Bundesministerium
für Familie, Senioren, Frauen
und Jugend

Deutsches
Jugendinstitut

Datenschutz in der Kindertagespflege

CARMEN STOCKER-PREISENBERGER

Die vorliegende Expertise wurde als zusätzliches Material zu folgender Publikation erstellt: Schuhegger, Lucia/Hundegger, Veronika/Lipowski, Hilke/Lischke-Eisinger, Lisa/Ullrich-Runge, Claudia (2019): Qualität in der Kindertagespflege. Qualifizierungshandbuch (QHB) für die Bildung, Erziehung und Betreuung von Kindern unter drei. Hannover.
Die Expertise gibt die persönlichen Auffassungen der Autorin auf Basis des aktuellen Standes wieder. Vom Deutschen Jugendinstitut e.V (DJI) wurde keine rechtliche Prüfung vorgenommen. Das DJI kann daher keinerlei Haftung übernehmen.
Redaktionsschluss: Mai 2020

DJI Deutsches Jugendinstitut

gefördert vom

Bundesministerium für Familie, Senioren, Frauen und Jugend

Impressum

Carmen Stocker-Preisenberger
Datenschutz in der Kindertagespflege

1. Auflage 2020

www.dji.de/qhb2

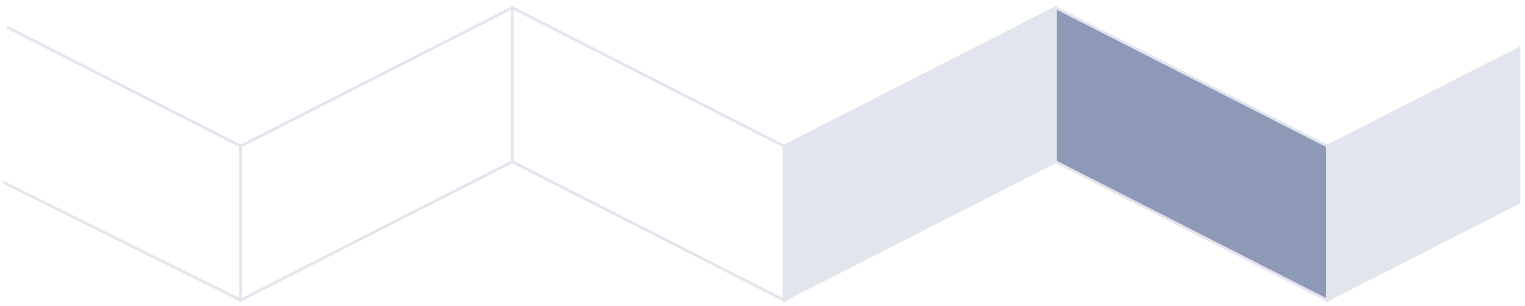
Lektorat: Punkt & Anker – Eva Weidner
Realisation: SchwabScantechnik, Göttingen

Die gesetzeskonforme Umsetzung des Datenschutzes ist in der Kindertagespflege eine herausfordernde Aufgabe. Gerade für selbständige Kindertagespflegepersonen kann es einen hohen Aufwand bedeuten, sich kontinuierlich zu informieren, geeignete Formulare und Prozesse zu entwickeln und den Datenschutz im Alltag zu gewährleisten. Die Berücksichtigung des Datenschutzes in der Grundqualifizierung nach dem Konzept des QHB ist für die Teilnehmenden und Referierenden in mehrfacher Hinsicht relevant, unter anderem wenn es um den Austausch von Daten mit der Fachberatung, dem Jugendamt, den Eltern sowie mit Auftragsverarbeitern oder Dritten, wie zum Beispiel Steuerberaterinnen/Steuerberatern, geht.

Diese Expertise soll sowohl Kindertagespflegepersonen beim datenschutzkonformen Aufbau und Betrieb ihrer Kindertagespflegestelle unterstützen, als auch Referierenden einen Überblick sowie Materialien für Seminare mit datenschutzrelevanten Inhalten bieten. Dazu werden in der Expertise grundlegende Kompetenzen der Teilnehmenden in der Grundqualifizierung für deren datenschutzkonformen Aufbau und Betrieb ihrer Kindertagespflegestelle formuliert sowie notwendige Kompetenzen der Referierenden für den Einbezug des Datenschutzes in die Grundqualifizierung.

Die Expertise wurde im Rahmen des Projektes *Überarbeitung und Erweiterung des QHB* erstellt.

Das Projekt wurde aus Mitteln des Bundesministeriums für Familie, Senioren, Frauen und Jugend (BMFSFJ) gefördert.



Carmen Stocker-Preisenberger ist niedergelassene Rechtsanwältin mit Sitz in Vaterstetten (Bayern) und beschäftigt sich bundesweit mit Rechtsfragen aus dem Bereich der Kindertagespflege. Zusätzlich zu ihrer anwaltlichen Tätigkeit bearbeitet sie seit mehreren Jahren damit verbundene Themenfelder und Fragestellungen im Rahmen von Vorträgen und Referaten bei verschiedenen Trägern.

Inhalt

I

Der Datenschutz in der Kindertagespflege

1 Einleitung

Im beginnenden 21. Jahrhundert werden die Menschen zunehmend mit einer Vielzahl neuer technischer Entwicklungen konfrontiert, die sich erheblich auf ihren privaten und beruflichen Alltag auswirken. Die neu entstandene Datensammelindustrie greift nahezu ungebremst die Flut an Informationen ab, welche inzwischen über jedes menschliche Lebewesen vor allem in digitaler Form und für alle leicht ersichtlich in die Welt gesetzt und nahezu ungebremst verbreitet werden – sei es über die sogenannten „sozialen Medien" wie Facebook, über Bewegungsprofile aus Mobiltelefonen, Fahrzeugen und Dashcams oder über Überwachungskameras auf öffentlichen Plätzen.

Die Vielfalt der Möglichkeiten macht es den technisch Versierten heutzutage leicht, diese als „Daten" bezeichneten Informationen zu sammeln, zu konzentrieren, aufzubereiten und für mannigfaltige Zwecke zu verwenden, ohne dass der jeweils betroffene Mensch als Urheber dieser Daten dies bemerken kann. Daten werden daher als das *„Gold des 21. Jahrhunderts"* (Diering 2014) bezeichnet. Es lohnt sich, nach diesen Daten zu schürfen („Data-Mining", Maurer 2017), um zu erfahren, was und wo Menschen einkaufen, mit wem sie kommunizieren, was sie tun, wie sie denken, was sie wählen. Diese Daten werden ausgewertet und in neue Datenpakete zusammengefasst, um übergreifende Muster zu erkennen. Die hieraus gewonnenen Erkenntnisse werden schließlich dazu genutzt, um in einem nächsten Schritt mit gezielt in die Welt gesetzten Daten und maßgeschneiderten Datenangeboten bestimmte Zwecke zu erreichen oder zukünftige Entwicklungen vorherzusagen (Maurer 2017). Nicht selten werden damit aber auch neue Identitäten geschaffen oder Identitäten existierender Menschen missbraucht.

Der „Cambridge Analytica"-Skandal rund um den amerikanischen Präsidentenwahlkampf im Jahr 2016 (Gruber 2018) oder der „Brexit"-Wahlkampf (Dierks 2018) desselben Jahres haben deutlich gemacht, wie leicht Menschen allein nach Auswertung ihrer Tätigkeiten und Äußerungen in sozialen Medien durch zielgerichtete Kommunikation zu bestimmten Entscheidungen geleitet werden können; wie umfassend es zum „gläsernen Menschen" kommt, der sogar in seinen Wahlentscheidungen einfach und für ihn gar nicht mehr erkennbar lenkbar ist, und welche Folgen hieraus entstehen können. Sie zeigen, wie die Fülle der Informationen und die Einfachheit, diese zu erheben und zu verwenden, viele unterschiedliche Begehrlichkeiten entstehen lassen, und wie mühelos Menschen durch gezielte, auf sie persönlich zugeschnittene Informationsweitergabe in die gewünschte Richtung gelenkt werden können, ohne dass sie es überhaupt bemerken.

Derartige Eingriffe und Manipulationen finden allerdings nicht nur im Großen statt. Sie haben längst auch Eingang in die Welt der Kindertagespflege gefunden: So können Fotografien betreuter Kinder, welche auf einer Website veröffentlicht oder in sozialen Medien geteilt wurden, noch lange nach der Betreuung aufgerufen werden. Je nach fotografierter Situation können diese Fotos selbst für Teenager oder sogar Erwachsene noch beschämend wirken und sie in ihrer Lebensführung gravierend behindern, indem die Betroffenen beispielsweise durch ein kursierendes Bild dem Spott ausgesetzt werden (Klein 2018). Zudem können die Fotografien durch technische Bearbeitung ver-

fremdet und zu rechtswidrigen Zwecken benutzt werden.
Ein weiteres Beispiel aus dem Alltag der Kindertagespflege: Im Rahmen der Kindertagesbetreuung müssen Informationen über den Gesundheitszustand eines Kindes erhoben werden, wenn sie Auswirkungen auf die Betreuung haben können. Werden diese Daten ungesichert gespeichert und deswegen gehackt oder gelangen sie im Rahmen der zulässigen Weiterleitung auf verschlungene Wegen an Stellen, für die sie nicht vorgesehen waren, können sie lange nach der Betreuung erhebliche Nachteile für das betroffene ehemalige Kind bedeuten. Aus der Praxis sind Fälle bekannt, in denen eine Berufsunfähigkeitsversicherung verweigert wurde oder eine private Krankenversicherung für ein mittlerweile erwachsenes Kind den Versicherungsschutz erheblich einschränkte, weil die Versicherung auf nachträglich nicht mehr nachvollziehbare Weise an die während einer Betreuung erhobenen und nicht gesicherten Daten gelangt, welche auf die Diagnose Mikrosomie (umgangssprachlich: Kleinwuchs) schließen ließen. Erhebungen zum Verhalten oder der Entwicklung eines Tagespflegekindes können darüber hinaus Jahre später beispielsweise auch für zukünftige Arbeitgeber von Interesse sein, um den Charakter einer Bewerberin oder eines Bewerbers einzuschätzen.
In der Mehrheit der Fälle ist gerade bei der Datenerhebung schlichtweg nicht absehbar, welchen anderen Verwendungszweck als den ursprünglich beabsichtigten, die erhobenen Daten zukünftig haben können. Viele Verwendungszwecke können zum Zeitpunkt der Datenerhebung nicht einmal erahnt werden. Diese für das menschliche Auge unsichtbare Welt benötigt daher Grenzen und Maßnahmen, welche die Datenerhebung und die Datenströme sichtbar machen. Denn nur sichtbargemachte Daten können überprüft, verfolgt und eingefangen werden; nur sichtbar gemachte Datenströme können eingedämmt werden. Dies ist Aufgabe des Datenschutzes: Durch den Datenschutz soll der unsichtbare und unkontrollierte Daten-*ab-fluss* erkennbar, greifbar und kontrollierbar gemacht werden. Auf diese Weise können die hiermit verbundenen Risiken erkannt und eingestuft werden; auf diese Weise kann einem zukünftigen Datenmissbrauch- oder Fehlgebrauch präventiv entgegengewirkt werden (Datenschutzkonferenz Kurzpapier Nr. 18).
Diese Erkenntnis führte bereits 1969 zum ersten diesbezüglichen Urteil des EuGH (Urteil vom 12.11.1969 Az 29/69 „Urteil Stauder"). 1977 kam es zur Verabschiedung des Bundesdatenschutzgesetzes (BDSG) in seiner ersten Fassung. Dem folgte die Verabschiedung von Landesdatenschutzgesetze. Im Dezember 1983 stellte das Bundesverfassungsgericht fest, dass sich das Recht eines jeden Menschen auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG (allg. Persönlichkeitsrecht) i.V.m. Art. 1 Abs. 1 GG (Menschenwürde) ableitet und daher Datenschutz ein Grundrecht ist (Urteil v. 15. Dezember 1983, Az. 1 BvR 209): *„Jeder muss selbst darüber entscheiden können, wer, wann, was und bei welcher Gelegenheit über ihn weiß"*, urteilte dabei das Bundesverfassungsgericht. Im Zuge der europäischen Harmonisierung kam es etwa ein Jahrzehnt später, im Jahre 1995, zu den ersten europarechtlichen Richtlinien, und schließlich am 14.04.2016 zur Verabschiedung der Datenschutz-Grundverordnung (DSGVO), sie trat zum 25.05.2016 in Kraft. Obwohl die DSGVO schon vor mehr als drei Jahren und das Bundesdatenschutzgesetz schon vor mehr als 30 Jahren verabschiedet wurden, erhält der Datenschutz erst seit ungefähr Anfang 2018 die breite Aufmerksamkeit, die ihm trotz seiner wachsenden Bedeutung seit Jahrzehnten vorenthalten blieb.
In der Kindertagespflege sind sämtliche Erwägungen und Schutzgedanken dieser Gesetze und Verordnungen ebenfalls vollumfassend zu berücksichtigen. Denn die Daten betreuter Tageskinder, ihrer Eltern und mitbefasster Dritter werden durch eine Kindertagespflegeperson aufgenommen, verarbeitet und an verschiedene Stellen weitergeleitet. Einfacher ausgedrückt: Mit dem Datenschutz soll auch in der Kindertagespflege gewährleistet sein, welche Daten von einer Kindertagespflegeperson weitergegeben dürfen und welche nicht (Stichwort: Vertraulichkeit/Schweigepflicht). Darüber hinaus wird mit Hilfe des Datenschutzes festgelegt, ob die Kindertagespflegeperson diese Daten überhaupt kennen und im beruflichen Bereich für eigene Zwecke nutzen und weiterverarbeiten darf. Gerade der alltägliche, praktische Datenaustausch im Kleinen, – beispielsweise das fast schon selbstverständlich gewordene gegenseitige Sammeln und Weiterleiten von Informationen und Momentaufnahmen über soziale Medien – muss in Anbetracht des allgegenwärtigen und unsichtbar im Hintergrund laufenden Data-Minings aufgrund der nun gel-

Durch den Datenschutz soll der unsichtbare und unkontrollierte Daten-*ab-fluss* erkennbar, damit greifbar und kontrollierbar gemacht werden, damit die hiermit verbundenen Risiken erkannt sowie eingestuft und einem zukünftigen Datenmissbrauch oder Fehlgebrauch präventiv entgegengewirkt werden kann (Datenschutzkonferenz Kurzpapier Nr. 18).

tenden Vorgaben kritisch hinterfragt und zur Bewahrung des informationellen Selbstbestimmungsrechts überprüft werden. Dies gilt vor allem in der Kindertagespflege: hier werden aus der Fremdbeobachtung des betreuten Tageskindes und seiner Bezugspersonen heraus eine Vielzahl an höchst sensiblen Daten gewonnen, die besonders schutzbedürftig sind. Untrennbar verbunden mit den Ergebnissen dieser Fremdbeobachtung ist überdies die unvermeidbare Eigenoffenbarung einer Kindertagespflegeperson, welche in diese Daten einfließt. Die Informationen, die sich hieraus über die Kindertagespflegeperson ableiten lassen, sind ebenfalls schutzbedürftig.
Im Folgenden soll ein Überblick über den derzeit gültigen Stand der Datenschutzgesetzgebung und die damit verbundenen Handlungsmaximen für Kindertagespflegepersonen gegeben werden. Sie sollen dadurch im Rahmen ihrer Grundqualifizierung auf der Basis des Qualifizierungshandbuches Kindertagespflege (QHB) (Schuhegger u. a. 2019) als Bedingung der Erteilung einer Pflegeerlaubnis dazu befähigt werden, angemessen mit ihren Daten und den Daten der betreuten Kinder zu arbeiten.

Ein weiterer Schwerpunkt liegt darauf, die notwendigen Datenschutzkompetenzen einer Kindertagespflegeperson darzustellen. Die verschiedenen Handlungsanforderungen an eine Kindertagespflegeperson werden in Form eines Leitfadens präsentiert und sollen als Hilfestellung für die praktische Umsetzung des Datenschutzes im Betreuungsalltag dienen. Zurückgegriffen wird dabei insbesondere auf die Standard-Kommentare Datenschutzrecht (Spiros/Hornung/Spiecker 2019, Spiros 2014) und Datenschutz-Grundverordnung (Ehmann/Selmayr 2017), Auch die Kurzpapiere der Datenschutzkonferenz, die derzeit eher spärlich vorhandene einschlägige Fachliteratur, Befragungen von Kindertagespflegepersonen zu ihrem Betreuungsalltag und vor allem die Hinweise und Stellungnahmen der Bundes- und Landesdatenschutzbeauftragten fließen in die Überlegungen ein.

Gerade die DSGVO ist noch nicht allzu lange in Kraft. Mit ihrer praktischen Umsetzung haben sich bereits nach kurzer Zeit eine Vielzahl an Detailfragen und Unklarheiten in ihrer Auslegung ergeben, die erst in den kommenden Jahren schrittweise gelöst werden können. Daher kann diese Abhandlung nur eine Momentaufnahme darstellen. Sie entbindet den Leser nicht von seiner beständigen Verpflichtung, sich in Sachen Datenschutz stets eigenverantwortlich fortzubilden und sich über Neuerungen oder Weiterungen zu informieren. Dies vor allem, da schon jetzt (Stand: Februar 2020) absehbar ist, dass die DSGVO in nächster Zukunft in einigen Teilen reformiert und in anderen Teilen präzisiert werden wird – in Bezug auf die Auslegung einiger Definitionen und Ziele ebenso wie in Bezug auf Handlungsanforderungen an die Anwender, hier insbesondere klein- und mittelständische Unternehmen und Berufstätige (Communication from the Commission to the European Parliament and the Council 2019, S. 7 ff.; Arbeitsrecht aktiv Sonderausgabe 2019, S. 16 f.).

Merke:
- Der Datenschutz steckt noch in den Kinderschuhen. Die Datenerhebungs- und Austauschtechniken entwickeln sich ständig weiter.
- Diese Expertise stellt daher nur eine Momentaufnahme dar.
- Der Datenschutz bei der Kindertagespflegeperson muss Schritt halten mit allgemeinen rechtlichen und technischen Entwicklungen und sich deswegen ebenfalls fortlaufend weiterentwickeln.
- Kindertagespflegepersonen müssen sich daher auch immer wieder in eigener Verantwortung über die Neuerungen und Präzisierungen informieren und diese umsetzen.
- Hierzu empfiehlt es sich, insbesondere die Veröffentlichungen der jeweils zuständigen Landesdatenschutzbehörde und der Datenschutzkonferenz DKS regelmäßig zur Kenntnis zu nehmen.
- Fachverbände wie z. B. der Bundesverband für Kindertagespflege e. V., Landesverbände oder Tagespflegebüros stellen u. U. Veröffentlichungen und Hilfestellungen zum Datenschutz zur Verfügung.

2 Rechtlicher Rahmen und Grundsätze

2.1 Anwendbarkeit des Datenschutzes auf die Kindertagespflege

In der in § 43 SGB VIII geregelten Kindertagespflege werden die Tageskinder zumeist im Haushalt der Kindertagespflegeperson betreut. Die Betreuung kann jedoch auch in angemieteten Räumen erfolgen. In einigen Bundesländern findet zudem eine Betreuung im Verbund mehrerer Kindertagespflegepersonen in einer sogenannten Großtagespflege statt.
Allen Formen ist gemeinsam, dass die Kindertagespflege an sich bereits dem sachlichen und persönlichen Schutzbereich des Art. 12 GG unterfällt und zu einer beruflichen Tätigkeit erstarkt ist. Sie erfüllt alle Voraussetzungen, die hierzu von der Rechtsprechung entwickelt wurden (BVerfG Urteil vom 11.06.1958–1 BvR 596/56 „Apotheken-Urteil"; Urteil vom 28.11.1984–1 BvL 13/81 = BVerfGE 68, 272; VG Bremen Urteil vom 10.07.2017–3 K 1064/13).
Gemeinsam ist allen Formen der Kindertagespflege, dass zur Ausübung der Kinderbetreuungstätigkeit umfassend Informationen – Daten – über das Kind, seine Bezugspersonen (meistens die Eltern, aber auch die Geschwister, Verwandte, Freunde und Dritte, wie z. B. Abholberechtigte) gesammelt, verwendet und weitergeleitet werden. Die gesammelten Informationen können unter die umgangssprachlichen Oberbegriffe „Stammdaten" und „besondere Daten" gefasst werden. Unter „Stammdaten" fallen Angaben allgemeiner Natur, die dazu dienen, die Vertragspartner und das zu betreuende Kindes zu identifizieren und die Organisation der Betreuung zu unterstützen. Bei diesen Daten handelt es sich insbesondere um: Name, Vorname des Tagespflegekindes und seiner Erziehungsberechtigten, Adresse, Telefonnummer, E-Mail-Adresse, Alter, Beginn und Ende der Betreuung, Betreuungsumfang. Die „besonderen Daten" bestehen aus der sensibleren allgemeinen Wissenssammlung über das Tagespflegekind und seine Erziehungsberechtigten, beispielsweise Gesundheitsdaten wie Erkrankungen oder Entwicklungsverzögerungen des Tagespflegekindes, Erkrankungen seiner Erziehungsberechtigten (z. B. Alkohol- oder Drogenkonsum), finanzielle Verhältnisse der Familie, Beziehungsprobleme der Erziehungsberechtigten, Trennungs- und Scheidungshintergründe, weltanschauliche Einstellungen und vieles mehr.

Möchten Kindertagespflegepersonen diese Daten erheben, speichern, verarbeiten und weitergeben, so müssen sie die im Folgenden aufgeführten Verordnungen, Gesetze und Grundsätze beachten.

2.2 Überblick über die gesetzlichen Grundlagen

Auf europäischer Ebene ebenso wie in der Rechtsordnung der Bundesrepublik Deutschland ist das Prinzip des Mehrebenensystems verankert (König/Rieger/Schmitt 1996, S. 16 ff.). Dies gilt auch für den Datenschutz. Seit Inkrafttreten des Vertrags von Lissabon verfügt die Europäische Union aufgrund Art. 16 Abs. 2 Unterabs. 1 AEUV hierfür über eine umfassende Kompetenz. Sie wurde ermächtigt, Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zu verabschieden.
Damit kann auf jeder Ebene – auf Gemeinschaftsebene gleichermaßen wie auf Ebene der Mitgliedstaaten und ihrer jeweiligen Untergliederung – die Rechtsmaterie Datenschutz so geregelt werden, wie es auf der entsprechenden Ebene nötig und sinnvoll ist, umso einerseits staaten- und länderübergreifende Mindeststandards schaffen zu können und andererseits die Souveränität der einzelnen Mitgliedstaaten und ihrer Untergliederungen nicht in Mitleidenschaft zu ziehen.
Diesem Grundgedanken ist es zu verdanken, dass ein komplexes System mehrerer ineinandergreifender und aufeinander aufbauender Gesetze entstanden ist, welches schwer durchschaubar ist. Häufig stellt sich der betroffenen Bürgerin oder dem betroffenen Bürger und umso mehr der betroffenen Kindertagespflegeperson die Frage, welches dieser vielen Gesetze nun eigentlich einzuhalten ist. Um Klarheit zu schaffen, werden im Folgenden zuerst einmal die wichtigsten Verordnungen und Gesetze der jeweiligen Ebene kurz vorgestellt.

Die DSGVO

Auch in der Kindertagespflege ist die sogenannte **DSGVO** einzuhalten. Mit der Kurzbezeichnung „DSGVO" ist die *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Perso-*

nen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG gemeint. Sie hat die schon zuvor geltende *Richtlinie 95/46/EG* (Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) ersetzt. In ihr werden nunmehr die innerhalb der Europäischen Union gleichermaßen geltenden Mindestvoraussetzungen an den Umgang mit Daten durch Unternehmerinnen oder Unternehmer und Unternehmen gesetzt.

Da Kindertagespflege bereits entsprechend ihrer Definition und Zielrichtung als Erwerbstätigkeit und damit zur Erzielung eines Verdienstes ausgeübt wird (Wiesner § 43 Rn. 20 ff.), müssen die Vorgaben der DSGVO in der Kindertagespflege eingehalten werden; es handelt sich schließlich um eine unternehmerische berufliche Tätigkeit mit einem wirtschaftlichen Bezug (Simitis 2019 Art. 2 Rn. 7, 26). Dementsprechend ist die DSGVO bei jeglicher Datenverarbeitung zu beachten, die in Zusammenhang mit der Kindertagespflegetätigkeit stehen. Die DSGVO muss in der Kindertagespflege i. d. R. grundsätzlich angewendet werden, weil der Ausnahmetatbestand des Art. 2 Abs. 2c DSGVO nicht greift. In Art. 2 Abs. 2c DSGVO ist geregelt, dass sich Privatpersonen nicht an diese Verordnung halten müssen, wenn sie ausschließlich persönliche oder familiäre Tätigkeiten ausüben und keinerlei Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit erkennbar ist (Simitis 2019 Art. 2 Rn. 7, 26). Kindertagespflegepersonen verarbeiten jedoch im Rahmen ihrer Kinderbetreuungstätigkeit Daten der Kinder und ihrer Erziehungsberechtigten, um ihre Tätigkeit auszuüben. Sie erheben diese Daten i. d. R. nicht, um rein persönliche und private Kontakt mit ihnen zu pflegen Auch die gemischte Sammlung von Daten befreit nicht von der Verpflichtung, die DSGVO einzuhalten. Eine doppelte Nutzungsmöglichkeit für private und gleichzeitig berufliche Zwecke – wenn beispielsweise Kontaktdaten eines Tagespflegekindes zur privaten Freundschaftspflege genutzt werden oder eine einzige Telefonliste im Mobiltelefon mit Kontaktdaten sowohl privater als auch beruflicher Art angelegt wird – lässt diese Ausnahmeregelung in der weit überwiegenden Mehrheit der Fälle in der Kindertagespflege ebenfalls entfallen (Simitis 2019 Art. 2 Rn. 28).

Soweit sich im Einzelfall Abgrenzungsprobleme ergeben, ist anhand der tatsächlichen individuellen Kommunikation festzustellen, ob die Grenze zur echten, rein privat-persönlichen Tätigkeit überschritten wurde – dann wären die Vorgaben der DSGVO nicht zu beachten – oder nicht – dann müssen die Vorgaben der DSGVO eingehalten werden (Simitis 2019 Art. 2 Rn. 26; Simitis 2014 § 1 Rn. 151).

Merke:
- Daten, die zumindest auch zu unternehmerischen Zwecken verarbeitet werden, unterfallen den Vorgaben des DSGVO.
- Datenverarbeitungssysteme, in denen private und unternehmerisch genutzte Daten gespeichert sind, sind entsprechend der Vorgaben der DSGVO zu behandeln und insbesondere zu sichern. Dies gilt beispielsweise vor allem für Kontaktlisten in Mobiltelefonen.

Bundesrecht

Auf Bundesebene gelten das **Bundesdatenschutzgesetz** (BDSG) sowie die **Sozialgesetzbücher Nr. 8** (SGB VIII) und **Nr. 10** (SGB X). Sie befassen sich mit dem Sozialdatenschutz. Durch diese bundesweit geltenden Gesetze werden Vorgaben der DSGVO konkretisiert und ergänzt, soweit sie umgesetzt oder präzisiert werden müssen oder soweit Gestaltungsspielräume für den Bundesgesetzgeber eröffnet wurden.

Beinhaltet die DSGVO für einen Bereich oder eine Thematik bereits unmittelbar und direkt geltende Vorschriften, so gilt die DSGVO direkt, damit es nicht zu Anwendungskonflikten kommt (§ 1 Abs. 5 BDSG). Bereiche, die durch die DSGVO offengelassen wurden oder nicht der europäischen Regelungskompetenz unterliegen, werden durch das BDSG geregelt. Die DSGVO sieht mindestens vier Dutzend solcher sogenannten Öffnungs- oder Spezifizierungsklauseln vor (Ehmann/Selmayr Einf. Rn 84). Daher finden sich im BDSG auf die DSGVO aufbauende Regelungen wie insbesondere Strafvorschriften (§§ 42 BDSG), ergänzende Verpflichtungen zur Bestellung eines Datenschutzbeauftragten (§ 38 BDSG) oder Datenschutzvorschriften für Beschäftigungsverhältnisse oder Bewerbungsverfahren (§ 26 BDSG). Soweit Kindertagespflege in – nach derzeitiger Rechtsprechung zulässiger (VGH Baden-Württemberg, Urteil vom 12.07.2017 – Az 12 S 102/15) – Festanstellung betrieben wird (z. B. in Form der Festanstellung einer Kindertagespflegeperson in einer Großtagespflegestelle eines Trägers), muss die Arbeitgeberin oder der Arbeitgeber in Bezug auf die angestellte Kindertagespflegeperson neben den Vorgaben der DSGVO auch den zusätzlichen Beschäftigtendatenschutz nach BDSG beachten.

Weitere im BDSG besonders geregelte, aber für die Kindertagespflege i. d. R. nicht relevante Bereiche sind die Themen Scoring und Bonitätsauskunft.

Die **Sozialgesetzbücher SGB VIII und X** regeln den durch die öffentlichen Jugendhilfeträger anzuwendenden zusätzlichen Sozialdatenschutz, also den Schutz besonders sensibler persönlicher Daten eines Menschen. Allerdings wird dabei in weiten Bereichen auf die DSGVO verwiesen. Hieran gebunden sind gem. § 61 SGB VIII die öffentlichen Jugendhilfeträger sowie Gemeinden und Gemeindeverbände, nicht jedoch die einzelne Kindertagespflegeperson. Träger der freien Jugendhilfe wie Trägervereine, welche eine Großtagespflege betreiben, müssen diesen Sozialdatenschutz aber zumindest indirekt berücksichtigen. Gemäß § 61 SGB VIII ist der öffentliche Jugendhilfeträger verpflichtet, bei Trägern der freien Jugendhilfe, welche er in Anspruch nimmt, für einen entsprechenden Sozialdatenschutz zu sorgen.

Landesrecht

In Umsetzung des föderalen Prinzips finden sich auch auf Länderebene in Ergänzung zu den oben angeführten staatlichen Gesetzen Landesdatenschutzgesetze und entsprechende Verordnungen, welche in Einzelbereichen Detailregelungen vorgeben. Sie stellen die Handlungsgrundlage für die jeweiligen Landesbehörden und vor allem für die jeweiligen Landesdatenschutzbeauftragten sowie für die Kreis- bzw. Regions- und Kommunalverwaltungen dar. Insbesondere wird mit diesen Gesetzen die Rechtsstellung der oder des jeweiligen Landesbeauftragten für Datenschutz geregelt. Weiterhin werden dort Bereiche geregelt, welche der Ländergesetzgebung unterfallen, beispielsweise das Medienrecht.

Die derzeit gültigen Landesdatenschutzgesetze werden unter **V. Gesetzesquellen und Datenschutzbehörden** aufgelistet.

Kirchenrecht

In den Kirchen und religiösen Vereinigungen in Deutschland gelten eigene Datenschutzbestimmungen, die allerdings in Einklang mit den Grundgedanken der DSGVO zu bringen sind.

Bereits aufgrund Art. 17 Abs. 1 des Vertrages über die Arbeitsweise der Europäischen Union ist festgelegt, dass die Union den unabhängigen Status der Kirchen und religiösen Vereinigungen oder Gemeinschaften in den Mitgliedstaaten nach deren Rechtsvorschriften achtet und ihn nicht beeinträchtigt. In derartigen Einrichtungen ist die DSGVO daher nicht direkt anwendbar, denn auch zivilrechtlich organisierte Einrichtungen der Kirche wie Vereine oder Stiftungen (z. B. als Träger von Kindertageseinrichtungen) nehmen am Selbstverwaltungsrecht der Kirche teil, solange und soweit sie nur nach ihrem eigenen Selbstverständnis zur betroffenen Kirche bzw. Religionsgemeinschaft gehören und ein Stück des kirchlichen Auftrages mitverwirklichen (BVerfG: „Goch-Beschluss“ vom 11.10.1977 – 2 BvR 209/76). Die vor diesem Hintergrund erlassenen **kirchenrechtliche Datenschutzregelungen** sind als sogenannter „Dritter Weg“ Ausfluss der verfassungsrechtlich gewollten Trennung von Kirche und Staat in Deutschland (Art. 137 Abs. 5 WRV). Laut Art. 91 DSGVO können religiöse Vereinigungen oder Gemeinschaften, die schon bisher nach nationalem Recht eigene Datenschutzregeln hatten, diese nach wie vor anwenden – vorausgesetzt, sie werden in Einklang mit der DSGVO gebracht. Hierdurch soll Religionsgemeinschaften und Kirchen weiterhin ermöglicht werden, ihre spezifisch religiösen Besonderheiten im Verhältnis der Religionsgemeinschaft oder Kirche zu ihren Anhängerinnen und Anhängern bzw. Mitgliedern (Communio) in ihrem Datenschutzrecht adäquat zu berücksichtigen (nach: datenschutz-kirche.de/frage 1: Welches Recht wendet die Katholische Kirche zum Schutz personenbezogener Daten an?).

Von diesem Recht haben die verschiedenen Kirchen und Religionsgemeinschaften in Deutschland Gebrauch gemacht und ihren Datenschutz in Anlehnung an die DSGVO und das BDSG neu geregelt. Dabei wurden entsprechend der jeweiligen Rechtsordnungen insbesondere eigene Vorgaben zur Implementierung eigener Datenschutzbeauftragter, eigener Sanktionierungen und eines eigenen Rechtsweges eingeführt. So kann die Rechtsverfolgung von Datenschutzverstößen innerhalb religiöser bzw. kirchlicher Einrichtungen auch weiterhin frei von jeglicher staatlichen Aufsicht und Kontrolle bleiben, dennoch wird aber der Datenschutz wirksam umgesetzt und gewahrt.

Die **Evangelischen Kirchen in Deutschland** haben zum 24.05.2018 das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland **DSG-EKG** verabschiedet. Dort werden die Vorgaben und Grundprinzipien des DSGVO berücksichtigt. Bereits 2015 wurde die Verordnung zur Sicherheit der Informationstechnik ITSVO erlassen. Weiterführende Informationen finden sich beispielsweise bei Claessen, Herbert (2004): Datenschutz in der

Evangelischen Kirche. München oder Ziekow, Arne: (2002) Datenschutz und evangelisches Kirchenrecht, Tübingen.
Die **Katholische Kirche in Deutschland** hat ebenfalls in Ergänzung zu den bereits zuvor bestehenden Vorschriften zum 24.05.2018 das Gesetz über den kirchlichen Datenschutz **KDG** verabschiedet. Dies berücksichtigt nun die Wertungen der DSGVO. Die hierauf basierenden Verordnungen werden derzeit überarbeitet. Näheres zur Rechtslage vor 2018 findet sich bei Fachet, Siegfried: (1998) Datenschutz in der katholischen Kirche, München; eine Neuauflage des Werkes bzw. ein Nachfolgewerk unter Berücksichtigung der DSGVO ist nach derzeitigem Stand geplant.
Diese kirchlichen Datenschutzgesetze geben ihrerseits jedoch die Vorgaben und Regelungen der DSGVO wieder. Daher können die weiteren Ausführungen zur DSGVO auch für solche religiös bzw. kirchlich getragenen Einrichtungen sinngemäß angewandt werden. Eine Großtagespflege, welche von einer religiösen Gemeinschaft, einer Kirche oder einem kirchlichen Träger betrieben wird, hat sich folglich rein formal zunächst an die entsprechenden kirchlichen Gesetze zu halten und nicht an die DSGVO – es sei denn, das jeweilige Kirchenrecht verweist auf die DSGVO oder es besteht eine Regelungslücke im jeweiligen Kirchenrecht. Die grundlegenden Wertungen sowie Ge- und Verbote der DSGVO sind somit zumindest sinngemäß auch für solche Großtagespflegen anwendbar, da die verschiedenen Rechtsordnungen miteinander in Einklang stehen, sich die entsprechenden Regelungen der DSGVO also in der entsprechenden innerkirchlichen bzw. innerreligiösen Gesetzgebung finden lassen werden.
Jüdische und muslimische Religionsgemeinden regeln den Datenschutz nach derzeitigem Stand auf Gemeindeebene. Sie berücksichtigen dabei ebenfalls DSGVO und BDSG, wenngleich, soweit derzeit ersichtlich, keine übergeordneten eigenständigen Rechtsgrundlagen verabschiedet wurden.
Die evangelische ebenso wie die katholische Kirche verfügen über entsprechende, nach Regionen (z. B. Nord, Süd, West, Ost) weitergehende Datenschutzbestimmungen mit insbesondere organisatorischem Inhalt.

Anwendungsvorrang

Soweit einzelne Regelungen bzw. Gesetze im Widerspruch zueinanderstehen, empfiehlt es sich als Faustregel, bei der Anwendung zunächst die DSGVO dem BDSG vorzuziehen, da das Unionsrecht allgemeinen Vorrang gegenüber staatlichem Recht hat. Dieser Gedanke hat sich auch in § 1 Abs. 5 BDSG niedergeschlagen und wäre nur dann eingeschränkt, wenn der europäische Datenschutzstandard unter das deutsche Schutzniveau absinken würde (BVerfG Beschluss vom 22.10.1986 – 2 BvR 197/83 „Solange II“). Aufgrund des derzeitigen hohen europäischen Schutzniveaus erscheint dies aktuell kaum vorstellbar. Innerhalb der deutschen Rechtsordnung ist sodann wegen Art. 31 GG im Zweifel das BDSG einzelnen Gesetzen oder Verordnungen auf Länderebene vorzuziehen.

2.3 Die DSGVO im Einzelnen

Herzstück des nunmehr geltenden, aktualisierten Datenschutzrechts ist die DSGVO. Sie wurde von der Europäischen Union erlassen, um in Zeiten einer sich radikal wandelnden Kommunikationsgesellschaft einen einheitlichen, starken und damit wirksamen Datenschutz aller europäischen Bürgerinnen und Bürger innerhalb aller Mitgliedstaaten durchzusetzen. In den nächsten Jahren sind Ergänzungen, Änderungen und Präzisierungen der DSGVO zu erwarten.
Die in der DSGVO niedergelegten Ziele und Grundprinzipien dienen in der Praxis vor allem als nützliche Auslegungshilfe bei Unklarheiten bezüglich einzelner Vorschriften. Daher sollen sie hier kurz vorgestellt werden:

Die Ziele der DSGVO

Die Zielrichtung dieser Verordnung ist der **Schutz der Grundrechte und der Grundfreiheiten von natürlichen Personen,** also Menschen. Es sollen die Daten dieser Menschen (Simitis 2019 Art. 1 Rn. 39) geschützt werden, nicht die Daten vor den Menschen. So soll verhindert werden, dass beispielsweise mächtige Großunternehmen ohne oder gar gegen den Willen der Menschen Gewinne mit Informationen erzielen können, die sie über diese Personen gewonnen haben.

Merke:
Als Faustregel gem. Art. 1 Abs. 1, 2 DSGVO gilt: „Der Datenschutz dient dem Schutz der Daten *von* Menschen, nicht dem Schutz von Daten *vor* Menschen.“

Gleichzeitig soll der freie Datenverkehr innerhalb der Europäischen Union nicht über Gebühr erschwert werden, Art. 1 Abs. 3 DSGVO.

In der Kindertagespflege ist dieser Grundsatz uneingeschränkt anwendbar. Hier gilt: Die Daten des Kindes und seiner Erziehungsberechtigten müssen vor unnötiger Erhebung, Verarbeitung und Weitergabe, vor zweckfremden Gebrauch, vor Zweckentfremdung und vor Missbrauch geschützt werden. Die Daten der Betroffenen müssen aber nicht vor den Betroffenen geschützt werden. Sie dürfen ihnen nicht vorenthalten werden.

Die Grundprinzipien der DSGVO

Grundlegender Gedanke aller Regelungen in der DSGVO ist das sogenannte **Verbotsprinzip.** Danach ist jegliche Art von Datenerhebung und -sammlung über eine natürliche Person (= Mensch) grundsätzlich verboten – es sei denn, es liegen Rechtfertigungsgründe für die Datenerhebung vor (Art. 6 Abs. 1 DSGVO) oder die betroffene Person hat nach vollumfassender Aufklärung freiwillig zugestimmt. Damit soll das Selbstbestimmungsrecht der jeweils betroffenen Person gestärkt, in Zeiten einer sich stark verändernden und sich beschleunigenden digitalen Kommunikation aber vor allem auch nachhaltig geschützt werden, denn Wissen ist Macht (Simitis 2019 Einl. Rn. 20, Art. 6 Rn. 4 ff.).

Eng damit verbunden ist das **Gebot der Datensparsamkeit** (Art. 5 DSGVO) und der **Zweckbindung.** Damit Menschen nicht unbegrenzt verdatet und damit als Datensammlung zur verkäuflichen Ware degradiert werden, sollen nur diejenigen Daten erhoben werden dürfen, welche für den (erlaubten) Zweck wirklich notwendig sind *(„das notwendige Maß"):* Daten, die gar nicht erhoben werden, können nicht gebraucht, missbraucht oder zweckentfremdet werden.

Über das Stichwort des „notwendigen Maßes" einer Datenerhebung wird auch der Grundsatz der **Speicherbegrenzung** *(„Recht auf Vergessenwerden")* und der **Datenrichtigkeit** leicht verständlich: Ist die Datenspeicherung sachlich oder zeitlich nicht mehr erforderlich, um den Zweck zu erreichen, so sind die Daten ohne konkretes Verlangen der betroffenen Person zu löschen, damit sie nicht auf ewige Zeiten virtuell vorhanden bleiben. Eng damit verbunden ist das schützenswerte Interesse jeder betroffenen Person, dass über sie nur korrekte Daten gespeichert werden. Damit sollen Kontrollverlust, Identitätsverfälschungen und Nachteile jeglicher Art verhindert werden. Denn jeder hat das Recht, dass das über ihn gezeigte Bild richtig ist (Simitis 2019 Einl. Rn. 10; Simitis 2014 § 20 Rn. 14).

Damit Daten möglichst korrekt sind, sollen sie weiterhin möglichst bei der betroffenen Person selbst erhoben werden (Prinzip der **Datendirekterhebung**). Um diese grundlegenden Gebote zu kontrollieren und wirksam umzusetzen, wurde das **Konzept des Verantwortlichen** gestärkt: In Art. 4 DSGVO wird definiert, wer für die Datenerhebung, Speicherung und Verarbeitung verantwortlich ist und dementsprechend für Verstöße haftbar gemacht werden kann. Gleichzeitig wurden die **Transparenzpflichten** erweitert und ausgebaut (Art. 12 ff. DSGVO). Die Verantwortlichen müssen in klar verständlicher Sprache offenlegen, welche Daten sie zu welchem Zweck sammeln und wem sie sie weiterleiten. Nur auf diese Weise kann ein Datenfluss nachverfolgt und gegebenenfalls Missbrauch oder Fehlgebrauch aufgedeckt und abgestellt werden.

Schließlich wurden erstmals Bußgeldvorschriften eingeführt und die Eingriffsrechte der Aufsichtsbehörden gestärkt. So finden die getroffenen Regelungen wirklich Beachtung und ihre tatsächliche Einhaltung kann wirksam durchgesetzt werden. Es muss deswegen damit gerechnet werden, dass die Landesdatenschutzbehörden in nächster Zeit ihre intern entwickelten Bußgeldzumessungskataloge anwenden und dementsprechend häufiger als bisher Bußgelder verhängen werden. Berlin hat bereits auf der Zwischenkonferenz der DSK im Juni 2019 ein Bußgeldzumessungsmodell vorgestellt, das allgemein begrüßt wurde und daher Vorbild sein dürfte für andere Aufsichtsbehörden (https://www.datenschutzkonferenz-online.de/media/pr/20190622_pr_mainz.pdf, dort S. 6; letzter Zugriff: 10.02.2020).

Nach dem Berliner Berechnungsmodell soll nicht nur der weltweite Umsatz des Unternehmens Grundlage für die Bußgeldzumessung sein. Um einen Tagessatz festzulegen, soll der Umsatz zudem anscheinend mit einem Faktor multipliziert werden, der den Schweregrad des Verstoßes wiedergeben soll. Die Dauer des Verstoßes, der Verschuldensgrad, die Anzahl der betroffenen Personen und der Umfang des Schadens sollen ebenso berücksichtigt werden wie die Häufigkeit von Verstößen, bereits ergriffene Maßnahmen oder die Zusammenarbeit mit den Aufsichtsbehörden. Auch wenn hierzu noch nichts Genaueres bekannt ist, lässt diese Berechnungsweise vermuten, dass zukünftig auch in Deutschland schmerzhafte Bußgelder verhängt werden dürften (Heidrich 2020).

Der räumliche und sachliche Anwendungsbereich

In der Praxis stellt sich zuallererst die Frage, für welche Art von Daten und wann die DSGVO anzuwenden ist. Gem. Art. 3 DSGVO findet diese Verordnung grundsätzlich immer dann Anwendung, wenn die Tätigkeit im räumlichen Geltungsbereich, also innerhalb eines Mitgliedstaates der Europäischen Union, ausgeführt wird (Niederlassungsprinzip; Simitis 2019 Art. 3 Rn. 25). Die Kindertagespflege in Deutschland, die aufgrund der Regelungen des § 43 SGB VIII stets räumlich an das Vorhandensein konkreter kindgerechter und geeigneter Räume gebunden ist, unterfällt damit in allen Spielarten uneingeschränkt der DSGVO.

Ausweislich Art. 2 Abs. 1 DSGVO, der den sachlichen Anwendungsbereich regelt, gelten die Vorschriften der DSGVO weiterhin für alle Arten von Informationen über einen anderen real existierenden Menschen (also nicht über die Sammelnden selbst), welche in irgendeiner Form dauerhaft festgehalten werden, um sie zu nutzen.

Wie diese Informationen (= Daten) gesammelt werden, ob digital – beispielsweise unter Anwendung einer spezifischen Software – oder auf Papier – zum Beispiel in Form eines Aktenordners –, ob manuell oder in automatisierter Weise, ist dabei völlig irrelevant. Auch Filmaufnahmen oder Fotografien (Fotoalben, Portfolioarbeiten, Sammel-CD-Rom über z. B. Sommerfeiern etc.) sowie Fließtexte (E-Mail-Kommunikationen, fortlaufende Unterhaltungen in sozialen Medien) stellen eine solche Datensammlung dar.

Alle derartigen Sammlungen von – anders definiert – Wissen über ein Tagespflegekind, seine Familie oder seine Betreuung in der Kindertagespflege stellen also eine Datensammlung i.S.d. DSGVO dar, die vor anderweitiger Verwendung geschützt werden muss.

Soweit eine Kindertagespflegeperson in diesem Zusammenhang Daten über sich selbst verarbeitet, unterfallen diese Daten nicht dem Schutz der DSGVO, denn eine Kindertagespflegeperson muss nicht vor sich selbst geschützt werden: Sie kann also beispielsweise ein Selfie von sich in einem Flyer abdrucken, in dem sie sich und ihre Tätigkeit vorstellt. Fotografien betreuter Kinder in demselben Flyer zu verwenden, ist jedoch nur unter Einhaltung der im folgenden dargestellten Voraussetzungen möglich. Verwendet eine Kindertagespflegeperson Daten einer anderen Kindertagespflegeperson, sind die Daten dieser anderen Kindertagespflegeperson ebenfalls DSGVO-konform von ihr zu behandeln.

Weiterhin muss es sich um Daten handeln, die in Zusammenhang mit der unternehmensbezogenen Tätigkeit erhoben werden. Ausschließlich rein persönliche oder rein privat-familiäre Tätigkeiten unterfallen nicht der DSGVO, da sich der europäische Gesetzgeber gegen eine staatliche Überwachung dieses höchst privaten Bereichs entschlossen hat (Simitis 2014 § 1 Rn. 149).

Die Pflege rein privater Freundschaften oder Kontakte zu anderen Personen ohne jeglichen Bezug zur Kindertagespflege unterfallen somit nicht dem DSGVO. Dies gilt beispielsweise für das private Fotoalbum, die Zusammenstellung der eigenen Urlaubsfotos in einer Cloud für die eigenen Verwandten oder Freunde. Wird jedoch ein berufliches Fotoalbum oder eine Fotogalerie aller jemals betreuten Tagespflegekinder oder der Aktivitäten mit den aktuellen Tagespflegekindern (z. B. die gesammelt weitergeleiteten Fotos des Ausfluges mit den Tagespflegekindern zum Streichelzoo) erstellt, so richtet sich die Zulässigkeit nach der DSGVO. Auch vom rein privaten Gebrauch abzugrenzen ist es, wenn die Kindertagespflegeperson Kontaktdaten über ehemalige Tagespflegekinder und deren Erziehungsberechtigten sammelt und eine „Interessentenliste Kindertagespflege“ oder eine entsprechende Warteliste anlegt. Solche Listen anzulegen und zu pflegen ist nur dann zulässig, wenn die verschiedenen datenschutzrechtlichen Vorgaben eingehalten werden.

Der Informationsaustausch innerhalb eines geschlossenen Kreises ist ebenfalls nicht mehr der rein privaten Lebensführung zuzuordnen, wenn ein nicht-privater Bezug besteht (Simitis 2014 § 1 Rn. 151; Simitis 2019 Art. 2 Rn. 23 ff). Dies gilt insbesondere für Netzwerktreffen oder -chats von Kindertagespflegepersonen untereinander. Hier werden Daten anderer Personen ausgetauscht und damit zwangsläufig verarbeitet, nämlich zumindest die Daten der anderen Kindertagespflegepersonen im Chat und, soweit im Chat über bestimmte Tagespflegekinder gesprochen wird, die Daten dieser Tagespflegekinder. In diesem Zusammenhang wird nochmals darauf hingewiesen, dass ein Austausch zu bestimmten Tagespflegekindern auch in einem solchen Rahmen in anonymisierter Form stattfinden sollte.

Definitionen

Dreh- und Angelpunkt allen Schutzes ist die Frage, welche Daten überhaupt geschützt werden müssen. Gem. **Art. 4 Nr. 1 DSGVO** (und § 46 BDSG; Simitis 2019 Art. 4 Rn. 14 ff.) unterfallen dem Schutzzweck alle **personenbezogenen Daten,** also alle

> *„**Informationen,** die sich auf eine identifizierte oder identifizierbare **natürliche Person** (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann."*

Kurz und bündig sind personenbezogene Daten entsprechend der früheren Definition in § 3 BDSG (alt):

> *„Personenbezogene Daten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person, also eines Menschen, egal in welcher Form sie vorliegen, und egal welchen Inhalts."*

Im Bereich der Kindertagespflege sind dies beispielsweise: Name, Vorname, Geburtsort, Geburtsdatum, Adresse, Telefonnummer, Angaben zu den Erziehungsberechtigten, alle Angaben zum Kind wie Vorlieben, Abneigungen, Entwicklungszustand, Größe, Allergien, Erkrankungen, Vorgeschichte etc.
Abstrakt gehaltene Informationen (insbesondere abstrahierte Sammlungen) zu dem Kind oder dessen Erziehungsberechtigten, welche diese zwar nicht direkt bezeichnen, aber identifizierbar i.S.v. „bestimmbar" bzw. „rückverfolgbar" machen, können beispielsweise sein: Fotografien und Filmaufnahmen, „Problemverhaltensaktenordner", anonyme Elternbewertungen in einer Sammelmappe zur Ansicht für Interessenten oder die Sammlung anonymisierter Elternbeschwerden.
Insbesondere anonymisierte Elternbewertungen lassen auf den ersten Blick keine Zuordnung zu einer bestimmten Person zu. Bei entsprechender Vorkenntnis kann allerdings über Zwischenschritte – beispielsweise aus dem konkreten Inhalt der Bewertung und insbesondere aus Beschreibungen zum Betreuungsalltag, zur Dauer und dem Zeitpunkt der Betreuung sowie zu individuellen Besonderheiten des Tagespflegekindes, mit denen die Kindertagespflegeperson besonders einfühlsam umgegangen ist – leicht auf ein bestimmtes Kind geschlossen werden. Auch auf derartige Daten identifizierbarer Personen ist die DSGVO anzuwenden (Simitis 2019 Art. 4 Rn. 46).
Unter **Datenverarbeitung** werden schlicht alle Tätigkeiten erfasst, die mit oder an diesen Informationen durchgeführt werden: Die Erhebung dieser Informationen, die Organisation und Ordnung (z. B. systematische Aufbereitung in Wartelisten anhand gewünschter Eintrittsdaten in die Tagespflege), die Speicherung (auch in Aktenordnern und auf Papier), die Anpassung und Veränderung (z. B. die Abänderung von Namen, Änderung des Betreuungsbedarfs oder der Betreuungszeiten), die Offenlegung durch Übermittlung (z. B. an Vermittlungs- oder Trägervereine oder an den öffentlichen Jugendhilfeträger bei Beantragung der Förderung nach § 23 SGB VIII), der Abgleich (z. B. in Form von Belegbögen über die monatliche Betreuungstätigkeit, Umfang und Anzahl der betreuten Tagespflegekinder), aber auch die Einschränkung (z. B. die Sicherung vor unkontrollierten Zugriff durch Wegsperren oder Passwortsicherung), das Löschen oder die Vernichtung (Simitis 2019 Art. 4 Rn. 10 ff.).
Bereits diese beispielhafte Aufzählung zeigt, dass sämtliche Informationen in sämtlichen Arbeitsschritten erfasst sind. Ebenso sind sämtliche **Dateisysteme** erfasst: Jede Art einer strukturierten Sammlung von Informationen über einen anderen Menschen, dessen Daten aus nicht-privatem Anlass erhoben wurden, ist mit dem Begriff „Dateisystem" gem. Art. 4 Nr. 6 gemeint. Es reicht dabei schon aus, wenn ein einziges Strukturelement vorhanden ist (Simitis 2019 Art. 4 Nr. 6 Rn. 7 ff.; Ehmann/Selmayr Art. 2 Rn. 32), beispielsweise ein einziger Aktenordner „Kindertagespflege", in dem alle Unterlagen zu allen Tagespflegekindern abgeheftet sind.
Ebenfalls von Bedeutung ist die Unterscheidung von „nur" personenbezogenen Daten und „besonderen personenbezogenen Daten". Letztere Daten sind besonders zu schützen.
Der Kategorie „nur" **personenbezogene Daten** unterfallen in der Kindertagespflege insbesondere die umgangssprachlich als „Stammdaten" (häufig auch: „Kontaktdaten") bezeichneten Daten. Das sind insbesondere die Daten, die erforderlich sind, um rein sachlich das zu betreuende Tagespflegekind und seine Erziehungsberech-

tigten zu identifizieren, Kontakt zu den Erziehungsberechtigten aufzunehmen oder um Allgemeines rund um den Vertrag abzuwickeln: Name, Vorname, Adresse, Telefonnummern, E-Mail-Adressen.
Die für die Kindertagespflege wichtigste Gruppe der **„besonderen personenbezogenen Daten"** stellen die **Gesundheitsdaten** dar. Gesundheitsdaten werden nach der DSGVO definiert als

> *„personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen".*

Irrelevant ist, woher die Daten kommen oder aus welcher Sphäre (Intim-, Privat- oder Familiensphäre) sie stammen (Simitis 2019 Art. 4 Rn. 30.). Sie können vom Nachbarn, von einem Arzt oder Apotheker, aber auch durch ein Fitnessarmband oder eben eine Kindertagespflegeperson erhoben worden sein. Insbesondere die Erstellung und Pflege von Entwicklungsprotokollen, um Entwicklungsverzögerungen des Kindes zu ermitteln und zu analysieren, ist eine Sammlung derartiger Gesundheitsdaten, denn alle Informationen, welche unmittelbar oder mittelbar Rückschlüsse auf den Gesundheitszustand einer Person zulassen, unterfallen dieser Definition: Allergien, Nahrungsmittelunverträglichkeiten, Ernährungsgewohnheiten, Krankheiten, auftretende Nebenwirkungen oder Komplikationen gesundheitlicher Art während der Betreuung (z. B. Neigung zu Fieberkrämpfen, aber auch indirekte Informationen wie z. B. Größe oder Gewicht, die aus dem jeweiligen Verwendungszusammenhang Rückschlüsse auf den Gesundheitszustand eines Kindes erlauben (Simitis, Art. 4 Nr. 15 Rn. 3ff). Dazu zählen darüber hinaus Informationen über Entwicklungsstand, Entwicklungsverläufe, Aufenthalte in gesundheitsrelevanten Einrichtungen wie Kur-, Reha- oder Klinikaufenthalte u. ä. Auch Daten, die nur in einer Gesamtschau oder mittelbar Rückschlüsse auf den Gesundheitszustand der betroffenen Person zulassen – beispielsweise Informationssammlungen über die Reizbarkeit und Konzentrationsfähigkeit eines Kindes oder Arzneimitteleinnahmen, welche das Vorliegen einer Diagnose wie ADHS vermuten lassen, – sind Gesundheitsdaten i.S.d. DSGVO.
Diese besonders sensible Kategorie von personenbezogenen Daten darf nur nach **besonderer Einwilligung** der betroffenen Person oder nur bei Vorliegen eines der Erlaubnistatbestände des Art. 9 DSGVO i.V.m. § 22 BDSG in engen Grenzen erhoben werden. Hier gilt ebenfalls das Prinzip des Verbots mit Erlaubnisvorbehalt und des Koppelungsverbotes.
Gesundheitsdaten, die nicht erforderlich sind, um einen Vertrag abzuschließen oder umzusetzen, dürfen nicht erhoben werden. Ihre Preisgabe darf dementsprechend nicht zwingend zum Abschluss des Vertrages verlangt werden. So kann eine Kindertagespflegeperson beispielsweise darauf pochen, dass Allergien, Lebensmittelunverträglichkeiten und Erkrankungen, die auch während der Betreuung auftreten können, preisgegeben werden; nach Sinn und Zweck des Schutzgedankens hinter Art. 9 DSGVO kann sie das Tagespflegekind nur dann richtig und sicher betreuen, wenn sie diese potentiellen Risiken kennt, also nur auf diese Weise das Kindeswohl wahren und schützen.
Hier dürfte eine Erforderlichkeit zur Gesundheitsvorsorge und zur Versorgung im Sozialbereich (Betreuungstätigkeit als Sozialleistung nach den §§ 22 ff. SGB VIII) gem. § 22 BDSG oder zumindest zum Schutz lebenswichtiger Interessen des Betroffenen (Schutz vor Gesundheitsbeeinträchtigungen während der Betreuung) vorliegen, auch wenn dies gesetzlich noch nicht klar geregelt ist. Es bleibt daher zu hoffen, dass entsprechende Präzisierungen in den geplanten Änderungen zu den Sozialgesetzbüchern Eingang finden werden.
Zu verlangen, dass alle bekannten – auch die nicht relevanten – Diagnosen des Kindes, uneingeschränkt offengelegt werden, ist vor dem Hintergrund des Schutzgedankens dahingegen unzulässig. So darf der Abschluss eines Betreuungsvertrages oder die Durchführung der Betreuung nicht davon abhängig gemacht werden, ob beispielsweise eine Diagnose wie Café-au-lait-Flecken – eine gutartige, nicht behandlungsbedürftige Hautveränderung ohne relevanten Krankheitswert – preisgegeben wird; Hautveränderungen ohne Krankheitswert sind nicht geeignet, die Betreuung des Kindes in irgendeiner Weise zu beeinflussen.
Es ist vor diesem Hintergrund daher empfehlenswert, sich nicht nur auf die Erhebungsermächtigungsgrundlagen nach Art. 9 Abs. 2 b ff. DSGVO zu verlassen, sondern zusätzlich eine Einwilligung nach Art. 9 Abs. 2a DSGVO einzuholen.
Es muss sich allerdings um eine ausdrückliche und unmissverständliche Einwilligung der Erziehungsberechtigten für das Tagespflegekind handeln. In diesem Falle muss die betroffene Person vor der Einwilligung genau über die Art der erhobenen Daten, den Zweck der Erhebung (oder die Zwecke, wenn mehrere) und die Emp-

fänger der Daten informiert worden sein. Es wird dringend angeraten, die Einwilligung zu Beweissicherungszwecken schriftlich vorzunehmen, auch wenn die Schriftform hier nicht vorgeschrieben ist und – bei entsprechender Sicherung der zukünftigen Datenzugänglichkeit – beispielsweise elektronisch möglich ist. Sie ist von anderen Einwilligungen deutlich abzugrenzen und klar und unmissverständlich als Einwilligung i.S.d. Art. 9 DSGVO zu kennzeichnen (Simitis Art. 9 Rn. 32 ff.; Datenschutzkonferenz Kurzpapier Nr. 20).
Die Einwilligung sollte sich ausdrücklich auf die Erhebung von Gesundheitsdaten *des Tagespflegekindes* beziehen, die für die Betreuung erforderlich sind. Gesundheitsdaten der Erziehungsberechtigten dürften für die Betreuung des Kindes i. d. R. nicht notwendig sein. Soweit es im Einzelfall zur Betreuung des Tagespflegekindes erforderlich wäre, Gesundheitsdaten der Erziehungsberechtigten zu erheben, sollte hierfür eine gesonderte Einwilligung bei den Erziehungsberechtigten eingeholt werden.

Die Erlaubnistatbestände nach Art. 6 DSGVO

Datenschutzrechtlich gilt der Grundsatz des **Erlaubnisvorbehalts.** Dies bedeutet, dass Daten über eine natürliche Person grundsätzlich gar nicht erhoben werden dürfen, es sei denn, es liegt ein Erlaubnistatbestand vor (Erwägungsgrund Nr. 40 zu Art. 6 DSGVO). Die zulässigen Erlaubnistatbestände finden sich in Art. 6 DSGVO, der zentralen Vorschrift der DSGVO. Die für die Kindertagespflege wichtigsten Erlaubnistatbestände sind nach Art. 6 Abs. 1 DSGVO:

a. Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
b. Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.
c. Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.
d. Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person *oder einer anderen natürlichen Person* [vorliegend: des Tagespflegekindes] zu schützen.
e. Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

> Für jede Art von Daten, die verarbeitet (= auch schon: erhoben) werden, muss ein zum dahinterstehenden Zweck passender Erlaubnistatbestand vorliegen.

Die beiden zentralen Erlaubnistatbestände, welche in der Kindertagespflege die meisten der üblichen Datenverarbeitungen erlauben dürften, sind dabei Art. 6 Abs. 1 b (zur Erfüllung eines Vertrags/vorvertraglicher Maßnahmen, rechtlicher Verpflichtung) und Abs. 1a (Einwilligung).
Haupterlaubnistatbestand ist dabei Art. 6 Abs. 1b Alt. 1 DSGVO: Die Erhebung und Verarbeitung dieser Daten ist erforderlich zur Erfüllung (Umsetzung) eines Vertrages. Werden die Daten des Tagespflegekindes und seiner Erziehungsberechtigten (wie die häufig als Stammdaten bezeichneten Informationen wie Name, Vorname, Adresse, Geburtsdatum, Kontaktdaten, Betreuungswünsche, Beginn, Dauer, Betreuungsgrund wegen § 24 SGB VIII: Berufstätigkeit, Arbeitssuche etc.) nicht erhoben, kann die Betreuung nicht durchgeführt werden und eine Förderung des Betreuungsverhältnisses nicht in die Wege geleitet bzw. unterstützt werden. Ist keine Förderung des Betreuungsverhältnisses beabsichtigt, ist von der Kindertagespflegeperson zu prüfen, ob die Erhebung des Betreuungsgrundes von einem anderen der Erlaubnistatbestände des Art. 6 DSGVO gedeckt sein könnte.
Im vorvertraglichen Bereich müssen zumindest einige Kerndaten wie Name, Adresse, Kontaktdaten, gewünschtes Eintrittsdatum, Alter des Kindes (zur Planung der Altersstruktur in der Gruppe oder zur Prüfung der Einhaltung von Auflagen in der Pflegeerlaubnis) erhoben werden. Dies ist gem. Art. 1 Abs. 1b Alt. 2 DSGVO zulässig, damit der anfragende potentielle zukünftige Vertragspartner überhaupt erst identifizierbar und ansprechbar wird. Zur Nachweissicherung sollte jedoch dringend vor der Erhebung eine kurze Information über die diesbezügliche Datenerhebung herausgegeben werden.

Merke:
- Vor Vertragsschluss sollten nur die notwendigsten Kerndaten zum Tagespflegekind und seinen Erziehungsberechtigten verarbeitet werden.
- Vor dieser Datenverarbeitung sind die Betroffenen über die Datenverarbeitung und ihre Zwecke zu informieren. Ihre Einwilligung ist einzuholen.
- Die durchgeführte Information und die Einwilligung sind bis zur Datenlöschung zu archivieren.

Dieser Erlaubnistatbestand rechtfertigt jedoch nicht die Verarbeitung aller Daten, die im Laufe einer Betreuung anfallen können. Daneben ist eine Kindertagespflegeperson nach § 43 Abs. 3 S. 6 SGB VIII über die normale, alltägliche und routinemäßige Datenverarbeitung hinaus im Einzelfall verpflichtet, *„wichtige Ereignisse"*, welche für die Betreuung des Tagespflegekindes bedeutsam sein können, an den öffentlichen Jugendhilfeträger zu melden. Ziel dieser Vorschrift ist es, Gefährdungen des Kindeswohls rechtzeitig zu erkennen, abzuwenden oder abzustellen. Aufgrund dieser Verpflichtung ist sie also angehalten, auch Beobachtungen anlässlich der Betreuung zu verarbeiten, beispielsweise Veränderungen im Betreuungsumfang, Unfälle des Kindes, Verletzungen am Kind (inklusive der Lage), Entwicklungsverzögerungen, aber auch Anzeichen für Verwahrlosung, wobei eine Abgrenzung zu Meldungen i.S.d. § 8a SGB VIII in der Praxis oft schwer möglich ist. Der entsprechende datenschutzrechtliche Erlaubnistatbestand ist in der Mehrheit der Fälle jedoch Art. 6 Abs. 1 S. 1c DSGVO i.V.m. § 43 Abs. 3 S. 6 SGB VIII.

Soweit auch eine Verpflichtung einer Kindertagespflegeperson zur Meldung „gewichtiger Anhaltspunkte" gem. § 8a Abs. 1, 5 SGB VIII besteht (eher bejahend Wiesner § 8a Rn. 68), kommt Art. 6 Abs. 1 S. 1c DSGVO i.V.m. § 8a SGB VIII als Erlaubnistatbestand in Frage. Es spricht in der Tat einiges dafür, dass § 8a SGB VIII für Kindertagespflegepersonen zumindest in analoger Form anwendbar ist. Tagespflegekinder würden andernfalls in der Kindertagespflege nicht dieselbe Schutzstandard genießen wie in Kindertagesstätten oder sonstigen Betreuungseinrichtungen. Eine derartige Benachteiligung von Tagespflegekindern dürfte nicht der gesetzgeberischen Intention entsprechen.

§ 8a SGB VIII dürfte jedoch nicht uneingeschränkt auf die Kindertagespflege anwendbar sein, denn Kindertagespflegepersonen sind meist keine besonders ausgebildeten Fachkräfte im Sinne dieser Vorschrift. Sie können auch nicht auf interne Fachkräfte zur Gefährdungseinschätzung zurückgreifen, da sie i. d. R. alleine arbeiten. Sie können daher keine eigene Gefährdungseinschätzung vornehmen und die Erziehungsberechtigten beraten, sondern lediglich Wahrnehmungen erfassen und dem „zuständigen Fachpersonal" (im Zweifel: der zuständigen Sachbearbeiterin oder dem zuständigen Sachbearbeiter beim öffentlichen Jugendhilfeträger) melden. In analoger Anwendung des § 8a SGB VIII dürften sie zumindest ähnlich einem Träger der Verpflichtung unterliegen, zunächst das Gespräch mit den Erziehungsberechtigten zu suchen und diese im Falle einer Datenweitergabe an den öffentlichen Jugendhilfeträger zu informieren.

Unabhängig von § 8a SGB VIII haben Kindertagespflegepersonen aber in jedem Falle Anspruch darauf durch den öffentlichen Jugendhilfeträger nach § 8b SGB VIII beraten zu werden. Allerdings können sie keiner der vom Gesetz zur Kooperation und Information im Kinderschutz (KKG) aufgezählten besonderen Berufsgruppen zugeordnet werden. Daher dürfen sie nach dieser Vorschrift gemäß § 4 KKG weder bei den Erziehungsberechtigten auf die Inanspruchnahme von (ggf. auch frühen) Hilfen hinwirken, noch nach dieser Vorschrift „Klar"-Daten an den öffentlichen Jugendhilfeträger weiterleiten. Eine Kindertagespflegeperson darf jedoch im Falle einer Beratung i.S.d. § 8b SGB VIII in ergänzender Heranziehung des § 4 Abs. 2 KKG während der Beratung pseudonymisierte Daten verwenden (siehe Art. 4 Nr. 5 DSGVO), um die generelle Fragestellung mit der Fachkraft besprechen zu können (z. B. Wiesner 2015 § 8b Rn. 23).

Vor dem Hintergrund der möglicherweise unklaren Rechtslage empfiehlt es sich daher zur eigenen Absicherung, vor einer Weitergabe konkreter Daten i.S.d. § 8a oder 8b SGB VIII an den öffentlichen Jugendhilfeträger auf die vorherige (schriftliche) Einwilligung der Erziehungsberechtigten zum „Klar"-Datenaustausch hinzuwirken. Auf diese Weise kann die Kindertagespflegeperson dann im Ernstfall zumindest den Erlaubnistatbestand der Einwilligung gemäß Art. 6 Abs. 1a DSGVO vorweisen. Soweit diese Einwilligung verweigert wird, ist im Einzelfall noch der Rückgriff auf den Erlaubnistatbestand des Art. 6 Abs. 1d (Erforderlichkeit zum Schutz lebenswichtiger Interessen des/der Betroffenen) denkbar.

Tipp:
Wenn *Sie als Kindertagespflegeperson* Beobachtungen am Tagespflegekind oder bei den Erziehungsberechtigten gemacht haben, die eine Kindeswohlgefährdung vermuten lassen könnten:

- Dokumentieren Sie Ihre Beobachtungen möglichst genau (Tag, Uhrzeit, Anlass, genaue Beschreibung, spontane Äußerungen dazu).
- Bevor Sie sich hilfesuchend an Behörden wenden, suchen Sie zuerst das Gespräch mit den Erziehungsberechtigten und – soweit altersbedingt möglich – mit dem Kind, um den Wahrheitsgehalt Ihrer Beobachtungen zu verifizieren.
- Sind Ihre Bedenken dann immer noch nicht ausgeräumt, nehmen Sie Kontakt mit Ihrer/m Sachbearbeiter/in beim öffentlichen Jugendhilfeträger auf, um eine allgemeine, pseudonymisierte Beratung anzufordern.
- Erarbeiten Sie im Rahmen dieser allgemeinen Beratung weitere mögliche Handlungsschritte und versuchen Sie, diese im konkreten Fall umzusetzen.
- Verbleiben weiterhin Bedenken, holen Sie zuerst die (schriftliche oder elektronische) Einwilligung am besten beider Erziehungsberechtigten (= Unterschrift) ein, bevor Sie Daten eines bestimmten Tagespflegekindes und seiner Erziehungsberechtigten an den öffentlichen Jugendhilfeträger weitergeben.
- Dokumentieren Sie jeden einzelnen Ihrer Schritte in einer Weise, dass die Dokumentation später zuverlässig abrufbar ist. Es empfiehlt sich die Papierform.

Tipp:

- Bittet *der öffentliche Jugendhilfeträger Sie* im Rahmen einer (ggf. aus anderem Anlass eingeleiteten) Einschätzungsmaßnahme um Auskunft, verlangen Sie eine schriftliche Aufforderung und klare Benennung der konkret von Ihnen angeforderten Daten (insb. auch Beobachtungen) sowie der Rechtsgrundlage hierfür.
- Beantworten Sie derartige Anfragen, soweit möglich, nicht mündlich oder telefonisch, sondern schriftlich.
- Klären Sie mit dem öffentlichen Jugendhilfeträger, ob Sie berechtigt sind, die Erziehungsberechtigten über die erfolgte Auskunft zu informieren.
- Dokumentieren Sie jeden Schritt und jede Auskunft. Bewahren Sie eine Kopie Ihrer Auskunft auf. Auch hier empfiehlt sich die Schriftform.

Damit die Kindertagespflegeperson gesundheitliche Verschlechterungen am Kind korrekt erkennen bzw. einordnen und rechtzeitig die richtigen medizinischen Maßnahmen in die Wege leiten kann, muss sie über betreuungsrelevante Erkrankungen und gesundheitlicher Beeinträchtigungen wie Allergien, Asthma, Neigung zu Fieberkrämpfen, Organinsuffizienzen etc. in Kenntnis gesetzt sein.
Zielsetzung dieser Datenerhebungen ist demnach der Schutz lebenswichtiger Interessen *„des Betroffenen oder einer anderen betroffenen Person"*, nämlich des Tagespflegekindes, dessen Gesundheit und Wohlbefinden geschützt werden sollen.
Der entsprechende datenschutzrechtliche Erlaubnistatbestand für diese Datenerhebungen sind im Zweifel Art. 6 Abs. 1c und d DSGVO.
Weiterhin kann es in Einzelfällen erforderlich sein, beispielsweise Daten der Arbeitgeberin oder des Arbeitgebers eines erziehungsberechtigten Vertragspartners zu erheben, um vertragliche Vergütungsansprüche durchzusetzen (z. B. Gehaltspfändung, wenn die vereinbarte Vergütung nicht bezahlt wird). Derartige Datenerhebungen können durch Art. 6 Abs. 1f DSGVO gedeckt sein.

Merke:
Allen genannten Erlaubnistatbeständen ist gemein, dass der nachträgliche Beweis ihres Vorliegens in der Praxis für den Verantwortlichen – die Kindertagespflegeperson – u. U. erschwert sein kann.

Vor diesem Hintergrund ist daher dringend zur umfassenden Absicherung anzuraten, den Erziehungsberechtigten vor Vertragsschluss zusätzlich eine umfassende Aufklärung zukommen zu lassen, in der alle denkbaren Datenverarbeitungsfälle, ihre Zwecke und ihre Rechtsgrundlagen aufgeführt sind. Im Anschluss hieran sollte die Einwilligung zur Datenerhebung (Unterschrift) eingefordert werden.

Die Einwilligung in die Datenverarbeitung

Soweit kein anderer Erlaubnistatbestand vorliegt, muss die betroffene Person in die Datenerhebung, Verarbeitung und Weiterleitung zu einem bestimmten Zweck einwilligen. Um eine ausreichende Einwilligung i.S.d. Art. 6 Abs. 1a, 4 Nr. 11 handelt es sich nur dann, wenn die oder der Betroffene **vor** der Einwilligung umfassend informiert wurde über

- Art der Daten, die erhoben werden
- Rechtsgrundlage der Datenerhebung

- Zweck der einzelnen Datenerhebungen
- Darlegung der einzelnen Erhebungs- und Verarbeitungsschritte
- Kreis der Verantwortlichen und Auftragsverarbeiter mit Zugriff auf diese Daten
- Kreis der Empfänger der Daten
- Art und Dauer der Speicherung inkl. Löschfrist
- Auskunftsrechte

Die Einwilligung muss freiwillig erfolgen. Sie ist dann nicht mehr freiwillig, wenn die oder der Betroffene gezwungen wird Daten preiszugeben, um die erwünschte Gegenleistung zu erhalten („Take-it-or-leave-it-Konstellationen"). Es gilt das Prinzip des **Koppelungsverbotes.** Danach ist die Freiwilligkeit einer Einwilligung insbesondere dann zu hinterfragen, wenn der Abschluss eines Vertrags davon abhängig gemacht wird, ob jemand in die Verarbeitung solcher personenbezogenen Daten einwilligt, deren Verarbeitung zur Vertragserfüllung nicht erforderlich sind.
Die Preisgabe von Daten, die zur Durchführung eines Vertrages unbedingt erforderlich sind, führt dahingegen i. d. R. nicht zum Entfall der Freiwilligkeit (Datenschutzkonferenz Kurzpapier Nr. 20).
So ist i. d. R. beispielsweise zulässig, als Bedingung für den Abschluss eines Betreuungsvertrages eine Einwilligung zur Erhebung grundlegender Daten wie Name, Vorname, Adresse des Tagespflegekindes und der vertragsabschließenden Erziehungsberechtigten sowie des Geburtsdatums des Tagespflegekindes zu verlangen. Ohne diese grundlegenden Informationen kann eine Betreuung nicht durchgeführt werden. Andererseits dürfte die Einwilligung in die Erhebung von Daten wie beispielsweise der Verwandtschaftsbeziehung eines Abholberechtigten zum Tagespflegekind nicht erforderlich sein., um die Kindertagespflege durchzuführen Um die Frage zu klären, wer das Tagespflegekind bei Verhinderung der Erziehungsberechtigten abholen darf, ist lediglich die Angabe des Namens der abholberechtigten Person und ihrer Kontaktdaten nötig. Ein Verwandtschaftsverhältnis ist nicht erforderlich, denn Erziehungsberechtigte können Teile ihres Sorgerechts wie beispielsweise die Aufsichtspflicht über ihr Kind auch an nicht mit ihnen verwandte Personen übertragen. Inwieweit es erforderlich ist, Informationen zur Religionszugehörigkeit zu erheben, um die Kindertagespflege auszuüben, muss im Einzelfall geprüft werden. Soweit die Erhebung nur dazu dienen würde, religiöse Ge- und Verbote in der Speisenzubereitung beachten zu können, dürfte dies unnötig sein, denn Informationen über Essensvorlieben und -abneigungen können direkt abgefragt werden.
Erstaunlicherweise verlangt die DSGVO in ihrer aktuellen Fassung kein Schriftformerfordernis für die Einwilligung in die Erhebung personenbezogener Daten mit Ausnahme der besonderen personenbezogenen Daten (Gesundheitsdaten, Art. 4 Nr. 15 DSGVO). Soweit es sich nicht um solche besonders schützenswerten Daten handelt, kann die Einwilligung also auch durch konkludentes Handeln erteilt werden, solange die Handlung eindeutig, klar und unmissverständlich als Einwilligung ausgelegt werden kann (Simitis 2019 Art. 9 Rn. 33). Häufig sind damit aber im Nachhinein Nachweisprobleme zu Lasten der Kindertagespflegeperson verbunden. Im eigenen Interesse sollte daher auf Verschriftlichung gepocht werden.
Übereicht eine Interessentin/ein Interessent einer Kindertagespflegeperson also beispielsweise ihre oder seine Visitenkarte, damit diese sie kontaktieren kann, wenn ein Betreuungsplatz frei wird, hat die Interessentin/der Interessent damit konkludent ihre Einwilligung zur Aufbewahrung und Benutzung ihrer auf dieser Karte vorhandenen Daten erteilt. Gleiches gilt nach derzeitigem Stand für die ungefragte Zusendung beispielsweise einer E-Mail-Nachricht durch interessierte Eltern zum Zwecke der Kontaktaufnahme. Allerdings kann der Vorgang an sich und insbesondere der Anlass, warum, oder die Art und Weise, wie eine Visitenkarte übereicht wurde, im Nachhinein von der Kindertagespflegeperson nicht mehr bewiesen werden. Der entsprechende Nachweis bei einer E-Mail-Nachricht ist unter Rückgriff auf passende Anwendungsprogramme und bei Speicherung der Nachricht zumindest, wenn auch mit erhöhtem Aufwand, möglich.

> Da die Kindertagespflegeperson jedoch als Verantwortliche i.S.d. DSGVO jederzeit nachweisen muss, dass sie die bei ihr vorhandenen Daten korrekt erhoben hat (also mit vorheriger freiwilliger Einwilligung des Betroffenen), empfiehlt es sich in der Praxis aus Gründen der Rechtssicherheit und insbesondere der eigenen Absicherung vor Haftungsfällen, sich in jedem Fall eine schriftliche Einwilligung zur Datenerhebung und Verarbeitung unterschreiben zu lassen.

Die Einwilligung in die Datenerhebung von Daten der Erziehungsberechtigten und des Tagespflegekindes erfolgt stets durch einen Erziehungsberechtigten, da das in aller Regel nicht

geschäftsfähige Tagespflegekind nicht selbst einwilligen kann. Dies ist zulässig (Art. 6 Abs. 1a i.V.m. Art. 8 DSGVO, §§ 107 ff. BGB), sollte aber bei der Formulierung der Einwilligung berücksichtigt werden. Gerade im vorvertraglichen Kontakt mit Interessenten kann eine solche Einwilligung beispielsweise dadurch erfolgen, dass Interessenten selbst einen „Anmeldebogen" ausfüllen. Am Kopfende des kurzen Formulars könnte sich eine kurze Belehrung zur Datenerhebung und der Gründe hierzu (vorvertragliche Maßnahme: Erreichbarkeit für ein späteres Auswahlverfahren für eine zukünftige Platzvergabe) befinden. Die Daten aus dem Anmeldebogen können dann in einem weiten Schritt intern von der Kindertagespflegeperson in eine Datei übertragen und aufbereitet werden. Für Interessentenunterlagen und -listen sollten kürzere Löschfristen vorgesehen sein als für vertragliche Unterlagen und Daten. Nach Ablauf von ca. drei Jahren entfällt üblicherweise der Bedarf an einem Betreuungsplatz in der Kindertagespflege, sei es, weil das Kind altersbedingt bereits in den Kindergarten gewechselt ist, sei es, weil es einen anderen Betreuungsplatz erhalten hat (es sei denn, die Platzanfrage bleibt für ein Geschwisterkind aufrechterhalten). In diesen Fällen dürften auch keine Schadensersatz- oder Haftungsfragen für die Kindertagespflegepersonen zu befürchten sein, sodass es schwer begründbar sein dürfte. Die Erhebung von Gesundheitsdaten, die in der Kindertagespflege bei Vertragsschluss nicht vermeidbar ist, muss in jedem Falle unmissverständlich, schriftlich und gesondert geregelt werden – am besten durch ein Dateninformationsblatt und indem entsprechende Klauseln im Betreuungsvertrag aufgenommen werden.

Weitere Begriffsbestimmungen: der Verantwortliche, der Auftragsverarbeiter und der Empfänger[1]

Entsprechend der Definition in Art. 4 Nr. 7 DSGVO ist **Verantwortlicher** i.S.d. DSGVO, wer zur Erreichung eines eigenen nicht-privaten Zweckes Daten über eine andere natürliche Person erhebt. Natürliche Personen und hier insbesondere Selbstständige wie Kindertagespflegepersonen, aber auch Ärztinnen und Ärzte oder Handwerkerinnen und Handwerker, sind damit ebenso sehr Verantwortliche in diesem Sinne wie beispielsweise ein öffentlicher Jugendhilfeträger als Behörde (Simitis 2019 Art. 4 Nr. 7 Rn. 14 ff.; Gesetzesbegründung zum BayDSG S. 70).

Als Faustregel gilt:
Verantwortliche/r ist dabei diejenige Person, welche die Entscheidungshoheit über die Erhebung sowie über Zweck und Mittel der Verarbeitung hat (Simitis 2019 Art. 4 Nr. 7 Rn. 20). Diese/r Verantwortliche trägt sodann im Außenverhältnis zur betroffenen Person und gegenüber den Datenschutzaufsichtsbehörden die Verantwortung für die Datenerhebung und -verarbeitung und haftet für Datenschutzverstöße. Dieser Grundsatz findet sich bereits in § 11 Abs. 1 BDSG a.F.
Notiert eine Kindertagespflegeperson beispielsweise die Kontaktdaten und Betreuungsbedürfnisse von Interessentinnen und Interessenten, ist sie demnach die Verantwortliche für die Datenerhebung, da sie im eigenen beruflichen Interesse handelt.
Wer Daten lediglich erhebt oder verarbeitet, um eine andere Person und deren Tätigkeit zu unterstützen, ist nicht Verantwortlicher i.S.d. Art. 4 DSGVO, sondern eher Hilfspersonal, dessen Handlungen und Verstöße sich der Verantwortliche zurechnen lassen muss.

> Eine Lebensgefährtin oder ein Lebensgefährte bzw. eine Ehepartnerin oder ein Ehepartner einer Kindertagespflegeperson, die oder der diese in der allgemeinen Verwaltung unterstützt und für sie beispielsweise in einer Computerdatei eine Liste der Interessentinnen/Interessenten erstellt, wird nicht aus eigenem beruflichem Interesse aktiv, sondern handelt ausschließlich auf Weisung der Kindertagespflegeperson für deren berufliches Interesse. Als Hilfspersonal der Kindertagespflegeperson unterliegt sie oder er der unmittelbaren Verantwortung der Kindertagespflegeperson und darf die Daten nur in deren Auftrag verarbeiten. Eine Kenntnisnahme rein aus privater Neugier ist nicht zulässig. Die Kindertagespflegeperson als Verantwortliche hat die Einhaltung des Datenschutzes ebenso laufend zu überwachen, wie auch die Einhaltung der Verschwiegenheitsverpflichtung.

Ein **Auftragsverarbeiter** ist nach Art. 4 Nr. 8 ein natürlicher (Mensch) oder eine juristische Person (GmbH usw.), Behörde, Einrichtung oder andere Stelle, welche personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet (Simitis 2019 Art. 4 Nr. 8 Rn. 5 ff.; Bayr. Landesbeauftragte für Datenschutz: Auftragsverarbeitung S. 5).
Es handelt sich dabei um eine Person oder Stelle, welche beispielsweise im Rahmen eines Auftragsverhältnisses für den Verantwortlichen tätig wird, aber außerhalb dessen Einwirkungsbereiches steht. Sie ist diesem lediglich

1 hier wird analog zu den Formulierungen in den jeweiligen Rechtsgrundlagen die maskuline Form verwendet

über einen Auftrag verbunden, aber dennoch weisungsabhängig. Dieser Auftragsverarbeiter muss ebenso wie der Verantwortliche sämtliche Datenschutzvorschriften einhalten; der Verantwortliche hat ihn hierzu zu verpflichten und regelmäßig zu überwachen.
Wer als Tagespflegeperson eine Steuerberaterin oder einen Steuerberater heranzieht, um die Einkommenssteuererklärung zu erstellen, beschäftigt damit allerdings keinen Auftragsverarbeiter. Steuerberaterinnen und Steuerberater sind als Freiberufler weisungsunabhängig und eigenverantwortlich tätig. Das Merkmal der für einen Auftragsverarbeiter erforderlichen **Weisungsgebundenheit** im Sinne von Art. 28 Abs. 3 a DSGVO liegt nicht vor. Dennoch sollte auch hier darauf geachtet werden, dass die DSGVO eingehalten wird.
Beauftragt die Kindertagespflegeperson jedoch beispielsweise einen sogenannten „Dienstleister" (Dienstleistermodell anstelle eines Trägermodells im Betreiben einer Großtagespflegestelle), handelt es sich um einen Auftragsverarbeiter, der lediglich über den konkreten Auftrag (Übernahme von Verwaltungstätigkeiten, Organisation des Nachschubs von Betriebsmitteln wie insb. Lebensmittel) mit der Kindertagespflege verbunden ist. Im Rahmen des konkret erteilten Auftrages ist ein solcher Dienstleister weisungsgebunden. Üblicherweise erhält er Einblick in die von der Kindertagespflegeperson gesammelten Daten der Tagespflegekinder und ihrer Erziehungsberechtigten, um seinen Auftrag zu erledigen. Dementsprechend ist er zum Datenschutz zu verpflichten und zu kontrollieren.
Auch bei Auslagerung der Daten in eine Cloud (Cloud Computing) wird auf einen externen Dienstleister als Auftragsverarbeiter zurückgegriffen, dessen DSGVO-Konformität überprüft werden muss. Im Zweifel ist der Cloud-Anbieter für den unternehmerischen Bereich zu wechseln.
Empfänger von Daten sind nach Art. 4 Nr. 9 DSGVO Stellen, denen gegenüber die gesammelten und erhobenen Daten offen gelegt werden, die gegenüber dem Verantwortlichen eigenständig sind und von diesem nicht zur Verwirklichung eigener Zwecke herangezogen werden (Simitis 2019 Art. 4 Nr. 9 Rn. 3 ff.). Zur oft nicht leichten Abgrenzung ist also zunächst zu klären, ob die betreffende Stelle in irgendeiner Form in die Organisation des Verantwortlichen eingebunden ist oder diese unterstützt oder ob sie eine gewisse organisatorisch-institutionelle Eigenständigkeit aufweist (Simitis 2019 Art. 4 Nr. 9 Rn. 3 ff.).
Verlangt ein öffentlicher Jugendhilfeträger beispielsweise die Offenlegung von Betreuungsdaten zu einem bestimmten Kind, um zu überprüfen, ob und inwieweit dieses tatsächlich betreut und dementsprechend der Förderauftrag gem. §§ 23, 24 SGB VIII umgesetzt wurde, muss die Tagespflegeperson die angefragten Daten zur Durchführung eines behördlichen Ermittlungsauftrages an diesen öffentlichen Jugendhilfeträger weiterleiten. Diese Weiterleitung geschieht also aufgrund einer gesetzlichen Verpflichtung. Die Behörde ist weiterhin organisatorisch nicht bei der Tagespflegeperson eingebunden, sondern übt dieser gegenüber vielmehr ein übergeordnetes Wächteramt aus. Letztendlich kann die rechtlich diffizile Unterscheidung in der Praxis aber häufig dahinstehen. Wichtig in der Praxis ist vor allem, dass interessierten Erziehungsberechtigten vor Abschluss eines Betreuungsvertrages ein allgemeines Datenschutzinformationsblatt ausgehändigt wird, in dem auf den Datenaustausch mit allen im jeweiligen Einzelfall in Frage kommenden Empfängern, Auftragsbearbeitern und anderen Stellen hingewiesen wird.

Die Sicherung der Daten und die technisch-organisatorischen Maßnahmen (TOM)

Die DSGVO verlangt nicht nur eine Datenverarbeitung im erlaubten Rahmen. Die Verantwortlichen für die Datenverarbeitung haben darüber hinaus auch sicherzustellen, dass die gesammelten Daten gegen die bei ihnen potenziell eintretenden Risiken angemessen gesichert werden. Welche Sicherungsmaßnahmen sie durchführen und ob diese den Anforderungen der DSGVO genügen, haben sie schließlich auch zu begründen und nachzuweisen, Art. 24 DSGVO. Auch diesbezüglich haften die Verantwortlichen. Ihre Haftung erstreckt sich ebenso auf Handlungen von Auftragsverarbeitern oder allen anderen Personen, die für sie tätig werden (z. B. Mitarbeiter, Ehefrau oder Ehemann, Lebensgefährtin oder Lebensgefährte). Sie sind dementsprechend angehalten, dafür zu sorgen, dass auch diese geeignete Bemühungen zur Datensicherung betreiben. Die Verantwortlichen sind hier auch in der Verpflichtung zur regelmäßigen Überprüfung (Simitis Art. 24 Rn. 16 ff.).

Gefordert ist, dass sie, basierend auf einer Analyse der bei ihnen potenziell vorhandenen Risiken, die Daten mit entsprechend *„geeigneten technisch-organisatorischen Maßnahmen“* (TOM) sichern. Das in dieser Verpflichtung verankerte Vorsorgeprinzip erfordert also, dass die Verantwortlichen alle erforderlichen Maßnahmen unternehmen, die bei ihnen, in ihrer konkreten Betreuungspraxis nötig sind, damit Risiken entweder nicht entstehen oder aber – bei nicht vermeidbaren Risiken – der Schaden zumindest begrenzt wird. Die in dieser Expertise aufgeführten Maßnahmen stellen lediglich nicht abschließende Beispiele dar. Welche TOM im Einzelfall durchgeführt werden müssen, ist von der verantwortlichen Kindertagespflegeperson anhand ihrer Gegebenheiten zu beurteilen und hängt vom jeweiligen Risiko für die Rechte und Freiheiten der Betroffenen ab.

Damit die abzusichernden Risiken überhaupt identifiziert werden können, bedarf es einer anfänglichen Bestandsaufnahme. Danach empfiehlt sich die Erstellung eines kurzen Datenschutzkonzepts (siehe Muster Nr. 1).
Die Kindertagespflegeperson sollte sich durch diese Bestandsaufnahme einen Überblick zu den folgenden Fragen verschaffen, die sie sodann im Datenschutzkonzept beantworten muss:

- **Welche Art von Daten erhebe ich überhaupt? Sind es „einfache“ personenbezogene Daten oder auch besonders schützenswerte personenbezogene Daten, beispielsweise Gesundheitsdaten?**
  - ➔ Die Schutzbedürftigkeit der Daten bestimmt den erforderlichen Schutzumfang: je heikler die erhobenen Daten sind, desto besser müssen sie geschützt werden.

- **Auf welche Art und in welchem Umfang verarbeite ich Daten (technische Infrastruktur)? Welche Übertragungswege nutze ich? Auf welche Art speichere ich Daten? An wen übertrage ich welche Daten und warum? Wer hilft mir dabei?**
  - ➔ Je nach Speicherart und Übertragungsweg sind unterschiedliche Sicherungsmaßnahmen erforderlich.

- **Welche Risiken können bei mir eintreten? Es muss zwischen materiellen (z. B. Zerstörung durch Feuer, Diebstahl) und immateriellen Risiken (Hackerangriff, Virenbefall) unterschieden werden.**
  - ➔ Art und Schwere der möglicherweise eintretenden Schäden helfen, die richtigen Sicherungsmaßnahmen zu identifizieren.

- **Welche Nachteile können durch ein Risiko entstehen, das sich verwirklicht hat?**
  - ➔ Hier wird erwartet, eine Gewichtung der möglichen Risiken (unterschieden in „Risiken“ und „hohe Risiken“) sowie der Schäden vorzunehmen. Hierdurch sollen die Verantwortlichen erkennen, welche Risiken sie besonders gewissenhaft und gut absichern müssen, um den passenden Schutzbedarf zu erlangen. Bei letzterem wird dabei unterschieden zwischen „normalem Schutzbedarf“, „hohem Schutzbedarf“ und „sehr hohem Schutzbedarf“ (Datenschutzkonferenz Kurzpapier Nr. 18; Bock 2018 S. 30 ff. S. 36). Die Lektüre des Kurzpapiers Nr. 18 der Datenschutzkonferenz „Risiko für die Rechte und Freiheiten natürlicher Personen“ wird empfohlen.

Diese Fragen verdeutlichen, dass drei Bereiche zu betrachten sind:
- Die Art der personenbezogenen Daten, die geschützt werden sollen,
- die passende Sicherung der beteiligten technischen Systeme (Hardware, Software, Infrastruktur) und
- die Sicherung der personellen (menschlichen) Verarbeitungsprozesse (Bock 2018 S. 29). Die verschiedenen Maßnahmen müssen transparent, nachvollziehbar und stimmig sein.

Eine Kindertagespflegeperson wird in aller Regel neben den „einfachen“ personenbezogenen Daten wie Namen, Adressen und Kontaktdaten auch besonders schützenswerte Gesundheitsdaten erheben (insbesondere Krankheiten, Allergien, Entwicklungsfortschritte). Die unbefugte Weiterverbreitung insbesondere dieser Daten kann weitreichende Schäden für die Betroffenen auslösen. Kommen Gesundheitsdaten in falsche Hände, kann sich der Schaden erst sehr spät und an nicht vorhersehbarer Stelle offenbaren. Dies bedeutet, dass die Schutzbedürftigkeit dieser zweiten Datenkategorie bereits von Beginn an die Einführung gehobener Schutzmaßnahmen erfordert. Die DSGVO gibt dabei keine speziellen technisch-organisatorischen Maßnahmen vor; sie verlangt „nur“ wirksame, mithin erforderliche und angemessene Maßnahmen auf dem Stand der Technik. Diese sind regelmäßig zu überprüfen und zu aktualisieren, wenn sich der Stand der Technik verändert hat (Simitis 2019 Art. 24 Rn. 19; Bock 2018 S. 10 ff.). Wer Daten in Papierform (z. B. Aktenordnern) speichert, hat vor diesem Hintergrund andere Schutzmaßnahmen zu ergreifen als jemand,

der elektronisch speichert. **Akten** sind vor allem vor physischer Zerstörung durch Vandalismus, Brand, Wasser u. ä. zu schützen. Weiterhin sind sie vor unbefugter Kenntnisnahme (neugierige Eltern, Reinigungspersonal, Verwandte) und vor Diebstahl zu schützen. Es ist sicherzustellen, dass die Übertragung von Daten in Papierform durch Übertragungswege erfolgt, die die Daten vor einer Kenntnisnahme durch Unbefugte schützt (z. B. Versendung nur in verschlossenen Briefumschlägen)

> Die weit verbreitete „griffbereite" Lagerung der Akten auf einem offenen Regal im Kinderbetreuungszimmer genügt daher nicht mehr den Anforderungen der DSGVO, da die Akten damit für jedermann frei zugänglich sind. Akten müssen nun verschlossen aufbewahrt werden.

Die Anschaffung eines verschließbaren, brandsicheren Aktenschrankes ist daher eine angezeigte und geeignete Maßnahme, um Akten vor unbefugtem Zugriff, Zerstörung und Diebstahl zu schützen. Denkbar ist auch, die Akten in einem verschließbaren Raum aufzubewahren, der nicht frei zugänglich ist und ebenfalls einen Grundschutz gegen Feuer und Wasser aufweist.
Die Weitergabe von Daten in Papierform geschieht regelmäßig per verschlossenem **Brief** mit der Post. Da dieser durch das Postgeheimnis geschützt ist, gilt dieser Übertragungsweg als sicher. Bei einer Übertragung via **Telefax** handelt es sich um eine Art offener Zustellung. Es ist sicherzustellen, dass bei der Übertragung der Daten diese nicht unbefugt gelesen, kopiert, verändert, gelöscht oder an einen falschen Adressaten übertragen werden (z. B. Tippfehler bei der Faxnummer). Letzteres ist durch besonders sorgfältige Verifizierung der korrekten Faxnummer der Adressatin oder des Adressaten und durch sorgfältige Kontrolle der Eingabe zu vermeiden. Datenschützer empfehlen weiterhin Faxdeckblätter sowie die gesicherte Aufstellung des Faxgerätes, damit es keinen unbefugten Dritten zugänglich ist (Auslesegefahr). Faxprotokolle sollten zu Beweissicherungszwecken mindestens ein Jahr aufbewahrt werden (https://www.datenschutz-bayern.de/technik/orient/telefax.htm, letzter Abruf: 05.05.2020).

> Wer Daten elektronisch speichert, hat weitergehende Bemühungen zu entfalten, welche die Hardware, Software und die Übertragungswege (Übertragungsinfrastrukur) ausreichend absichern.

Die Vielzahl der elektronischen Angriffsmöglichkeiten ist inzwischen kaum mehr überschaubar. Neben den bereits bekannten Angriffsarten wie Malware in E-Mails oder verlockenden Links kann die Gefahr auch aus ganz anderer Richtung drohen: So wird inzwischen beispielsweise vor auf einem Parkplatz „verlorenen" fremden USB-Sticks mit Schadcode (ggf. mit verlockenden Aufklebern wie „Bitcoin" oder „Rechenschaftsbericht Vorstand"), elektronischen Grußkarten oder gar extra präparierten E-Zigaretten gewarnt, welche mittels USB-Anschluss an einem Computer aufgeladen werden können und dabei Malware einschleusen (Zahl u. a. 2018, S. 16). Der kriminellen Phantasie scheinen keine Grenzen gesetzt zu sein; eine ständige Achtsamkeit ist daher nötig.

> Deswegen ist jedes Gerät, auf dem unternehmerisch genutzte personenbezogene Daten gespeichert sind (Mobiltelefon, Laptop, etc.), besonders gegen unbefugten Zugriff zu sichern, beispielsweise durch ein ausreichend sicheres Passwort oder eine andere Zugangsbeschränkung. Vorsichtsmaßnahmen gegen ein sogenanntes „Shoulder Surfing" (Mitlesen von Passwörtern etc. über die Schulter hinweg) oder gegen einen Datenabgriff in öffentlichen, ungeschützten Netzwerken sind ebenfalls zu ergreifen. USB-Sticks u. ä. unklarer Herkunft sollten niemals auf unternehmerisch genutzte Geräte aufgespielt werden; Links, Grußkarten u. ä. niemals auf solchen Geräten heruntergeladen werden.

Tipp: Passwörter
Der Passwortschutz ist sicherlich eine der wichtigsten Maßnahmen zur Datensicherung. Nach den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sollte auf die folgenden Punkte geachtet werden:

- Das Passwort soll mindestens 8 Zeichen (besser: mindestens 15 Zeichen, soweit systembedingt möglich) lang sein.
- Das Passwort sollte aus möglichst vielen verschiedenen Zeichentypen (Buchstaben, Ziffern, Sonderzeichen) bestehen.

- Sonderzeichen möglichst nicht nur am Anfang oder am Ende des Passwortes einsetzen, sondern mittendrin.
- Nicht verwenden: gängige Zeichenfolgen (12345, abcde, etc.), persönliche Informationen wie Geburts- und Heiratsdaten, bekannte Telefonnummern, Adressen, Worte, Namen von Verwandten, Freunden, Haustieren, Orten, Vorbildern etc., denn mittels sogenannter „Brute-Force-Attacken" nehmen Eindringlinge vor allem Wörterbuchangriffe vor.
- Eine unterschiedliche Groß- und Kleinschreibung innerhalb der Zeichenfolge (nicht: nur der erste Buchstabe) sollte ebenfalls vorhanden sein.
- Möglich: Die Anfangsbuchstaben der Worte z. B. aus einer Zeile eines Gedichts können mit Zahlen (nicht aber mit persönlichen Daten) und Sonderzeichen kombiniert werden.
- Für Dritte unzugängliche Lagerung.
- Häufige Passwortwechsel führen dazu, dass man Passwörter vergisst und sich neue Datenschutzrisiken einschleichen (z. B. Klebezettel am Bildschirm).
- Passwörter sollten entsprechend der Empfehlung des BSI zwar nicht mehr häufig oder regelmäßig, aber dennoch nach einer längeren Verwendungsdauer erneuert werden.
- Starke Passwörter sind besser als häufige Wechsel.
- Da für jeden Dienst und für **jedes** Konto nach Möglichkeit ein anderes Passwort gewählt werden soll, empfiehlt sich die Nutzung eines Passwort-Managers.
- Passwortmanager helfen bei der Generierung und der sicheren Aufbewahrung starker Passwörter.
- Wenn ein Dienst gehackt oder ein Passwort kompromittiert wurde, sollte das Passwort geändert werden.
- Auch wenn der Verdacht einer Kompromittierung besteht, sollten Passwörter umgehend geändert werden.

Merke: Sowohl das BSI als auch z. B. der baden-württembergische Landesdatenschutzbeauftrage raten derzeit (Stand: Februar 2020) von einem periodischem Wechsel ab. Die Kindertagespflegeperson muss dann aber sicherstellen, dass sie ausreichend starke Passwörter nutzt und alle empfohlenen erforderlichen Sicherheitsmaßnahmen verwendet, um eine Kompromittierung zu vermeiden. Dazu gehört auch eine fortlaufende Passwortpflege.

Es ist zudem sicherzustellen, dass die Daten ausreichend vor Zerstörung (materiell und immateriell) geschützt werden, also verfügbar bleiben. Ziel ist, die Verfügbarkeit der Daten zu gewährleisten.
Die folgenden Maßnahmen (z. B. nach Bock 2018, S. 22 ff.) stellen sicher, die Datenverfügbarkeit zu gewährleisten. Es handelt sich jedoch nur um Mindestmaßnahmen, die angesichts der üblicherweise begrenzten Möglichkeiten einer Kindertagespflegeperson dennoch zumutbar sein dürften. Darüber hinausgehende weitere Maßnahmen je nach konkreter Situation können aber nicht schaden:

- **Anfertigung von Sicherheitskopien von Daten (Back-up-Systeme, externe Festplatten),**
- **Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, Backdoors, höhere Gewalt),**
- **Entwicklung von Reparaturstrategien.**

Eine allein tätige Kindertagespflegeperson wird im Normalfall die meisten Tätigkeiten selbst ausüben. Es sollten jedoch Vertretungsregelungen für Ausfallzeiten eingeführt werden, damit die Daten im Notfall zugänglich bleiben.
Die angewandte Software muss dem Stand der Technik entsprechen. Somit muss sich auch die allein tätige Kindertagespflegeperson *im unternehmerischen Bereich* davon verabschieden, ihre altvertrauten, aber leider veraltete Software zu nutzen – vor allem dann, wenn die Software beispielsweise schon so alt ist, dass die Bereitstellung von Sicherheitsupdates eingestellt wurde oder es für sie keine Virenschutzprogramme mehr gibt. Soweit ein Online-Zugang besteht, ist dieser ebenfalls zu sichern, beispielsweise durch den aktuellen Stand der Technik entsprechende Maßnahmen wie Deaktivieren nicht benötigter Netzwerkdienste zur Unterbindung ungewollter Fernzugriffe, Installation von Firewallprogrammen, Intrusion-Prevention-Systeme oder ähnlichem. Bezüglich der Übertragungsinfrastruktur (Server) ist darauf zu achten, dass der gewählte Anbieter DSGVO-konform und mit aktueller Verschlüsselung arbeitet. Es sind auch auf dieser Ebene Sicherungssysteme einzurichten.

Die angewandte Software muss dem Stand der Technik entsprechen.

Nach Art. 32 DSGVO muss ein angemessenes Schutzniveau beim Transport von E-Mails über das Internet sichergestellt werden, wie beispielsweise die bayerische Landesdatenschutzbehörde treffend erklärt (https://www.lda.bayern.de/de/faq.html). Empfehlenswert ist neben einer Transport- auch eine Inhaltsverschlüsselung (z. B. PGP, PDF, ZIP-Datei mit

Bezüglich der Übertragungsinfrastruktur (Server) ist darauf zu achten, dass der gewählte E-Mailanbieter DSGVO-konform und mit aktueller Verschlüsselung arbeitet.

Passwort), wenn besonders sensible Daten verschickt werden (https://www.lda.bayern.de/de/faq.html). Dies gilt auch für USB-Sticks oder CD-ROMs.

Eine weitere, eng mit dem DSGVO verwandte, aber schwerer zu beherrschende Gefahrenquelle ist die Datenverarbeitung durch den Menschen. Eine Vielzahl von Daten über das Tagespflegekind oder seine Erziehungsberechtigten sind nur im Kopf der Kindertagespflegeperson „gespeichert". Auch diese Daten müssen „gesichert" werden. Die Sicherung besteht darin, dass die Kindertagespflegeperson Dritten gegenüber nicht vollkommen unbedacht und ungefiltert über ein Tagespflegekind bzw. seine Erziehungsberechtigten spricht. Die gefährlichen Situationen sind dabei vielfältig: So können Informationen über ein Tagespflegekind anderen zu Ohren kommen, wenn die Kindertagespflegeperson beispielsweise in öffentlichen Verkehrsmitteln in ihrer Anwesenheit telefoniert und dabei vertrauliche Belange bespricht; im Rahmen von Tür- und Angelgesprächen oder auf dem Spielplatz kann über ein anderes Tagespflegekind „gequatscht" werden; im Rahmen von Feiern finden angeregte Vergleiche zwischen den einzelnen Tagespflegekindern statt; eine Kindertagespflegeperson kann unbedacht spontane Auskünfte erteilen, wenn sie unerwartet angerufen und um Auskunft gefragt wird; in Netzwerktreffen werden unter Verwendung von Klarnamen Probleme mit einzelnen Kindern besprochen.

Jede Kindertagespflegeperson sollte ihr alltägliches Kommunikationsverhalten vor diesem Hintergrund daher einer kritischen Kontrolle unterziehen und gegebenenfalls im Sinne einer erhöhten Vertraulichkeit verbessern.

Auch die Bandbreite der weiteren menschlichen Fehler ist vielfältig. Das beginnt bereits beim einfachen, vermeintlich harmlosen Tippfehler beim Eingeben einer E-Mail-Adresse. Das Ergebnis: ein Irrläufer. Ein solcher verhältnismäßig kleiner Fehler kann jedoch dazu führen, dass höchst sensible Daten über ein Kind an die falsche Person gelangen. Geeignete Sicherheitsmaßnahmen, um diese häufigen Risikoquellen in der Kindertagespflege zu beherrschen, können sein:

- Wahl nur sicherer und geeigneter Übertragungswege, auch wenn diese nicht so „bequem" oder „praktisch" sind;
- Versenden der eigentlichen Inhalte mittels passwortgeschützter und verschlüsselter Anhänge;
- Keine „Nebenbei-Kommunikation": Wer neben der Kommunikation durch andere Tätigkeiten wie beispielsweise der Aufsichtspflicht abgelenkt ist, macht schneller Fehler *und* könnte sogar noch die Aufsichtspflicht verletzen;
- Sorgfältige Pflege der elektronischen Kontaktdateien des eigenen E-Mail-Programms;
- Standartmäßige zweite Eingabekontrolle vor Abschicken einer Nachricht;
- Beständige Fehlerauswertung und Entwicklung eines Sollverhaltens (Vermeidung gängiger Fehlverhaltens z. B. bei Pishing-Mails usw.).

Soweit in einer Großtagespflegestelle Daten auf einem Gerät gespeichert werden, auf das mehrere Personen Zugriff haben, müssen mehrere Benutzerebenen erstellt werden, um sicherzustellen, dass jede dieser Personen nur Zugriff auf diejenigen Daten haben kann, welche sie für die Ausübung ihrer Tätigkeit benötigt.

Lese- und Bearbeitungsrechte einzuführen, kann unter Umständen dann angezeigt sein, wenn der Zugriff durch alle Mitarbeiter einer Großtagespflegestelle sinnvoll ist (z. B. bei interner Ersatzbetreuung). In diesem Falle sollten neben klaren vertraglichen Verpflichtungen auf Datengeheimnis und Verschwiegenheit auch die verschiedenen Rechte und Pflichten intern in Form eines Rechtekonzepts organisatorisch definiert und abgegrenzt sein (Bock 2018, S. 23).

Das Recht auf Vergessenwerden: Datenlöschung und Löschfrist

Gemäß Art. 17 DSGVO hat jede natürliche Person das Recht, vergessen werden zu dürfen. Dies bedeutet, dass jede Person verlangen darf, dass die über sie erhobenen Daten gelöscht und vernichtet werden, sobald sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind, diese Person ihre Einwilligung widerrufen oder gegen die Verarbeitung Widerspruch erhoben hat (Simitis 2019 Art. 17 Rn. 5 ff.). Natürlich sind erst recht solche Daten zu vernichten, welche unrechtmäßig verarbeitet wurden. Löschung bedeutet dabei die Vernichtung der Daten in einer Art und Weise, dass sie end-

Jede Person darf verlangen, dass die über sie erhobenen Daten gelöscht und vernichtet werden, sobald sie für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind, diese Person ihre Einwilligung widerrufen oder gegen die Verarbeitung Widerspruch erhoben hat (Simitis 2019 Art. 17 Rn. 5 ff.).

gültig nicht mehr rekonstruiert werden können. Speichert eine Kindertagespflegeperson die erhobenen Daten in einem **Aktenordner,** ist dieser dementsprechend so zu schreddern, dass die Daten nicht mehr lesbar sind. Ein einfaches Wegwerfen der Unterlagen ist nicht ausreichend. Diese könnten aus dem Altpapier gezogen und gelesen werden.

Werden die Daten **elektronisch** gespeichert, muss eine umfassende physikalische Löschung erfolgen; eine logische Löschung ist nicht ausreichend. Die Daten müssen dabei auf dem Datenträger so vernichtet werden, dass sie nicht wiederhergestellt werden können. Dies kann entweder durch physische Vernichtung des Datenträgers (z. B. Zerstörung einer CD-ROM) oder aber durch mehrfaches Überschreiben und durch die Kappung aller denkbaren Verknüpfungen zum fraglichen Dateisystem erfolgen. Eine einfache Kappung von Verknüpfungen („logische Löschung“) ist nicht ausreichend, weil die Datei damit nicht gelöscht, sondern nur schwerer auffindbar gemacht wird (Simitis 2019 Art. 17 Rn. 5; Datenschutzkonferenz Kurzpapier Nr. 11). Dies bedeutet, dass ein einfaches Löschen und Leeren des Papierkorbes nicht ausreicht. Die Kindertagespflegeperson muss entweder zusätzliche Software wie z. B. sogenannte File Shredder erwerben oder aber sich ausreichende Programmierkenntnisse aneignen, um passende manuelle Programmierbefehle ausführen zu können.

Sobald die Daten nicht mehr erforderlich sind, müssen sie sogar gelöscht werden. Die Daten müssen unverzüglich, also ohne schuldhaftes Zögern, gelöscht werden. Da die Kindertagespflege ihrem Wesen nach eine Dauerdienstleistung ist, ist es in jedem Falle erforderlich, die Daten bis zum Ende des Vertragsverhältnisses beizubehalten. Andernfalls kann die Betreuung nicht durchgeführt werden. Der Löschzeitpunkt, der nach Beendigung des Vertragsverhältnisses zu bestimmen ist, ist danach allerdings nicht mehr so leicht zu ermitteln, weil es hierzu derzeit noch keine klaren Vorgaben gibt. Dem Sinn der Vorschrift entsprechend entfällt die Notwendigkeit einer Datenspeicherung jedenfalls dann, wenn der Verantwortliche keinerlei Schadensersatz-, Haftungs- oder Bußgeldverfahren mehr erwarten muss, sobald Verjährung eingetreten ist.

Im Bereich der Kindertagespflege erscheint es unter Berücksichtigung der steuerlichen und zivilrechtlichen Verjährungsregelungen sinnvoll, die Daten zu einem betreuten Kind und seinen Erziehungsberechtigten erst nach Ablauf von zehn Jahren ab Ende des Jahres, in dem das Vertragsverhältnis endete, zu löschen.

Aufgrund der allgemeinen zivilrechtlichen Verjährungsfristen (insb. § 195 BGB) kann eine Kindertagespflegeperson nach Beendigung der Betreuung bzw. nach Vertragsende noch mindestens drei Jahre lang der potentiellen Gefahr von Schadensersatzverfahren ausgesetzt sein. Bei einer vorsätzlichen Verletzung des Lebens, der Gesundheit, des Körpers, der Freiheit u. a. tritt entsprechend § 197 BGB sogar erst nach dreißig Jahren Verjährung ein. Die Strafverfolgungsverjährung für Steuerhinterziehung kann derzeit sogar bis zu zehn Jahre betragen. Damit eine Kindertagespflegeperson vor allem gegenüber einer Finanzbehörde unter Vorlage der Daten zu einer abgeschlossenen Betreuung noch belegen kann, dass sie durch Falschangaben keine Steuern hinterzogen hat, sollte diese steuerrechtliche Frist angewendet werden. Soweit einzelne Jugendhilfeträger im Rahmen von Sonderförderprogrammen (z. B. Investitionskostenzuschüsse) noch längere Aufbewahrungsfristen verlangen, ist zu prüfen, ob diese herangezogen werden müssen, und wenn ja, für welche Daten sie gelten.

Es dürfte sinnvoll sein, die nicht mehr benötigten Daten einmal jährlich zu einem festgesetzten Zeitpunkt zu löschen.

Es dürfte sinnvoll sein, die nicht mehr benötigten Daten einmal jährlich zu einem festgesetzten Zeitpunkt zu löschen. So wird diese Verpflichtung nicht vergessen. Die Löschung von Daten ist im Löschverzeichnis zu vermerken.

Weitere Verpflichtungen des Verantwortlichen nach der DSGVO

Die DSGVO verlangt von den Verantwortlichen der Datenerhebung und -verarbeitung, dass weitere begleitende Pflichten eingehalten werden, damit das im Ergebnis gewünschte übergeordnete Ziel des Datenschutzes wirksam umgesetzt und kontrolliert werden kann. Zunächst stehen den Betroffenen, von denen Daten erhoben wurden, Informations- und Auskunftsrechte sowie Berichtigungs- und Übertragungsrechte zu. So können Umfang und Inhalt der Datenverarbeitung von den Betroffenen selbst wirksam kontrolliert werden.

Bevor Daten erhoben werden, müssen die Betroffenen über die Datenerhebung, die Person des Verantwortlichen, den Zweck und den Erlaubnistatbestand, die Erhebungswege, die Verarbeitungswege und die Weitergabe ihrer Daten **informieren** werden (Art. 12 DSGVO). In der Kindertagespflege muss in einer solchen Information darauf geachtet werden, zwischen der Datenerhebung zur Person der Erziehungsberechtigten und zur Person des Tagespflegekindes zu unterscheiden. Daten sollten dabei, wenn möglich, stets direkt bei den Betroffenen erhoben werden (direkte Datenerhebung). Die Information sollte vor Vertragsschluss erfolgen (siehe Muster Nr. 2).
Nach Datenerhebung haben die Betroffenen nach Art. 15 DSGVO ein **Recht auf Auskunft** über die tatsächlich erhobenen Daten und insbesondere, an wen diese weitergegeben wurden. Die Auskunft muss detailliert erfolgen (z. B. Mitteilung der konkreten IBAN-Nummer), damit die Betroffenen prüfen können, ob die Datenspeicherung richtig war. Außerdem muss nach Art. 15 Abs. 4 eine Kopie der Daten zur Verfügung gestellt werden. Diese Auskunft ist zu erteilen, egal, ob die Daten in Papierform oder elektronisch gespeichert wurden. Erfolgt die Auskunft nicht richtig oder vollständig, kann sie durch die Verhängung eines empfindlich hohen Zwangsgeldes durchgesetzt werden (z. B. AG Wertheim, Beschluss vom 12.12.2019 AZ 1 C 66/19).
Wurden Daten falsch gespeichert, steht den Betroffenen ein **Recht auf Berichtigung** (Art. 16) und ein Recht auf Beschwerde (Art. 77 DSGVO) sowie auf Widerruf einer Einwilligung (Art. 7 DSGVO) zu. Haben die Betroffenen der Datenspeicherung und -verarbeitung **widersprochen** (Art. 21 DSGVO), beispielsweise, weil die Daten unrichtig waren oder unerlaubt erhoben wurden, können sie verlangen, dass die **Verarbeitung eingeschränkt** wird (Art. 18 DSGVO) oder die Daten **gelöscht** werden (Art. 17 DSGVO). Schließlich haben die betroffenen Personen nach Art. 20 DSGVO das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und einem anderen Verantwortlichen ohne Behinderung zu übermitteln, sofern die Datenverarbeitung auf einer Einwilligung oder einem Vertrag beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt. Ist durch die Datenverarbeitung im weitesten Sinne – von der Erhebung über die Speicherung bis zur Verarbeitung und Weiterleitung – für die Betroffenen ein materieller oder immaterieller Schaden entstanden, können sie gem. Art. 82 DSGVO **Schadensersatz** verlangen. Es sind also folgende Betroffenenrechte zu berücksichtigen: Recht auf Widerruf einer Einwilligung (Art. 7), Recht keinen Entscheidungen unterworfen zu werden, die ausschließlich auf automatisierten Verarbeitungen beruhen (Art. 22), Beschwerderecht bei einer Aufsichtsbehörde (Art. 77 DSGVO). Die Umsetzung der Betroffenenrechte ist i. d. R. zeitkritisch. Die Auskunft muss innerhalb eines Monats erteilt werden. Nur in gut begründeten Einzelfällen ist eine Verlängerung dieser Frist möglich.

> Weiterhin ist die Einhaltung des Datenschutzes auch von Aufsichtsbehörden wirksam zu kontrollieren. Die Aufsichtsbehörde muss sich im Ergebnis einen guten Überblick über die angewendeten Maßnahmen zur Informationssicherheit machen können.

Dies geschieht mit den folgenden Unterlagen, die, in angemessener Form, auch von Kindertagespflegepersonen vorzubereiten sind:
So ist ein kurzes **Datenschutzkonzept** zu erstellen, das nach einer Darstellung der Tätigkeit abstrakt erläutert, welche personenbezogenen Daten erhoben und verarbeitet werden, welche Rechtsgrundlagen angewandt werden, welche Risiken und Schadensverläufe eintreten könnten, wem Daten weitergeleitet werden und vor allem, wie die Daten technisch und organisatorisch geschützt werden. Ziel dieses Konzepts ist es, Kontrolleurinnen oder Kontrolleuren der Aufsichtsbehörde einen ersten umfassenden Überblick über die getroffenen Maßnahmen zu ermöglichen, damit sie feststellen können, ob die Bemühungen dem Grunde nach angemessen sind oder ob Fehler oder Lücken vorhanden sind. Da es für die Kindertagespflege, soweit derzeit ersichtlich, noch keinerlei offizielle Handreichungen gibt, erscheint es sinnvoll, sich für diesen Tätigkeitsbereich nach den Empfehlungen für kleine Vereine zu richten. Diesbezügliche Muster und Vorlagen können als Basis für die Erstellung eines eigenen Datenschutzkonzepts und der erforderlichen Verzeichnisse herangezogen werden.
Da Kindertagespflegepersonen regelmäßig sensible Daten i.S.d. Art. 9 DSGVO (Gesundheitsdaten) erheben, ist davon auszugehen, dass sie **Verzeichnisse** zur Datenverarbeitung zu erstellen haben, auch wenn sie Kleinstunternehmen im Sinne des Erwägungsgrundes Nr. 13 zu Art. 30 Abs. 5 DSGVO sein dürften. Derzeit ist

es daher empfehlenswert, die folgenden nichtöffentlichen Verzeichnisse anzulegen und zu führen, um sie im Falle einer Prüfung der Aufsichtsbehörde vorlegen zu können:

1. **Verzeichnis der Verarbeitungstätigkeiten („Verfahrensverzeichnis"), Art. 30 DSGVO**
2. **Löschverzeichnis**

Im Sinne einer Schnellübersicht wird durch das Verzeichnis der Verarbeitungstätigkeiten verdeutlicht, welche Kategorie von wem verarbeitet wurde, zu welchem Zweck und unter welchem Erlaubnistatbestand. Die einschlägigen Sicherungsmaßnahmen sind kurz anzuführen. Schließlich ist die Löschfrist anzugeben.

In der Kindertagespflege sollte das **Verzeichnis der Verarbeitungstätigkeiten** die folgenden Angaben aufweisen:

- Name und Kontaktdaten des Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten (soweit vorhanden)
- Verarbeitungstätigkeiten (jede Tätigkeit gesondert angeben)
- Rechtsgrundlagen und (alle in Frage kommenden) Zwecke der Verarbeitung pro Tätigkeit pro Tätigkeit
- Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder werden,
- Speicherdauer, Löschfristen für die verschiedenen Datenkategorien
- Stichwortartig: technische und organisatorische Maßnahmen

Soweit Übermittlungen in ein Drittland oder an internationale Organisationen stattfinden, ist dies natürlich ebenfalls anzugeben.

Im **Löschverzeichnis** sollte verzeichnet werden:

- Name und Kontaktdaten des für die Löschung Verantwortlichen, ggf. des Vertreters des Verantwortlichen (soweit vorhanden)
- Gegenstand der Löschung (Kategorien der gelöschten Daten)
- Kurzbezeichnung der Betroffenen
- Stichwortartig: Löschmaßnahmen
- Löschdatum

Wie hoch die Anforderungen an solche Verzeichnisse einer einzelunternehmerisch tätigen Kindertagespflegeperson sein könnten, ist noch nicht eindeutig erkennbar. Entsprechend der bisherigen Aussagen und Wertungen einzelner Datenschutzbeauftragter könnte eine „einfache Verzeichnisführung" ausreichend sein. Vereinzelt wird erwähnt, dass bei Kleinbetrieben eine sogenannte Vollprotokollierung im Sinne einer umfassenden und lückenlosen Mitaufzeichnung aller Datenverarbeitungstätigkeiten „wenig akzeptabel" (Bock 2018, S. 33) sei. Auch für Vereine, die Gesundheitsdaten verarbeiten, wird es verschiedentlich als ausreichend angesehen, wenn sie ein „einfaches" Verfahrensverzeichnis führen. Diese Wertung könnte auf Kindertagespflegepersonen übertragbar sein. Eine eigenständige und regelmäßige Recherche nach neueren Veröffentlichungen oder Stellungnahmen zu dieser Frage wird aber dringend angeraten.

Die Verzeichnisse sind „schriftlich" zu führen, wobei unter diesem Begriff nach der DSGVO sowohl die Papierform als auch die elektronische Form zu verstehen ist. Erste Anbieter haben bereits Produkte auf den Markt gebracht, die mittels spezieller Software im Hintergrund jede elektronische Datenverarbeitungstätigkeit mitprotokollieren. Da diese Programme derzeit jedoch für die durchschnittliche Kindertagespflegeperson noch zu teuer sein dürften, empfiehlt es sich, vorerst selbstorganisierte Verzeichnisse zu erstellen. Die Landesdatenschutzbeauftragten der Bundesländer stellen Mustervorlagen zur Erstellung der Verzeichnisse zur Verfügung, an denen man sich – neben den im Anhang angeführten Mustern, die hierauf basieren – orientieren kann.

Zu guter Letzt wird die **Meldung** von Datenschutzverstößen erwartet. Datenschutzverstöße geringerer Art könnte beispielsweise ein Fehler in der Anlage der Stammdaten sein. Inwieweit das versehentliche Versenden einer E-Mail-Nachricht an einen falschen Adressaten meldepflichtig ist oder nicht, lässt sich noch nicht abschließend beurteilen. Die Kindertagespflegeperson sollte sich in so einem Fall bei der für sie zuständigen Datenschutzbehörde erkundigen, ob eine Meldung erforderlich ist oder nicht, da einige Aufsichtsbehörden aufgrund Überlastung derzeit darum bitten, von einer solchen Meldung abzusehen, während andere eine Meldung erwarten. Schwerwiegende Datenschutzverstöße sind den Behörden zu melden, vorzugsweise online.

Die Meldung hat jedoch an die richtige Behörde zu erfolgen. Die zuständigen Behörden können je nach Bundesland variieren. So sind beispielsweise in Bayern Meldungen zu Verstößen in der Verarbeitung personenbezogener Daten durch eine bayerische öffentliche Stelle an den Bayerischen Landesbeauftragten für den Da-

tenschutz heranzutragen (Art. 51, 77 DSGVO, Art. 20 Abs. 1, Art. 28 Abs. 2 S. 1 Nr. 6 BayDSG). Verstöße einer *nicht-öffentlichen Stelle*, also eines in Bayern ansässigen privatwirtschaftlichen Unternehmens, sind an das Landesamt für Datenschutzaufsicht zu richten (https://www.lda.bayern.de/de/beschwerde.html).
Der Träger der öffentlichen Kinder- und Jugendhilfe ist keine Aufsichtsbehörde im Sinne der DSGVO und somit nicht einsichtsberechtigt.

***Exkurs:* Datenschutz in der Großtagespflege**

Soweit Großtagespflege im jeweiligen Bundesland zulässig ist, ergeben sich in dieser Form der gemeinsamen Betreuung von Tagespflegekindern einige zusätzliche datenschutzrechtliche Verpflichtungen.
Die einzelnen Kindertagespflegepersonen betreuen dabei ihre Tagespflegekinder mit einer gewissen Zusammenarbeit. Gemeinschaftliche Tätigkeiten sind unvermeidbar; sie prägen diese Betreuungsform sogar.

> Auf diese Weise erlangen alle anwesenden Kindertagespflegepersonen unvermeidbar Kenntnis von besonders sensiblen Gesundheitsdaten des Kindes. Häufig tauschen sie sich hierüber auch intern aus, beispielsweise, um zu entscheiden, wie mit Problemen umgegangen werden soll. Dieser interne Datenaustausch sollte durch entsprechende vertragliche Klauseln und Einwilligungen seitens der Erziehungsberechtigten abgesichert werden.
> Gleiches gilt, wenn die Großtagespflege Ersatzbetreuung nutzt, egal ob intern, extern, gefördert oder nicht gefördert.

Wird die Großtagespflegestelle in Form einer Gesellschaft des bürgerlichen Rechts (GbR) betrieben, ist zu klären, wer i.S.d. DSGVO der Verantwortliche für die Datenverarbeitung ist. Je nach Gesellschaftsvertrag und tatsächlicher Organisation kann dies die einzelne Kindertagespflegeperson oder aber alle Kindertagespflegepersonen können als Gesellschafterinnen und Gesellschafter gemeinsam Verantwortliche sein.
Betreuen in einer Großtagespflege Kindertagespflegepersonen als abhängig Beschäftigte, ist die Arbeitgeberin oder der Arbeitgeber der Verantwortliche für den Datenschutz in der Großtagespflegestelle. Die Verantwortlichkeit zur Erstellung des Datenschutzkonzepts, die Führung der Verzeichnisse und die Einrichtung sowie Einhaltung der technisch-organisatorischen Maßnahmen verbleibt dort, auch wenn die Ausführung und Einhaltung dieser Maßnahmen durch Arbeitgeberweisung oder Arbeitsvertrag intern der abhängig beschäftigten Kindertagespflegeperson zugewiesen werden kann.
Besonderes Augenmerk ist daher darauf zu legen, abhängig beschäftigte Kindertagespflegepersonen durch regelmäßig wiederholte Schulungen und Belehrungen auf den Datenschutz zu verpflichten. Sie erhalten im Rahmen ihrer Betreuungstätigkeit eine Vielzahl sensibler Daten über die betreuten Tagespflegekinder, die sie dokumentieren müssen. In der Belehrung ist sinnvollerweise darauf hinzuweisen, dass die abhängig beschäftigte Kindertagespflegeperson gegenüber dem öffentlichen Jugendhilfeträger denselben Unterrichtungs- und Mitteilungsverpflichtungen unterliegt wie jede andere Kindertagespflegeperson auch. Vorab sollte in Zusammenarbeit mit dem öffentlichen Jugendhilfeträger festgelegt werden, welche Meldeketten von abhängig beschäftigten Kindertagespflegepersonen einzuhalten sind. Da insbesondere die Meldeverpflichtung gem. § 43 Abs. 3 S. 5 SGB VIII ihrem Wesen nach eher eine direkte Meldeverpflichtung der wahrnehmenden Kindertagespflegeperson ist, welche die Pflegeerlaubnis erst nach Prüfung ihrer höchstpersönlichen Eignung erhält, dürfte es vertretbar sein, wenn die Meldung an den öffentlichen Jugendhilfeträger durch die abhängig Beschäftigte persönlich erfolgt, der Arbeitgeber aber zumindest gleichzeitig, besser noch zuvor, ebenfalls informiert wird.
Schließlich sollte in der Großtagespflegestelle verbindlich festgelegt werden, welche Kommunikationsmittel von den Beschäftigten genutzt werden.

> Es ist nicht empfehlenswert, abhängig beschäftigte Kindertagespflegepersonen zur Kommunikation mit den Erziehungsberechtigten ihr privates Mobiltelefon nutzen zu lassen, möglicherweise sogar noch unter Verwendung von sozialen Medien wie WhatsApp. Die Betreiber dieser sozialen Medien können hierdurch Daten der Tagespflegekinder und ihrer Erziehungsberechtigten ohne deren Erlaubnis an sich ziehen und zu eigenen Zwecken verwenden. Die Arbeitgeberin oder der Arbeitgeber hat in so einem Falle keinerlei Möglichkeit, einen solchen rechtswidrigen Datenabflusses zu kontrollieren oder einzudämmen, müsste als Verantwortlicher aber dennoch die Konsequenzen tragen (s. AG Bad Hersfeld).

Werden abhängig beschäftigte Kindertagespflegepersonen eingesetzt, ist zusätzlich zu den bereits geschilderten Maßnahmen und Ver-

pflichtungen auch der arbeitsrechtliche Beschäftigtendatenschutz zu beachten, der bereits mit dem Bewerbungs- und Auswahlverfahren vor der Einstellung beginnt.

Zunächst haben Bewerberinnen oder Bewerber und abhängig beschäftigte Kindertagespflegepersonen dieselben Rechte auf Information, Auskunft, Widerspruch, Löschung, Korrektur etc. wie sonstige Betroffene (Mareck 2019, S. 103 ff.). Auch für die Verarbeitung von Daten angestellter Kindertagespflegepersonen gilt: Für jede Kategorie von Daten, die erhoben wird, müssen ein Erlaubnistatbestand und ein zulässiger Zweck vorliegen. Die Religionszugehörigkeit zu erheben ist z. B. bei Aufnahme des Arbeitsverhältnisses zulässig, da sie entsprechend Art. 26 DSGVO i.V.m. § 26 BDSG erforderlich ist, um ein Beschäftigungsverhältnis zu begründen oder durchzuführen (Kirchensteuer). Die weiteren Daten werden aufgrund steuerrechtlicher Vorgaben oder zur Beachtung des Nachweisgesetzes (NachwG) zulässigerweise erhoben.

Auch in diesem Kontext empfiehlt es sich aber für den Arbeitgeber zu Nachweiszwecken, die Beschäftigten über die Datenerhebung und ihre Zwecke und Erlaubnistatbestände zu informieren und bei den Beschäftigten darüber hinaus eine Einwilligungserklärung in die Datenerhebung und -verarbeitung einzuholen, wenn Daten verarbeitet werden sollen, die über das im Arbeitsverhältnis notwendige Maß hinausgehen und gegebenenfalls eine Zusatzleistung des Arbeitgebers darstellen (wenn beispielsweise Geburtstage in Geburtstagslisten eingetragen werden, dienstliche Geräte wie Mobiltelefon oder Dienstwagen privat genutzt werden, betriebliches Gesundheitsmanagement). Die Einwilligung hat in diesem Falle tatsächlich schriftlich zu erfolgen (Datenschutzkonferenz Kurzpapier Nr. 14).

Auch zur **Bewerbung** dürfen Daten über die Arbeitswilligen erhoben und für längstens sechs Monate aufbewahrt werden, um bei Klagen nach dem Allgemeinen Gleichbehandlungsgesetz (AGG) reagieren zu können, Art. 6 Abs. 1b DSGVO. Bewerberinnen und Bewerber sind Beschäftigte, § 26 Abs. 8 Satz 2 BDSG. Somit dürfen die Daten gem. § 26 Abs. 1 BDSG zur Begründung des Beschäftigungsverhältnisses verarbeitet werden. Sollen die Daten abgelehnter Bewerber nach Beendigung des Bewerbungsverfahrens z. B. für zukünftige Anfragen weiter gespeichert werden, ist es ratsam, bereits bei Bewerbung eine Einwilligung zur Speicherung über den zulässigen Zeitraum von sechs Monaten hinaus einzuholen. Allerdings kann eine solche Speicherung nicht länger als ein Jahr andauern, wenn keine zwischenzeitliche Kontaktaufnahme erfolgte. Längere Speicherungen könnten eine rechtswidrige Vorratsdatenspeicherung bedeuten und könnten auch nicht durch Einwilligungen legitimiert werden. Wird in einer Großtagespflegestelle beispielsweise eine Bewerberdatei angelegt, um für einen späteren Bedarf auf frühere Arbeitsanfragen zurückgreifen zu können, ist bei den Betroffenen zuvor eine ausdrückliche diesbezügliche Einwilligung einzuholen. In allen anderen Fällen sind die Daten von Bewerberinnen und Bewerbern „unverzüglich“ nach Entfall der Erforderlichkeit für die Datenspeicherung zu löschen (Haslach 2018, S. 9 f.).

Unverzüglich heißt aber auch hier nicht unmittelbar: Da Bewerberinnen und Bewerber nach dem Allgemeinen Gleichbehandlungsgesetzes (AGG) einen potentiellen Arbeitgeber verklagen können, weil dieser sie nicht eingestellt hat, besteht die Erforderlichkeit für einen gewissen Zeitraum noch fort.

Es empfiehlt sich wegen § 15 AGG eine Aufbewahrungsfrist von sechs Monaten: Abgelehnte Bewerberinnen oder Bewerber müssen ihren Anspruch innerhalb von zwei Monaten nach Zugang der Ablehnung geltend machen. Danach haben sie weitere drei Monate Zeit, ihren Anspruch prozessual geltend zu machen. Werden die durchschnittlichen Postlaufzeiten berücksichtigt, ergibt dies den Zeitraum von sechs Monaten bis zur Löschung. Der gesamte Vorgang inklusive der Löschung ist in den entsprechenden Verzeichnissen einzutragen.

3 Leitfaden für den Datenschutz in der Kindertagespflege

Im Folgenden wird die Umsetzung des Datenschutzes in der Kindertagespflege anhand des folgenden idealtypischen Verlaufs eines Betreuungsverhältnisses Schritt für Schritt skizziert. Da die Kindertagespflege in der Praxis jedoch in zahlreichen Varianten ausgeübt wird, muss jede Kindertagespflegeperson eigenverantwortlich erheben, welche Schritte sie im Einzelfall ausübt und eigenverantwortlich ermitteln, welche Datenschutzerfordernisse hieraus entstehen.

Diese datenschutzrechtlichen Maßnahmen sind interne Vorarbeiten. Sie sind nicht öffentlich. Nur die Datenschutzbehörden dürfen Einsicht nehmen, nicht jedoch der öffentliche Jugendhilfeträger.

TIPP:
Um zu erkennen, welche Tätigkeitsabläufe in der eigenen Betreuungspraxis vorkommen, ist es sinnvoll, während eines „Probemonats" für mindestens ein konkret betreutes Kind die verschiedenen Tätigkeiten und Handlungen stichwortartig mitzuprotokollieren und danach auszuwerten.

Erste Schritte in der Kindertagespflege: Die „Vorarbeiten"

Wird erstmalig ein Tagespflegekind aufgenommen, muss sich die angehende Kindertagespflegeperson nicht nur um die Pflegeerlaubnis kümmern und die Räume kindgerecht einrichten. Sie muss zudem in datenschutzrechtlicher Hinsicht einige technische und wirtschaftliche Grundentscheidungen treffen, da diese Entscheidungen die weiteren datenschutzrechtlichen Arbeiten wesentlich beeinflussen:

- **Soll ein „dienstliches" Mobiltelefon genutzt werden oder wird das private Mobiltelefon gemischt genutzt?**
- **Auf welchen Kontaktkanälen soll die Kindertagespflegeperson überhaupt erreichbar sein? Wird sie via E-Mail, Post und Telefon ansprechbar sein oder sollen auch Messengerdienste wie z. B. Signal oder soziale Medien genutzt werden?**
- **Wird eine Website erstellt? Soll sie rein als Schaufenster (ohne Interaktion) fungieren oder soll darüber ebenfalls Datenaustausch stattfinden, beispielsweise über ein Kontaktformular?**
- **Wird für die Betreuung ein PC genutzt? Wird hierfür extra ein eigener PC angeschafft oder wird eine Mischnutzung des privaten PC stattfinden?**
- **Welche Dokumentationsarbeiten (nur stichwortartige Niederschrift besonderer Vorkommnisse während der Betreuung; Foto- und/oder Filmdokumentation, Portfolio, Ich-Bücher, Fotoalben, …) sind beabsichtigt?**

Ausgehend von diesen ersten Grundentscheidungen sollte die Tagespflegeperson ein kurzes **Datenschutzkonzept** erstellen, in dem sie die Tätigkeit und die damit verbundenen datenschutzrechtlichen Risiken und potenziellen Schäden beschreibt (siehe Muster Nr. 1). Sie sollte die Kategorien der Daten („Stammdaten", Gesundheitsdaten, sonstige besondere personenbezogene Daten), welche sie vor und zum Vertragsschluss und später in der Betreuung erheben und verarbeiten wird, kurz darzustellen. Auf dieser Stufe empfiehlt es sich, bereits ein Muster eines **Betreuungsvertrages** vorliegen zu haben, aus dem die Kindertagespflegeperson ablesen kann, welche Daten von wem erhoben und an wen sie zu welchem Zweck weitergeleitet werden.
Weiterhin sollte die angehende Kindertagespflegeperson wissen, auf welche Art und Weise bei ihr vor Ort der **Datenaustausch** mit dem öffentlichen Jugendhilfeträger durchgeführt wird, wenn das Betreuungsverhältnis öffentlich gefördert werden soll: Werden die Interessenten von diesem zur Kindertagespflegeperson geschickt oder umgekehrt? Wird erwartet, dass die Kindertagespflegeperson die Erziehungsberechtigten beim Ausfüllen des Förderantrages unterstützt (z. B. „Elternpaket" in München) und diesen zusammen mit dem Betreuungsvertrag einschickt? Ist ein Verein zwischengeschaltet, der im Auftrag des öffentlichen Jugendhilfeträgers Anträge vorbearbeiten und den Kontakt mit den Erziehungsberechtigten pflegen soll? Diese Abläufe sollte sie ebenfalls berücksichtigen und gegebenenfalls mit Verträgen absichern (z. B. Kooperationsverträge mit zwischengeschalteten Vereinen).
In einem weiteren Schritt sollte die Kindertagespflegeperson im Konzept kurz darzustellen, auf welche Art die Daten gespeichert und wie sie weitergeleitet werden (z. B. nur in Papierform/Aktenordner oder auch elektronisch). Diese unternehmerische Entscheidung sollte sie früh fällen, denn an diese Grundentscheidung knüpfen zahlreiche weitere Folgeverpflichtungen und -kosten an, u. a. zur Sicherung der Daten wie z. B. die Einrichtung von Virenschutzpro-

grammen, die Verwendung von Verschlüsselungsprogrammen bei E-Mail-Nutzung oder bei Verwendung von USB-Sticks. Diese müssen im Konzept ebenfalls dargestellt werden. Möchte die Kindertagespflegeperson über eine Website auffindbar sein, sind die technischen Maßnahmen zum Datenschutz für die Website ebenfalls anzuführen. Auf der Internetseite ist ein passender Datenschutzhinweis anzubringen.
Soweit mit **Auftragsverarbeitenden** wie beispielsweise einem Dienstleister oder einem Trägerverein zusammengearbeitet wird, sind diese auf den Datenschutz zu verpflichten (siehe Muster Nr. 4). Sie sind auch später regelmäßig an den Datenschutz zu erinnern und zu kontrollieren. Schließlich sind die Aufbewahrungs- und Löschfristen festzulegen und – entsprechend der Speicherart (Papierakten/elektronische Dateien) – zu entscheiden, wie Daten nach Ablauf dieser Fristen vernichtet werden sollen.
Im Anschluss daran ist zunächst das **Verzeichnis** der Verarbeitungstätigkeiten anzulegen. Sinnvoll dürfte es sein, bereits zu diesem Zeitpunkt auch das Löschverzeichnis aufzusetzen, damit es nicht vergessen wird (siehe Muster Nr. 5).
Die ersten Einträge erfolgen mit Arbeitsaufnahme, also mit der ersten Kontaktaufnahme durch interessierte Erziehungsberechtigte.
Sodann ist das **Informationsblatt** zur Datenerhebung vorzubereiten (s. Muster Nr. 2). Wird eine Interessenten- oder Warteliste geführt, sollte ein abgespecktes Formular zur Abfrage der wichtigsten Kontaktdaten erstellt werden. Es sollte im Formularkopf eine kurze Information über Zweck und Erlaubnistatbestand der Datenerhebung enthalten und eine kurze Datenerhebungseinwilligung zu diesem Zwecke (z. B. Interessentenliste zur Kontaktaufnahme zur zukünftigen Platzvergabe) aufweisen.
Im **Betreuungsvertrag** sollten Datenschutz- und **Einwilligungsklauseln** eingefügt werden (siehe Muster Nr. 3). Werden Portfolioarbeiten durchgeführt, Ich-Bücher oder sonstige Dokumentationen wie beispielsweise Fotobücher erstellt (bitte beachten: Fotografien sind auch Daten), sind diese Maßnahmen durch entsprechende Einwilligungsklauseln abzusichern. Zu beachten ist jedoch, dass nicht jede Einwilligung ewig gilt. So hat das Landgericht Frankfurt a. M. entschieden, dass eine neunzehn Jahre alte Einwilligung zur Veröffentlichung einer Fotografie keine erneute Veröffentlichung zulasse (LG Frankfurt a. M., 2019). Die Erhebung von Daten Dritter wie abholberechtigter Personen oder der Kinderärztin bzw. des Kinderarztes, die oder der im Notfall zu verständigen ist, ist i. d. R. durch Art. 6 Abs. 1b, d DSGVO gedeckt.Empfehlenswert ist es, wenn möglich bereits in diesem Stadium ein Grundmuster für ein **Auskunftsformular** zu erstellen (siehe Muster Nr. 6).
Die erforderlichen **technischen und organisatorischen Maßnahmen** sind einzurichten (z. B. Kauf einer aktuellen Software, Virenschutz, Wahl eines sicheren Servers, Einrichtung sicherer Übertragungswege usw.).
Die Kindertagespflegeperson kann sodann guten Gewissens nach oder parallel zur de Erlaubniserteilung versuchen, über Kontaktanzeigen oder durch Vermittlung des öffentlichen Jugendhilfeträgers Kontakt zu potentiellen Interessenten zu erlangen.
Eine eigene kurze datenschutzrechtliche „To-Do-Liste" für den Alltag zu erstellen, ist sicherlich hilfreich, um im laufenden Betreuungsbetrieb einzelne dieser zahlreichen Schritte und Maßnahmen nicht zu übersehen. Eine Basis für eine solche Liste findet sich im Anhang (4. Kurzanleitung: Maßnahmenkatalog Datenschutz in der Kindertagespflege, S. 38).
Bevor eine Großtagespflegestelle eröffnet wird, sind die Mitarbeiterinnen und Mitarbeiter auf den Datenschutz zu verpflichten (siehe Muster 7: Mitarbeiterverpflichtung zur Einhaltung des Datenschutzes, S. 67). Diese Verpflichtung ist im laufenden Betreuungsalltag periodisch zu wiederholen.

Erste Kontaktaufnahme mit interessierten Erziehungsberechtigten

Vor Annahme von Daten sind die Erziehungsberechtigten zu informieren (siehe Muster 2: Informationsblatt zur Erhebung von personenbezogenen Daten gem. Art. 13 DSGVO, S. 54). Ihre Einwilligung zur Datenverarbeitung im jeweiligen Rahmen ist einzuholen. An dieser Stelle ist sorgfältig darauf zu achten, dass nachweislich zuerst die Information und dann die freiwillige Einwilligung erfolgt. Dies kann z. B. durch Ausfüllen des Interessentenblattes (mit entsprechendem Formularkopf) durch die Erziehungsberechtigten selbst erfolgen. Im Rahmen der Kennenlerntreffen ist mit den Erziehungsberechtigten neben den zahlreichen pädagogischen und allgemeinen organisatorischen Fragen auch der Datenschutz zu bespre-

Vor Annahme von Daten sind die Erziehungsberechtigten zu informieren. Ihre Einwilligung zur Datenverarbeitung im jeweiligen Rahmen ist einzuholen und es sollte ihnen klar und unmissverständlich bereits vor Beginn der Betreuung erklärt werden, welche Handlungen und insbesondere welche Kommunikationswege (wie z. B. derzeit WhatsApp oder Facebook) nicht benutzt werden können.

chen: Den Erziehungsberechtigten muss die Bedeutung näher gebracht werden. Es sollte ihnen klar und unmissverständlich bereits vor Beginn der Betreuung erklärt werden, welche Handlungen und insbesondere welche Kommunikationswege (wie z. B. derzeit WhatsApp oder Facebook) nicht benutzt werden können.
Im Rahmen der Besprechung des **Betreuungsvertrages** sollten die Passagen zum Datenschutz und insbesondere zur Einwilligung in die Erhebung von Gesundheitsdaten explizit angesprochen werden (siehe Muster Nr. 3). In der Praxis hat es sich bewährt, die Bedeutung der Erhebung von Gesundheitsdaten zum Schutze der Gesundheit des Kindes durch konkrete Beispiele zu erklären.
Es wird geraten, diese vorvertraglichen Besprechungen zumindest kurz zu dokumentieren.
Mit Vertragsabschluss wird dann die erste umfassende Datenspeicherung vorgenommen, sei es, indem der Vertrag in einer Akte abgeheftet und ein Schnellinformationsblatt erstellt wird (zur raschen Auffindung der wichtigsten Informationen für den Notfall), sei es, indem der Vertrag in einer Datei auf einem PC abgespeichert wird. Parallel erfolgen die ersten Einträge (stichwortartig, kurz) im Verzeichnis der Verarbeitungstätigkeiten (siehe Muster Nr. 5). Sodann wird der Betreuungsvertrag (oder Teile davon oder ein hierauf basierender „Belegbogen") üblicherweise an den öffentlichen Jugendhilfeträger weitergeleitet. Dies ist ebenfalls ins Verzeichnis einzutragen.

In der laufenden Betreuung

Die Art und Weise, wie Kindertagespflege durchgeführt wird, ist sehr unterschiedlich. Es ist jedoch inzwischen recht verbreitet und wird teilweise auch gefordert, dass Kindertagespflegepersonen zumindest kurze Dokumentationen zum Verlauf der Betreuung, zum Verhalten des Kindes, zu Fortschritten oder Problemen bzw. Auffälligkeiten machen. In manchen Fällen werden sogenannte Entwicklungsbücher, Portfoliobücher, Ich-Bücher oder Fotosammlungen erstellt. Diese Tätigkeiten sind im Verzeichnis ebenso aufzuführen wie beispielsweise eine Kommunikation mit dem öffentlichen Jugendhilfeträge oder die Antwort auf eine Anfrage (siehe Muster 5: Verzeichnis der Verarbeitungstätigkeiten, S. 62). Soweit sich in der laufenden Betreuung Neuerungen ergeben, weil sich die gesetzlichen Vorgaben geändert haben oder ein neuer technischer Standard eingeführt wurde, sind die eigenen Maßnahmen und insbesondere der eigene technische Standard an die neuen Anforderungen anzupassen. Dies gilt im besonderen Maße, wenn elektronische Medien verwendet werden.

Bei Beendigung der Betreuung

Endet die Betreuung, so sollte die Kindertagespflegeperson die Daten des ehemaligen Tagespflegekindes aus der Datei oder dem Ordnungssystem für die laufende Betreuung **entnehmen** und in ein Ordnungssystem „beendete Betreuungsverhältnisse" **verschieben bzw. umsortieren.** Dieses Ordnungssystem ist getrennt aufzubewahren. Gleichzeitig sollte vermerkt werden, wann die Aufbewahrungszeit endet und die Unterlagen somit zu löschen sind. Die Kindertagespflegeperson bestimmt dabei die Aufbewahrungszeiten für das beendete Betreuungsverhältnis anhand der vorab generell von ihr im Datenschutz festgelegten Aufbewahrungszeiten (z. B. zehn Jahre).
Es muss auch damit gerechnet werden, dass Erziehungsberechtigte **Auskunft** über die Datenverarbeitung bei der Kindertagespflegeperson verlangen. Diese ist dann zu erteilen, sodass es sich anbietet, ein Muster für eine solche Auskunft anzulegen. (siehe Muster Nr. 6). Wenn die Kindertagespflegeperson von den Erziehungsberechtigten dazu aufgefordert wird, hat sie zudem auch die von ihr verarbeiteten Daten für die Erziehungsberechtigten **auszulesen** und diesen mitzugeben, damit diese sie einfach an andere Einrichtungen transferieren können. Dies kann mittels CD-ROM oder USB-Stick erfolgen, wenn die Daten elektronisch gespeichert waren. Bei Datenspeicherung in Papierform bieten sich Kopien an.
Nach Ablauf der Aufbewahrungszeit, die zuvor im Datenschutz festgelegten wurde, müssen die Daten auch aus diesem Ordnungssystem entfernt und gelöscht bzw. vernichtet werden
Diese verschiedenen Schritte sind im Verzeichnis der Verarbeitungstätigkeiten zu notieren. Die Löschung und Vernichtung ist zu dokumentieren und in das Löschverzeichnis einzutragen.

Typische Problemfelder in der laufenden Betreuung

Häufig erwarten Erziehungsberechtigte, dass die Kindertagespflegeperson mit ihnen über **soziale Medien** kommuniziert. Die nahezu permanente Dauerkommunikation und der Austausch von Filmen und Fotos über diese Medien hat in den letzten Jahren stark zugenommen. Unabhängig davon, ob eine derart ausufernde Dauerkommunikation pädagogisch sinnvoll ist, weil

sie die Konzentration auf das Tagespflegekind und seine Betreuung beeinträchtigt und in manchen Fällen sogar zu einer Verletzung der Aufsichtspflicht führen kann, öffnet sie auch noch einer Dauerüberwachung Tür und Tor. Werden hier zudem keine datenschutzkonformen Kanäle benutzt, beobachten und lesen unberechtigte Dritte gleich mit. **Daher sind hier grundsätzlich nur Medien zu wählen, die DSGVO-konform sind.** Insgesamt wird zu einer zurückhaltenden Verwendung solcher zulässigen Medien geraten. Sie sollte außerdem möglichst außerhalb der Betreuungszeiten stattfinden.

WhatsApp, Facebook und ähnliche außereuropäische Formate erfüllen die europäischen Datenschutzstandards derzeit nicht in ausreichendem Maße. Sie setzen trotz einiger Änderungen in ihrem Angebot (insbesondere bei den sogenannten Cookies) weiterhin auch bei Personen, die keine Nutzer sind, Cookies mit Identifikatoren. Ihre Daten werden dann nach bestimmten, teilweise nicht abänderbaren voreingestellten Kriterien von diesen Medien ausgewertet und Betreibern zur Verfügung gestellt, ohne dass die Betroffenen davon wissen oder dies unterbinden könnten (Datenschutzkonferenz, Beschluss vom 05.09.2018 „Facebook-Fanpages"). Solche Dienste sollten daher im unternehmerischen Bereich auch dann nicht genutzt werden, wenn die Kindertagespflegeperson technische Maßnahmen zur Eindämmung datenschutzwidriger Anwendungen wie z. B. Exchange-Container anwendet. Da die Social-Media-Unternehmen ihre Datenverarbeitung nicht transparent darstellen, kann auch die Kindertagespflegeperson nicht darüber aufklären. Deshalb wird der rechtssichere Einsatz von Social Media in Unternehmen momentan als faktisch unmöglich betrachtet (vgl. dazu auch „https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Handlungsrahmen_Soziale_Medien_20200306.pdf" Handlungsrahmen für die Nutzung von Social Media durch öffentliche Stellen, S. 6; letzter Abruf: 01.05.2020).

WhatsApp, Facebook und ähnliche außereuropäische Formate erfüllen die europäischen Datenschutzstandards derzeit nicht in ausreichendem Maße und sollten daher im unternehmerischen Bereich, also auch in der Kindertagespflege, nicht genutzt werden.

Insbesondere bei dem weit verbreiteten Messengerdienst WhatsApp registrierten sich die Nutzerinnen und Nutzer mit ihrer Mobiltelefonnummer. Danach liest die Anwendung das Adressbuch der Nutzerinnen und der Nutzer aus (s. auch im Folgenden AG Bad Hersfeld). In diesem Zusammenhang werden die Namen aller dort eingetragenen Kontakte und ihre Telefonnummern an den Server der Anwendung übertragen. Die Kontakte können dies bemerken, da ihnen danach angezeigt wird, welche ihrer eigenen Kontakte ebenfalls WhatsApp nutzen. Die Daten von Personen, die diese Anwendung nicht nutzen, werden damit aber ebenfalls übermittelt. Weiterhin behält sich die Anwendung das Recht vor, die so erlangten Daten umfassend für Messungen, Analysen und sonstige Dienste zu nutzen. Nachrichten und insbesondere Fotografien können bis zu 30 Tage oder länger auf Servern gespeichert bleiben, die außerhalb Europas liegen. Standortdaten werden regelmäßig erfasst (siehe hierzu die Nutzungsbedingungen unter: https://www.whatsapp.com/legal?eea=1&lang=de, Abruf: 13.08.2019).
Es ist davon auszugehen, dass diese Informationen sodann mit anderen Unternehmen des Konzerns geteilt werden. Damit werden Daten von Betroffenen über ein Mobiltelefon der unternehmerisch tätigen Kindertagespflegeperson übermittelt, ohne dass hierfür eine Einwilligung der Betroffenen i.S.d. Art. 6 DSGVO vorliegt. Verantwortlicher i.S.d. DSGVO ist die Kindertagespflegeperson. Zivilrechtlich stellt dieser Vorgang daher eine schadensersatzauslösende deliktische Handlung dar, wie das Amtsgericht Bad Hersfeld in sehr klaren Worten zusammenfasst:

> *„Wer den Messenger-Dienst „WhatsApp" nutzt, übermittelt nach den technischen Vorgaben des Dienstes fortlaufend Daten in Klardaten-Form von allen in dem eigenen Smartphone-Adressbuch eingetragenen Kontaktpersonen an das hinter dem Dienst stehende Unternehmen. Wer durch seine Nutzung von „WhatsApp" diese andauernde Datenweitergabe zulässt, ohne zuvor von seinen Kontaktpersonen aus dem eigenen Telefon-Adressbuch hierfür jeweils eine Erlaubnis eingeholt zu haben, begeht gegenüber diesen Personen eine deliktische Handlung und begibt sich in die Gefahr, von den betroffenen Personen kostenpflichtig abgemahnt zu werden."*
>
> (Amtsgericht Bad Hersfeld Beschluss vom 20.03.2017 Az. F 111/17).

Die Daten werden daraufhin an Standorte außerhalb Europas übermittelt und dort voraussichtlich mit anderen Unternehmen geteilt, ohne dass der Anwenderinnen oder Anwender und die Betroffenen davon Kenntnis erlangen oder hiergegen widersprechen könnten. Dieser Datenabfluss kann nach derzeitigem Stand nur

verhindert werden, wenn der Zugriff auf die Kontakte durch WhatsApp technisch dauerhaft ausgeschlossen wird, was in einigen Fällen zumindest sehr schwierig ist (Überblick z. B. bei Welling Praxistipps Chip 2017). Nach derzeitigem Stand muss hierfür vor der ersten Anwendung die Berechtigung zum Zugriff verweigert werden, sofern dies beim jeweiligen Betriebssystem des Mobiltelefons überhaupt möglich ist. Dies schränkt jedoch die Funktionstauglichkeit gerade der als praktisch und bequem empfundenen Anwendungen erheblich ein.
Da die überwiegende Mehrheit der WhatsApp-Nutzungen erfahrungsgemäß uneingeschränkt stattfindet, fließen im Normalfall fortdauernd Daten ohne Einwilligung ab.
Privatpersonen, die den Verpflichtungen der DSGVO gerade nicht unterliegen, können derartige sozialen Medien nutzen, wobei ihnen bewusst sein muss, dass das Datenschutzniveau in diesen Medien sehr dürftig ist und sie damit fortlaufend sehr intime Einblicke gewähren.

> Nutzt eine Kindertagespflegeperson jedoch diese Medien, verstößt sie damit derzeit klar gegen die Vergaben der DSGVO und setzt sich der Gefahr eines Datenschutzverletzungsverfahrens mit anschließender Bußgeldverhängung und sogar Schadensersatzforderungen aus, wie das AG Bad Hersfeld bereits 2017 festgestellt hat.

Eine Kindertagespflegeperson sollte sich daher keinesfalls dazu überreden lassen, aus Bequemlichkeit den manchmal mit Vehemenz vorgebrachten Forderungen von Erziehungsberechtigten, man solle gefälligst über WhatsApp kommunizieren, uneingeschränkt nachzukommen. Dies, zumal nicht davon auszugehen ist, dass eine Einwilligung der Erziehungsberechtigten in die Nutzung überhaupt geeignet wäre, die datenschutzrechtliche Rechtswidrigkeit der Nutzung zu beseitigen.
Um die Gefahr zu verdeutlichen, sei darauf hingewiesen, dass die französische Datenschutzaufsichtsbehörde am 21.01.2019 gegen Google LLC das bisher höchste Bußgeld schlechthin (50 Millionen Euro) verhängte, weil dieses Unternehmen eklatant und nachhaltig gegen die datenschutzrechtlichen Transparenz- und Informationspflichten nach Art. 12 und 13 DSGVO verstoßen hat. Zudem wurden auf Android-Mobiltelefonen unzulässigerweise Daten auf Grundlage unwirksamer Einwilligungen verarbeitet (Oberwetter Legal Tribune Online, 2019). Es dürfte eine Frage der Zeit sein, bis auch gegen Messengerdienste wie WhatsApp vergleichbare Bußgelder verhängt werden.

> **Lösungsmöglichkeiten:**
> - Nutzung getrennter Mobiltelefone für den unternehmerischen und privaten Bereich (privat kann WhatsApp dann weiter genutzt werden)
> - Bei gemischter Nutzung eines einzigen Gerätes *und* ausreichender technischer Kenntnis: Wirksame Unterbindung der unzulässigen Datenweiterleitung
> - Umsteigen auf datenschutzkonforme Messengerdienste wie z. B. Threema, Signal, Hoccer oder SimsMe etc.

Bevor **Foto- und Filmaufnahmen** des Tagespflegekindes (insbesondere Gruppenaufnahmen der Tagespflegegruppe) erstellt werden, ist die Einwilligung der Erziehungsberechtigten einzuholen (Solmecke 2019, S. 29.). Dies kann vorab durch einschlägige Klauseln im Betreuungsvertrag oder einmalig vor dem konkreten Anlass erfolgen. In dieser Einwilligung sollte klar definiert sein, an wen die Foto- oder Filmaufnahmen weitergeleitet, und welche (datenschutzkonformen) Übermittlungskanäle gewählt werden. Der Zweck der Datenerhebung mittels Foto- oder Filmaufnahme ist anzugeben (Aushang in den Betreuungsräumen, zur Erstellung von Fotobüchern, zur Dokumentation der Betreuung, zur Erstellung von Erinnerungsalben, etc.). Den Erziehungsberechtigten sollte das Recht eingeräumt werden, einzelnen Verwendungszwecken zu widersprechen (z. B. durch Ankreuzen/Durchstreichen).
Zur Übermittlung bieten sich die folgenden Wege an:

- CD-ROM, USB-Stick, Weiterleitung via E-Mail oder als MMS; Nutzung datenschutzkonformer Messengerdienste wie Threema, Signal, Hoccer oder SimsMe.

Es ist dabei jeweils auf Verschlüsselung bzw. Sicherung durch Passwortvergabe sowie auf die Wahl eines datenschutzkonformen Servers zu achten. Bei Gruppen-E-Mails sollte die Kindertagespflegeperson die Nachricht im Adressfeld wieder an sich selbst schicken und die Gruppe an sich im Blindverteiler („bcc“) eingeben. Werden Foto- und Filmaufnahmen versendet, ist darauf zu achten, dass sie nur an die tatsächlich beabsichtigten Adressaten verschickt werden. Eine Versendung an die gesamte Tagespflegegruppe (dann über Blindverteiler) kann nur erfolgen, wenn alle ihre Einwilligung zur Erstellung von Gruppenaufnahmen erteilt haben.

Der **Datenaustausch mit der Ersatzbetreuungsperson** sollte ebenfalls vertraglich geregelt werden (siehe Muster 4: Vertrag Auftragsverarbeiter, S. 60). Hier kann in den meisten Fällen ein Auftragsverarbeitervertrag verwendet werden. Alternativ kann eine Einwilligungserklärung der Erziehungsberechtigten zum Datenaustausch mit der Ersatzbetreuungsperson eingeholt werden.

Ersatzbetreuungspersonen sind im selben Maße dem Datenschutz verpflichtet wie Kindertagespflegeperson. Sie haben daher eigenständige, angemessene technisch-organisatorische Schutzmaßnahmen zu ergreifen. Die Kindertagespflegeperson muss kontrollieren, dass der Datenschutz eingehalten wird.

Datenaustausch in Problemfällen sollte nur auf besonders sicheren Wegen erfolgen. Je nach technischer Ausstattung der Kindertagespflegeperson kann dies eine Übermittlung mittels verschlüsselter E-Mail sein (Verschlüsselung des Transportweges und der angehängten Datei mit Passwortvergabe) oder – klassisch – mittels Brief. Selbstverständlich muss das Passwort seinerseits in gesicherter Form und getrennt verschickt werden.

Datenaustausch in Problemfällen sollte nur auf besonders sicheren Wegen erfolgen.

4 Kurzanleitung: Maßnahmenkatalog Datenschutz in der Kindertagespflege

a. Bestandsaufnahme

Zu Beginn jeder Einführung oder Verbesserung des Datenschutzes steht die Analyse des eigenen Betreuungsalltages und der aktuell bestehenden Datenverarbeitungen. Es muss für jede Datenweitergabe jeweils der dahinterstehende Zweck, der Erlaubnistatbestand und der konkrete Kreis der Personen, Unternehmen und Behörden, an die Daten weitergeleitet werden, ermittelt werden (Ist-Zustand). Dies erfolgt am besten anhand der Datenverarbeitung in einem konkreten Betreuungsfall.

b. Handlungsbedarf feststellen

In einem zweiten Schritt wird dieser Ist-Zustand mit dem Soll-Zustand verglichen; Lücken sind zu identifizieren.

c. Schrittweise Anpassung des allgemeinen Datenschutzniveaus

In der Praxis dürften daraufhin die folgenden zehn Maßnahmen am häufigsten durchzuführen oder zu verbessern sein:

- Erstellung/Anpassung eines kurzen, auf den eigenen Betreuungsalltag angepassten Datenschutzkonzepts unter Verwendung der öffentlich zugänglichen Vorlagen, Einfügung eines Datenschutzabsatzes in das Betreuungskonzept.
- Erstellung/Anpassung der eigenen Vertragsvorlagen (Einfügung von Datenschutzklauseln in die Verträge) und Einwilligungserklärungen (Art. 6 und 9 DSGVO).
- Erstellung/Anpassung eines Datenschutzinformationsblatts zur Aushändigung während des Erstgespräches.
- Erstellung/Anpassung des Formularkopfs von Warte- oder Interessentenlisten.
- Erstellung/Anpassung und periodische Pflege des Verfahrens-/Löschverzeichnisses.
- Erstellung/Anpassung der Datenschutzhinweise auf der Website bzw. in sozialen Netzwerken.
- Erstellung/Anpassung des E-Mail-Disclaimers (Impressum!), ggf. mit Verlinkung auf die Datenschutzhinweise auf der Website/ in den sozialen Medien.
- Vertragliche Verpflichtung der Auftragsverarbeiter.
- Erstellung/Anpassung von Vorlagen zur Auskunftserteilung, zur Information über erfolgte Auskunftserteilungen und zur Meldung von Datenschutzpannen.
- Anpassung der Betreuungspraxis (Nichterhebung nicht erforderlicher Daten).

d. Einführung der IT-Sicherheit

- Sicherung der Datensammlung entweder durch abschließbaren Aktenschrank oder durch technische Sicherungen des unternehmerisch genutzten Computers.
- Sicherung der Datenübertragungswege (z. B. Verschlüsselung der Übertragung, Wahl sicherer Übertragungswege).
- Wahl datenschutzkonformer Server und Anbieter.
- Verwendung datenschutzkonformer Kommunikationswege (Verschlüsselung).
- Regelung der Nutzung von Mobiltelefonen (Trennung private – unternehmerische Nutzung durch getrennte Geräte oder besondere technische Sicherung der unternehmerischen Daten bei Mischnutzung eines einzigen Gerätes).

Weiterführender Überblick:
Datenschutzkonferenz – Kurzpapier Nr. 8: (2018) Maßnahmenplan „DSGVO“ für Unternehmen Version 2.0 vom 17.12.2018 (www.govdata.de/dl-de/by-2-0 unter https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_8.pdf), letzter Abruf: 05.02.2020)

5 Offene Fragen, Anlaufstellen

Da die DSGVO verhältnismäßig jung ist, sind viele Detailfragen noch nicht oder nicht abschließend geklärt; die ersten Verfahren befinden sich erst im Weg durch die Instanzen.
So ist bisher unklar, ob (auch) eine unternehmerisch tätige Kindertagespflegeperson bei einer Datenschutzverletzung neben einem Datenschutzverletzungsverfahren und zivilrechtlichen Schadensersatzforderungen mit einer **Abmahnung** nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) rechnen muss. So bejahen beispielsweise das Landgericht Würzburg (Beschluss vom 13.09.2018 Az 11 O 1741/18) und (tendenziell auch) das Oberlandesgericht Hamburg (Urteil vom 25.10.2018 Az 3 U 66/77) die Abmahnfähigkeit von Verstößen gegen die DSGVO, während das Landgericht Bochum (Urteil vom 07.08.2018 Az 12 O 85/18) oder das Landgericht Stuttgart (Urteil vom 20. Mai 2019, Az.: 35 O 68/18 KfH) eine solche nicht erkennen können.
Zunächst fallen Kindertagespflegepersonen auch nach den Feststellungen des Bundesgesetzgebers unter das UWG. Sie handeln geschäftlich im Sinne von § 2 Abs. 1 Nr. 1 UWG, da sie gegenüber ihren Kundinnen und Kunden Leistungen gegen Entgelt erbringen. Verstöße gegen Vorschriften der DSGVO können nach der derzeitig wohl überwiegenden Meinung jedenfalls dann nach dem UWG abgemahnt werden, wenn diese zumindest auch als Marktverhaltensregelungen im Sinne von § 3a UWG anzusehen sind. Dies ist nach dem bisherigen Stand der Rechtsprechung zum UWG nicht für sämtliche Vorschriften der DSGVO der Fall (Bundestag Drucksache DS 19/11843 vom 23.07.2019 S. 5). Eine derartige Abmahnung erscheint jedoch denkbar, denn wer sich nicht an den Datenschutz hält, kann mit einer erheblichen Zeitersparnis und spürbar weniger Kosten rechnen. Dies könnte ein unzulässiger Wettbewerbsvorteil i.S.d. UWG sein, weshalb Marktkonkurrenten abgemahnt werden könnten. Andererseits gibt es Bestrebungen, das Wesen der Abmahnung einzuschränken, da sich in verschiedenen Bereichen eine rechtsmissbräuchliche Abmahnindustrie etabliert hat. Schließlich wird die Auffassung vertreten, dass Art. 80 DSGVO die Rechtsfolgen bei Verstößen abschließend regelt und gegenüber dem UWG vorrangig ist, sodass dessen Anwendung gesperrt ist. Bereits die uneinheitliche Rechtsprechung zeigt aber, dass sich Unternehmerinnen und Unternehmer – somit auch Kindertagespflegepersonen – zumindest einem erheblichen Risiko aussetzen, wenn sie sich nicht um den Datenschutz kümmern.
Auch, was das **Melden** von Datenschutzverstößen gem. Art. 33 DSGVO betrifft, bestehen in der Praxis zahlreiche offene Fragen. Art. 33 DSGVO verpflichtet den Verantwortlichen oder den Auftragsverarbeiter dazu, den Verstoß innerhalb von 72 Stunden ab Kenntnis zu melden. Führt die Verletzung des Schutzes personenbezogener Daten hingegen voraussichtlich nicht bzw. nur zu einem geringen Risiko für die Rechte und Freiheiten natürlicher Personen, besteht keine Meldepflicht. In der Praxis ist es herausfordernd, richtig zu erkennen, ob eine Meldung zu erfolgen hat, und wenn ja, an wen, zumal es hier bisher wenige Entscheidungen gibt. Entsprechend der im Folgenden herangezogenen lesenswerten Zusammenstellung der Landesbeauftragten für den Datenschutz Niedersachsen (nachzulesen unter: https://www.lfd.niedersachsen.de/startseite/datenschutzreform/DSGVO/faq/meldung-von-datenschutzverstoeen-167312.html, letzter Abruf: 05.02.2020) verfolgt die DSGVO einen **risikobasierten** Ansatz. Die Frage, ob gemeldet werden muss, ist demnach weniger danach zu beurteilen, wie gravierend die Verletzung ist, sondern welches Risiko für die Betroffenen und ihre Rechte und Freiheiten eintritt und wie hoch es ist.
Die Meldepflicht soll daher nur entfallen, wenn lediglich ein **geringes Risiko** für die Rechte und Freiheiten natürlicher Personen besteht und mit der Meldung die Möglichkeit bei den Betroffenen eröffnet wird, etwas gegen den Schadenseintritt zu unternehmen. Können die Betroffene etwas unternehmen, um den Schaden zu vermeiden oder zu verringern, soll ihnen die Datenschutzverletzung gemeldet werden. Andernfalls ist dies nicht nötig. Mittlere bis gravierende Datenschutzverletzungen mit hohem Risiko sind weiterhin der zuständigen Datenschutzbehörde zu melden. Die folgenden Beispiele für ein Entfallen oder Bestehen der Meldepflicht werden dabei angeführt:

- Unbefugte erhalten Zugang zu verschlüsselten Daten, indem sie die Sicherung „geknackt“ haben (Stand der Technik: es dürfen keine überholten Sicherungstechniken verwendet werden!). Da das Risiko, dass *nach dem aktuellen Stand der Technik* verschlüsselte Daten geknackt werden, als eher gering einzustufen ist, muss keine Meldung an die Betroffenen erfolgen. Eine Meldeverpflichtung besteht im Umkehrschluss aber

dann, wenn die Verschlüsselung aufgrund einer veralteten Verschlüsselungstechnik geknackt worden ist.

- Auch der Verlust von *verschlüsselten* USB-Sticks oder *zugangsgeschützten* Smartphones ist nicht meldepflichtig, *wenn* der aktuelle Stand der Technik eingehalten worden ist.
- Hacking von Online-Accounts, Stehlen von Passwörtern: Meldeverpflichtung an die Betroffenen, damit sie die Zugangsdaten ändern und einen Schaden verhindern können
- Versehentlich an den falschen Adressaten verschickte Briefe werden i. d. R. ungeöffnet zurückgeschickt, sodass keine Meldeverpflichtung besteht. Verschlüsselte E-Mails, die falsch versandt wurden, können zwar von unbefugten Dritten an sich wahrgenommen werden (Mailadresse), der Inhalt ist aber geschützt. Ein solcher einfacher Fehlversand ist den Betroffenenwohl aber nicht den Datenschutzaufsichtsbehörden zu melden, wenn davon auszugehen ist, dass eine unzulässige Weiterverwendung der Mailadresse durch den Dritten nicht zu befürchten ist. Eine Meldung an die Datenschutzbehörde könnte dann aber in Frage kommen, wenn mit der E-Mail höchst sensible besondere personenbezogene Daten ungesichert (= nicht verschlüsselt und passwortgesichert) versandt worden wären und deren Verlust zu einer erhöhten Gefährdung der Betroffenen führen würde. Es empfiehlt sich daher, besonders kritische Daten wie z. B. Gesundheitsdaten oder Meldungen nach § 43 Abs. 3 S. 6 oder nach den §§ 8a,b SGB VIII nur in Form verschlüsselter und passwortgesicherter E-Mail-Anhänge zu verschicken.

Bei Zweifeln zur Frage, ob oder wem etwas gemeldet werden muss, empfiehlt es sich, sich bei den jeweils zuständigen Landesdatenschutzbeauftragten zu erkundigen.

II

Die notwendigen Datenschutzkompetenzen einer Kindertagespflegeperson

Das Niveau für die geforderten Kompetenzen orientiert sich an der aktuellen Mehrheit der Kindertagespflegeperson, welche allein in eigenen Räumen tätig ist. Für Kindertagespflegepersonen in Großtagespflege werden nur punktuell in der tätigkeitsbegleitenden Grundqualifizierung eigene Punkte angeführt.

1 Kompetenzen in der tätigkeitsvorbereitenden Grundqualifizierung

Ziel der tätigkeitsvorbereitenden Grundqualifizierung nach dem Konzept des QHB (Schuhegger u. a. 2015, 2019, vgl. Anhang Aufbau der Grundqualifizierung nach dem Konzept des Qualifizierungshandbuches Kindertagespflege, S. 81) (vor Erlaubniserteilung) ist es, Berührungsängste abzubauen und Berührungsbereitschaft zum Datenschutz aufzubauen. Ein Grundverständnis sollte erzielt werden. Es wird dabei davon ausgegangen, dass bei den angehenden Kindertagespflegepersonen zu Beginn dieses Qualifizierungsteiles noch kaum Datenschutzkenntnisse vorhanden sind.
In fachlicher Hinsicht sollten sich angehende Kindertagespflegepersonen mit Abschluss der tätigkeitvorbereitenden Grundqualifizierung in den folgenden Punkten ein Grundwissen angeeignet haben:

- Sie sollten die Fertigkeit und Bereitschaft erworben haben, sich die wichtigsten, für sie relevanten Vorschriften der Datenschutzgesetze (DSGVO, BDSG, SGB, Landesdatenschutzgesetz) durch eigene Recherche und Lektüre anzueignen sowie diese im Ansatz in ihrer Bedeutung für ihren Betreuungsalltag nachzuvollziehen.
- Sie sollten wissen, wo und wie sie diese Vorschriften abrufen können.
- Sie sollten wissen, welche Kommunikationskanäle (insbesondere E-Mail, soziale Medien) und Speichermedien (Papierform, Dateiform) in der Kindertagespflege üblicherweise angewandt werden und wie diese datenschutzrechtlich einzuordnen sind.
- Vor diesem Hintergrund sollten sie am Ende dieser Qualifizierungsphase befähigt sein, die für ihr künftiges persönliches Betreuungssetting passenden Kommunikationskanäle und Speichermedien auszuwählen.
- Sie sollten erste Kenntnisse des für ihren Betreuungsalltag notwendigen technischen Sicherungsstandards für diese Kommunikationskanäle und Speichermedien erworben haben.
- Sie sollten die wichtigsten grundlegenden Entscheidungen für ihr Datenschutzkonzept gefasst und in einer (kurzen) Anfangsversion desselben fixiert haben.

Im Bereich der Sozialkompetenz soll ein Grundverständnis dafür erarbeitet werden, welche Bedeutung und Erfordernis der Datenschutz an sich hat. Die Kindertagespflegepersonen sollen grundsätzlich und nachhaltig bereit dazu sein, sich dauerhaft mit dem Datenschutz auseinanderzusetzen:

- Es sollte ihnen vor Aufnahme der Betreuungstätigkeit bewusst geworden sein, dass auch sie den Datenschutz zu berücksichtigen haben, damit der Datenschutz insgesamt in der Masse wirksam umgesetzt und verteidigt werden kann.
- Sie sollten erkennen, dass ihre für die sogenannte „große" Welt vermeintlich uninteressanten „kleinen" Daten in vielfältiger Weise und auf unterschiedlichen Wegen abgeschöpft und weiterverwendet werden können, sie als künftige Kindertagespflegepersonen also wachsam und problembewusst handeln müssen.
- Einzelne größere und besonders einprägsame Datenschutzskandale sollten ihnen präsent sein, aus denen sie erfolgreich die wichtigsten Gefahren und daraus folgend die wichtigsten Datenschutzziele für ihre Tätigkeit im Kern ableiten können.

Die teilnehmenden Kindertagespflegepersonen sollten am Ende der tätigkeitsvorbereitenden Grundqualifizierung insgesamt selbstkompetent fähig sein, ihr eigenes bisheriges Datenschutzverhalten kritisch zu reflektieren und neue Verhaltensweisen für ihre künftige Betreuungstätigkeit zu entwickeln. Sie sollen verinnerlicht haben, dass Datenschutz umfassend und beständig betrieben werden muss, um den steten (unsichtbaren) Datenmissbrauch zu minimieren. Zu guter Letzt sollte als Ausfluss dieser Einsichten die tatsächliche Bereitschaft vorhanden und erkennbar sein, das eigene Verhalten künftig zu verändern.

2 Kompetenzen in der tätigkeitsbegleitenden Grundqualifizierung

Ziel in der tätigkeitsbegleitenden Grundqualifizierung an sich ist die erste erfolgreiche praktische Umsetzung der zentralen Datenschutzmaßnahmen. Es sollen ausreichende Kompetenzen zur selbstständigen und erfolgreichen Umsetzung des Datenschutzes im eigenen Bereich erworben werden.
In fachlicher Hinsicht sollten Kindertagespflegepersonen mit Abschluss der tätigkeitsbegleitenden Grundqualifizierung

- ein erstes (kurzes) Datenschutzkonzept und ein erstes Verfahrens- und Löschverzeichnis erstellt haben;
- erste eigene Vorlagen für ein Datenschutzinformationsblatt, Einwilligungserklärungen und Datenschutz-Vertragsklauseln entwickelt haben;
- ein Formularkopf für Warte- oder Interessentenlisten entworfen haben;
- Grundzüge eines ersten, auf die eigenen Betreuungsverhältnisse zugeschnittenes Verfahrens- und Löschverzeichnisses verfasst haben;
- eine eigene E-Mail-Adresse und erste Entwürfe für einen passenden E-Mail-Disclaimer mit Datenschutzhinweis eingerichtet haben.

In Bezug auf die Sozialkompetenz sollte mit Abschluss der tätigkeitsbegleitenden Grundqualifikation die Einsicht entstanden sein, dass

- die private Sphäre von der beruflichen Sphäre strikt getrennt werden sollte (E-Mail-Accounts, Gerätenutzung, Nutzung sozialer Medien);
- die Anforderungen an die Datenverarbeitung im privaten und beruflichen Bereich strikt getrennt betrachtet und abgegrenzt werden sollten;
- die künftige Kindertagespflegeperson die i. d. R. alleinige Verantwortliche für den korrekten Umgang mit den Daten der künftigen Tagespflegekinder und ihrer Erziehungsberechtigten ist;
- die künftigen Kindertagespflegepersonen bei den Erziehungsberechtigten umfassende Aufklärungsarbeiten durchführen und bei diesen auf die dauerhafte Einhaltung ihrer Datenschutzregeln achten muss.

Die angehenden Kindertagespflegepersonen sollten weiterhin die Bereitschaft aufweisen, vertieft selbstkritisch auf die bei ihnen vorhandenen Abläufe und Werkzeuge zu blicken und diese ggf. zu verbessern bzw. auszutauschen. Sie sollten fähig sein, neue Arbeitsabläufe einzuüben und neue Werkzeuge anzuwenden.
In persönlicher Hinsicht sollten die teilnehmenden Kindertagespflegepersonen die Bereitschaft entwickelt haben, sich mit komplexen datenschutzrechtlichen Begriffen, Fragen und Anwendungen auseinanderzusetzen und die Notwendigkeit erkennen, sich kontinuierlich eigenständig fortzubilden und zu informieren.

3 Fortbildungsphase

Nach erfolgreichem Abschluss der tätigkeitsvorbereitenden Grundqualifikation nach dem Konzept des QHB wird i. d. R. die Pflegeerlaubnis gem. § 43 SGB VIII erteilt. In der Folge absolviert die so qualifizierte Kindertagespflegeperson neben einer ersten Betreuungstätigkeit die tätigkeitsbegleitende Grundqualifizierung und erhält als Nachweis das sogenannte Bundeszertifikat bzw. eine Teilnahmebestätigung seitens des Bildungsträgers. Danach nimmt sie an den verpflichtenden jährlichen Fortbildungen teil. Die Fortbildungsverpflichtung bleibt über den gesamten Zeitraum der Ausübung der Kindertagespflegetätigkeit hinweg bestehen; die Fortbildungsverpflichtung umfasst auch die Verpflichtung zur Fortbildung in Datenschutzfragen.

Ab dieser Phase sollten Kindertagespflegepersonen unter Anwendung ihrer ersten praktischen Erfahrungen ihre zuvor erstellten eigenen Vorlagen und Entscheidungen fortwährend an die nun eingetretene konkrete Betreuungssituation anpassen:

- Da die Kindertagespflegepersonen jetzt andere Personen in unterstützender Form zur Ausübung ihrer Betreuungstätigkeit heranziehen (Auftragsverarbeiter wie z. B. Unterstützung in der Verwaltung, eigenorganisierte Ersatzbetreuungspersonen etc.), müssen sie mit diesen Auftragsverarbeitungsverträge zur Einhaltung des Datenschutzes abschließen.
- Die angewandten Sicherungsmaßnahmen für die benutzten Datenspeichersysteme und die verwendeten Kommunikationskanäle sind auf ihre Praxistauglichkeit zu überprüfen und ggf. auszutauschen.
- Das Datenschutzkonzept ist mit diesen neuen Entwicklungen zu ergänzen und weitestgehend zu finalisieren.
- Im Betreuungskonzept sollte ein kurzer Absatz zum Datenschutz eingefügt werden.
- Der Ablauf eines Meldeverfahrens bei Verstößen sollte bekannt sein; die entwickelten eigenen Vorlagen zur Meldung von Verstößen sollten anwendungsreif sein.
- Die Kindertagespflegepersonen sollten die für sie konkret zuständigen Beratungs-, Auskunfts- und Meldestellen an einer leicht erreichbaren Stelle gespeichert haben.

Weiterhin sollte spätestens mit Aufnahme der Betreuungstätigkeit bei den Kindertagespflegepersonen die Kompetenz vorhanden sein, Erziehungsberechtigten die Notwendigkeit des Datenschutzes zu vermitteln, sondern und zudem im konkreten Einzelfall datenschutzfeindlichen Forderungen der Erziehungsberechtigten erfolgreich zu widerstehen. Sie sollten mit Beginn der Betreuungstätigkeit die Fertigkeit einüben und verfeinern, erkannte Probleme unter Anwendung der korrekten datenschutzrechtlichen Begriffe möglichst prägnant zu formulieren und während einer Diskussion den Kern des Problems unter Verwendung der korrekten Begriffe zu benennen.

Kindertagespflegepersonen in der Fortbildungsphase sollten zudem fähig sein, unter Verwendung ihrer Vorlagen eine Meldung von Datenschutzverstößen und eine Auskunft zu formulieren. Sie sollten Aufbewahrungs- und Löschfristen berechnen und festsetzen können sowie ihre Verzeichnisse periodisch pflegen.

Sie sollten erfolgreich in der Lage sein, sich eigenständig kontinuierlich fortzubilden und zu informieren und dabei die Relevanz neuer Informationen für ihren Betreuungsalltag zu erkennen.

Als erfolgreichen Abschluss der Fortbildung sollte im Bereich der persönlichen, sozialen Kompetenzen die Bereitschaft bestehen, eigene Schwachstellen und Lücken zu offenbaren, diese zu reflektieren und daran zu arbeiten. Eng damit verbunden sollte der Wille vorhanden sein, Beratung in Anspruch zu nehmen.

III

Methodik und Kompetenzen der Referierenden

Das methodisch-didaktische Vorgehen und die Kompetenzen der Referierenden sollen zur Erleichterung entsprechend den bisherigen Ausführungen entlang der verschiedenen Phasen einer datenschutzrechtlichen Aus- und Fortbildung gegliedert werden.

1 Tätigkeitsvorbereitende Grundqualifizierung

Methodisch-didaktisch bietet es sich an, die künftigen Kindertagespflegepersonen in der tätigkeitsvorbereitenden Grundqualifizierung für den Gedanken des Datenschutzes zu öffnen und zugänglich zu machen. Häufig begegnen den Referierenden zu Beginn in diesem Bereich Unverständnis und Unwille, die Bedeutung und Tragweite des Datenschutzes zu erkennen, weil dies in der Folge eine Vielzahl an neuen und unbekannten Anstrengungen bedeutet. Als Einstieg in die Thematik Datenschutz könnte daher die Entwicklung der Fragestellung gewählt werden. Nutzbar sind dabei Kommentare wie

- *Ich habe nichts zu verbergen, warum also soll ich so einen Aufwand betreiben, um Daten zu schützen?*
- *Ich bin doch nur eine kleine und unbedeutende Kindertagespflegeperson, die zu Hause betreut. Wer interessiert sich schon für die Daten bei/von mir oder von den Tagespflegekindern? Wer soll denn überhaupt mitbekommen, dass ich Daten erhebe und weiterleite?*
- *Warum muss ich mich um dieses Thema kümmern? Das Jugendamt muss hier doch zuerst tätig werden!*
- *Das ist mir alles zu viel. Ich verstehe nichts von dieser ganzen Technik. Lieber erhebe ich keine Daten mehr, dann muss ich mich mit dieser Thematik gar nicht mehr auseinandersetzen.*
- *Wie soll ich das jetzt auch noch schaffen? Ich soll die Tagespflegekinder gut betreuen, mich um meine eigene Familie kümmern und nun in der wenigen Freizeit, die mir bleibt, einen Haufen an Formularen produzieren?*
- *Da bleibt zur Betreuung ja gar keine Zeit mehr, wenn ich ständig mitdokumentieren soll, so ähnlich wie Krankenschwestern, die protokollieren auch nur und pflegen fast gar nicht mehr. Ich bin aber Kindertagespflegeperson, ich will betreuen.*
- *Dafür reicht das Geld doch gar nicht, das ich für die Betreuung bekomme. Womit soll ich all diese technischen Maßnahmen bezahlen?*

Erfahrungsgemäß ist das Thema Datenschutz mit viel Angst und Unsicherheit verbunden, was häufig in Ablehnung mündet. Diese Tatsache kann für den Problemeinstieg genutzt werden. Zunächst kann den Teilnehmerinnen und Teilnehmern im Rahmen einer fragend-entwickelnden Methode nahegebracht werden, welche Dimension und Relevanz der Datenschutz für alle und insbesondere für kleine Kinder hat. Hierzu ist die Kenntnis praxisrelevanter Beispiele aus der Lebensrealität in der Kindertagespflege unabdingbar, um die weiterhin nötige Empathie zu erzeugen.
Indem konkrete Beispiele aus dem täglichen Leben (z. B. aus der Presse) herangezogen werden, kann den Teilnehmerinnen und Teilneh-

mern verständlich gemacht werden, dass gerade die Daten der „kleinen Leute“ in der Masse für Unternehmen interessant sind, da sie in der Masse ausgewertet und weiterverwendet werden können.
Indem gemeinsam weitere Beispiele (z. B. mittels Brainstormings) erarbeitet werden, soll den Teilnehmerinnen und Teilnehmern sichtbar und bewusstgemacht werden, wie das unsichtbare Abfließen des Datenstromes von ihnen selbst als Personen, aber auch durch sie über andere Personen – Tagespflegekind und Erziehungsberechtigte – abläuft.
Im Anschluss daran können die ersten grundlegenden Datenschutzgedanken und Prinzipien vermittelt und besprochen werden. Ziel ist, dass die Teilnehmerinnen und Teilnehmer der Grundqualifizierung erkennen, wie sinnvoll und notwendig ein umfangreicher Datenschutz ist.
Als notwendige **Kompetenz** müssen die Referierenden fachliche Kenntnisse über die Anfänge und Grundgedanken des Datenschutzes mitbringen. Sie sollten in der Lage sein, diese Grundgedanken auf die konkreten Bedürfnisse in der Kindertagespflege anzuwenden. In persönlicher Hinsicht sollten sie fähig sein, diese Grundgedanken durch praxisnahe allgemeine, aber auch fachbezogene Beispiele – beispielsweise aus Film oder Presse– mit Leben zu füllen. Eigene Kenntnislücken sollten dabei stetig reflektiert und geschlossen werden.
Besonders die Tatsache, dass selbst Referierende in so einem weiten und komplexen Thema nicht allwissend sein können, eröffnet ihnen die Möglichkeit, ein emotionales Band zu den angehenden Kindertagespflegepersonen aufzubauen. Auf diese Weise können sie ihnen die Angst davor nehmen, sich mit Datenschutz zu befassen und sie schrittweise dafür begeistern.
In diesem Zusammenhang ist jedoch auch eine gewisse Kenntnis davon nötig, wie die unternehmerischen Realität der anwesenden Kindertagespflegepersonen aussieht: Wer kaum Geld verdient, kann in Bezug auf technisch-organisatorische Maßnahmen schlechter aus dem Vollen schöpfen als Gutverdienende. Dies sollte mitberücksichtigt werden und bei der Erarbeitung von ersten Handlungsanweisungen und Maßnahmen in angemessener Weise einfließen.

2 Tätigkeitsbegleitende Grundqualifizierung

Ziel der Grundqualifizierung sollte es in **methodisch-didaktischer** Hinsicht sein, das Wissen über die datenschutzrechtlichen Vorgaben und die hieraus ableitbaren erforderlichen Maßnahmen bei den angehenden Kindertagespflegepersonen so zu vertiefen, dass diese befähigt werden, für ihren Praxisalltag Datenschutz erfolgreich einzusetzen. Sie sollen ausreichend und selbstständig medienkompetent werden.
Um das Problembewusstsein, aber auch Lösungsmöglichkeiten zu implementieren und fortzuentwickeln, könnten Referierende zunächst in einer offenen Frage-Antwort-Situation die digitale Lebensrealität der anwesenden Kindertagespflegepersonen abfragen. Die so erarbeiteten lebensnahen Anwendungsbeispiele können sie dann gewinnbringend in den weiteren Ablauf einbauen, denn durch die Besprechung konkreter Beispiele lassen sich die folgenden fachlichen Informationen im Allgemeinen besser verankern.
So kann beispielsweise abgefragt werden, wer Facebook oder WhatsApp nutzt, wie die Nutzung ausschaut, wie umfangreich sie ist, welche Erfahrungen die Teilnehmerinnen und Teilnehmer damit gemacht haben. Sodann könnte gefragt werden, wieviel Kenntnis über das Geschäftsmodell hinter diesen sozialen Medien vorhanden ist.
Als nächstes könnte an diesen Beispielen und gegebenenfalls unter Heranziehung aktueller Presseberichte erläutert werden, wo Daten überall landen können. In diesem Zusammenhang können die Teilnehmerinnen und Teilnehmer ermuntert werden, sich zukünftig eigenständig Gedanken zur Datennutzung von Anwendungen zu machen und auf eigene Faust nach genaueren Auskünften hierzu zu suchen, bevor sie neue Anwendungen nutzen.
In einem nächsten Schritt können die Referierenden unter Verwendung von Vorlagen das Aussehen und die nötigen Inhalte eines Datenschutzkonzeptes, von Verfahrens- und Löschverzeichnissen, Einwilligungserklärungen usw. erläutern.
Im Bereich der **Kompetenzen** sollten Referierende bereits in der Grundqualifikation Grundkenntnisse technischer Art aufweisen, damit sie erklären können, wie beispielsweise WhatsApp funktioniert, wie eine Website aufgebaut ist, welche Technik hinter einer E-Mail steckt und welche datenschutzrechtlichen Konsequenzen hieraus zu ziehen sind.
Sie sollten einige Beispiele gängiger technischer Sicherungsmaßnahmen kennen, welche dem jeweils geforderten Stand der Technik genügen. In datenschutzrechtlicher Hinsicht sollten sie über Kenntnisse der DSGVO und der Besonderheiten des jeweiligen Landesdatenschutzrechts verfügen. Weiterhin müssen ihnen die jeweiligen länderspezifischen Besonderheiten in der Kindertagespflege (z. B. Vorhandensein und Struktur der Großtagespflege) bekannt sein. Die einzelnen wichtigen Begriffe, Grundgedanken und erforderlichen Maßnahmen müssen in ausreichend detaillierter Form vorgestellt werden. Die Referierenden sollten beispielsweise anhand eines Musters das Aussehen und die wichtigsten Inhalte eines Datenschutzkonzepts, von Informationsblättern und den erforderlichen Verzeichnissen erklären können.
Insbesondere die Wertungen und Vorgaben der jeweiligen Landesdatenschutzbeauftragten sollten beständig in aktueller Form bekannt sein. Die Referierenden sollten in der Lage sein, für ihr Bundesland Anlaufstellen für weitergehende Fragen zu nennen. Kenntnisse über datenschutzrechtliche Besonderheiten in ihrem Bundesland für die Großtagespflege sowie bei kirchlichen Trägern sollten ebenfalls vorhanden sein. In Bezug auf die **Selbstkompetenz** ist in dieser Phase die Bereitschaft nötig, sich kontinuierlich weiterzubilden, gerade in Hinblick auf die technischen Erfordernisse. Zudem müssen die Neuerungen im Datenschutzrecht mitverfolgt werden.
Im Rahmen der Sozialkompetenz sollte die Referierenden die anwesenden Kindertagespflegepersonen befähigen können, problematische Verhaltensweisen (z. B. zwecklose, ausufernde Datenanhäufung), Instrumente oder Strukturen selbst zu erkennen. Sie sollten weiterhin fähig sein, die Kindertagespflegepersonen dabei zu unterstützen, eigene Datenschutzkonzepte und Verzeichnisse anhand von zur Verfügung gestellten Muster zu entwickeln und sie in Phasen der Mutlosigkeit zu motivieren.

3 Fortbildungsphase

Methodisch-didaktisch sollten Referierende in der Fortbildungsphase berufsbegleitend zur Betreuungstätigkeit Kindertagespflegepersonen weiter zur Selbstbefähigung anleiten. Mittels ausgewählter Beispiele – wie dem Besprechen eines konkreten Datenschutzkonzepts oder der Besprechung eines konkreten Problemfalles und möglicher Lösungswege (u. a. durch Brainstorming) – kann das flexible Anwenden der datenschutzrechtlichen Klaviatur eingeübt werden.
Ziel ist, dass die Teilnehmerinnen und Teilnehmer der Fortbildung am Ende genügend Wissen und vor allem Selbstvertrauen haben, um eigenständige datenschutzrechtliche Einschätzungen und Anpassungen an ihren eigenen Vorlagen vorzunehmen und hierauf basierend entsprechende Entscheidungen zu treffen. Insbesondere sollten sie befähigt werden, angemessene Handlungsinstrumente und -wege für den Fall von Datenschutzverletzungen oder für Problemfälle zu entwickeln.

Dies erfordert im Rahmen der Fachkompetenz ein vertieftes Wissen über die in der Praxis benutzten Kommunikations- und Speichermedien und darüber, wie sie datenschutzrechtlich korrekt einzuordnen sind. Da zu erwarten ist, dass detaillierte Fragen vor allem zum Datenschutzkonzept und zur Führung der Verzeichnisse gestellt werden, sollte hierzu ebenfalls eine vertiefte Kenntnis vorhanden sein. Sie kann gegebenenfalls geübt werden, indem selbst ein solches Verzeichnis erstellt wird.
Referierende sollten in der Lage sein, die Teilnehmerinnen und Teilnehmer dazu anzuleiten, eigenständig problematische Verhaltensweisen, Anwendungen und Medien zu erkennen, beispielsweise durch Workshops oder Rollenspiele.
Im Rahmen der Selbstkompetenz sollte schließlich die Bereitschaft vorhanden sein, in eigenen Fortbildungen oder mittels Fachlektüre nach weiteren pädagogischen Mitteln zur erfolgreichen Kompetenzvermittlung zu forschen.

IV

Mustervorlagen

Vorbemerkung: Diese Muster können als Diskussionsgrundlage verwendet werden, um eigene Konzepte und Verzeichnisse zu erstellen. Da Kindertagespflege in sehr unterschiedlichen Variationen ausgeübt wird, sind diese Mustervorlagen, welche Standardformulierungen enthalten, jedoch unbedingt an die eigene konkrete Betreuungssituation anzupassen und entsprechend zu ergänzen. Von einer unreflektierten Übernahme wird abgeraten. Textbausteine, die in jedem Fall individuell eingefügt werden müssen (wie z. B. der Name und die Anschrift einer Kindertagespflegeperson), sind kursiv gesetzt. Formulierungsvorschläge für Großtagespflegestellen finden sich in Klammern.

Kindertagespflegepersonen sollten bei Erstellung ihrer Formulare unbedingt auch die Vorlagen der für sie zuständigen Landesdatenschutzbeauftragten zu Rate ziehen. Im Rahmen ihres Rechts auf Beratung gem. § 43 Abs. 4 SGB VIII können sie zudem eine Beratung des öffentlichen Jugendhilfeträgers in Anspruch nehmen.

Muster 1: Datenschutzkonzept (einfach)

Hinweis: Diese Vorlage dient als Formulierungshilfe und orientiert sich an häufig vorkommenden Erfordernissen der Kindertagespflege. Die Inhalte sind nicht abschließend. Die Inhalte der Vorlage müssen geprüft und je nach konkretem Anwendungsfall ergänzt oder modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden. Diese Vorlage stellt keine rechtliche Beratung durch die Autorin oder das Deutsche Jugendinstitut e. V. dar. Für die Richtigkeit und Vollständigkeit wird keine Gewähr und keinerlei Haftung übernommen. Die rechtliche Bewertung dieser Vorlage obliegt allein den Verwenderinnen und Verwendern.

1. Verantwortliche/r

Name, Vorname der Kindertagespflegeperson/Name der Großtagespflege, Inhaber
Adresse
Kontaktdaten wie E-Mail, Telefonnummern, etc.

2. Ziel des Datensicherheitskonzeptes

➔ Kurze Beschreibung der Ziele und Rechtsgrundlagen:

Der Datenschutz dient unter Berücksichtigung vor allem der DSGVO und des BDSG dem Schutz der Privatsphäre von Personen und garantiert jedem ein Recht auf informationelle Selbstbestimmung sowie den Schutz vor missbräuchlicher Verwendung seiner Daten.
Dieses Konzept regelt und dokumentiert für die unternehmerische Tätigkeit der verantwortlichen Kindertagespflegeperson bzw. der Großtagespflegstelle den sicheren Umgang mit den personenbezogenen Daten der Tagespflegekinder und ihrer Erziehungsberechtigten und informiert unter Berücksichtigung der angewandten Speichersysteme über die eingesetzten Sicherungssysteme und Maßnahmen. Dieses Datenschutzkonzept dient darüber hinaus als Grundlage und zum Nachweis für datenschutzrechtliche Prüfungen.

3. Schutzbedarf verarbeiteter Daten und Stellenwert der Datensicherheit

Die verantwortliche Kindertagespflegeperson verarbeitet eine Vielzahl von Informationen und personenbezogene Daten von Tagespflegekindern und Erziehungsberechtigten, um ihren Aufgaben und Pflichten gegenüber den betreuten Tagespflegekindern, den Erziehungsberechtigten als Vertragspartnern, Dienstleistern wie Steuerberatern, öffentlichen Stellen wie dem öffentlichen Jugendhilfeträger und sonstigen Dritten nachzukommen. Die Sicherheit der Datenverarbeitung und der Schutz von personenbezogenen Daten haben daher einen besonderen Stellenwert. Viele wesentlichen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt.

Bei der Erfüllung ihrer Kernaufgabe verarbeitet die verantwortliche Kindertagespflegeperson [Großtagespflege]-Daten, die der Vertraulichkeit unterliegen und die daher in besonderem Maße vertraulich sind, beispielsweise Gesundheitsdaten oder Daten zur Entwicklung des Kindes.

Insgesamt unterstellt die verantwortliche Kindertagespflegeperson einen hohen Schutzbedarf bei den meisten der von ihr verarbeiteten personenbezogenen Daten und legt dies als Maßstab für die zu ergreifenden technischen und organisatorischen Maßnahmen zugrunde.

4. Organisation des Datenschutzes

Da die verantwortliche Kindertagespflegeperson allein tätig ist,

[Großtagespflegen: Da bei der Verantwortlichen der Großtagespflege regelmäßig weniger als zehn/künftig 20 Personen mit der dauerhaften Datenverarbeitung beschäftigt sind]

ist/sind sie gesetzlich nicht verpflichtet, einen Datenschutzbeauftragten zu benennen und hat/haben dies auch nicht auf freiwilliger Basis getan.

Außer der verantwortlichen Kindertagespflegeperson sind keine weiteren Personen, welche dauerhaft Daten verarbeiten, vorhanden.

[Variante z. B. bei Großtagespflegestellen:

Außer den folgenden zur Datenverarbeitung eingesetzten Personen

Name, Vorname
Position
Adresse
Kontaktdaten

sind keine weiteren Personen, welche dauerhaft Daten verarbeiten, vorhanden. Diese Personen werden einmal jährlich neu auf den Datenschutz verpflichtet und anlässlich der Verpflichtung belehrt.]

[Soweit ein Datenschutzbeauftragter beauftragt wurde:
Für die Belange des Datenschutzes und der Datensicherheit ist verantwortlich:

Name, Vorname
Position
Adresse
Kontaktdaten

Zu seinen Aufgaben gehört es insbesondere, Ansprechpartner zu sein in Fragen des Datenschutzes, die Überwachung der Einhaltung der geltenden Datenschutzvorschriften sicherzustellen, datenschutzrelevante Ereignisse zu untersuchen, Sensibilisierungs- und Schulungsmaßnahmen zu initiieren, Datensicherheitsmaßnahmen regelmäßig zu überprüfen und konkrete Verbesserungsmaßnahmen zu erarbeiten. Er ist befugt und angehalten, besonders in technischen Fragen fachkundige Unterstützung zu suchen.]

5. Rechtlicher Rahmen

Art. 32 DSGVO verlangt technische und organisatorische Sicherungsmaßnahmen (TOM), um die erhobenen Daten zu sichern. Der Stand der Technik ist unter angemessener Berücksichtigung der zumutbaren 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 zu berücksichtigen. Es ist insgesamt durch entsprechende geeignete technische und organisatorische Maßnahmen ein angemessenes Schutzniveau zu gewährleisten.

6. Periodische Überprüfung und Verbesserung der Maßnahmen

Die verantwortliche Kindertagespflegeperson überprüft, bewertet und evaluiert einmal jährlich innerhalb der ersten zwei Monate des Jahres die bisher eingesetzten technischen und organisatorischen Maßnahmen. Diese werden daraufhin untersucht, ob sie nach wie vor umsetzbar, angemessen und effektiv sind. Sie prüft bei dieser Gelegenheit auch, ob neue gesetzliche Regelungen in Kraft getreten oder neue technische Standards eingeführt worden sind, welche eine zeitnahe Anpassung der Maßnahmen erfordern. Durch die regelmäßige Revision wird sichergestellt, dass der technologische Wandel, das Auftreten neuer Risiken und Sicherheitslücken, neue gesetzliche Anforderungen zur Wahrung des Datenschutzes und der Datensicherheit auf Dauer und regelmäßig berücksichtigt werden.

7. Mitarbeitende [Anmerkung: bei Großtagespflegestellen mit abhängig Beschäftigten]

Gefährdungen entstehen oft aus Unkenntnis, mangelndem Problembewusstsein, Bequemlichkeit oder werden durch diese Faktoren verstärkt. Deshalb sorgt die verantwortliche Kindertagespflegeperson mit einschlägigen arbeitsrechtlichen Verpflichtungen im Arbeitsvertrag, durch Arbeitsanweisungen, jährliche Belehrungen und stichprobenartige Kontrollen der Einhaltung der Dienstregeln dafür, dass alle Mitarbeitenden über das erforderliche aktuelle Wissen in Bezug auf Datenschutz und Datensicherheit verfügen, dass sie ihre Verantwortung verinnerlichen und sie ihren Sicherungsverpflichtungen im erforderlichen Maß nachkommen.

8. Technische und organisatorische Maßnahmen
Die Sicherung der Daten erfolgt vor allem durch die folgenden Maßnahmen:

Variante Aktenordner:
- Die Daten werden ausschließlich in Papierform in Aktenordnern aufbewahrt. Eine elektronische Übermittlung findet nicht statt.
- Die Akten werden in einem verschließbaren brand- und wassersicheren Aktenschrank aufbewahrt.
- Der Aktenschrank ist nicht frei zugänglich und bleibt verschlossen.
- Die Akten werden unmittelbar nach Bearbeitung wieder in den Aktenschrank gelegt.
- Bei Bearbeitung der Akten werden diese nicht unbeaufsichtigt gelassen.
- Eine Übermittlung der Daten an z. B. Erziehungsberechtigte, öffentlichen Jugendhilfeträger oder Steuerberater (nur soweit zur Erstellung der ESt-Erklärung nötig) erfolgt ausschließlich in Briefform mit der Post.

Variante elektronische Speicherung
- Die Daten werden auf einem rein unternehmerisch verwendeten, zugangsgesicherten PC gespeichert und verarbeitet.
- Es existiert das folgende ebenfalls zugangsgesicherte Back-up-System: *Name des Systems.*
- Diese Hardware wird brand- und wassersicher gelagert in: *Benennung des Lagerortes.*
- Es wird eine aktuelle Software verwendet, für die regelmäßig Sicherheitsupdates veröffentlicht werden: *Name und Version der Software.*
- Sicherheitsupdates werden unverzüglich aufgespielt.
- Die Übertragung erfolgt ausschließlich durch die folgenden gesicherten (verschlüsselten) Übertragungswege: *Name des Übertragungsweges.*
- Die Übertragungswege werden durch den folgenden datenschutzkonformen Server betrieben: *Name des Servers.*
- Wenn möglich, werden personenbezogene Daten verschlüsselt und verschlüsselt übertragen (passwortgeschützte ZIP-Datei, Verschlüsselung der Übertragungswege, verschlüsselter USB-Stick).
- Die Speicherung von Daten unbekannter Herkunft findet nicht statt.
- Es ist die Installation folgender angemessener Datensicherungssysteme mit periodischem Update erfolgt: *Name der Firewall,* des *Virenschutzprogramms* und/oder des *Spamfilters,* etc.
- Die folgenden nicht benötigten Netzwerkdienste wurden deaktiviert, um einen unbefugten Fernzugriff zu verhindern: *Name der deaktivierten Dienste.*
- Zur Sicherung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung werden diese ausschließlich durch die verantwortliche Kindertagespflegeperson [Großtagespflegestellen: durch die oben genannten Personen] verarbeitet.
- Ein Zugang anderer Personen außer der unten genannten Vertretungsperson findet nicht statt.
- Das Passwort muss ausreichend komplex sein. Das Passwort wird unter Berücksichtigung der Empfehlungen des BSI erstellt.
- Es sind Rauchmelder installiert.

Vertretungsperson:

Name, Vorname
Anschrift
Kontaktdaten

Die Vertretungsperson wird jährlich auf den Datenschutz verpflichtet und belehrt. Die Vertretungsperson ist lediglich zum Lesen berechtigt.
[Großtagespflegen: Die Vertretungsperson hat die folgenden Bearbeitungs- und Leserechte: Aufzählung der einzelnen Rechte]

Als weitere technische und organisatorische Maßnahmen sind vorhanden:

Zugangskontrollen: Die Betreuungsräume sind nicht frei zugänglich.

Hier z. B. einfügen: *Beschreibung der Räume: Ort, Stockwerk, Schließanlage, Dokumentation der Schlüssel, die im Umlauf sind.*

Besucher und Erziehungsberechtigte werden persönlich in Empfang genommen. In den Aufenthalts-/Betreuungsräumen besteht kein Zugang zu Akten oder Daten.
Kontrolle zugangsberechtigter Dritter: Das beauftragte Reinigungsunternehmen/Reinigungspersonal wurde zur Vertraulichkeit verpflichtet und erwies sich in wiederholten Kontrollen als vertrauenswürdig.
Datenträger (z. B. CD-ROM, USB-Stick usw.) werden verschlossen aufbewahrt und sind stets **verschlüsselt.** Kopien werden nur bei Erforderlichkeit gefertigt und rückstandsfrei gelöscht oder vernichtet, wenn sie nicht mehr benötigt werden.
Ausgemusterte Datenträger oder Geräte werden unbrauchbar gemacht, indem sie physisch vernichtet werden. **Papiermüll** wird geschreddert. Die Vernichtung wird dokumentiert.

8. Auftragsverarbeiterkontrolle

Die folgenden externen Dienstleister werden herangezogen:
Gebäudereinigung: *Name Vorname Adresse Kontaktdaten*
IT-Wartungsunternehmen: *Name Vorname Adresse Kontaktdaten*
Server: *Name Vorname Adresse Kontaktdaten*
E-Mail-Anbieter: *Name Vorname Adresse Kontaktdaten*
Die Dienstleister wurden sorgfältig ausgewählt und vertraglich zur Einhaltung des Datenschutzes verpflichtet. Sie werden regelmäßig kontrolliert. Einzelweisungen werden dokumentiert.

9. Sonstige Besonderheiten und Maßnahmen

An dieser Stelle sind die Besonderheiten der konkreten Kindertagespflege anzuführen und anzugeben, welche besonderen Maßnahmen sich hieraus ergeben.

Ort, Datum *Verantwortliche Kindertagespflegeperson*

Aktualisierung

Die folgenden Aktualisierungen wurden vorgenommen:

Kurze Beschreibung der Aktualisierungen

Ort, Datum *Verantwortliche Kindertagespflegeperson*

Ein Beispiel für ein gelungenes, ausführliches Datenschutzkonzept kann auf der Homepage des Westfälischen Kinderdorf e.V. unter dem folgenden Link eingesehen werden:
https://www.wekido.de/dmwp-content/uploads/WEKIDO-Datenschutzkonzept.pdf
Es wird ausdrücklich darauf hingewiesen, dass eine unerlaubte Übernahme fremder Konzepte oder einzelner Passagen aus Konzepten anderer Unternehmen nicht zulässig ist.

Muster 2: Informationsblatt zur Erhebung von personenbezogenen Daten gem. Art. 13 DSGVO

Hinweis: Diese Vorlage dient als Formulierungshilfe und orientiert sich an häufig vorkommenden Erfordernissen der Kindertagespflege. Die Inhalte sind nicht abschließend. Die Inhalte der Vorlage müssen geprüft und je nach konkretem Anwendungsfall ergänzt oder modifiziert werden, um dem bei der jeweiligen Kindertagespflegeperson gegebenen Sachverhalt gerecht zu werden. Diese Vorlage stellt keine rechtliche Beratung durch die Autorin oder das Deutsche Jugendinstitut e. V. dar. Für die Richtigkeit und Vollständigkeit wird keine Gewähr und keinerlei Haftung übernommen. Die rechtliche Bewertung dieser Vorlage obliegt allein der Verwenderin oder dem Verwender.

Mit den folgenden Informationen soll Ihnen einen Überblick über die Verarbeitung Ihrer personenbezogenen Daten durch die Kindertagespflegestelle und Ihre daraus entstehenden Rechte gegeben werden. Welche Daten im Einzelnen verarbeitet und in welcher Weise genutzt werden, richtet sich maßgeblich nach den jeweils vereinbarten Betreuungsdienstleistungen.

Verarbeitungstätigkeit

Bezogen auf die Betreuung in der Kindertagespflegestelle finden die folgenden Verarbeitungstätigkeiten statt:

- Abschluss von Betreuungsverträgen
- Dokumentation der Betreuung
- Erstellung von Interessenten- und Wartelisten

1. Name und Kontaktdaten des Verantwortlichen

Verantwortliche Kindertagespflegeperson im Sinne der DSGVO ist:
Name, Vorname
Adresse
Kontaktdaten

2. Art der erhobenen personenbezogenen Daten

Es werden die folgenden personenbezogenen Daten verarbeitet, die im Rahmen der Geschäftsbeziehung von Ihnen erlangt werden:
Vor Vertragsabschluss

- Name, Vorname, Adresse und Verwandtschaftsbeziehung der Erziehungsberechtigten
- Name, Vorname, Adresse und betreuungsrelevante Informationen des zu betreuenden Kindes
- Beabsichtigte Betreuungsdauer, Betreuungsumfang, Betreuungszeiten

Vor Vertragsabschluss zusätzlich

- Geburtsdatum des zu betreuenden Kindes, Grund für die Fremdbetreuung
- Bankverbindung zur Abwicklung des Zahlungsverkehrs
- Gesundheitsdaten des zu betreuenden Kindes (Allergien, Unverträglichkeiten, betreuungsrelevante Erkrankungen oder Krankheitsneigungen)
- Weitere personenbezogene und betreuungsrelevante Daten wie allgemeine Vorlieben und Abneigungen, Gewohnheiten des Kindes, Erziehungsgrundsätze der Erziehungsberechtigten, etc.

Im Laufe der Betreuung

- Anwesenheiten des Kindes in der Betreuung
- Bring- und Abholberechtigungen sowie einzelne Bring- und Abholvorgänge
- Informationen zum Entwicklungsverlauf
- Inhalte von Eltern- und Erziehungsgesprächen
- Information zum Betreuungsalltag/Portfolio
- Foto- und Filmaufnahmen zur Dokumentation von Entwicklungsfortschritten
- Wichtige Tatsachen i.S.d. § 43 SGB VIII, gewichtige Anhaltspunkte i.S.d. § 8a SGB VIII

3. Zweck und Rechtsgrundlage der Datenverarbeitung
Die Verarbeitung der personenbezogenen Daten steht im Einklang mit den Bestimmungen der europäischen Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG):

3.1. Zur Erfüllung von vertraglichen Pflichten (Art. 6 Abs. 1 Buchst. b DSGVO)
Die Verarbeitung von Daten erfolgt zur Durchführung unseres Vertrages bzw. zur Durchführung vorvertraglicher Maßnahmen.

3.2. Aufgrund gesetzlicher Vorgaben (Art. 6 Abs. 1 Buchst. c DSGVO) und zum Schutz lebenswichtiger Interessen (Art. 6 Abs. 1 Buchst. d DSGVO) sowie zur Wahrung berechtigter Interessen (Art. 6 Abs. 1 Buchst. f DSGVO).
Wir unterliegen verschiedenen gesetzlichen Verpflichtungen, die eine Datenverarbeitung nach sich ziehen. Hierzu zählen z. B.:

- SGB VIII, *[einfügen: Landesrecht wie z. B. BayKiBiG]*
- Steuergesetze
- die Erfüllung von Anfragen und Anforderungen von Aufsichtsbehörden
- die Erfüllung steuerrechtlicher Kontroll- und Meldepflichten

Darüber hinaus kann die Offenlegung personenbezogener Daten im Rahmen von behördlichen/gerichtlichen Maßnahmen zu Zwecken der Beweiserhebung, Strafverfolgung oder Durchsetzung zivilrechtlicher Ansprüche erforderlich werden.

4. Empfänger der personenbezogenen Daten
Zur Erfüllung unserer gesetzlichen Aufgaben übermitteln wir die Daten an folgende Stellen

- Amt für Kinder, Jugend und Familie *[einfügen; Name, Adresse, Kontaktdaten]*
- Öffentlich geförderte Ersatzbetreuungsperson *[einfügen; Name, Adresse, Kontaktdaten]*
- Trägerverein *[einfügen; Name, Adresse, Kontaktdaten]*
- *Im Einzelfall: Wohnortgemeinde [dann einfügen; Name, Adresse, Kontaktdaten]*

Im Rahmen von Auftragsverarbeitungen
Zur Durchführung der selbstorganisierten, nicht geförderten Ersatzbetreuungsperson als zusätzlichen Service werden relevante Daten weitergegeben an: *[einfügen; Name, Adresse, Kontaktdaten]*

Für die Finanzbuchhaltung relevante Daten werden an die folgenden Dienstleister weitergegeben:

- Finanzbuchhaltung *[einfügen; Name, Adresse, Kontaktdaten]*
- Steuerberatung *[einfügen; Name, Adresse, Kontaktdaten]*

Sämtliche Dienstleister sind vertraglich gebunden und insbesondere dazu verpflichtet, Ihre Daten vertraulich zu behandeln.

Sonstige Dritte
Eine Weitergabe von Daten an Empfänger außerhalb der Kindertagespflege erfolgt nur unter Beachtung der anzuwendenden Vorschriften zum Datenschutz. Empfänger personenbezogener Daten können z. B. sein: Öffentliche Stellen und Institutionen (z. B. Finanz- oder Strafverfolgungsbehörden, Gerichte) bei Vorliegen einer gesetzlichen oder behördlichen Verpflichtung; Steuerberater oder Wirtschafts-, Lohnsteuer- und Betriebsprüfer (gesetzlicher Prüfungsauftrag).

5. Übermittlung von personenbezogenen Daten an ein Drittland
Eine Übermittlung von Daten an ein Drittland findet nicht statt.

6. Vorgesehene Fristen für die Löschung der Daten
Wir verarbeiten und speichern Ihre personenbezogenen Daten, solange dies für die Erfüllung unserer vertraglichen und gesetzlichen Pflichten erforderlich ist. Sind die Daten für die Erfüllung vertraglicher oder gesetzlicher Pflichten nicht mehr erforderlich, werden diese regelmäßig gelöscht. Dies erfolgt nach spätestens *[Vorschlag: zehn]* Jahren.

7. Betroffenenrechte

Sie haben das Recht auf Auskunft nach Artikel 15 DSGVO, das Recht auf Berichtigung nach Artikel 16 DSGVO, das Recht auf Löschung nach Artikel 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Artikel 18 DSGVO, das Recht auf Widerspruch aus Artikel 21 DSGVO sowie das Recht auf Datenübertragbarkeit aus Artikel 20 DSGVO.
Beim Auskunftsrecht und beim Löschungsrecht gelten ggf. Einschränkungen nach §§ 34 und 35 BDSG.
Darüber hinaus besteht ein Beschwerderecht bei einer zuständigen Datenschutzaufsichtsbehörde (Artikel 77 DSGVO i.V.m. § 19 BDSG). Die für uns zuständige Aufsichtsbehörde ist:
Beispiel Bayern:
Bayerisches Landesamt für Datenschutzaufsicht
Promenade 18, 91522 Ansbach

8. Pflicht zur Bereitstellung der Daten

Im Rahmen des Vertragsverhältnisses müssen Sie diejenigen personenbezogenen Daten bereitstellen, die für die Aufnahme, Durchführung und Beendigung des Betreuungsverhältnisses und zur Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung eine gesetzliche Verpflichtung besteht. Ohne diese Daten ist eine Tagesbetreuung in der Regel nicht durchführbar, sodass der Vertrag mit Ihnen nicht geschlossen oder ausgeführt werden kann.

Ort, Datum *Name, Vorname Kindertagespflegeperson*

Diese Vorlage bezieht sich ausschließlich auf die Datenverarbeitungen zur Vertragsdurchführung und Förderung. Weitere Datenverarbeitungen, die auf Grundlage weiterer Einwilligungen stattfinden (z. B. Anfertigungen von Fotografien zum privaten Gebrauch durch die Eltern oder zu ihrer Information über den Betreuungsalltag), werden von dieser Vorlage nicht abgedeckt. Die Vorlage ist in einem derartigen Fall entsprechend den Anforderungen des Einzelfalles anzupassen.

Muster 3: Vertragsklauseln: Datenschutz, Einwilligung, Fotografien

Hinweis: Diese Vorlage dient als Formulierungshilfe und orientiert sich an häufig vorkommenden Erfordernissen der Kindertagespflege. Die Inhalte sind nicht abschließend. Die Inhalte der Vorlage müssen geprüft und je nach konkretem Anwendungsfall ergänzt oder modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden. Diese Vorlage stellt keine rechtliche Beratung durch die Autorin oder das Deutsche Jugendinstitut e. V. dar. Für die Richtigkeit und Vollständigkeit wird keine Gewähr und keinerlei Haftung übernommen. Die rechtliche Bewertung dieser Vorlage obliegt allein den Verwenderinnen und Verwendern.

§ XX[2] Informationsaustausch, Vertraulichkeit

(1) Die Vertragsparteien *[Anmerkung: Dies sind i. d. R. die Kindertagespflegeperson/Großtagespflege und die Erziehungsberechtigten]* arbeiten zum Wohle des Tagespflegekindes vertrauensvoll zusammen und verpflichten sich zum regelmäßigen Austausch über Entwicklung, Erziehung und Erlebnisse des Tagespflegekindes. Ereignisse, die die Kindertagespflege oder die Entwicklung des Tagespflegekindes beeinflussen können, müssen dem jeweils anderen Vertragspartner berichtet werden.

(2) Die Kindertagespflegeperson *[Großtagespflege]* ist verpflichtet, sowohl während des Betreuungsverhältnisses als auch nach dessen Beendigung Dritten gegenüber (z. B. weiteren Familienangehörigen, Freunden, Bekannten, Eltern anderer betreuter Kinder) Stillschweigen über Informationen über das Tagespflegekind oder seine Familie zu wahren. Die Erziehungsberechtigten sind verpflichtet, sowohl während des Betreuungsverhältnisses als auch nach dessen Beendigung Dritten gegenüber über Belange, die sie während, anlässlich, vor oder nach der Betreuung über die Kindertagespflegeperson *[Großtagespflege]* erfahren haben, ebenfalls Stillschweigen zu bewahren.

(3) In Bezug auf wichtige Tatsachen i.S.d. § 43 SGB VIII oder gewichtige Anhaltspunkte i.S.d. § 8a SGB VIII gilt obenstehende Vertraulichkeitsverpflichtung der Kindertagespflegeperson *[Großtagespflege]* nicht gegenüber dem zuständigen öffentlichen Jugendhilfeträger.

§ XX Datenschutz

(1) Die Kindertagespflegeperson *[Großtagespflege]* verpflichtet sich, die Betreuung so zu gestalten, dass sie den datenschutzrechtlichen Vorgaben entspricht. Sie wird technische und organisatorische Maßnahmen treffen, um die Daten der Erziehungsberechtigten und des Tagespflegekindes angemessen sichern. Die Erziehungsberechtigten verpflichten sich, die Kindertagespflegeperson *[Großtagespflege]* unverzüglich über fehlerhafte Daten oder Änderungen zu informieren.

(2) Die Löschung der zu den Erziehungsberechtigten und dem zu betreuenden Tagespflegekind erhobenen Daten erfolgt aus steuerrechtlichen Gründen nach Ablauf von *zehn* Jahren, gerechnet ab 31.12. desjenigen Jahres, in dem das Vertragsverhältnis beendet wurde.

(3) Die Erziehungsberechtigten erklären, dass sie das im Anhang zu diesem Vertrag vorhandene Datenschutzinformationsblatt *vor* Unterzeichnung des Vertrages gelesen und zur Kenntnis genommen haben. Auf die dortigen Auskünfte und Hinweise wird verwiesen.

2 Nummerierung wird entsprechend Einordnung in den Betreuungsvertrag vorgenommen

§ XX Einwilligung in die Datenerhebung, Art. 6 Abs. 1a DSGVO

(1) Unbeschadet der Erlaubnistatbestände nach Art. 6 Abs. 1 b – f DSGVO willigen die Erziehungsberechtigten gem. Art. 6 Abs. 1a DSGVO hiermit in die Datenverarbeitung durch die Kindertagespflegeperson *[Großtagespflege]* im folgenden Umfang ein *(Beispiele – bitte anpassen bzw. ergänzen!):*

- Name, Vorname *[Erziehungsberechtigte und Tagespflegekind],*
- Adresse,
- Telefonnummern,
- E-Mail-Adressen,
- Geburtsdatum des Kindes,
- Angaben zur Sorgeberechtigung,
- Grund des Betreuungsbedarfes, Beginn und Umfang des Betreuungsbedarfes
- Kontoverbindungsdaten.

Diese Daten dürfen an die folgenden Behörden und Einrichtungen weitergeleitet werden:

- an den zuständigen Träger der öffentlichen Kinder- und Jugendhilfe zur Erfüllung eines Vertrages und zur Erfüllung einer rechtlichen Verpflichtung,
- an das Finanzamt zur Erfüllung rechtlicher Verpflichtungen,
- im Einzelfall an Sozialversicherungsträger und Gerichte zur Wahrung berechtigter Interessen,

sowie an Dritte und Auftragsverarbeiter wie

- Steuerberater zur Erfüllung einer rechtlichen Verpflichtung,
- Rechtsanwälten zur Wahrung berechtigter Interessen im Einzelfall,
- Trägervereine zur Erfüllung einer rechtlichen Verpflichtung und
- Kreditinstitute zur Erfüllung eines Vertrages.

(2) Vorstehende Einwilligung kann von den Erziehungsberechtigten jederzeit mit Wirkung für die Zukunft widerrufen werden. Daten, die nach Widerruf nicht auf der Grundlage eines der Erlaubnistatbestände nach Art. 6 Abs. 1 b–f DSGVO erhoben werden dürfen, werden ab diesem Zeitpunkt nicht mehr verarbeitet.

§ XX Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten gem. Art. 9 Abs. 2a DSGVO

(1) Unbeschadet der Erlaubnistatbestände nach Art. 9 Abs. 2 b, c, f, g, h DSGVO i.V.m. § 43 Abs. 3 S. 6 und § 8a SGB VIII willigen die Erziehungsberechtigten gem. Art. 9 Abs. 2 a DSGVO hiermit in die Verarbeitung besonderer Kategorien personenbezogener Daten wie Gesundheitsdaten, Daten über die Entwicklung des Kindes, wichtige Tatsachen oder gewichtige Anhaltspunkte durch die Tagespflegeperson *[Großtagespflege]* im folgenden Umfang ein *(Beispiele!):*

- Migrationshintergrund;
- Gesundheitszustand, insbesondere betreuungserhebliche Erkrankungen und Krankheitsneigungen (z. B. Neigung zu Fieberkrämpfen), Allergien, Nahrungsmittelunverträglichkeiten, Entwicklungsstand und -verzögerungen, Entwicklungsverläufe;
- im Einzelfall wichtige Ereignisse wie Unfälle des Kindes, Verletzungen des Kindes, Allgemeinzustand des Kindes, Größe, Gewicht;
- im Einzelfall Hintergrundinformationen wie z. B. Scheidung/Trennung der Erziehungsberechtigten.

(2) Diese Daten dürfen an die folgenden Behörden und Einrichtungen weitergeleitet werden:

- an den zuständigen Träger der öffentlichen Kinder- und Jugendhilfe oder an Trägervereine zur Erfüllung einer rechtlichen Verpflichtung aus den §§ 43, 8a SGB VIII;
- im Einzelfall an Gerichte und Rechtsanwälte zur Wahrung berechtigter Interessen.

(3) Vorstehende Einwilligung kann von den Erziehungsberechtigten jederzeit mit Wirkung für die Zukunft widerrufen werden. Daten, die nach Widerruf nicht auf der Grundlage eines der Erlaubnistatbestände nach Art. 9 Abs. 2 b, c, f, g, h DSGVO i.V.m. § 43 Abs. 3 S. 6 und § 8a SGB VIII erhoben werden dürfen, werden ab diesem Zeitpunkt nicht mehr verarbeitet.

§ XX Foto- und Filmerlaubnis

(1) Es darf kindbezogenes Foto- und Filmmaterial von der Kindertagespflegeperson [Großtagespflege] erstellt werden.

(2) Dieses Bild- und Filmmaterial darf *(Beispiele!):*
- auf Bilderleisten innerhalb der Räumlichkeiten ausgehängt,
- für die Fotoalben, Erstellung von Ich-Büchern und Portfolioarbeiten verwendet und
- bei internen Veranstaltungen gezeigt werden. (Nichtzutreffendes bitte durchstreichen)

(3) Eine Verwendung von Bild- und Filmmaterial für Werbemaßnahmen, Pressemitteilungen und sonstige Medienauftritte findet [nicht] statt/findet wie folgt statt:
- ……
- ……
- ……

und bedarf im Einzelfall der ausdrücklichen Zustimmung der Erziehungsberechtigten.

(4) Die Kindertagespflegeperson [Großtagespflege] übernimmt keine Haftung dafür, dass derartiges Bildmaterial auf anderen Wegen in soziale Medien gerät (z. B. unbefugtes Abfotografieren von Bildern durch andere Erziehungsberechtigte und posten/senden in Portalen wie z. B. Facebook, Twitter und WhatsApp). Soweit sie hiervon Kenntnis erlangt, informiert sie die Betroffenen.

Merke:
Je pauschaler und umfassender eine Einwilligung zu Foto- und Filmaufnahmen gestaltet ist, desto eher besteht die Gefahr einer grundsätzlichen Verweigerung der Einwilligung. Es empfiehlt sich, die Möglichkeit zur Verweigerung einzelner Zwecke z. B. mittels Durchstreichen anzubieten.

Muster 4: Vertrag Auftragsverarbeiter

Hinweis: Diese Vorlage dient als Formulierungshilfe und orientiert sich an häufig vorkommenden Erfordernissen der Kindertagespflege. Die Inhalte sind nicht abschließend. Die Inhalte der Vorlage müssen geprüft und je nach konkretem Anwendungsfall ergänzt oder modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden. Diese Vorlage stellt keine rechtliche Beratung durch die Autorin oder das Deutsche Jugendinstitut e. V. dar. Für die Richtigkeit und Vollständigkeit wird keine Gewähr und keinerlei Haftung übernommen. Die rechtliche Bewertung dieser Vorlage obliegt allein den Verwenderinnen und Verwendern.

Die
FIRMA, NAME, KONTAKTDATEN
[Beispiel: Reinigungsfirma „Die kleinen Saubermänner“
Mustermannstraße 5
12345 Musterstadt]

im Folgenden: Auftragsverarbeiter
verpflichtet sich hiermit wie folgt:

I. Dienstleistung/Tätigkeit

Die folgende Dienstleistung/Tätigkeit wird ausgeübt:

Beschreibung der Tätigkeit und der Betreuungsräume, in denen diese ausgeübt werden soll
[ggf. Näheres hierzu wie Vergütung, Dauer, Inhalt, wechselseitige Verpflichtungen gesondert vereinbaren]

II. Datenverarbeitung

Zur Durchführung der vereinbarten Dienstleistung/Tätigkeit werden die folgenden Daten durch den Auftragsverarbeiter verarbeitet:

(Beschreibung der Daten, Kategorie, Zweck, Weiterleitungsart, Speicherungsart)

Anlässlich der Tätigkeit kann der Auftragsverarbeiter Kenntnis der folgenden Daten erlangen:

(Beschreibung der Daten, Zweck, Speicherungsart)

III. TOM

Folgende technische und organisatorische Maßnahmen (TOM) zur Gewährleistung der Sicherheit, Vertraulichkeit und Integrität der Daten werden beim Auftragsverarbeiter durchgeführt:

Benennung der einzelnen erforderlichen Maßnahmen wie Absperren von Schränken, in denen Unterlagen aufbewahrt werden, Firewall, Virenschutz, Verschlüsselung, Passwörter, etc.

Soweit Zertifizierungen zum Datenschutz und zur IT-Sicherheit vorliegen, sind diese nachzuweisen.

IV. Datenschutzverpflichtung

Der Auftragsverarbeiter erlangt im Rahmen seiner oben genannten Beauftragung sowie der Bereitstellung der Dienstleistung/Tätigkeit Kenntnis von den Vorgängen der Kindertagesbetreuung und kann Kenntnis von personenbezogenen Daten und Informationen erlangen.

Der Auftragsverarbeiter verpflichtet sich hiermit zur Einhaltung der jeweils geltenden datenschutzrechtlichen Vorschriften sowie zur Wahrung der Sicherheit, Vertraulichkeit und Integrität der betroffenen Daten.

V. Verpflichtung zur zweckgebundenen Datenverwendung, Löschung

Der Auftragsverarbeiter ist verpflichtet, sich nur insoweit Kenntnisse von personenbezogenen Daten von Tagespflegekindern und Erziehungsberechtigten zu verschaffen, als dies zur Erfül-

lung seines Auftrages/Vertrags mit der Kindertagespflegeperson [Großtagespflege] unbedingt erforderlich ist.

Er verpflichtet sich, die Daten nur zweckentsprechend zu verwenden, sie nicht bzw. nur unter Einhaltung der hier vereinbarten Regelungen sowie ggf. nach vorheriger Zustimmung weiterzuleiten und spätestens *zehn* Jahre nach Beendigung der Dienstleistung/Tätigkeit zu löschen.

VI. Verschwiegenheitsverpflichtung, Geheimhaltungsverpflichtung

Der Auftragsverarbeiter verpflichtet sich gegenüber der Kindertagespflegeperson [Großtagespflege] zur Verschwiegenheit über alle Vorgänge innerhalb und außerhalb der Betreuungsstätte, auch nach einer etwaigen Beendigung der Zusammenarbeit sowie der einzelnen Kauf-, Werk-, Miet-, Dienstleistungsverträge.

Dies gilt ganz besonders im Hinblick auf Informationen über betreute Tagespflegekinder und deren Erziehungsberechtigte sowie für alle besonderen personenbezogenen Daten (Gesundheitsdaten etc.).

Es ist untersagt, Unterlagen, Schriftstücke, Abschriften, Ablichtungen, Daten und/oder sonstige Informationsträger unbefugten Personen innerhalb oder außerhalb der Kindertagesbetreuung bzw. Betriebsstelle des Auftragsverarbeiters zugänglich zu machen. Diese Geheimhaltungspflicht gilt auch über das Ende des Auftragsverhältnisses hinaus. Hiervon ausgenommen ist die Weiterleitung an Gerichte und Behörden im Rahmen einer gesetzlichen Verpflichtung.

VII. Hilfspersonal

Der Auftragsverarbeiter ist befugt, weitere Personen zur Vertragserfüllung heranzuziehen. Bei Hinzuziehung von Dritten als Subunternehmer ist dies vor Beauftragung mitzuteilen und bedarf der Zustimmung.

Der Auftragsverarbeiter verpflichtet sich, diese Personen/Dritte nach den vorgenannten Grundsätzen in Textform zu belehren und zu verpflichten. Die hinzugezogenen Personen/Dritten sind zu benennen und die Belehrung und Verpflichtung ist auf Anforderung nachzuweisen.

Ort, Datum *Unterschrift/Stempel Auftragsverarbeiter*

Ort, Datum *Unterschrift Kindertagespflegeperson*

Muster 5: Verzeichnis der Verarbeitungstätigkeiten

Hinweis: Diese Vorlage dient als Formulierungshilfe und orientiert sich an häufig vorkommenden Erfordernissen der Kindertagespflege. Die Inhalte sind nicht abschließend. Die Inhalte der Vorlage müssen geprüft und je nach konkretem Anwendungsfall ergänzt oder modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden. Diese Vorlage stellt keine rechtliche Beratung durch die Autorin oder das Deutsche Jugendinstitut e. V. dar. Für die Richtigkeit und Vollständigkeit wird keine Gewähr und keinerlei Haftung übernommen. Die rechtliche Bewertung dieser Vorlage obliegt allein den Verwenderinnen und Verwendern.

Angaben zum Verantwortlichen	
Verantwortliche Stelle (gemäß Art. 4 Nr. 7 DSGVO)	*(Name, Vorname, Anschrift, Kontaktdaten der Kindertagespflegeperson oder der/des Inhaberinnen/Inhaber der Großtagespflege*
Ggf. gemeinsamer Verantwortlicher	*(Name, Vorname, Anschrift, Kontaktdaten)*
Gesetzlicher Vertreter	*Name, Vorname, Anschrift, Kontaktdaten z. B. des Vereinsvorsitzenden oder Geschäftsführers des Trägers einer Großtagespflege*
Datenschutzbeauftragter	*Name, Kontaktdaten, nur soweit vorhanden*

Grundsätzliche Angaben zur Verarbeitung	
Bezeichnung der Verarbeitungstätigkeit:	*Beispiele:* • *Anlage Vertragsbeziehung durch Speicherung der Vertragsdaten* • *E-Mailverarbeitung* • *Allgemeine Verwaltung im Betreuungsalltag* • *Dokumentation von Erkrankungen, Entwicklungsfortschritten etc.* • *Abrechnung der Bescheide /Belegbögen / Finanzverwaltung*
Verantwortlicher Ansprechpartner (Telefonnummer und E-Mail-Adresse):	*Da die Kindertagespflegeperson i. d. R. meistens selbst handelt, kann sie hier wieder voreingetragen werden.*
Bei gemeinsamer Verantwortlichkeit: Name und Kontaktdaten des/der weiteren Verantwortlichen:	*s. o. (relevant z. B. bei Großtagespflege)*
Art der Verarbeitung / Name der Software: (optionale Angabe)	*Eigenentwickelte Software, Standardsoftware, Auftragsdatenverarbeitung, Excel* *Oder: Papierform, Aktenordner?*
Ort der Verarbeitung:	*Wo werden die Daten verarbeitet und gespeichert?* *Z. B. im Haus, in einem Rechenzentrum in Deutschland oder Ausland. Server? Cloud?*

Allgemeine datenschutzrechtliche Anforderungen DSGVO	
Rechtmäßigkeit der Verarbeitung, Art. 6 DSGVO	*Hinweis: im Folgenden handelt es sich nur um Beispiele:* • *Einwilligung (Art. 6 Abs. 1 lit. a, Art. 7)* • *Einwilligung für ein Kind (Art. 6 Abs. 1 lit. a, Art. 8 Abs. 1 S. 2)* • *Vertrag oder Vertragsanbahnung (Art. 6 Abs. 1 lit. b)* • *Wahrung berechtigter Interessen des Verantwortlichen/des Dritten (Art. 6 Abs. 1 lit. f)* • *Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs.)*

Erhebung der Daten	
Kreis der betroffenen Personengruppen	*Erziehungsberechtigte, Tagespflegekinder, Interessenten, Ersatzbetreuungspersonen, etc.*
Art der gespeicherten Daten bzw. Datenkategorien:	*Beispiele:* • *Name/Vorname/Titel* • *Adressdaten* • *Kontaktdaten* • *Bankverbindungsdaten* • *Geburtsdatum* • *Vorlieben/Abneigungen* • *Impfstatus (Masern!)* • *Allergien, Krankheiten, Entwicklungsstand* • *Qualifikationsdaten/Leistungsbeurteilung (Solvenz)* • *Sozialversicherungsdaten, z. B. Kranken-versicherungsnummer* • *Vertragsdaten wie z. B. Beginn, Dauer* • *Zahlungsdaten* • *Zeiterfassungsdaten (Buchungszeiten)*
Unmittelbarkeit der Datenerhebung/Herkunft der Daten	*Woher stammen die Daten? Von Betroffenen selbst oder von einem Dritten?*

Empfänger, denen die Daten mitgeteilt werden können	
Interne Empfänger (innerhalb der verantwortlichen Stelle)	*Empfänger innerhalb des Verantwortlichen, z. B. der eigene IT-ler, der/die eigene „Sekretär/in", die eigene Buchhaltungsstelle*
Externe Empfänger und Dritte (jeder andere Empfänger, soweit nicht Auftragsverarbeiter)	*Dritte, die nicht Auftragsverarbeiter sind, z. B. Finanzamt, Steuerberater, Anwalt, Versicherungen, Jugendamt, Trägerverein, geförderte Ersatzbetreuungsperson usw.*

Zugriffsberechtigte Personen	
Zugriffsberechtigte Personen	*Benennung der berechtigten Gruppen z. B. Buchhaltung, Auftragsverarbeiter*
Nachweis	*Skizzierung des Berechtigungsverfahrens: z. B. Berechtigungskonzept, Vertrag*

Auftragsverarbeitung als Auftraggeber (optionale Angabe)	
Auftragsverarbeiter	*Dieser Abschnitt ist auszufüllen, falls von dem Verantwortlichen bei der Verarbeitungstätigkeit Auftragsverarbeiter bzw. Sub-Auftragsverarbeiter eingesetzt werden (Art. 28 DSGVO).* *Bei mehr als einem Auftragsverarbeiter bzw. Sub-Auftragsverarbeiter ist jeweils eine neue Tabelle anzulegen, welche nummerisch fortlaufend zu kennzeichnen ist*
Schriftlicher datenschutzkonformer Vertrag	*Ist ein Auftragsverarbeitungsvertrag vorhanden?*
Geeignetheit des Auftragsverarbeiters	*Hier sollte das Ergebnis der Erstkontrolle angeführt werden.*
Standort der Verarbeitung	*In der EU oder im Drittland (d. h. außerhalb der EU/des EWR)? An die Übertragungswege denken!*

Regelfristen für die Löschung der Daten	
Speicherdauer	*Anzugeben sind hier die konkreten Aufbewahrungs- und Löschfristen, die in Verarbeitungstätigkeiten implementiert sind. Empfehlung 10 Jahre ab Ende des Jahres, in dem das Vertragsverhältnis endete* *Soweit diese in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf das vorhandene (und in der Verarbeitungstätigkeit umgesetzte) Löschkonzept aus.*
Nachweis	*Dokument in dem der Nachweis zur Löschung geschaffen wird, z. B. Löschkonzept*

Beurteilung der Angemessenheit techn. und org. Maßnahmen (TOM)	
Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g, Art. 32 Abs. 1 DSGVO)	*Hier kann stichpunktartig auf die TOM im Datenschutzkonzept verwiesen werden.*
Verbleibendes Risiko unter Berücksichtigung der eingesetzten TOM	*Beispiel: gering*

Prüfung durch den Verantwortlichen	
Prüfung	*Erfolgt/nicht erfolgt, Datum (Regelmäßig wiederholen)*
Datum, Unterschrift	

Muster 6: Auskunft über die Verwendung von Daten

Hinweis: Diese Vorlage dient als Formulierungshilfe und orientiert sich an häufig vorkommenden Erfordernissen der Kindertagespflege. Die Inhalte sind nicht abschließend. Die Inhalte der Vorlage müssen geprüft und je nach konkretem Anwendungsfall ergänzt oder modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden. Diese Vorlage stellt keine rechtliche Beratung durch die Autorin oder das Deutsche Jugendinstitut e. V. dar. Für die Richtigkeit und Vollständigkeit wird keine Gewähr und keinerlei Haftung übernommen. Die rechtliche Bewertung dieser Vorlage obliegt allein den Verwenderinnen und Verwendern.

Sehr geehrte Frau Müller, sehr geehrter Herr Müller,

hiermit beantworten wir Ihre Datenschutzauskunftsanfrage wie folgt:

Im Rahmen der Betreuung von Tagespflegekinder erheben wir grundsätzlich nur diejenigen Daten, welche zur Durchführung der Betreuung erforderlich sind, bzw. die wir auf Veranlassung des zuständigen Trägers der öffentlichen Jugendhilfe zu erheben haben. Diese sind vorliegend:

Daten zu Ihrer Person als Erziehungsberechtigte und Vertragspartner und zu Ihrem Kind, das in Kindertagespflege betreut werden soll bzw. betreut wird. Zur korrekten Durchführung der Betreuung müssen auch persönliche Daten erhoben werden, beispielsweise Daten zum Gesundheitszustand Ihres Kindes. Diese Daten werden entsprechend der datenschutzrechtlichen Vorgaben behandelt. ***Beispiel einer weiteren Verwendung:*** *Zusätzlich haben Sie sich aus eigenen Wunsch an der elektronischen Elterngruppe in der Anwendung Signal beteiligt.*

Mit den nachfolgenden Informationen können Sie sich einen Überblick verschaffen, welche Daten in Ihrem Falle erhoben wurden und wie wir damit verfahren haben. Bei Fragen können Sie sich jederzeit gerne an uns wenden.

Für den Datenschutz verantwortlich ist:
Frau/Herr [*Name, Vorname,* Kindertagespflegeperson]

Art der erhobenen Daten:

- Erziehungsberechtigte:
  - Name, Vorname, Anschrift
    (Maria Müller, Mario Müller, Müllerstraße 1 23456 Müllerstadt)
  - Kontaktinformationen
    (Telefonnummern: 012345 765433)
    E-Mail-Adressen: maria.müller[at]müller.info
  - Vertragsunterlagen:
    Betreuungsvereinbarung vom *1.1.2000;* Abtretungs- und Verzichtserklärung vom *1.1.2000,* Einverständniserklärung Datenerhebung vom *1.1.2000,* Arbeitszeitennachweise Müller Maria und Mario vom *1.1.2000;* Förderbescheid vom *1.1.2000*, Datenerhebungsbogen, Kündigungsschreiben vom *1.1.2000.*
  - Sorgeberechtigungsstand: gemeinsame Sorge
  - Zuständiges Jugendamt:
    Stadtjugendamt Müllerstadt, Fachstelle: Kindertagespflege,
    Maierstraße 3, 23456 Müllerstadt, Tel. 0123–456789

- Kind:
  - Name, Vorname, Geburtsdatum, Anschrift:
    (Marius Müller, geb. 1.1.2000),
    wohnhaft in Müllerstraße 1, 23456 Müllerstadt)
  - Besondere, betreuungsrelevante Gesundheitsinformationen:
    Erdnussallergie
  - Dritte:
    Kinderarzt Müllermann, Hansenstraße 1, 23456 Müllerstadt

Rechtsgrundlage:
- Die Rechtsgrundlage ergibt sich aus Art. 6. Abs. 1 Buchst. b DSGVO (Erfüllung eines Vertrags) in Verbindung mit BDSG und *[Landesdatenschutzgesetz]*
- Durchführung der gesetzlichen Mitteilungsverpflichtungen nach § 43 SGB VIII u. a.

Zwecke der Datenverarbeitung:
- Vertragsumsetzung
- Durchführung Mitteilungsverpflichtungen
- Abrechnung
- Kontaktaufnahme zu: Erziehungsberechtigten, Jugendamt, Kinderarzt, Versicherungen entsprechend der gesetzlichen Verpflichtungen

Empfänger der Daten:
Die hier erhobenen, verarbeiteten und gespeicherten Daten wurden von uns an folgende Stellen übermittelt:
- Steuerberater Müller, Adresse: Zahlungseingänge, Bankverbindungsdaten, Förderbeträge zur Wahrnehmung gesetzlicher Verpflichtungen
- Öffentlicher Jugendhilfeträger: Sachbearbeiterin Meier, *Adresse:* Betreuungszeiten, Fehlzeiten, Urlaubszeiten zur Wahrnehmung gesetzlicher Verpflichtungen
- Rechtsanwalt *Name, Adresse:* Betreuungszeiten, Fehlzeiten, Urlaubszeiten, Vergütungshöhe, Zahlungsstand, Vertrag zur Wahrnehmung berechtigter Interessen
- Kreditinstitut Maierbank, *Adresse:* Bankverbindungsdaten zur Zahlungsabwicklung zur Vertragsumsetzung
- Finanzamt Müllerstadt *Adresse:* Förderbescheide, Zahlungseingänge zur Wahrnehmung gesetzlicher Verpflichtungen
- Telekommunikationsunternehmen XX Adresse: Telefonnummern zur Ermöglichung der Kontaktaufnahme
- Server *Name, Adresse* zur Durchführung internet-basierter Services via Email/für Termin-Bestätigungen und -absagen, Informationsweitergaben zu einzelnen Ereignissen während oder aufgrund der Betreuung u. a. auch durch Fotografien

Die Adress- und Namensdaten der Erziehungsberechtigten und des Kindes sowie die Vertragsunterlagen und -anlagen werden entsprechend der steuerrechtlichen Vorgaben nach Ablauf des Jahres *2020 [Beispiel!]* noch weitere 10 Jahre gespeichert.

Alle Portfolios mit Lichtbildern des Kindes wurden an die Erziehungsberechtigten übergeben, dies ohne Rückbehalt einer Kopie. Damit sind diesbezüglich bereits jetzt keinerlei derartige Daten mehr vorhanden. Sämtliche Gesundheitsdaten des Kindes, welche anlässlich der Betreuung erhoben wurden, wurden ebenfalls schon restlos gelöscht (mit Ausnahme der Angaben im Betreuungsvertrag).

Wir gehen hiermit davon aus, dass wir Ihnen wie gefordert Auskunft erteilt haben.

Soweit Daten unrichtig sind, bitten wir um Hinweis, damit wir diese berichtigen können. Sollten nach Ihrer Auffassung noch Auskünfte fehlen oder diese aus Ihrer Sicht lückenhaft sein, bitten wir ebenfalls um Hinweis, dann werden wir gerne weiter Auskunft erteilen.

Sie haben uns darüber hinaus gebeten, die über Sie und Ihr Kind gespeicherten Daten mittels Datenträger an Sie herauszugeben.
Diesen Wunsch erfüllen wir gerne durch Überreichung des beigefügten passwortgeschützten USB-Sticks. Das Passwort wurde Ihnen gesondert überreicht.

Mit freundlichen Grüßen,

Kindertagespflegeperson [Verantwortliche/r]

Muster 7: Mitarbeiterverpflichtung zur Einhaltung des Datenschutzes*

Hinweis: Diese Vorlage dient als Formulierungshilfe und orientiert sich an häufig vorkommenden Erfordernissen der Kindertagespflege. Die Inhalte sind nicht abschließend. Die Inhalte der Vorlage müssen geprüft und je nach konkretem Anwendungsfall ergänzt oder modifiziert werden, um dem gegebenen Sachverhalt gerecht zu werden. Diese Vorlage stellt keine rechtliche Beratung durch die Autorin oder das Deutsche Jugendinstitut e. V. dar. Für die Richtigkeit und Vollständigkeit wird keine Gewähr und keinerlei Haftung übernommen. Die rechtliche Bewertung dieser Vorlage obliegt allein den Verwenderinnen und Verwendern.

Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Einwilligung bzw. eine andere gesetzliche Rechtsgrundlage (Artikel 6 DSGVO) die Verarbeitung gestattet. Es ist den Personen, die der verantwortlichen Kindertagespflegeperson unterstellt sind, untersagt, (besondere) personenbezogene Daten unbefugt außerhalb der Zwecke der verantwortlichen Stelle und der arbeitsbezogenen datenschutzrechtlichen Richtlinien zu verarbeiten. Die verantwortliche Kindertagespflegeperson ist hinsichtlich der technischen und organisatorischen Maßnahmen zur Einhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 2, 24 DSGVO rechenschaftspflichtig.
Die Grundsätze für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 DSGVO festgelegt und umfassen im Wesentlichen folgende Verpflichtungen:

(Besondere) Personenbezogene Daten müssen:

a. auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
b. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung“);
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 („Richtigkeit“);
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 („Speicherbegrenzung“);
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 (Art. 84 DSGVO, § 42 BDSG). Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadensersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben.
Der Mitarbeitende
Name, Vorname und Position/Tätigkeit einfügen
bestätigt, von der verantwortlichen Kindertagespflegeperson auf den Datenschutz verpflichtet worden zu sein. Die Verpflichtung gilt auch nach Beendigung der Tätigkeit fort.

Ort, Datum *Unterschrift des Mitarbeitenden*

* Erstellt unter Verwendung des Musters der DSK: https://www.datenschutzzentrum.de/artikel/1235-Kurzpapier-Nr.-19-Unterrichtung-und-Verpflichtung-von-Beschaeftigten-auf-Beachtung-der-datenschutzrechtlichen-Anforderungen-nach-der-DSGVO.html (letzter Abruf: 01.05.2020)

V

Gesetzesquellen und Datenschutzbehörden

1 Gesetzesquellen[3]

a) Europäische Verordnungen und Vorschriften

VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), http://data.europa.eu/eli/reg/2016/679/oj (letzter Abruf: 05.02.2020)

b) Bundesgesetze

Bundesdatenschutzgesetz BDSG
https://www.gesetze-im-internet.de/bdsg_2018/

Sozialgesetzbuch VIII SGB VIII
https://www.gesetze-im-internet.de/sgb_8/index.html

c) Ländergesetze

Baden-Württemberg
Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 – BW LDSG
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/06/LDSG-neu-GBl-2018173.pdf

Bayern
Bayerisches Datenschutzgesetz – BayDSG
https://www.gesetze-bayern.de/Content/Document/BayDSG?AspxAutoDetectCookieSupport=1

Berlin
Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung
https://www.datenschutz-berlin.de/datenschutz/rechtliche-grundlagen/berliner-datenschutzrecht/

Brandenburg
Gesetz zum Schutz personenbezogener Daten im Land Brandenburg – BbgDSG
http://bravors.brandenburg.de/gesetze/bbgdsg

3 Alle Links: letzter Abruf: 05.02.2020

Bremen
Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung – BremDSGVOAG
https://www.transparenz.bremen.de/sixcms/detail.php?gsid=bremen2014_tp.c.116884.de&asl=bremen203_tpgesetz.c.55340.de&template=20_gp_ifg_meta_detail_d

Hamburg
Hamburgisches Datenschutzgesetz – HmbDSG
http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&doc.id=jlr-DSGHA2018rahmen

Hessen
Hessisches Datenschutz- und Informationsfreiheitsgesetz – HDSIG
https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-DSIFGHErahmen

Mecklenburg-Vorpommern
Datenschutzgesetz für das LandMecklenburg-Vorpommern – DSG-M-V
https://www.datenschutz-mv.de/static/DS/Dateien/Rechtsgrundlagen/Landesdatenschutzgesetz.pdf

Niedersachsen
Niedersächsisches Datenschutzgesetz – NDSG
https://www.lfd.niedersachsen.de/recht/nieders_recht/ndsg/das-niedersaechsische-datenschutzgesetz-56264.html

Nordrhein-Westfalen
Datenschutzgesetz Nordrhein-Westfalen – DSG NRW
https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=35200711211004362 75

Rheinland-Pfalz
Landesdatenschutzgesetz – LDSG
http://landesrecht.rlp.de/jportal/?quelle=jlink&query=DSG+RP&psml=bsrlpprod.psml

Saarland
Gesetz zur Anpassung des Saarländischen Datenschutzgesetzes an die Verordnung (EU) 2016/679
http://sl.juris.de/cgi-bin/landesrecht.py?d=http://sl.juris.de/sl/DSG_SL_2018_rahmen.htm

Sachsen
Sächsisches Datenschutzdurchführungsgesetz – SächsDSDG
https://www.revosax.sachsen.de/vorschrift/17647

Sachsen-Anhalt
Datenschutzgesetz Sachsen-Anhalt – DSG LSA
http://www.landesrecht.sachsen-anhalt.de/jportal/portal/t/or0/page/bssahprod.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=jlr-DSGST2015rahmen&doc.part=X&doc.price=0.0

Schleswig-Holstein
Landesdatenschutzgesetz – LDSG
http://www.gesetze-rechtsprechung.sh.juris.de/jportal/?quelle=jlink&query=DSG+SH&psml=bsshoprod.psml&max=true&aiz=true

Thüringen
Thüringer Datenschutzgesetz
https://www.thueringen.de/mam/th3/tim/datenschutz/gesetz-und-verordnungsblatt-nr-06-2018.pdf

2 Kirchenrecht (Auswahl[4])

Katholische Kirche

Gesetz über den Kirchlichen Datenschutz KDG
https://www.datenschutz-kirche.de/sites/default/files/KDG%20i.d.%20Fassung%20des%20Beschlusses%20der%20VV%20vom%2020.11.2017.pdf

Diözesandatenschutzbeauftragter der (Erz-)Bistümer Hamburg u. a. (2018): Arbeitshilfe Nr. 100 Einführung in das Datenschutzrecht der Katholischen Kirche: Eine Erstinformation für Mitarbeiter. Bremen

Fachet, Siegfried: (1998) Datenschutz in der katholischen Kirche, München

Evangelische Kirche

EKD Datenschutzgesetz
https://www.kirchenrecht-ekd.de/document/41335

Claessen, Herbert: (2004) Datenschutz in der Evangelischen Kirche, München

Ziekow, Arne: (2002) Datenschutz und evangelisches Kirchenrecht, Tübingen

4 Alle Links: letzter Abruf 05.02.2020

3 Datenschutzbehörden

BUND
Bundesdatenschutzbeauftragter: Ulrich Kelber
Husarenstraße 30
D-53117 Bonn
Telefon: +49 228 997799-0
Telefax: +49 228 997799-5550
E-Mail: poststelle@bfdi.bund.de

Baden-Württemberg
Datenschutzbeauftragter: Dr. Stefan Brink
Postfach 10 29 32
70025 Stuttgart
Telefon: +49 711 615541-0
Telefax: +49 711 615541-15
E-Mail: poststelle@lfdi.bwl.de

Bayern
Datenschutzbeauftragter: Prof. Dr. Thomas Petri
Postfach 22 12 19
80502 München
Telefon: +49 89 212672-0
Telefax: +49 89 212672-50
E-Mail: poststelle@datenschutz-bayern.de

Berlin
Datenschutzbeauftragte: Maja Smoltczyk
Friedrichstraße 219
10969 Berlin
Telefon: +49 30 13889-0
Telefax: +49 30 21550-50
E-Mail: mailbox@datenschutz-berlin.de

Brandenburg
Datenschutzbeauftragte: Dagmar Hartge
Stahnsdorfer Damm 77
14532 Kleinmachnow
Telefon: +49 332 03356-0
Telefax: +49 332 03356-49
E-Mail: poststelle@lda.brandenburg.de

Bremen
Datenschutzbeauftragte: Dr. Imke Sommer
Arndstraße 1
27570 Bremerhaven
Telefon: +49 471 5962010- oder +49 421 3612010-
Telefax: +49 421 49618495
E-Mail: office@datenschutz.bremen.de

Hamburg
Datenschutzbeauftragter:
Prof. Dr. Johannes Caspar
Ludwig-Erhard-Str. 22 7.OG
20459 Hamburg
Telefon: +49 40 4285440-40
Telefax: +49 40 4285440-00
E-Mail: mailbox@datenschutz.hamburg.de

Hessen
Datenschutzbeauftragter:
Prof. Dr. Michael Ronellenfitsch
Postfach 31 63
65021 Wiesbaden
Telefon: +49 611 140-80
Telefax: +49 611 1408-900
E-Mail: poststelle@datenschutz.hessen.de

Mecklenburg-Vorpommern
Datenschutzbeauftragter: Heinz Müller
Erderstraße 74a
19055 Schwerin
E-Mail: info@datenschutz-mv.de

Niedersachsen
Datenschutzbeauftragte: Barbara Thiel
Prinzenstraße 5
30159 Hannover
Telefon: +49 511 12045-00
Telefax: +49 511 12045-99
E-Mail: poststelle@lfd.niedersachsen.de

Nordrhein-Westfalen
Datenschutzbeauftragte: Helga Block
Postfach 20 04 44
40102 Düsseldorf
Telefon: +49 211 38424-0
Telefax: +49 211 38424-10
E-Mail: poststelle@ldi.nrw.de

Rheinland-Pfalz
Datenschutzbeauftragter:
Prof. Dr. Dieter Kugelmann
Postfach 30 40
55020 Mainz
Hintere Bleiche 34
55116 Mainz
Telefon: +49 6131 20824-49
Telefax: +49 6131 20824-97
E-Mail: poststelle@datenschutz.rlp.de

Saarland
Datenschutzbeauftragte: Monika Grethel
Postfach 10 26 31
66026 Saarbrücken
Telefon: +49 681 94781-0
Telefax: +49 681 94781-29
E-Mail: poststelle@datenschutz.saarland.de

Sachsen
Datenschutzbeauftragter: Andreas Schurig
Sächsischer Datenschutzbeauftragter
Postfach 11 01 32
01330 Dresden
Telefon: +49 351/8547110-1
Telefax: +49 351/8547110-9
E-Mail: saechsdsb@slt.sachsen.de

Sachsen-Anhalt
Datenschutzbeauftragter: Dr. Harald von Bose
Postadresse: Postfach 1947
39009 Magdeburg
Telefon: +49 391 81803-0
Telefax:+49 391 81803-33
E-Mail: poststelle@lfd.sachsen-anhalt.de

Schleswig-Holstein
Datenschutzbeauftragte: Marit Hansen
Holstenstraße 98
24103 Kiel
Telefon: +49 431 9881200-
Telefax: +49 431 9881223-
E-Mail: mail@datenschutzzentrum.de

Thüringen
Datenschutzbeauftragter: Dr. Lutz Hasse
Postfach 90 04 55
99107 Erfurt
Telefon: 0361 57–3112900
Telefax: +49 361 57311290-+49 -
E-Mail: poststelle@datenschutz.thueringen.de

4 Sonstige

Bundesamt für Sicherheit in der Informationstechnik (BSI):
https://www.bsi.bund.de/DE/Home/home_node.html

Bundesverband für Kindertagespflege e. V.:
www.bvktp.de

Datenschutzkonferenz (DSK):
https://www.datenschutzkonferenz-online.de/

VI

Glossar

Dieses Glossar soll dem besseren Verständnis einiger der in der Expertise verwendeten Fachbegriffe dienen. Die hier aufgeführten Erklärungen entsprechen daher **nicht** den eingeführten Definitionen aus den jeweiligen Fachgebieten. Es handelt sich vielmehr um den Versuch einer Erklärung dieser Begriffe in der Allgemeinsprache.

Anwendungsbereich:

- **räumlich:** Festlegung des geografischen Raums, in dem die Vorgaben der DSGVO zu berücksichtigen sind (z. B.: Deutschland).
- **sachlich:** Festlegung der Tätigkeiten, bei denen die DSVO zu beachten ist.

Anwendungsvorrang:

Klarstellung, welche Rechtsvorschrift vorrangig anzuwenden ist, wenn mindestens zwei Rechtsvorschriften zum selben Thema auf unterschiedlichen Ebenen (z. B. Bundes- oder Länderebene) vorhanden sind.

Auftragsverarbeiter:

Ein Auftragsverarbeiter ist ein Mensch, eine Behörde, ein Verein oder eine sonstige juristische Person, welche Informationen/Einzelangaben über Menschen im Auftrag des Verantwortlichen verarbeitet, z. B. Ersatzbetreuungsperson, Trägerverein, Dienstleister.

Ausnahmetatbestand:

Juristischer Fachbegriff für die Ausnahme von der Regel.

Daten:

Unter Daten sind alle Informationen und Einzelangaben – somit alles Wissen– über einen anderen Menschen zu verstehen, welche geeignet sind, diesen in seinem Wesen und seiner Identität zu beschreiben.

- **Datenerhebung:**
  Kenntniserlangung von Informationen/Einzelangaben über einen anderen Menschen, gleichgültig auf welchem Wege.
- **Datenfluss:**
  Übertragung von Informationen/Einzelangaben eines anderen Menschen an andere Personen oder an Institutionen, gleich in welcher Art und Weise und gleich, an wen.
- **Datenlöschung:**
  Nachhaltige und endgültige Vernichtung und Zerstörung einer Information/Einzelangabe über einen anderen Menschen in einer Form, dass diese Information nicht wiederhergestellt werden kann.
- **Datensammlung:**
  Gesammeltes Wissen über einen anderen Menschen, das für Dritte zugänglich ist.
- **Datenschutz:**
  Schutz der Informationen über einen anderen Menschen vor nicht erlaubter Nutzung, nicht jedoch Schutz der Informationen vor dem betroffenen Menschen.
- **Datenspeicherung:**
  Fixierung von Informationen, dass so sie zu einem späteren Zeitpunkt zur Kenntnis genommen und benutzt werden können.
- **Dateisysteme:**
  – jede strukturierte und geordnete Ablage von Informationen über einen anderen Menschen, wobei bereits ein einziges Strukturmerkmal zur Anwendbarkeit der DSGVO genügt.
- **Datenverarbeitung:**
  Kenntniserlangung und Nutzung von Informationen/Einzelangaben über einen Menschen gleich welcher Art; von Beginn an (Erhebung) bis zum Ende (Löschung).

- **Datenverkehr:**
  Hin- und Herleitung von Informationen/Einzelangaben eines anderen Menschen, gleich in welcher Art und Weise und gleich, an wen.
- **Datenweitergabe:**
  Weiterleitung von Informationen/Einzelangaben eines anderen Menschen an andere Personen oder an Institutionen, gleich in welcher Art und Weise und gleich, an wen.
- **personenbezogene Daten:**
  Informationen/Einzelangaben jeglicher Art über einen anderen Menschen.
- **besondere Arten personenbezogener Daten:**
  Jegliche Informationen über einen anderen Menschen der folgenden Art: Rasse, ethnische Herkunft, politische Meinung, religiöse oder sonstige Weltanschauung, Gesundheit, Sexualleben.

Data-Mining:
Systematisches Zusammentragen von Informationen/Einzelangaben über andere Menschen unter Zuhilfenahme technischer Hilfsmittel.

Einwilligung:
Erklärung des Einverständnisses zu einer bestimmten Maßnahme oder Handlung vor Durchführung derselben durch den betroffenen Menschen oder dessen Vertreter (z. B. Erziehungsberechtigte).

E-Mail-Disclaimer:
Standartmäßig vorformulierte Informationen am Ende einer E-Mail, welche häufig auch die E-Mail-Signatur (= Person des Absenders, Kontaktdaten) enthalten.

Empfänger:
Eine Person, Behörde oder sonstige Institution, die Daten entgegennimmt.

Erforderlichkeit:
Erforderlich ist eine Maßnahme, wenn sie geeignet ist, das beabsichtigte Ziel zu erreichen und gleichzeitig das mildeste Mittel zur Zielerreichung darstellt. Eine Maßnahme ist dann erforderlich, wenn ohne sie das Ziel gar nicht erreicht werden kann, auch nicht auf andere Weise.

Erlaubnistatbestand, Erlaubnisvorbehalt:
Ein Erlaubnistatbestand ist ein Rechtfertigungsgrund, der die Durchführung einer an sich verbotenen Handlung ausnahmsweise erlaubt (im Strafrecht z. B. Verletzung einer anderen Person im Rahmen der Notwehr).

Erlaubnisvorbehalt:
Alle Maßnahmen der Datenverarbeitung sind verboten, es sei denn, einer der Erlaubnistatbestände der DSGVO liegen vor.

Formerfordernis:
Fixierung bestimmter Äußerungen und Willenserklärungen eines klar identifizierbaren Verfassers auf einem Medium und in einer Art und Weise, dass sie auch noch zu einem späteren Zeitpunkt zum Beweis in unverfälschter und unverfälschbarer Form wahrgenommen werden können (z. B. Schriftform auf Papier).

Genehmigung:
Nachträgliche Zustimmung durch den betroffenen Menschen oder dessen Vertreter (z. B. Erziehungsberechtigte) zu einer bestimmten Maßnahme oder Handlung nach ihrer Durchführung.

Gesundheitsdaten:
Informationen/Einzelangaben über den körperlichen Zustand eines anderen Menschen, beispielsweise über Krankheiten und andere körperliche Zustände jeglicher Art.

Gewichtige Anhaltspunkte (in Abgrenzung zu: Wichtige Ereignisse):
Gewichtige Anhaltspunkte i.S.d. § 8a SGB VIII sind Informationen, konkrete Hinweise von einigem Gewicht oder ernstzunehmende Vermutungen, welche insgesamt auf eine Gefahr für das Kindeswohl hindeuten können, beispielsweise Drogenkonsum der Erziehungsberechtigten, anhaltende und erhebliche Anzeichen einer Verwahrlosung etc.

Grundfreiheiten:
Die Grundfreiheiten sind die vier wesentlichen europäischen grundlegenden Rechte: freier Waren- und Zahlungsverkehr, Personenfreizügigkeit und Dienstleistungsfreiheit.

Grundprinzipien des Datenschutzes:

- **Datendirekterhebung:**
  Die Informationen über einen Menschen sind vorrangig direkt bei diesem anzufragen bzw. von diesem zu erlangen.
- **Datenrichtigkeit:**
  Gebot der Wahrhaftigkeit der erhobenen Daten: Die über einen anderen Menschen erhobenen Informationen müssen korrekt und vollständig sein.
- **Gebot der Datensparsamkeit:**
  Gebot, nur solche Informationen über einen anderen Menschen zu erheben, die für den beabsichtigten Zweck unbedingt erforderlich sind.
- **Speicherbegrenzung:**
  Begrenzung des Zeitraums, in dem die Informationen über einen anderen Menschen aufbewahrt werden, bevor sie endgültig und nachhaltig vernichtet werden.
- **Transparenzgebot:**
  Die Art und Weise der Erhebung von Informationen über einen anderen Menschen sowie Art und Zweck ihrer Benutzung müssen so erklärt werden, dass der Betroffene die verschiedenen Verarbeitungsschritte und die Zwecke zweifelsfrei verstehen und nachvollziehen kann.
- **Verbotsprinzip:**
  Juristischer Fachbegriff; eine Handlung ist grundsätzlich nicht erlaubt und darf ausnahmsweise nur dann durchgeführt werden, wenn ein bestimmter Erlaubnisgrund vorliegt.
- **Zweckbindung:**
  Eine bestimmte Handlung darf nur aus gesetzlich oder vertraglich genau festgelegten Gründen durchgeführt werden.

Grundrechte:

Dies sind die wesentlichen, im Grundrecht einklagbar zugesprochenen Rechte von Menschen, juristischen Personen etc., beispielsweise das Grundrecht auf Meinungsfreiheit, Berufsausübungsfreiheit, Religionsfreiheit etc.

Jugendhilfeträger:

Träger der öffentlichen Kinder- und Jugendhilfe, „Jugendamt".

Klardaten:

Nicht-anonymisierte Sammlung von Informationen über einen anderen Menschen.

Kompetenz; Gesetzgebungskompetenz:

Fähigkeit zu einem bestimmten Handeln; Gesetzgebungskompetenz: Fähigkeit und Recht einer gesetzgeberischen Institution zur Verabschiedung von Gesetzen, Richtlinien oder Verordnungen.

Konkludentes Handeln:

Schlüssiges Verhalten; nur durch ein klares Verhalten und ohne jeglichen Restzweifel an der Bedeutung dieses Verhaltens wird ohne Worte ein bestimmter Willen zum Ausdruck gebracht.

Mehrebenensystem:

Bezeichnung für das komplizierte Über- und Unterordnungsgefüge der verschiedenen Gesetzgebungsorgane auf europäischer und deutscher Ebene (EU-Bund-Land) bzw. danebenstehender Ebenen (z. B. Kirchen).

Niederlassungsprinzip:

Nähere Bestimmung des räumlichen Anwendungsbereichs der DSGVO; Ort der tatsächlichen Ausübung der Tätigkeit.

Öffnungs- oder Spezifizierungsklauseln:

Vorschriften in einem Gesetz, einer Richtlinie oder Verordnung, welche dem Adressaten dieser Vorschrift das Recht geben, Detailfragen im vorgegebenen Rahmen zu regeln oder genauer zu reglementieren.

Pseudonymisierung:

Entfernung derjenigen Informationen, welche sofort und unmittelbar, ohne jeglichen Zwischenschritt, auf einen bestimmten anderen Menschen schließen lassen. Die Identifikation des betroffenen Menschen wird durch Einfügung mindestens eines Zwischenschrittes wesentlich erschwert, z. B. durch Verwendung von Namenskürzeln oder Ziffern (z. B. „A." oder „Kind 1"). Bei pseudonymisierten Daten kann die Identität des betroffenen Menschen jedoch aus den Umständen des Einzelfalles ermittelt werden.

Richtlinie (EU):

Rechtsakt der EU, der nicht unmittelbar gilt, sondern auf Ebene der Mitgliedsstaaten der EU in nationales Recht umgewandelt werden muss.

Scoring:
Berechnung von Wahrscheinlichkeitswerten zur Vorhersage zukünftiger Entwicklungen oder zukünftigen Verhaltens eines Menschen oder bestimmter Gruppen von Menschen.

Shoulder Surfing:
Über die Schulter eines anderen linsen, um bei diesem mitzulesen und hierdurch weiterverwertbare Informationen zu erhalten.

Sozialdatenschutz:
Datenschutzregeln im deutschen Sozialrecht

Technisch-organisatorische Maßnahmen (TOM):
Organisatorische oder technische Handlungen mit dem Ziel, Informationen vor unzulässiger Verwendung oder unzulässigem Zugriff zu sichern.

Verantwortlicher:
Person oder Einheit, die Informationen über einen anderen Menschen erhebt, um sie für eigene unternehmerische oder wirtschaftliche Zwecke zu benutzen.

Verordnung (EU):
Rechtsakt der EU, der in allen Mitgliedsstaaten unmittelbar und direkt gilt, also nicht mehr auf Ebene der Mitgliedsstaaten der EU in nationales Recht umgewandelt werden muss.

Vorsorgeprinzip:
Maßnahmen und Bemühungen, um den zukünftigen Eintritt von Gefahren zu vermeiden (Gefahrenvorsorge).

Vorvertragliche Maßnahmen:
Handlungen im Vorfeld eines Vertragsabschlusses, z. B. Kennenlern-Treffen, Schnuppervormittage bei einer Kindertagespflegeperson.

Weisungsgebundenheit:
Begrifflichkeit aus dem Arbeitsrecht; Befugnis des Arbeitsgebers, Ort, Zeit und Ausführung der Arbeit vorzugeben.

Wichtige Ereignisse (in Abgrenzung zu: Gewichtige Anhaltspunkte):
Wichtige Ereignisse i.S.d. § 43 SGB VIII sind Informationen, die für die Betreuung des Tagespflegekindes bedeutsam sind, beispielsweise soziale Auffälligkeiten, Erkrankungen, Entwicklungsverzögerungen.

VII

Links

(jeweils letzter Abruf: 02.05.2020)

www.baden-wuerttemberg.datenschutz.de
https://www.bsi.bund.de/DE/Home/home_node.html
www.datenschutz-bayern.de/technik/orient/telefax.htm
https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Handlungsrahmen_Soziale_Medien_20200306.pdf
https://www.datenschutzzentrum.de/artikel/1235-Kurzpapier-Nr.-19-Unterrichtung-und-Verpflichtung-von-Beschaeftigten-auf-Beachtung-der-datenschutzrechtlichen-Anforderungen-nach-der-DSGVO.html
www.lda.bayern.de/de/beschwerde.html
www.lto.de/recht/nachrichten/n/DSGVO-bussgeld-strafe-frankreich-google-informationen/
www.praxistipps.chip.de/whatsapp-zugriff-auf-kontakte-verhindern-so-gehts_93842
www.spiegel.de/netzwelt/web/facebook-und-cambridge-analytica-leak-whistleblower-christopher-wylie-gesperrt-a-1198763.html
www.stmi.bayern.de
www.welt.de/wirtschaft/article127418980/Daten-sind-das-Gold-des-21-Jahrhunderts.html
https://www.whatsapp.com/legal?eea=1&lang=de

VIII

Literaturverzeichnis

A.

Arbeitsrecht aktiv (ohne Namensangabe) (2019): *Datenschutz, Geheimnisverrat, Whistleblower im Betrieb: Neue Regeln sind im Anmarsch*. In: Arbeitsrecht aktiv, Sonderausgabe 2019, S. 16 f.

- **Bayr. Landesbeauftragte für Datenschutz (2019):** Auftragsverarbeitung. Orientierungshilfe. München
- **Bayr. Landesbeauftragte für Datenschutz (?):** Datensicherheit beim Telefax-Dienst. https://www.datenschutz-bayern.de/technik/orient/telefax.htm (Abruf: 08.08.2019)

Bock, Kirsten (2018): *Das Standard-Datenschutzmodell*. Düsseldorf

Bundesamt für Sicherheit in der Informationstechnik: *Tipps für ein gutes Passwort* https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html (letzter Abruf: 10.02.2020)

Bundestag Drucksache DS 19/11843 vom 23.07.2019 http://dip21.bundestag.de/dip21/btd/19/118/1911843.pdf (letzter Abruf: 05.02.2020)

Communication from the Commission to the European Parliament and the Council (2019). Brüssel. https://ec.europa.eu/commission/sites/beta-political/files/communication_from_the_commission_to_the_european_parliament_and_the_council.pdf (Abruf: 03.09.2019)

Diering, Carsten (2014): *Daten sind das Gold des 21*. Jahrhunderts. In: Welt vom 29.04.2014. https://www.welt.de/wirtschaft/article127418980/Daten-sind-das-Gold-des-21-Jahrhunderts.html (Abruf: 16.05.2019)

Dierks, Benjamin (2018): *Propaganda, Lügen, Fake News*. In: Deutschlandfunk vom 18.10.2018. https://www.deutschlandfunk.de/soziale-medien-und-das-brexit-referendum-propaganda-luegen.724.de.html?dram:article_id=430936 (Abruf: 16.05.2019)

Diözesandatenschutzbeauftragter der (Erz-)Bistümer Hamburg u. a. (?): *Welches Recht wendet die Katholische Kirche zum Schutz personenbezogener Daten an?* https://www.datenschutz-kirche.de/frage_1 (Abruf: 17.05.2019)

Ehmann, Eugen/Selmayr, Martin (Hrsg.) (2017): *Datenschutz-Grundverordnung*. München

Gruber, Angela (2018): *Unbemerkt ausgespäht*. In: www.spiegel-online.de vom 19.03.2018. https://www.spiegel.de/netzwelt/web/facebook-und-cambridge-analytica-leak-whistleblower-christopher-wylie-gesperrt-a-1198763.html (letzter Abruf: 16.05.2019)

Haslach Katharina (2018): *Datenschutz achten! In: DATEV magazin 04/18, S.* 8–11

Heidrich, Jörg (2020): *Die DSGVO wird erst 2020 richtig scharfgestellt*. In: Spiegel Netzwelt vom 10.02.2020. https://www.spiegel.de/netzwelt/netzpolitik/dsgvo-wird-erst-2020-richtig-scharfgestellt-a-87b25b0b-2562-409a-bd7f-2b7ab4394642 (Abruf: 10.02.2020)

Klein, Susanne (2018): *Eltern sollten ihre Kinder bei jedem Bild fragen: Kinderbilder in sozialen Medien*. In: Süddeutsche Zeitung vom 21.12.2018. https://www.sueddeutsche.de/leben/fotos-kinder-soziale-medien-1.4262852 (Abruf: 20.11.2019)

König, Thomas/Rieger, Elmar/Schmitt, Hermann (Hrsg) (1996): *Das europäische Mehrebenensystem*. Frankfurt

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz). Abrufe: 10.02.2020

- Kurzpapier Nr. 11 Recht auf Löschung/Recht auf Vergessenwerden. Version 29.08.2017. https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/08/DSK_KPNr_11_Recht-auf-Vergessenwerden.pdf
- Kurzpapier Nr. 14 Beschäftigtendatenschutz. Version 2.0 vom 17.12.2018. www.govdata.de/dl-de/by-2-0Kurzpapier Nr. 18: Risiko für die Rechte und Freiheiten natürlicher Personen. Version 2.0 vom 26.04.2018. www.govdata.de/dl-de/by-2-0
- Kurzpapier Nr. 20: Einwilligung nach der DSGVO. Version 2.0 vom 22.02.2019. www.govdata.de/dl-de/by-2-0
- Datenschutzkonferenz, Beschluss vom 05.09.2018 „Facebook-Fanpages“, https://www.datenschutzkonferenz-online.de/media/dskb/20180905_dskb_facebook_fanpages.pdf
- Zwischenkonferenz 25.06.2019 https://www.datenschutzkonferenz-online.de/media/pr/20190622_pr_mainz.pdf

Landesbeauftragte für den Datenschutz Niedersachsen: *Meldung von Datenschutzverstößen*. https://www.lfd.niedersachsen.de/startseite/datenschutzreform/DSGVO/faq/meldung-von-datenschutzverstoeen-167312.html (Abruf: 06.08.2019)

Mareck, Heike (2019): *Wie weit reichen die Einsichts- und Auskunftsrechte des ArbN? In: ArbeitsrechtAktiv 06/2019, S.* 103–105

Maurer, Jürgen (2017): *Big-Data-Trends im Überblick*. In: Computerwoche vom 11.12.2017. https://www.computerwoche.de/a/was-ist-was-bei-predictive-analytics,3098583 (Abruf: 16.05.2019)

Oberwetter, Christian (2019): *Frankreich: 50 Millionen Euro Bußgeld für Google*. In: Legal Tribune Online vom 22.01.2019. https://www.lto.de/recht/nachrichten/n/DSGVO-bussgeld-strafe-frankreich-google-informationen/ (Abruf: 14.08.2019)

Schuhegger, Lucia/Hundegger, Veronika/Lipowski, Hilke/Lischke-Eisinger, Lisa/Ullrich-Runge, Claudia (2019): *Qualität in der Kindertagespflege*. Qualifizierungshandbuch (QHB) für die Bildung, Erziehung und Betreuung von Kindern unter drei. Hannover

Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döhmann, Indra (Hrsg.) (2019): *Datenschutzrecht 1*. Auflage. Baden-Baden

Simitis, Spiros (Hrsg.) (2014): *Bundesdatenschutzgesetz*. Kommentar. 8. Auflage. Baden-Baden

Solmecke, Christian (2019): *Abmahnungen vermeiden in: Praxis IT-Recht 08/2019 S.* 27–29

Staatsregierung Bayern (2017): *Gesetzesbegründung zum BayDSG vom 28*.09.2017. https://www.stmi.bayern.de/assets/stmi/ser/gesetzentwuerfe/baydsg_stand_28_09_2017.pdf (Abruf: 26.07.2019)

Wiesner, Reinhard (Hrsg.) (2015): *SGB VIII*. Kommentar. 5. Auflage. München

Welling, Kira (2017): *WhatsApp: Zugriff auf Kontakte verhindern – so geht's*. In: Praxistipp Chip vom 26.09.2017. https://praxistipps.chip.de/whatsapp-zugriff-auf-kontakte-verhindern-so-gehts_93842 (Abruf: 13.08.2019)

WhatsApp Inc. (2018): *Rechtliche Hinweise vom 24*.05.2018. https://www.whatsapp.com/legal?eea=1&lang=de (Abruf: 13.08.2019)

Zahl, Jennifer/Hager, Stefan/Mendel, Martina (2018): *Angriff auf allen Ebenen*. In: DATEV magazin 04/18, S. 15–16

B. Rechtsprechung

Europäischer Gerichtshof (EuGH): Abruf: 05.05.2019
- Urteil vom 12.11.1969 Az 29/69 „Urteil Stauder“, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A61969CJ0029, Abruf: 05.05.2019

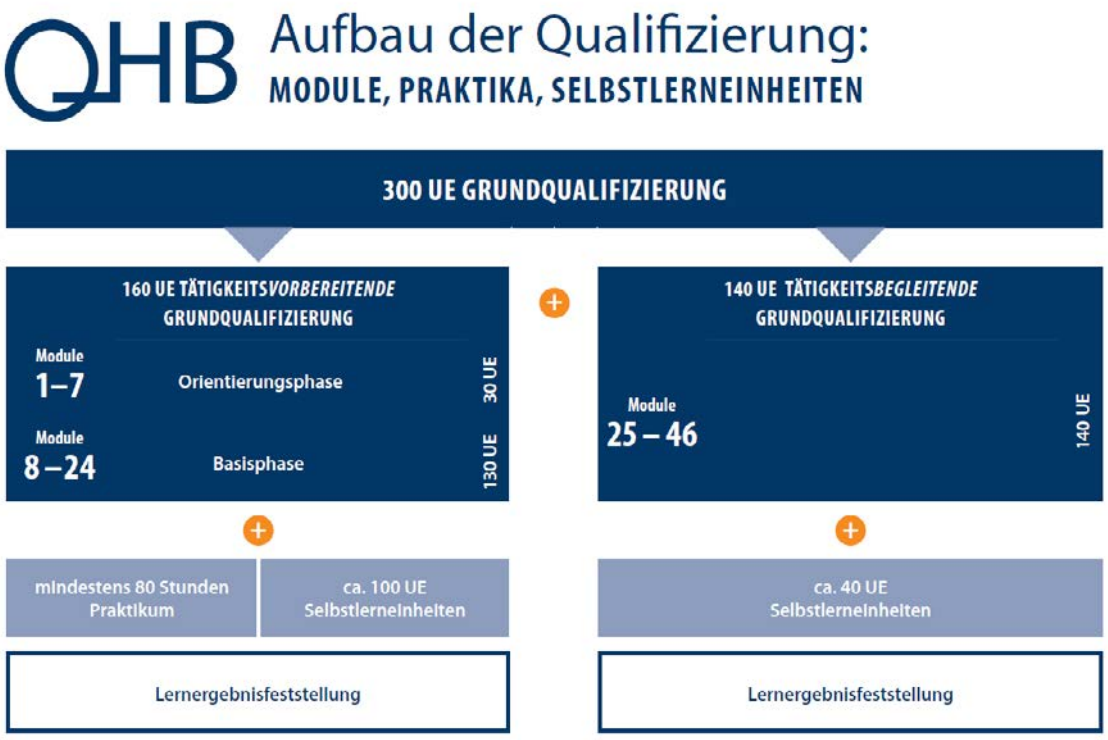
Bundesverfassungsgericht (BVerfG): Abrufe: 17.05.2019
- Urteil vom 11.06.1958 – 1 BvR 596/56 (BVerfGE 7, 377; „Apotheken-Urteil“), https://openjur.de/u/181986.html
- Beschluss vom 11.10.1977 – 2 BvR 209/76 BVerfGE 53, 366, 392 „Goch-Beschluss“, https://openjur.de/u/182348.html
- Beschluss des Bundesverfassungsgerichts vom 22.10.1986 – 2 BvR 197/83 „Solange II“, https://openjur.de/u/56233.html
- Urteil vom 15. Dezember 1983 – Az. 1 BvR 209 (BVerfGE 65, 1), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html

Verwaltungsgerichte: Abrufe: 08.08.2019
- **VGH Baden-Württemberg,** Urteil vom 12.07.2017 – Az 12 S 102/15, http://lrbw.juris.de/cgi-bin/laender_rechtsprechung/document.py?Gericht=bw&nr=22599
- **VG Bremen,** Urteil vom 10.07.2014 AZ 3 K 1064/13, https://www.bvktp.de/files/3_k_1064_13_urteil_00000059_095018anonym.pdf

Zivilgerichte: Abrufe 06.02.2020
- **LG Bochum,** Urteil vom 07.08.2018 Az.12 O 85/18 https://openjur.de/u/2157403.html
- **LG Frankfurt a.M.,** Urteil vom 29.08.2019 Az. 2-03 O 454/18 https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Frankfurt%2FMain&Datum=29.08.2019&Aktenzeichen=3%20O%20454%2F18
- **OLG Hamburg,** Urteil vom 25.10.2018 Az 3 U 66/77 https://openjur.de/u/2126095.html
- **LG Stuttgart,** Urteil vom 20. Mai 2019, Az. 35 O 68/18 KfH https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=LG%20Stuttgart&Datum=20.05.2019&Aktenzeichen=35%20O%2068%2F18
- **LG Würzburg,** Beschluss vom 13.09.2018 Az 11 O 1741/18 https://www.gesetze-bayern.de/Content/Document/Y-300-Z-BECKRS-B-2018-N-22735?hl=true
- **AG Bad Hersfeld,** Beschluss vom 20.03.2017 Az. F 111/17 https://openjur.de/u/2187467.html
- **AG Wertheim,** Beschluss vom 12.12.2019 Az. 1 C 66/19 https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=AG%20Wertheim&Datum=12.12.2019&Aktenzeichen=1%20C%2066%2F19

Anhang

Aufbau der Grundqualifizierung nach dem Konzept des Qualifizierungshandbuches Kindertagespflege



Quelle: Schuhegger u. a. (2019), Einführung S. 8