aus Arbeitsverhältnissen für 6 bzw. 10 Jahre (Frist läuft ab Jahresende, an dem die Leistungen erbracht sind bzw. die Verträge ende) sicher aufbewahrt, bevor sie ordnungsgemäß vernichtet werden dürfen.

Weitergabe von Daten von Vereinsfunktionären (Vorstand)

Der Vorstand eines Vereins ist gleichzeitig auch der rechtliche Vertreter. Aus diesem Grund muss er auch in einem offiziellen Register geführt und im Namen des Vereins erreichbar sein. Dazu werden (ausschließlich) die Namen der Vorstandsmitglieder im Vereinsregister geführt.
Allerdings besitzt auch der Vorstand alle Rechte des Datenschutzgesetzes. Somit entscheidet er selbst wo und in welchem Umfang persönliche Daten preisgegeben werden. Zur ständigen Erreichbarkeit reicht eine Vereinstelefonnummer, -Email-Adresse oder -Anschrift. Private Daten dürfen ohne ausdrückliche Einwilligungserklärung nicht herausgegeben werden.

Handeln Vertretungsberechtigte im Auftrag oder im Namen des Vorstands, so dürfen sie zwar die ihnen zugewiesenen Aufgaben erfüllen, aber die persönlichen Daten der Vorstandsmitglieder müssen trotzdem geschützt bleiben. Bei Vertragsabschlüssen mit Banken, Versicherungen, o.ä. bei denen der Vorstand als natürliche Personen Angaben über sich selbst als Vertretungsberechtigter des Vereins machen muss, darf also nicht im Auftrag oder im Namen gehandelt werden. Diese Aufgaben müssen die Vorstandsmitglieder persönlich erfüllen.

Sämtliche Daten von weiteren Vereinsfunktionären (Kassenprüfer, erweiterter Vorstand, etc.) sind für Geschäfte des Vereins nicht von Belang, da sie weder im Namen des Vereins nach außen handeln dürfen, noch vertretungsberechtigt sind. Die persönlichen Daten sind also ebenfalls streng vertraulich.

5. Datenschutz beim Bauzug

Das Bundesdatenschutzgesetz (BDSG) gibt in § 28, 1 vor, dass die Verarbeitung und Nutzung Personen bezogener Daten nur zulässig ist, wenn es der Zweckbestimmung eines Vertragsverhältnisses mit dem Betroffenen dient, es zur Wahrung der berechtigten Interessen erforderlich ist oder die Daten allgemein zugänglich oder veröffentlicht sind.

Übertragen auf das Mietverhältnis im Projektbereich Bauzug ist demnach die Speicherung zulässig, soweit die Daten zur ordnungsgemäßen Abwicklung des Vertragsverhältnisses benötigt werden. Dies ist der Fall bei Angaben über Namen und Anschrift des Vertragspartners, Bankverbindung, Zahlungseingänge und Mahnungen. Darüber hinausgehende Daten dürfen nur erfasst werden, wenn sie für die Erfüllung des Vertrages von Bedeutung sind. Dazu gehören Daten zur Zahlungsfähigkeit des Mieters (Auskünfte zu Einkommen, Arbeitsplatz und Familienstand), Art des Einkommens, Anzahl der in der Wohnung lebenden Personen sowie deren familiäre Stellung zum Mieter.

Der Mieter muss keine Auskunft geben bzgl. Rauchen, Religion/Konfession, Hobbys, Musikgeschmack, Schulden, Vorstrafen bzw. Gesetzesübertritte, Mobiliar, etc.
Eine Auskunftspflicht hingegen besteht bei Einkommen, Haustieren, Familienstand, etc.

Eine Weitergabe der Daten ist nur in Ausnahmefällen, wie zum Beispiel die Wahrung der Interessen eines Dritten oder die Verfolgung von Straftaten, möglich. Eine weitere Ausnahme entsteht, wenn Behörden auf den Vermieter zugehen und zur Erhebung von personenbezogenen Daten gesetzlich befugt sind. Dies kann z. B. dann gegeben sein, wenn die Polizei im Rahmen von Ermittlungen oder zur Gefahrenabwehr Auskünfte über den Mieter verlangt. Dasselbe gilt für Anfragen der Arbeitsagentur bzw. der Jobcenter, soweit diese im Rahmen ihrer Befugnisse handeln.

Neben der Funktion von Stups als Vermieter und Verwalter des Bauzugs, ist auch die Abrechnung der Nebenkosten ein Bereich, in dem personenbezogene Daten erhoben und notfalls weitergegeben werden müssen. Dabei ist klar festzustellen, dass sich der Mieter in diesem Zusammenhang nicht auf das Persönlichkeitsrecht berufen kann, da es kein Energiegeheimnis gibt. Der Energieverbrauch stellt also keine personenbezogenen Daten nach § 3 BDSG dar, da es sich nicht nach Daten wie in § 1 BDSG beschrieben (familiäre oder persönliche Daten, Krankheit, Einkommen, etc.) handelt. Somit dürfen die persönlichen Energieverbräuche der einzelnen Mieter auch ohne Einschränkung an Energieversorger weitergegeben werden.
Jedoch hat jeder Mieter das Recht in seine persönlichen und auch fremde Verbrauchsdaten Einsicht zu bekommen, um die Abrechnung durch den Vermieter überprüfen zu können und ggf. Vergleichswerte zu erhalten.

6. Datenschutz in Kinderbetreuungseinrichtungen

Allgemeines

Die Einhaltung und die Umsetzung des Datenschutzes ist in ihrem Kern nichts anderes als die Respektierung des Persönlichkeitsrechts von Erzieherinnen und Erziehern, Eltern und Kindern. Kinder sind Träger eigener Rechte, die in der UN-Kinderrechtskonvention (Übereinkommen über die Rechte des Kindes) niedergelegt sind. Datenschutz ist Schutz für das Kind, Datenschutz ist Schutz für die Familie, Datenschutz ist Schutz für den Träger und die Einrichtung: Somit ist Datenschutz nicht nur ein rechtliches, sondern auch ein pädagogisches Anliegen.
Das Datengeheimnis gilt für alle Personen, die im Umgang mit oder Zugang zu personenbezogenen Daten haben. Das betrifft auch Aushilfskräfte, PraktikantInnen, hospitierende Eltern oder Ehrenamtliche.

Eine Kindertageseinrichtung muss über die Aufnahme der Kinder entscheiden. Sie hat die Aufgabe, die Kinder entsprechend ihrer sozialen, emotionalen, körperlichen und geistigen Entwicklung zu fördern. Bei der Erziehung, Bildung und Betreuung der Kinder orientieren die Erzieherinnen und Erzieher ihre Angebote am Alter, am Entwicklungsstand, an den sprachlichen und sonstigen Fähigkeiten, an der Lebenssituation, an der ethnischen Herkunft sowie an den Interessen und Bedürfnissen der einzelnen Kinder. Um diese Aufgabe erfüllen zu können, benötigen die MitarbeiterInnen in den Kindertageseinrichtungen Informationen über das Kind, die Eltern und gegebenenfalls weitere Familienmitglieder (personenbezogene Daten).

Das Datenschutzrecht erlaubt der Kindertageseinrichtung für bestimmte Zwecke Daten zu erheben. Die Erhebung ist auf die zur Umsetzung des Betreuungsverhältnisses erforderlichen Daten zu beschränken. Soweit darüber hinaus noch Bedarf an personenbezogenen Daten besteht (z.B. zur Umsetzung besonderer pädagogischer Konzepte), dürfen diese nur mit Ihrer Einwilligung erhoben werden (so weit ein Erheben auf Grundlage einer Einwilligung zulässig ist).

Aufnahme & Betreuungsvertrag

Träger und Einrichtungen wollen oftmals im Rahmen der kommunalen Bedarfsplanung Mehrfachanmeldungen erkennen und die Anmeldedaten der einzelnen Kinder austauschen. Dies ist nur mit ausdrücklicher Einwilligung der Eltern möglich. Wenn eine Einwilligung gegeben wurde, muss sich der Austausch der Daten auf eine Liste mit Geburtstag und Straßenname beschränken. Manche Kommunen haben insbesondere in Zusammenhang mit der Aufnahme von Kindern unter drei Jahren zentrale Anmeldeverfahren entwickelt, die datenschutzrechtlichen Vorgaben entsprechen müssen.

Für die Betreuung eines Kindes innerhalb einer Kindertageseinrichtung wird ein Betreuungsvertrag geschlossen. Dieser darf folgende personenbezogene Daten erfassen:

Kindbezogen: Name, Geburtstag und Anschrift, Datum der Tetanusimpfung, Anschrift und Telefonnummer des Hausarztes, Krankheiten

Elternbezogen: Name, Anschrift, Telefonnummern für Notfälle

Geschwisterbezogen: Namen, Geburtstage

An die Erhebung zusätzlicher Daten im Aufnahme- bzw. Betreuungsvertrag (z.B. Krankenkasse der Eltern, Staatsangehörigkeit von Kindern und deren Eltern, Bildungsstand, Beruf oder Erwerbstätigkeit der Eltern) ist ein strenger Maßstab anzulegen. Werden solche zusätzlichen Daten erhoben, muss der Träger der Kindertageseinrichtung im Aufnahme- bzw. Betreuungsvertrag begründen, welchen Zweck sie erfüllen sollen und warum gerade diese zusätzlich zu erhebenden Daten erforderlich sind. Beispielsweise kann die Berufstätigkeit ein

Kriterium für eine Ganztagsbetreuung sein, worüber dann ein Nachweis verlangt werden darf.

Foto-, Ton- und Viedoaufzeichnungen – Berichte über Beobachtungen

Als besondere personenbezogene Daten bei Kindertageseinrichtungen gehören nach den allgemeinen personenbezogenen Daten auch Beobachtungen über Kinder und die daraus resultierenden Berichte. Die Bildungs- und Entwicklungsdokumentation beruht auf der freien Entscheidung der Eltern. Diese freie Entscheidung darf auch nicht dadurch eingeschränkt werden, dass die Kindertageseinrichtung die Einwilligung zur Voraussetzung für eine Aufnahme macht. Wenn Eltern keine solche Bildungs- und Entwicklungsdokumentation wollen, ist dies von der Kindertageseinrichtung zu respektieren.
Die Eltern haben jederzeit das Recht auf Auskunft über alle zu ihrer Person oder zu ihren Kindern gespeicherten Daten, elektronisch oder in Akten. Insbesondere können Beobachtungsbögen von diesem Recht auf Auskunft nicht ausgenommen werden. Auch dies verlangt eine objektive Dokumentation, die ggf. zu schulen ist. Der Inhalt von Beobachtungsbögen sowie von Bildungs- und Entwicklungsdokumentationen darf nur den Erzieherinnen und Erziehern und den betroffenen Eltern bekannt sein. Eine Kenntnisnahme durch weitere Personen oder Stellen ist nur zulässig, wenn und soweit die Eltern dem schriftlich zustimmen. Dies gilt auch für Fachberatungen der Kindertageseinrichtung und für die kooperierende Schule.
Fotos dürfen immer nur mit der schriftlichen Einwilligung der Eltern gemacht werden. Dies gilt auch dann, wenn mit Hilfe der Fotos Einblicke in das Alltagsgeschehen der Kindertageseinrichtung gewährt werden sollen. Fotos dürfen nur in der Kindertageseinrichtung selbst, keinesfalls im Außenbereich (Schaukasten), ausgehängt werden. Auf die Aushängepraxis in der Kindertageseinrichtung (z.B. Eingangsbereich) ist im Aufnahme- bzw. Betreuungsvertrag hinzuweisen. Eine Namensnennung im Zusammenhang mit Fotos sollte generell vermieden werden.
Sollen Gruppenfotos an Eltern weitergegeben werden, ist darauf zu achten, dass dies mit Einwilligung der Eltern geschieht, deren Kinder abgebildet sind.
Kindertageseinrichtungen dürfen Fotos ausschließlich nach schriftlicher Einwilligung der Eltern ins Internet stellen. Die Eltern müssen das betreffende Foto vorher sehen können und auf die Tragweite einer Veröffentlichung im Internet hingewiesen worden sein. Insbesondere ist auf das Risiko schriftlich hinzuweisen, dass die im Internet eingestellten Fotos von Dritten heruntergeladen, kopiert und mit anderen Daten verknüpft werden können. Als Einwilligungserklärung sind ausschließlich die vom Träger auf Rechtskonformität geprüften Formulare zu verwenden

Ton- und Videoaufzeichnungen sind für das Kind erhebliche Eingriffe in dessen Persönlichkeitsrecht und nicht zwangsläufig Bestandteil der Bildungs- und Entwicklungsdokumentation. Die Notwendigkeit von Ton- und Videoaufzeichnungen muss genau begründet werden, insbesondere, warum Beobachtungen und deren schriftliche Dokumentation nicht ausreichen. Aufzeichnungen können zwar helfen, individuelle Verhaltensmuster besser zu erkennen, um so bestimmte Unterstützungs- und Fördermaßnahmen zu ergreifen. Dennoch bedarf es immer der freiwilligen Einwilligung der Eltern, wobei zu beachten ist, dass Eltern die einmal gegebene Einwilligungserklärung jederzeit widerrufen können. Die entsprechende Einwilligungserklärung muss Auskunft über Anlass und Zeitraum, beinhaltete Personen und Dauer der Aufzeichnung beinhalten.
Die Aufzeichnungen sind nach Möglichkeit so anzufertigen, dass andere Kinder nicht aufgenommen werden. Ist dies nicht möglich, ist auch die Einwilligung der betroffenen Eltern einzuholen. Auf Verlangen sind die Aufzeichnungen den Eltern vorzuführen. Auch Aufzeichnungen aus dem Alltag einer Kindertageseinrichtung, z. B. im Zusammenhang mit Projekten, bedürfen der rechtzeitigen Ankündigung und Einwilligung. Das gilt auch, wenn die Ton- und Videoaufzeichnungen vorgeführt werden sollen. In diesem Fall muss vorab geprüft werden, ob Kinder in unvorteilhafter Weise aufgezeichnet wurden. Entsprechende Sequenzen sind zu löschen.

Elternlisten – Notfallnummern – Aushänge

Oft wünschen Eltern eine Liste mit Namen und Anschriften anderer Eltern. Die Erfassung, Erstellung, Führung, Nutzung oder Weitergabe solcher Listen seitens des Trägers oder der Mitarbeiterschaft ist grundsätzlich unzulässig. Hierfür werden die Einverständniserklärungen der Eltern benötigt. Dem kann Rechnung getragen werden, indem man etwa bei Elternabenden eine Liste herumreicht, auf der sich die Anwesenden selbst eintragen. Sie entscheiden damit selbst, ob und welche Angaben sie eintragen wollen. Der Verwendungszweck (Weitergabe der Liste an die Personen, die sich eingetragen haben) und die Freiwilligkeit eines Eintrags sind im Kopfbereich der Liste genau zu benennen.

Werden Notfallnummern in einem offen zugänglichen Bereich ausgelegt (z.B. direkt neben dem Telefon), so ist darauf zu achten, wer auf diese Nummern zugreifen kann. Können Dritte (z.B. Eltern) diese Liste einsehen, so ist vorher zu prüfen, ob alle eingetragenen Telefonnummern vorher durch Einwilligung der jeweiligen Betroffenen offen zugänglich gehalten werden dürfen. Gegebenenfalls sind Einwilligungserklärungen einzuholen bzw. einzelne Nummern zu löschen.

Für Aushänge in der Kita gelten die selben Richtlinien, wie für Elternlisten, sofern sie personenbezogene Daten enthalten. Eine Einwilligungserklärung ist immer dann notwendig, wenn persönliche Daten ausgehängt und von Dritten gesehen werden können.

Weitergabe von Daten an Dritte

Auf Grund von Rechtsvorschriften finden gesundheitliche Untersuchungen der Kinder statt. Darüber sind die Eltern unter Hinweis auf die Rechtsvorschriften rechtzeitig zu informieren. Dabei werden von allen beteiligten Stellen (insbesondere vom Gesundheitsamt) Datenschutz- und Verschwiegenheitsbestimmungen beachtet.

Es gibt gesetzliche Meldepflichten für den Träger von Kindertageseinrichtungen, die den Betrieb der Einrichtung betreffen (z. B. Mitteilung von Qualifikationen). In Bezug auf Eltern und Kinder gibt es gesetzliche Meldepflichten im Zusammenhang mit dem IfSG. Diese sind einzuhalten.

An Personen, die nicht bekannt sind oder deren Identität nicht festgestellt werden kann, dürfen keine mündlichen oder telefonischen Auskünfte erteilt werden. Auch dann nicht, wenn sie Titel, Ämter oder bestimmte Berufe (etwa Rechtsanwalt eines Elternteils, Richter in einem familienrechtlichen Verfahren) geltend machen. Im Zweifel muss durch Rückruf die Identität der Behörde oder der Person festgestellt werden. Liegen geschäftliche oder gewerbliche Gründe vor, dürfen Daten nicht weitergegeben werden.

Daten über das Kind oder den sorgeberechtigten Elternteil dürfen nicht an den nicht sorgeberechtigten Elternteil weitergegeben werden. Bei gemeinsamer Sorge haben beide Sorgeberechtigten das Recht auf Auskunft zu allen Daten des Kindes und zu allen eigenen Daten – nicht jedoch das Recht auf Auskunft zu Daten des anderen Sorgeberechtigten.

Aufbewahrung der Daten

Die personenbezogenen Daten werden in Akten oder Dateien gespeichert. Dabei wird streng darauf geachtet, dass nur befugte Personen Zugang zu diesen Daten haben. Nachdem das Kind die Einrichtung verlassen hat, werden diese Daten gelöscht bzw. vernichtet. Grundsätzlich gilt dies für alle personenbezogenen Daten, die nicht mehr benötigt werden. Nur wenn berechtigte oder rechtliche Interessen berücksichtigt werden müssen (z. B. bei gewährten Fördermaßnahmen, offenen Ansprüchen oder bei gesetzlicher Aufbewahrungsfrist), dürfen Daten länger aufbewahrt bzw. weitergegeben werden, sofern es dafür eine Rechtsgrundlage gibt oder Eltern eingewilligt haben. Dies gilt unabhängig von der Art des Datenträgers (Papier, Festplatte, Netzwerk).

Zulässig ist, den Eltern anzubieten, Dokumentationen sowie Zeichnungen und andere Werke der Kinder mitzunehmen, wenn sie die Einrichtung verlassen; bei Ton- und Videoaufzeichnungen nur zu den Teilen, auf denen ausschließlich ihr Kind zu hören bzw. zu sehen ist. Beobachtungsbögen sowie Bildungs- und Entwicklungsdokumentationen, die nach Verlassen der Einrichtung nicht ausgehändigt werden, sollen ein Jahr danach vernichtet werden.

7. Datenschutz im Unithekle

Datenschutz für die Mitarbeiterschaft

Für die interne Kommunikation und den reibungslosen Ablauf innerhalb des Geschäftsbetriebs ist es notwendig, dass für alle Mitarbeiter, Team-Mitglieder, die Geschäftsführung und bestimmte Vorstandsmitglieder die Kontaktdaten der anderen Mitarbeiter, Team-Mitglieder, Geschäftsführer und bestimmter Vorstandsmitglieder stets einsehbar sind. Aus diesem Grund werden Kontaktlisten ausgehängt. Diese sind zu keiner Zeit von Dritten einzusehen. Des weiteren gibt jeder Betroffene sein Einverständnis dazu ab, dass personenbezogene Daten auf diesen Listen geführt werden.

Zur Abrechnung und Dokumentation von Arbeitszeiten wird ein Arbeitsbericht geführt. Dieser ist für alle Mitarbeiter offen einsehbar und beinhaltet neben den Namen der Mitarbeiter auch Arbeitszeiten, Tagesumsätze und Bemerkungen über die Arbeitsleistung. Auch diese Liste ist nicht öffentlich einzusehen.

Der Arbeitsablauf innerhalb des wirtschaftlichen Geschäftsbetriebs erfordert es, dass Mitarbeiter bzw. die Geschäftsführung mit Gästen persönlich in Kontakt treten. In diesem Zusammenhang wurden klare Datenschutzregeln aufgestellt. So ist festgelegt, dass keine personenbezogenen Daten (v.A. Telefonnummern und Email-Adressen) an Dritte weitergegeben werden, ohne dass der/die Betroffene ausdrücklich zustimmt.

Daten für Wochenendveranstaltungen

Für die Buchung von Wochenendveranstaltungen wird ein Vertrag zwischen dem Veranstalter und dem Unithekle abgeschlossen. Dieser beinhaltet personenbezogene Daten über den Veranstalter. Allerdings ist darin vermerkt, wie mit diesen Daten umgegangen wird bzw. was damit nach der Veranstaltung geschieht. Grundsätzlich werden nur so viele personenbezogene Daten erhoben, wie für die Umsetzung des Zwecks – also der Durchführung der privaten Veranstaltung – und den damit einhergehenden Buchungsformalien benötigt werden. Dazu gehören Name, Vorname, Anschrift, Telefonnummer und Email-Adresse des Veranstalters.
Nach der Durchführung der Veranstaltung werden die personenbezogenen Daten bzw. die abgeschlossenen Verträge noch weiter aufbewahrt, um bei eventuellen Rückfragen die notwendigen Dokumente vorzeigen zu können. Wie lange diese Speicherung der Daten durchgeführt werden muss ergibt sich aus der Notwendigkeit der Speicherung oder aus offenen Ansprüchen. Für die Mietverträge gilt 6 Jahre Aufbewahrungsfrist, für die Abrechnungsformulare in der Buchhaltung sind es 10 Jahre.

Um den Mitarbeitern bei der Abwicklung von Veranstaltungsbuchungen einen Überblick über freie bzw. bereits reservierte Termine zu geben, wird ein Partykalender geführt. Dieser beinhaltet personenbezogene Daten über alle Veranstalter und ist für Mitarbeiter stets frei zugänglich. Ein Zugriff Dritter ist nicht möglich und alle Mitarbeiter mit Zugriff haben eine interne Datenschutz-Erklärung unterschrieben, die die Weitergabe von personenbezogenen Daten verbietet.

Für die Durchführung bzw. Betreuung von privaten Veranstaltungen ist stets ein Mitarbeiter des Unithekles betraut. Diese Betreuung wird selbständig unter der Mitarbeiterschaft koordiniert. Zu

diesem Zweck werden in einem Online-Schichtplaner die Kontaktdaten der Veranstalter hinterlegt. Zugriff haben lediglich Angestellte und Geschäftsführer des Unithekles bis zum Zeitpunkt ihrer Kündigung. Der Zugriff ist durch mit individuelle und selbständig festgelegte Passwörter eines jeden Mitarbeiters bzw. Geschäftsführers geschützt (https-Verschlüsselung).

Datenschutz im Gastbetrieb

Für den Besuch des Unithekle als Gast sind personenbezogene Daten unerheblich, da jeder Gast bezüglich seiner Person anonym bleiben darf bzw. muss. Ausnahmen stellen hierbei höherrangige schutzwürdige Interessen dar. Beispielsweise steht die Einhaltung des Jugendschutzgesetzes im Konflikt zum Persönlichkeitsrecht, weswegen beim Ausschank von Alkohol bzw. der Einhaltung der Sperrstunde für Minderjährige Geburtsdaten auf Nachfrage offen gelegt werden können. Willigt ein Gast dieser Überprüfung seiner persönlichen Daten mit Hilfe eines offiziellen Dokuments (Personalausweis, Reisepass, Führerschein, Studentenausweis, etc.) nicht ein, so muss er im Zweifel nicht bedient werden, das legt das Hausrecht fest. Die Anfertigung einer Kopie oder das Einbehalten eines solchen Dokuments ist in keinem Fall erlaubt.

Ein besonderes Angebot im Unithekle, nämlich das Bestellen eines „Bezwingers“, beinhaltet eine Dokumentation dieser Bestellung mit Hilfe eines Fotos der jeweiligen Person. Dieses Foto wird dann im Gastraum öffentlich ausgehängt. Bei diesem Ablauf stehen auf den ersten Blick Urheberrecht, Hausrecht und Persönlichkeitsrecht in Konflikt. Doch wie verhält es sich wirklich?
Das Urheberrecht besagt, dass der Schöpfer eines Bildes (also der Fotograf bzw. sein Auftraggeber) auch alle Rechte auf dieses Bild besitzt. Es darf also bspw. nicht ungefragt kopiert oder von Dritten weiterverbreitet werden. Das Hausrecht hingegen sagt grundsätzlich aus, dass die Möglichkeit Fotos zu machen und auszuhängen bei der mit dem Hausrecht betrauten Person bzw. dem Rechteinhaber verbleibt. Das Persönlichkeitsrecht beschreibt die Rechte am eigenen Bild. Entgegen der einhelligen Meinung bedeutet das aber nicht, dass Bilder von Personen automatisch diesen Personen gehören und sie bestimmen können was damit gemacht wird. Es sagt lediglich aus, dass kein Bild ohne Einverständnis des Abgebildeten gemacht und veröffentlicht werden darf. Im Rahmen dieses speziellen Falles sollte aber jedem Fotografierten klar sein, dass der Zweck des Bildes das Veröffentlichen ist, wodurch er konkludent einwilligt. Es ist also wichtig, dass keine Bilder ohne ausdrückliche Einwilligung gemacht werden, dann ist auch der Aushang dieser Bilder im Unithekle erlaubt. Wie es sich mit den selben Bildern verhält, wenn sie online gestellt werden, wird in dem Absatz „Der Verein im Internet – Online-Arbeit“ geklärt.

8. Der Verein im Internet – Online-Arbeit

Internet-Zugang und Email-Verkehr der Beschäftigten

Grundsätzlich gelten folgende Sachverhalte zu klären:
Stellt der Arbeitgeber dem Arbeitnehmer eine dienstliche Email-Adresse zur Verfügung? Darf diese auch privat genutzt werden?
Dürfen Arbeitnehmer die dienstliche Email-Adresse für Private Nachrichten verwenden, so verliert der Arbeitgeber das Recht, die Email-Verläufe ohne Zustimmung des Arbeitnehmers zu kontrollieren.

Darf der Arbeitnehmer das Internet am Arbeitsplatz auch privat nutzen?
Grundsätzlich ist die private Nutzung des Internets am Arbeitsplatz verboten, sofern sie nicht ausdrücklich vom Arbeitgeber erlaubt oder stillschweigend und wissentlich geduldet wird. Bei erlaubter privater Nutzung gelten trotzdem Regeln für den Arbeitnehmer. So darf er die private Nutzung nur auf arbeitsfreie Zeiten (Pausen) beschränken, es darf die Arbeitsleistung nicht beeinträchtigt werden, das Betriebssystem ist vor Virenbefall (z.B. durch Downloads) zu schützen, eine Rufschädigung des Arbeitgebers (z.B. durch Download von Pornografie) ist verboten, es dürfen keine zusätzlichen Kosten verursacht werden und es darf keine Fremdsoftware installiert

werden. Verstößt der Arbeitnehmer dagegen, kann eine fristlose Kündigung folgen.
Ist die private Nutzung des Internets am Arbeitsplatz nicht erlaubt, so kann der Arbeitgeber den PC (wenn auch nicht permanent) überwachen.

Homepages

Zur Umsetzung seines Zwecks und zur besseren Darstellung des Vereins in der Öffentlichkeit, ist es heutzutage durchaus gewöhnlich dass eine oder mehrere Homepages online gestellt werden.
Auch Vereine stellen eine Person des öffentlichen Rechts dar und sind somit genau so verpflichtet einen Datenschutzhinweis auf eigenen Internetseiten zu hinterlassen. Auch wenn der Verein selbst keine personenbezogenen Daten sammelt oder speichert, so gibt es immer die Möglichkeit, dass Provider oder externe Anwendungen auf der Website (Facebook, Google, etc.) genau das tun. Um die Besucher der Seite darauf hinzuweisen, muss also ein so genannter Disclaimer deutlich sichtbar und von jeder Unterseite zugänglich dargestellt werden. Dieser Disclaimer erklärt den Besuchern, dass beim Besuch der Homepage u.U. personenbezogene Daten erhoben werden können bzw. wie damit umgegangen wird.

Oftmals werden auf Homepages von Vereinen personenbezogene Daten dargestellt. So zum Beispiel vom Vorstand, von Mitgliedern, Geschäftspartnern, Jubilaren, Gästen, etc. Dabei sind die Datenschutzrichtlinien einzuhalten. Hierbei sind ebenfalls alle Richtlinien, die bereits unter der Überschrift „Allgemeines“ genannt werden gültig.
Gerade wenn es um Bilder von Personen geht, gibt es viele komplizierte Rechtsvorschriften. Grundsätzlich muss jede auf der Homepage abgebildete Person nach § 22 KunstUrhG vorher schriftlich oder mündlich einwilligen. Ausnahmeregelungen bedürfen der rechtlichen Prüfung.
Bei sogenannter Eventfotografie, also auf Partys und Veranstaltungen ist eine konkludente Einwilligung durch Posieren vor der Kamera gegeben. Wird dann das geschossene Foto vom Fotografen gezeigt und kenntlich gemacht, an welcher Stelle das Foto veröffentlicht werden soll, kann man von einer zulässigen Veröffentlichung aufgrund einer (konkludenten) Einwilligung ausgehen. Einzig die Beweisbarkeit wird mangels schriftlicher Erklärung schwierig; wirksam ist sie trotzdem. Eine Generaleinwilligung in die Veröffentlichung aller Bilder durch eine entsprechende Erklärung, z. B. am Eingang der Location, ist aber auch hier eher unzulässig.

Social Media

Branchenübergreifend gehört es mittlerweile für viele Unternehmen oder Vereine dazu, auf einem oder mehreren Social-Media-Kanälen wie beispielsweise Facebook, Xing, LinkedIn, Twitter oder einem eigenen Blog präsent zu sein. Als soziale Medien gelten dabei solche Angebote, bei denen der Nutzer nicht nur passiver Konsument ist, sondern einen direkten Rückkanal zum Verein erhält. Ein Social-Media-Auftritt kann dabei zum Anbieten allgemeiner Informationen über den Verein und seine Produkte bis hin zur Abwicklung eines Teils des Kundenservices genutzt werden.
Da der Verein selbst nicht in sozialen Medien handeln kann, sondern auch hier durch private Personen vertreten wird, sollte eine klare Trennung von privaten und betrieblichen Aktivitäten bei Social-Media-Diensten vorgenommen werden. Passiert dies nicht, ist die Folge häufig, dass Aussagen, die Mitarbeiter über diese Kanäle treffen, dem Unternehmen als Arbeitgeber zugerechnet werden. Dies kann Auswirkungen auf die betriebliche Kommunikation haben, aber auch handfeste Haftungsfragen nach sich ziehen. Häufig aus Argwohn oder unzureichender Medienkompetenz werden Unternehmensgeheimnisse in sozialen Netzwerken nach außen getragen oder abfällige Äußerungen über den Verein, Vorgesetzte, Kunden oder Kollegen veröffentlicht, die dem Unternehmen nicht selten erhebliche Schäden zufügen können.
Vereine müssen sich also, unabhängig davon, ob sie selbst aktiv soziale Netzwerke nutzen wollen, mit der Frage befassen, wie gehe ich mit der Nutzung dieser Medien durch meine Mitarbeiter um? Oftmals wird das in sog. Social-Media-Guidelines intern festgelegt.

Eine bestimmte Form von Social-Media stellen sog. Social-Plugins (etwa der „Gefällt-mir“/“Like“-Button von Facebook) dar. Problematisch bei der Einbindung solcher Social-Plugins ist, dass diese standardmäßig mit den sozialen Netzwerken kommunizieren. Es werden bereits durch deren bloße Einbindung auf einer Website, also vollkommen unabhängig von einem Klick, Daten an den Betreiber des sozialen Mediums gesendet. Somit wird aus dem Betrieb einer eigenen Website mit einem kleinen Plugin rein datenschutzrechtlich ein soziales Medium was wiederum Folgen auf die Darstellung des Impressums und des Datenschutz-Disclaimers hat.

Ein häufiges Problem ist die Übertragung von Rechten an die sozialen Medien bei deren Nutzung. So ist es keine Geheimnis, dass bspw. Facebook alle Bilder, die jemals hochgeladen wurden selbständig und grenzenlos zu nutzen kann. Das Recht am eigenen Bild ist also automatisch abgegolten. Daraus resultiert eine große Verantwortung, wenn der Verein oder eine Abteilung Bilder bei Social Media hochlädt oder Beiträge postet, die nicht der Meinung, dem gewünschten Bild oder Darstellung des Vereins widerspiegeln oder noch schlimmer: rechtswidrig bzw. verboten sind. Denn die Löschung dieser Bilder aus den Social Media ist praktisch unmöglich. Aus diesem Grund wird auf den Upload jeglicher Bilder mit personenbezogen schutzwürdigen Inhalten verzichtet, es sei denn es wird eine schriftliche Einwilligungserklärung eingeholt.

9. Betroffenen-Rechte

Innerhalb des Vereins hat jede Person, deren personenbezogene Daten erhoben werden, gemäß der Artikel 12-23 DSGVO, festgelegte Rechte, über die die Betroffenen unterrichtet werden müssen und welche sie immer in Anspruch nehmen können.

Auskunfts- und Informationsrecht

Nach Artikel 13-15 DSGVO werden jedem Betroffenen, dessen Daten erhoben werden, folgende Informationen zum Zeitpunkt der Datenerhebung mitgeteilt:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln

Darüber hinaus sind u.a. folgende Informationen bereitzustellen:

- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und

Werden die Daten nicht bei der betroffenen Person selbst erhoben, muss nach Artikel 14 DSGVO zusätzlich zu den oben genannten Informationen zusätzlich auch die Quelle der Daten angegeben werden.

Der Betroffene hat darüber hinaus das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so

hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

- die Verarbeitungszwecke;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Recht auf Berichtigung

Die betroffene Person hat nach Artikel 16 DSGVO das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen. Unter Berücksichtigung der Zwecke der Verarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten – auch mittels einer ergänzenden Erklärung – zu verlangen.

Recht auf Löschung / Vergessenwerden

Die betroffene Person hat gemäß Artikel 17 DSGVO das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung stützte, und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die betroffene Person legt Widerspruch gegen die Verarbeitung ein.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- Die personenbezogenen Daten wurden in Bezug auf angebotene Dienste der Informationsgesellschaft erhoben.

Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht und ist er zu deren Löschung verpflichtet, so trifft er unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen, auch technischer Art, um für die Datenverarbeitung Verantwortliche, die die personenbezogenen Daten verarbeiten, darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Links zu diesen personenbezogenen Daten oder von Kopien oder Replikationen dieser personenbezogenen Daten verlangt hat.

Recht auf Einschränkung der Verarbeitung

Die betroffene Person hat gemäß Artikel 18 DSGVO das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:

- die Richtigkeit der personenbezogenen Daten von der betroffenen Person bestritten wird, und zwar für eine Dauer, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,
- die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt;
- der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder
- die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Recht auf Datenübertragbarkeit

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern die Verarbeitung auf einer Einwilligung auf einem Vertrag beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Bei der Ausübung ihres Rechts auf Datenübertragbarkeit hat die betroffene Person das Recht, zu erwirken, dass die personenbezogenen Daten direkt von einem Verantwortlichen einem anderen Verantwortlichen übermittelt werden, soweit dies technisch machbar ist.
Dieses Recht gilt nicht für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
Das Recht darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Widerspruchsrecht

Die betroffene Person hat gemäß Artikel 21 DSGVO das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, Widerspruch einzulegen; dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.
Der Verantwortliche verarbeitet die personenbezogenen Daten nicht mehr, es sei denn, er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.
Werden personenbezogene Daten verarbeitet, um Direktwerbung zu betreiben, so hat die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen; dies gilt auch für das Profiling, soweit es mit solcher Direktwerbung in Verbindung steht.
Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

10. Übersicht über Verarbeitungstätigkeiten

Innerhalb des Vereins gibt es viele verschiedene Tätigkeiten bei denen verschiedenste Daten

erhoben, verarbeitet, gespeichert, weitergegeben oder gelöscht werden. Um festzustellen, welche dieser Prozesse riskante Folgen für Daten bzw. Betroffene beinhalten könnte, werden diese im Anhang 1 aufgelistet.

11. Folgenabschätzung

Ob bei der Verarbeitung von Daten negative Folgen für die Betroffenen entstehen können bzw. wie drastisch diese Folgen sind und ob Verbesserungsprozesse vorgenommen werden müssen, soll in der Übersicht der Folgenabschätzung in Anhang 2 dargestellt werden.

Alle hier aufgeführten Verarbeitungstätigkeiten und deren Folgenabschätzung wurden mehrfach auf eine geringere Risiko-Einschätzung geprüft. Für einige Abläufe, welche auch nach Prüfung und ggf. Anpassung der Abläufe ein mittleres bis hohes Risiko bzgl. Folgen beinhalten, ist keine sicherere Durchführung möglich. Manche Abläufe sind auf Grund ihrer Notwendigkeit, Zweckmäßigkeit oder der erzwungenen Weitergabe von Daten an Dritte nicht stärker vom vorhandenen Risiko der Verletzung von personenbezogenen Datenschutz-Rechten zu befreien.

Stups e.V. versucht dennoch weiterhin nach bestem Wissen und Gewissen sämtliche Vorgaben der Datenschutz-Verordnungen in ihrer jeweils aktuell gültigen Fassung einzuhalten und alle verfügbaren Mittel dafür einzusetzen, dass personenbezogene Daten einem bestmöglichen Schutz unterliegen.

Datenschutz-Ordnung verabschiedet in der ordentlichen Vorstandssitzung am 24. Juni 2018

der Vorstand Stups e.V.

Anhang 1 - Verarbeitungstätigkeiten

Verantwortlich:
Stups e.V. **Tel.: 0176-57668454**
Allmandring 17 **Mail: Info@stupsev.de**
70569 Stuttgart **Web: www.stupsev.de**

STUPS
STUDENTISCHES PROJEKT FÜR SOZIALE EINRICHTUNGEN E. V.

Hinweis: Keine Verarbeitungstätigkeit erfordert einen Drittlandstransfer von Daten (Ausnahme ggf. Drittanbieter bei Hosting-Anbietern von Homepages und Email-Verkehr)

Verarbeitungstätigkeit	Ansprechpartner	Zwecke der Verarbeitung	Kategorie betroffener Personen	Kategorie von personenbezogene Daten	Kategorie von Empfängern	Löschfristen
Vereinsverwaltung:						
Antrag auf Mitgliedschaft	Verwaltung / Buchhaltung: Heike Schuh Tel.: 0711-68562025 stupsstuttgart@arcor.de	Verwaltung der Vereinstätigkeiten bzgl. Mitgliedschaft	Vereinsmitglieder	Name, Vorname, Adresse, Email-Adresse, Kontoinformationen, Familienstand	Verwaltung / Buchhaltung Vereinsvorstand	10 Jahre gesetzliche Aufbewahrungsfrist
Mitgliederverwaltung						
Beitragsverwaltung					Steuerberater	
Buchhaltung		Verwaltung der Abteilungstätigkeiten	Angestellte Vereinsmitglieder Eltern	Name, Vorname, Kontoinformationen	Keine	
Betrieb der Websites* (über Hosting-Dienstleister)	Verwaltung: Dieter Ruß Tel.: 0176-57668454 info@stupsev.de	Außendarstellung	Öffentlich	Zugriffsstatistiken, Nutzungsdaten, Inhaltsdaten	Hosting-Anbieter, beteiligte Drittanbieter	IP-Adressen nach Richtlinie des Hosting-Dienstleisters
Email-Verkehr*		Verwaltung, Außendarstellung Mitarbeiterorganisation	Mitarbeiter, Dritte	Bestandsdaten, Inhaltsdaten, Verkehrsdaten	Hosting-Anbieter, beteiligte Drittanbieter	7 Tage nach Löschung
Arbeitsverträge Personal-Datenblätter		Mitarbeiterverwaltung	Angestellte	Name, Vorname, Adresse, Telefonnummer, Email-Adresse, Geburtsdatum, Staatsangehörigkeit, Sozialversicherungsnr., Steuer-ID, Krankenkasse, Ausbildung, Kontodaten, frühere Arbeitgeber, Steuerklasse	Buchhaltung	10 Jahre gesetzliche Aufbewahrungsfrist
Lohnabrechnung (über externen Dienstleister)			Angestellte		Externer Dienstleister	10 Jahre gesetzliche Aufbewahrungsfrist
Kindertageseinrichtungen:						
Betreuungsvertrag	Kita-Leitung Verwaltung / Buchhaltung	Pflichten der Vertragserfüllung	Eltern Kinder Geschwisterkinder zuständiger Arzt Notfallkontakt	Name, Vorname, Adresse, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Geschlecht, Krankenkasse, Beruf, Arbeitsstätte, Familienstand, Erkrankung, Impfung, Blutgruppe, Telefonnummer, Email	Kita-Leitung Verwaltung Buchhaltung	10 Jahre gesetzliche Aufbewahrungsfrist
Anmeldeformular						Sofort nach Austritt aus Einrichtung
Ärztliche Bescheinigung	Kita-Leitungen				Kita-Leitung	
Adressliste	Kita-Mitarbeiterinnen Eltern in Einrichtung	Interne Kommunikation zwischen Eltern und Kita	Eltern	Name, Vorname, Geburtsdatum, Adresse, Telefonnummer	Eltern	
Foto-, Film-, Ton- und Videoaufzeichnungen	Kita-Mitarbeiterinnen	Erfüllung Betreuungspflicht Dokumentation	Kinder		Kita-Mitarbeiterinnen	
Vollmacht Abholung	Kita-Leitung	Sicherheitsvorgaben	Dritte		Kita-Leitung	
Lastschrifteinzug	Verwaltung / Buchhaltung	Verwaltung / Buchhaltung	Eltern	Name, Vorname, Kontodaten	Verwaltung / Buchhaltung	10 Jahre gesetzliche Aufbewahrungsfrist
Meldelisten Jugendamt	Verwaltung / Buchhaltung	Verwendungsnachweise	Mitarbeiterinnen Kinder und Eltern	Gehälter, Lohn-NK, Krankheitstage	Jugendamt	

Verantwortlich:

Stups e.V.
Allmandring 17
70569 Stuttgart

Tel.: 0176-57668454
Mail: Info@stupsev.de
Web: www.stupsev.de

STUPS
STUDENTISCHES PROJEKT FÜR SOZIALE EINRICHTUNGEN E. V.

Hinweis: Keine Verarbeitungstätigkeit erfordert einen Drittlandstransfer von Daten (Ausnahme ggf. Drittanbieter bei Hosting-Anbietern von Homepages und Email-Verkehr)

Verarbeitungstätigkeit	Ansprechpartner	Zwecke der Verarbeitung	Kategorie betroffener Personen	Kategorie von personenbezogene Daten	Kategorie von Empfängern	Löschfristen
Unithekle:						
Arbeitsverträge Personal-Datenblätter	Geschäftsführung / Verwaltung Dieter Ruß Tel.: 0176-57668454 info@unithekle-stuttgart.de	Mitarbeiterverwaltung	Geschäftsführer Mitarbeiter	Name, Vorname, Adresse, Telefonnummer, Email-Adresse, Geburtsdatum, Staatsangehörigkeit, Sozialversicherungsnr., Steuer-ID, Krankenkasse, Kontodaten, Steuerklasse	Verwaltung Buchhaltung Lohnbuchhaltung	10 Jahre gesetzliche Aufbewahrungsfrist
Lohnabrechnung (über externen Dienstleister)						
Online-Schichtplaner (externer Online-Anbieter)*					Mitarbeiter Team Vorstand Verwaltung	nach Richtlinie des Anbieters (https-Verschlüsselung)
Arbeitsbericht						10 Jahre gesetzliche Aufbewahrungsfrist
Mitarbeiter- / Team-Liste						Nach Austritt / Kündigung
AGBs Wochenendveranstaltungen		Vertragserfüllung Veranstaltungsmiete	Veranstalter	Name, Vorname, Adresse, Telefonnummer, Email-Adresse, Geburtsdatum	Mitarbeiter Verwaltung	6 Jahre gesetzliche Aufbewahrungsfrist
Abrechnungen Wochenendveranstaltungen						10 Jahre gesetzliche Aufbewahrungsfrist
Veranstaltungskalender						Mit Ablauf des Jahres
Social-Media*		Außendarstellung	Öffentlich	Zugriffsstatistiken	Anbieter / Hoster	nach Richtlinie des Anbieters (https-Verschlüsselung)
Cloud-Backups*		Datenverarbeitung	Geschäftsführer Mitarbeiter / Team-Mitglieder Vertragspartner	Backup aller notwendigen Daten des laufenden Betriebs und der Mitarbeiterverwaltung	Geschäftsführer Verwaltung	Wenn nicht mehr aktuell oder nicht mehr benötigt bzw. nach gesetzlicher Aufbewahrungsfrist
Sponsoring		Sponsoring-Verträge und -Inhalte	Sponsoring-Partner	Firmenname, Anschrift, evtl. Kontodaten	Geschäftsführer Verwaltung	10 Jahre gesetzliche Aufbewahrungsfrist
Vertragspartnerschaften		Bewirtung auf Rechnung	Gäste	Name, Vorname, Anschrift, evtl. Kontodaten	Geschäftsführer Verwaltung	10 Jahre gesetzliche Aufbewahrungsfrist
Bauzug:						
Mietverträge	Verwaltung / Buchhaltung Heike Schuh Tel.: 0711-68562025 stupsstuttgart@arcor.de	Vertragserfüllung	Mieter	Name, Vorname, Adresse	Verwaltung Buchhaltung	6 Jahre gesetzliche Aufbewahrungsfrist
Einzug Miete						
Nebenkostenabrechnung						

***IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):**

✓ **Automatische Updates im Betriebssystem aktivieren**	✓ **Automatische Updates des Browsers aktivieren**	✓ **regelmäßige Backups (monatlich)**
✓ **Standard-Gruppenverwaltung (z.B. in Windows)**	✓ **Aktuelle Virensoftware / Virenscanner**	✓ **Papieraktenvernichtung in Standard-Shredder**
✓ **Zugang zu PCs mit sensiblen Daten nur für Befugte**	✓ **Zugang zu PCs mit sensiblen Daten mit Passwort**	✓ **regelmäßige Löschung des Email-Verkehrs von Server**
✓ **Vertraglich festgelegte Schweigepflicht**	✓ **schriftlich vereinbarte Datenschutz-Ordnung für Angestellte**	✓ **Regelmäßige Überprüfung des Sicherheitskonzepts**

Anhang 2 - Folgenabschätzung

	Datenerhebung	Datenverarbeitung	Datenspeicherung	Datenweitergabe	Datenlöschung	Risiko-Einschätzung
Vereinsverwaltung:						
Antrag auf Mitgliedschaft	Schriftliches Antragsformular mit Einwilligungserklärung und Unterschrift	Keine	Aufbewahrung des Antrags in Ordner in Verwaltungsbüro ohne Zugang Unbefugter	Vom Antragsteller auf direktem Weg (postalisch oder persönlich) an verarbeitende Stelle	Shredder	Gering
Mitgliederverwaltung	Durch Mitgliedsanträge	Mitgliederliste monatlich aktualisiert	Offline-Datei digital und analoge Liste in Verwaltungsbüro ohne Zugang Unbefugter	Von verarbeitender Stelle an Vereinsvorstand bei Mitgliederversammlung einmal jährlich (direkt/analog)	Löschung Datei Shredder	Gering
Beitragsverwaltung	Durch Mitgliederverwaltung	Anlage von SEPA-Lastschriftmandat bei Hausbank	SEPA-Lastschriftmandat bei Hausbank über Online-Banking-Zugang	Von verarbeitender Stelle an Hausbank durch Online-Banking-Zugang (Passwortgeschützt)	Löschung SEPA-Mandat bei Bank	Gering
Buchhaltung	Personal-Datenblätter Mitgliedsanträge Kita-Anmeldungen	Abgleich der Kontenbewegung mit Lohnbuchhaltung, Eltern- und Mitgliederliste (Lohnzahlung, Eltern- und Mitgliedsbeiträge)	Anlage von Personalakten, Mitgliederlisten, Elternlisten in digitalen Offline-Dateien und auf Papier in Verwaltungsbüro ohne Zugang Unbefugter	Steuerberater	Shredder	Mittel
Betrieb der Websites (über Hosting-Dienstleister)	Laut AGBs und Datenschutzverordnung Hosting-Anbieter	Laut AGBs und Datenschutzverordnung Hosting-Anbieter	Laut AGBs und Datenschutzverordnung Hosting-Anbieter	Laut AGBs und Datenschutzverordnung Hosting-Anbieter	Laut AGBs und Datenschutz-verordnung Hosting-Anbieter	Mittel
Email-Verkehr						
Arbeitsverträge Personal-Datenblätter	Vertrag mit Unterschrift bzw. Schriftliches Formular	Erstellung von Arbeitsverträgen	Offline-Datei digital und Personalakte in Verwaltungsbüro ohne Zugang Unbefugter	An Lohnabrechnung (externer Dienstleister)	Shredder	Gering
Lohnabrechnung (über externen Dienstleister)	Durch Personal-Datenblätter und Arbeitsverträge	Lohnabrechnung nach gesetzlichen Vorgaben	Nach gesetzlichen Vorgaben	An Sozialversicherungsträger, Krankenkassen, etc. nach gesetzlichen Vorgaben	Shredder	Gering
Kindertageseinrichtungen:						
Betreuungsvertrag	Schriftlich mit Einwilligungserklärung und Unterschrift	Keine	Aufbewahrung in Ordner in Verwaltungsbüro ohne Zugang Unbefugter	Auf direktem Weg (postalisch oder persönlich) an verarbeitende Stelle	Shredder	Mittel
Anmeldeformular		Anlage Akte und Betreuungsvertrag				
Ärztliche Bescheinigung	Durch zuständigen Arzt					
Adressliste	Durch Eltern schriftlich	Keine	Aufbewahrung an für Eltern sichtbarem Ort	Keine	Shredder	Mittel
Foto-, Film-, Ton- und Videoaufzeichnungen	Durch Digitalisiserungsgeräte	Im Rahmen der Erfüllung der Betreuungsarbeit (Portfolio, Entwicklung)	Digital auf PC in Leitungsbüro ohne Zugang Unbefugter	Keine	Löschung der Daten	Mittel
Vollmacht Abholung	Schriftliches Formular	Keine	Aufbewahrung in Ordner in Verwaltungsbüro ohne Zugang Unbefugter	Auf direktem Weg (postalisch oder persönlich) an verarbeitende Stelle	Shredder	Gering
Lastschrifteinzug	Schriftlich mit Einwilligungserklärung und Unterschrift	Anlage von SEPA-Lastschriftmandat bei Hausbank	SEPA-Lastschriftmandat bei Hausbank über Online-Banking-Zugang	Von verarbeitender Stelle an Hausbank durch Online-Banking-Zugang (Passwortgeschützt)	Löschung SEPA-Mandat bei Bank	Gering
Meldelisten Jugendamt	Mitarbeiterlisten Elternlisten	Übertrag in Formular Jugendamt	Offline-Datei digital und analoge Liste in Verwaltungsbüro ohne Zugang Unbefugter	Von verarbeitender Stelle postalisch zum Jugendamt	Löschung Datei Shredder	Mittel

	Datenerhebung	Datenverarbeitung	Datenspeicherung	Datenweitergabe	Datenlöschung	Risiko-Einschätzung
Unithekle:						
Arbeitsverträge Personal-Datenblätter	Vertrag mit Unterschrift bzw. Schriftliches Formular	Erstellung von Arbeitsverträgen	Offline-Datei digital und Personalakte in Verwaltungsbüro ohne Zugang Unbefugter	An Lohnabrechnung (externer Dienstleister)	Shredder	Gering
Lohnabrechnung (über externen Dienstleister)	Durch Personal-Datenblätter und Arbeitsverträge	Lohnabrechnung nach gesetzlichen Vorgaben	Nach gesetzlichen Vorgaben	An Sozialversicherungsträger, Krankenkassen, etc. nach gesetzlichen Vorgaben	Shredder	Gering
Online-Schichtplaner (externer Online-Anbieter)*	Anlage Profil mit Email-Adresse	Laut AGBs und Datenschutzverordnung Anbieter	Laut AGBs und Datenschutzverordnung Anbieter	Laut AGBs und Datenschutzverordnung Anbieter	Laut AGBs und Datenschutzverordnung Anbieter	Mittel
Arbeitsbericht	Formular ausgefüllt durch Mitarbeiter	Erstellung von Lohnabrechnungen	Offline-Datei digital und analoge Liste in Verwaltungsbüro ohne Zugang Unbefugter	Keine	Löschung Datei Shredder	Gering
Mitarbeiter- / Team-Liste	Durch Personalblatt	Erstellung einer Liste	Offline-Datei digital und analoge Liste in nur für Mitarbeiter zugänglichem Raum	Keine (Absicherung durch Datenschutz-Erklärung mit Unterschrift)	Shredder	Mittel
AGBs Wochenendveranstaltungen	Durch AGBs schriftlich ausgefüllt mit Einwilligungserklärung und Unterschrift	Keine	Analog in Ordner in Verwaltungsbüro ohne Zugang Unbefugter	An Mitarbeiter, die die Veranstaltung durchführen und abrechnen (Absicherung durch Datenschutz-Erklärung mit Unterschrift)	Shredder	Mittel
Veranstaltungskalender		Erstellung einer Abrechnung			Shredder	Gering
Abrechnungen Wochenendveranstaltungen		Keine		An Buchhaltung zur Kontenführung	Shredder	Gering
Social-Media	Durch Nutzer	Laut AGBs und Datenschutzverordnung Anbieter	Laut AGBs und Datenschutzverordnung Anbieter	Laut AGBs und Datenschutzverordnung Anbieter	Laut AGBs und Datenschutzverordnung Anbieter	Mittel
Cloud-Backups	Sammlung aller notwendigen Daten des laufenden Betriebs und der Mitarbeiterverwaltung	Keine	In Cloud Laut AGBs und Datenschutzverordnung Anbieter	Laut AGBs und Datenschutzverordnung Anbieter	Laut AGBs und Datenschutzverordnung Anbieter	Mittel
Sponsoring	Durch Verträge ausgefüllt von Sponsoring-Partner	Keine	Analog in Ordner in Verwaltungsbüro ohne Zugang Unbefugter	Keine	Shredder	Gering
Bauzug:						
Mietverträge	Durch Verträge ausgefüllt von Mieter	Keine	Analog in Ordner in Verwaltungsbüro ohne Zugang Unbefugter	Keine	Shredder	Gering
Einzug Miete	Durch Überweisung Mieter		Eingangsnachweis in Ordner in Verwaltungsbüro ohne Zugang Unbefugter	Keine	Shredder	Gering
Nebenkostenabrechnung	Durch Abrechnung Versorger	Aufteilung je nach Teilbeträgen der Mieter		An Mieter	Shredder	Gering