Dienstanweisung KVL DA 01-2018

KINDERVEREINIGUNG® Leipzig e.V.

KVL DA 01-2018 / Datenschutz in der KINDERVEREINIGUNG® Leipzig e.V.

In diesem Dokument ist stellvertretend für alle männlichen und weiblichen Mitarbeiter immer von Mitarbeiter*in bzw. Mitarbeiter*innen die Rede. Ferner wird an Stellen, an denen zweimal das Wort Mitarbeiter*in einem Satz stehen würde, nach der Erstnennung dann das Wort Mitarbeitende verwendet. In beiden Fällen dient dies der sprachlichen Vereinfachung und ist in keinem Fall diskriminierend gemeint.

Die vorliegende Dienstanweisung gilt ausnahmslos für alle Mitarbeiter*innen der KINDERVEREINIGUNG® Leipzig e.V.

Diese Dienstanweisung ist, dem wichtigen Sachgebiet geschuldet, äußerst umfangreich. Dennoch ist der Datenschutz immer auch ein dynamischer Prozess. Daher wird diese Unterlage in Abständen ergänzt werden müssen. Die Ergänzungen sind mit **KVL DA 01-2018 Zusatz xx** gekennzeichnet und werden mit ihrer betriebsüblichen Bekanntgabe (per E-Mail) unmittelbar Bestandteil dieser Dienstanweisung. Ebenso unmittelbar **müssen** diese Ergänzungen in Einrichtungen mit mehreren Mitarbeiter*innen durch die entsprechenden Leiter*innen dann **allen Mitarbeitenden** auf geeignete Weise **bekannt gegeben werden** (Aushang, Übergabe etc.).

Nachfolgende Regelungen sind bindend für alle Mitarbeiter*innen und verstehen sich als Ergänzung / Präzisierung der Datenschutzleitlinie der KINDERVEREINIGUNG® Leipzig e.V., die ebenfalls Bestandteil dieser Dienstanweisung ist.

Es gibt noch weiterführende Vorschriften für die Geschäftsstelle, die Bereiche Feriendienst und Internationale Arbeit, sowie EBI, die gesondert ausgereicht werden.

Begriffsklärung personenbezogene Daten

Personenbezogene Daten (pbD) sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Eine Person wird als bestimmbar angesehen, wenn sie direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

1 Grundsätzliches

1.1 Den Datenschutz in der KINDERVEREINIGUNG® Leipzig e.V. realisiert nicht der Datenschutzbeauftragte (DSB), sondern jede einzelne Mitarbeiter*in fortwährend und ohne Beachtung möglicher Leitungs- oder Bereichsverantwortung in ihrem direkten Arbeitsumfeld vorwiegend selbstständig!

1.2 Über die nachfolgenden Regelungen dieser Dienstanweisung hinaus, setzt dieser Anspruch die hohe Eigenverantwortung der Mitarbeiter*in und ein gewisses Maß an (gesundem) Rechtsempfinden voraus.

1.3 Die Mitarbeiter*in ist verpflichtet auf mögliche Risiken oder Probleme den Datenschutz betreffend Kolleg*innen, Leiter*innen, das Q-Team, die Fachbereichsleitung, die Geschäftsführung und insbesondere den DSB hinzuweisen, allgemein bei der Einhaltung von Datenschutzvorschriften mitzuwirken und sich proaktiv aktuelle Informationen zum Thema Datenschutz für ihren Arbeitsbereich anzueignen.

1.4 Es gibt eine „Holschuld“ der Mitarbeiter*in, sich Dokumente und Formulare, auf die in dieser Dienstanweisung Bezug genommen wird, verfügbar zu machen. Sie kann sich nicht darauf berufen, dass ihr die entsprechenden Unterlagen gleichzeitig mit Aushändigung dieser Dienstanweisung hätten zugänglich gemacht werden müssen.

2 Grundsatz der Rechtmäßigkeit

Jede Datenverarbeitung erfordert einen gesetzlich anerkannten Erlaubnistatbestand. Das sind für den Geschäftsbereich der KINDERVEREINIGUNG® Leipzig zutreffend:

a) Die Einwilligung des Betroffenen
b) Die Erhebungen / Verarbeitungen zur Vertragserfüllung
c) Die Erfüllung rechtlicher Pflichten
d) Der Schutz lebenswichtiger Interessen
e) Die Datenverarbeitung im Beschäftigungskontext
f) Zusammenarbeit mit Ermittlungsbehörden*(1)
g) Und die Wahrnehmung berechtigter Interessen des Verantwortlichen, 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

**(1) In diesem Fall ist jedoch vorher und unmittelbar der DSB zu informieren und verbindlich seine Zusage zur geplanten Maßnahme abzuwarten. Ausnahme bildet hier einzig der Umstand von „Gefahr im Verzug".*

3 Grundsätze für die Verarbeitung von pbD (Art. 5 EU DS-GVO)

Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden ***(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 /Datensparsamkeit)***

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein ***(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)***

4 Allgemeine Vorschriften

4.1 Diese Dienstanweisung ist jeder neuen Mitarbeiter*in (auch (länger beschäftigten) Praktikant*innen oder Bundesfreiwilligendienstleistenden) unmittelbar bei Aufnahme ihrer Tätigkeit in ausgeduckter Form und gegen Unterschrift zu übergeben. Mit der Übergabe geht eine kurze Belehrung einher, die auf die Notwendigkeit der umgehenden Kenntnisnahme der Inhalte der DA durch die Mitarbeiter*in hinweist.
Ein entsprechendes Formular wird mit der Kennzeichnung **KVL Übergabe DA Datenschutz** seitens des DSB bereitgestellt.

4.2 Verantwortlichkeiten:

- im Bereich Kindertagesstätten obliegt dieser Vorgang den jeweiligen Kitaleiter*innen oder den hausintern beauftragten Kräften für Belehrungen
- im Bereich Projekte sind die beiden Fachkoordinatorinnen zuständig, diesen Vorgang mit der Unterzeichnung des Arbeitsvertrages / beim Antrittsgespräch zu realisieren
- im Bereich Verwaltung / GS ist die Personalsachbearbeiterin verantwortlich

4.3 Die unterschriebenen Übergabe- / Belehrungsbögen sind dem DSB im Original und spätestens innerhalb einer Woche (7 Kalendertage) zuzuleiten (siehe auch Punkt 5!).

4.4 Erst wenn der DSB den Erhalt der Bögen für die einzelne neue Mitarbeiter*in mit einer E-Mail bestätigt, gilt die Unterlage als ordnungsgemäß zugestellt. **Bleibt diese Bestätigung innerhalb einer Woche (nach dem (vermeintlichen) Zugang) aus, wird ein Versäumnis der Verantwortlichen angenommen.**

4.5 Im Falle längerer urlaubs- oder krankheitsbedingter Abwesenheit des DSB wird diesbezüglich per Rundmail informiert. Die entsprechende Bestätigungsfrist (4.4) gilt dann als stillschweigend bis zur Arbeitsaufnahme des DSB verlängert.

4.6 Diese Dienstanweisung ist verbindlich einmal im Jahr als Grundlage einer aktenkundigen Belehrung aller Mitarbeiter*innen heranzuziehen.

4.7 Verantwortlichkeiten:

- im Bereich Kindertagesstätten obliegt diese Aufgabe den jeweiligen Kitaleiter*innen oder den hausintern beauftragten Kräften für Belehrungen
- im Bereich Projekte zeichnen die jeweiligen Q-Teamleiter*innen verantwortlich
- im Bereich Verwaltung / GS wird diese Aufgabe durch den DSB realisiert

4.8 Der DSB ist, ausnahmslos, über den Termin der entsprechenden Belehrung im Vorfeld, mindestens aber eine Woche (7 Kalendertage) vorher, zu informieren.

4.9 Mitarbeiter*innen die zum genannten Termin nicht belehrt wurden, sind innerhalb von maximal vier Wochen aktenkundig nach zu belehren. Sollte dies auf Grund von längerer Erkrankung der Mitarbeiter*in nicht möglich sein, ist dies unmittelbar nach der (Wieder)Arbeitsaufnahme zu realisieren.

4.10 Die entsprechenden Unterschriftenlisten werden in Kopie in der Kita oder bei den Q-Teamleiter*innen archiviert. Das Original ist dem DSB unaufgefordert und nach den Vorgaben unter Punkt 4.3 (und Punkt 5) zuzuleiten.

4.11 Unterbleibt die Belehrung, ist die Belehrung als unzureichend anzusehen, wurden Mitarbeiter*innen nicht nachbelehrt oder es fehlen Unterschriften, **stellt dies ein schweres Versäumnis der Verantwortlichen dar.** Die formelle Umsetzung der Belehrung obliegt den Verantwortlichen selbst. Am zweckmäßigsten scheint aber die Vorgabe an die Mitarbeiter*innen, sich im Vorfeld der Beratung / Sitzung mit der DA (wieder) zu beschäftigen (diese durchzulesen) und dann zum Termin gemeinsam darüber zu diskutieren. Andere Verfahrensweisen sind möglich, wenn der Zweck -Die fundierte Wiederauffrischung der Datenschutzvorgaben- erfüllt wird.

4.12 Zusätzlich zu den voranstehenden Vorschriften, ist der DSB verbindlich mindestens einmal im Jahr in jede Kindertageseinrichtung, den Hort oder die Q-Teams einzuladen. Zu diesem Termin soll über aktuelle Probleme und Fragestellungen diskutiert werden. Vorschläge zu Themen können sowohl vom Team als auch vom DSB eingebracht werden. Hiermit soll sichergestellt werden, dass der Datenschutz wenigstens halbjährlich Thema ist und bei allen Mitarbeiter*innen präsent bleibt.

Davon unberührt bleiben aktuelle Ereignisse die eine Einbeziehung des DSB auch häufiger notwendig machen können, bzw. das ständige Kontrollrecht des DSB.

4.13 Auch (Kurzzeit)Praktikant*innen, Hospitant*innen oder kurzfristige Projektmitarbeiter*innen (wenn sie Zugang zu pbD haben (oder haben könnten)) sind aktenkundig auf die Wahrung des Datengeheimnisses zu verpflichten. Dazu ist das betriebsübliche Formular zu verwenden. Das Dokument ist im Original in der Kita oder der direkten Einsatzstelle zu archivieren. Eine Kopie an den DSB ist in diesem Fall nicht notwendig.

5 Kommunikation mit dem DSB / Terminsetzung und Fristen

5.1 Bei der Einreichung von Unterlagen wird die Büroadresse des DSB (siehe Ende des Dokuments) als sicherste und angestrebte Variante angesehen. Die Ablage von Unterlagen im Fach in der Geschäftsstelle (GS), die Versendung an die Postadresse der GS oder die Übergabe durch Beauftragte ist aus verfahrenstechnischen und datenschutzrechtlichen Gründen als nicht sicher einzustufen.
Hier gehen die Verantwortlichen ein (vermeidbares) Risiko des Versäumnisses ein!

5.2 Vom DSB genannte Termine sind nach Möglichkeit immer mit einer großzügigen Frist gesetzt.
Bei Notwendigkeit sind aber auch (sehr) kurzfristige Terminsetzungen möglich. In jedem Fall sind die genannten Fristen jedoch verbindlich und von der Mitarbeiter*in / den Verantwortlichen unbedingt einzuhalten. Abweichende Lösungen von dieser Grundregel können nur individuell mit dem DSB vereinbart werden.

5.3 Es wird mit Inkrafttreten dieser Dienstanweisung grundsätzlich **KEINE Erinnerungen mehr an Fristen** geben! Die Mitarbeiter*in / die Verantwortlichen ist (sind) verpflichtet innerhalb gesetzter Fristen die geforderten Maßnahmen zu treffen bzw. Unterlagen beizubringen. **Ansonsten stellen Fristversäumnisse schwerwiegende Verletzungen im Sinne dieser Dienstanweisung dar und können dienstrechtliche Konsequenzen nach sich ziehen!**

5.4 Darüber hinaus hat jede Mitarbeiter*in das Recht sich jederzeit und in jeder Form an den DSB zu wenden. Anfragen werden, so es gewünscht wird und die Umstände es zulassen, anonym behandelt.
Die Vertraulichkeit wird seitens des DSB als wichtiges Gut angesehen und dementsprechend gewürdigt.
Ferner stellt es keine Verletzung des Dienstweges dar, den DSB direkt zu kontaktieren und einzubeziehen.

Fälle in denen der DSB verpflichtend zu kontaktieren ist werden im weiteren Verlauf dieser Dienstanweisung behandelt.

6 Technisch Organisatorische Maßnahmen (TOM)

6.1 Bauliche Maßnahmen

6.1.1 Beim Vorhandensein einer Alarmanlage (deren Betreiber die KV ist, also z.B. nicht die Schule) sind die Leiter*innen / Projektleiter*innen verpflichtet, diese in funktionstüchtigem Zustand zu halten bzw. halten zu lassen (z.B. durch regelmäßige Wartung und ggf. Funktionstests).

6.1.2 Die Aufstellung eines funktionierenden Alarmverfahrens ist zwingend erforderlich. Also was passiert im Alarmfall (Zuständigkeiten von Mitarbeiter*innen, Wachschutz etc.).

6.1.3 Videoüberwachungsanlagen müssen zwingend beim DSB beantragt werden. Dieser wird die Notwendigkeit und die Voraussetzungen für einen Betrieb in einem gesonderten Verfahren prüfen und mit Auflagen genehmigen bzw. den Betrieb untersagen. Das Betreiben einer Videoüberwachung ist unter engen Voraussetzungen möglich, jedoch in der KINDERVEREINIGUNG® Leipzig e.V. kein angestrebtes Mittel.

6.1.4 Der DSB hat jederzeit das Recht, den Betrieb genehmigter Anlagen mit Begründung zu wiederrufen.

6.1.5 Der Betrieb von nichtgenehmigten Anlagen, die Aufstellung von (echtwirkenden) Attrappen oder die Nichteinhaltung von Auflagen stellen schwerwiegende Verstöße im Sinne dieser Dienstanweisung dar.

6.1.6 Analoge Datenbestände und EDV sind auf geeignete Weise vor Beschädigung oder Verlust, auch insbesondere durch Wassereintritt, Verwitterung oder möglichen Brandgefahren, zu sichern.

6.2 Arbeitsorganisatorische Maßnahmen

6.2.1 Jede Mitarbeiter*in stellt sicher, dass der Zugang zu personenbezogenen Daten nur berechtigten Personen möglich ist. Dies meint sowohl analoge Daten (Akten, Papiere, Ausdrucke, handschriftliche Dokumente, Fotos etc. als auch Daten in jedweder digitalen Form (auf PCs, Laptops, externen Datenträgern, CDs und DVDs usw.).

6.2.2. Es soll hierbei der Zugang insofern beschränkt sein, dass verhindert werden kann, dass pbD gestohlen, unberechtigt verwendet, manipuliert oder zerstört werden.

6.2.3 Achten Sie daher besonders auf:

- den (mehrfachen) Verschluss von Eingangstüren, Zwischentüren, Büros, Schränken, Archiven oder Bereichen in denen pbD lagern (in jedem Falle bei Abwesenheit und sinnvoller Weise in Teilen auch bei der täglichen Arbeit)
- halten Sie die entsprechenden Schließanlagen in Funktion, ergänzen ggf. Schlösser an Schränken etc. und tauschen Schlösser bei dem Verdacht auf einen (möglichen) Missbrauch aus, achten Sie auf den Verschluss von Fenstern bei Abwesenheit / Verlassen von Räumen, insbesondere auch zu Büros, Aktenlagern oder anderen Bereichen in den pbD lagern
- achten Sie auf (mögliche) unberechtigte Personen in teilöffentlichen und nichtöffentlichen Bereichen
- achten Sie auch auf Dienstleister die sich für beauftragte Arbeiten im Haus / Projekt aufhalten

6.2.4 Büros und Arbeitsplätze in (Gruppen)Räumen, auch temporäre Arbeitsplätze durch Laptops sind nach Möglichkeit so zu gestalten und zu nutzen, dass die unter **3 f** und **6.2.2** genannten Szenarien durch unberechtigte Dritte nicht möglich sind. Lassen Sie keine Papiere, Datenträger etc. offen zugänglich liegen und verhindern Sie (nach Möglichkeit) die Einsichtnahme auf Bildschirme.

6.2.5 Achten Sie auch auf Vertraulichkeit von Gesprächen.

6.2.6. Generell ist darauf zu achten, dass insbesondere die täglichen Arbeitsunterlagen (Papiere), Laptops, Fotokameras, mobile Datenspeicher etc. spätestens bei Arbeitsende auf geeignete Weise unter Verschluss zu bringen sind.

6.2.7 Aushänge, Fotos, digitale Bilderrahmen, Einrichtungen zum Abspielen von Videos etc. (mit pbD) müssen so angebracht sein, dass ein Entwenden der Sache an sich bzw. Teilen davon (insbesondere von Speichermedien) nicht möglich ist.

6.2.8 Mit Inkrafttreten dieser Dienstanweisung gilt in den Kindertagesstätten und dem Hort der KINDERVEREINIGUNG® Leipzig e.V. ein allgemeines Fotografie Verbot für alle nicht bei der KV beschäftigten Personen. Über dieses Verbot sind alle Außenstehenden in geeignete Weise (Schilder) zu informieren und dieser Umstand ist zukünftig in die Elternverträge / Elterngespräche zu implementieren.

6.2.9 Jede Mitarbeiter*in hat die Verpflichtung, auf Verstöße gegen das allgemeine Fotografie Verbot in den genannten Einrichtungen zu achten, bzw. das mögliche illegale Kopieren von pbD (abfotografieren von Inhalten) zu unterbinden und beides ggf. auf dem Dienstweg oder dem DSB zu melden.

6.2.10 Bei Veranstaltungen (sowohl im Innen- als auch im Außenbereich) kann durch Einzelfallentscheidung der jeweiligen Kitaleiter*in vom Fotografie Verbot abgewichen werden. Voraussetzung ist, dass mit Maßgabe der EU DS-GVO, der Datenschutzleitlinie der KINDERVEREINIGUNG® Leipzig e.V., dieser Dienstanweisung und dem pädagogischen Konzept des Hauses die Rechte des Einzelnen, nach Treu und Glauben, in ausreichendem Maße gewürdigt und geschützt werden.

6.2.11 Ein Fotografie Verbot soll auch in anderen Einrichtungen und (oder bei) Projekten gelten, wenn der Schutz der persönlichen Einzelinteressen von Besuchern, Kunden, Klienten oder Mitarbeiter*innen im Einzelfall höher zu bewerten ist als der Wunsch von Dritten bzw. der Allgemeinheit zur fotografischen Dokumentation. Diese Entscheidung soll die jeweils verantwortliche Mitarbeiter*in unter Berücksichtigung pädagogischer Aufgaben und Erfordernisse und mit „Augenmaß“ treffen. Auf Wunsch kann auch der DSB im Vorfeld zu Rate gezogen werden.

6.2.12 Die Kita Leiter*innen und Projektleiter*innen in Häusern mit mehreren Mitarbeitenden sind angehalten, den Zugang zu pbD auch für die Mitarbeiter*innen so zu organisieren, dass in jedem Bereich entsprechend der pädagogischen Konzeption oder der Rahmenvereinbarung frei und vollumfänglich gearbeitet werden kann. Jedoch muss der Zugriff auf pbD, die nicht zur unmittelbaren Erfüllung der Arbeitsaufgabe der einzelnen Mitarbeiter*in oder einer Gruppe von Mitarbeitenden notwendig sind, eingeschränkt oder unterbunden sein. Dies gilt in besonderem Maße für Praktikant*innen und Bundesfreiwilligendienstleistende.

7 Verarbeitung / Lagerung von Daten außerhalb der KINDERVEREINIGUNG®

7.1. Dienstliche pbD verlassen den Einflussbereich der KINDERVEREINIGUNG® Leipzig e.V. nicht!
Als Einflussbereich gelten dabei alle Betriebsstätten der KV und elektronische Server die von der KV betrieben werden bzw. Server mit deren Anbietern ein Vertrag zu Auftragsverarbeitung geschlossen wurde.

7.2. Der Mitarbeiter*in ist es grundsätzlich untersagt, pbD außerhalb der Einrichtungen und Projekte der KV zu verarbeiten oder zu lagern. Dies gilt sowohl für analoge als auch digital gespeicherte Daten.

7.3 Insbesondere und ausnahmslos ist es nicht gestattet Portfolios, Entwicklungsberichte, Kinderakten, Schülerakten, Einschätzungen, § 8a Unterlagen, Personalakten, Sozialdaten, Gesundheitsdaten, Mitarbeiterdaten, Zeugnisse, Bewerbungen, Teilnehmerlisten, Adressdaten(banken), Fotos, Videos und sämtliche Daten außerhalb von dienstlichen Räumen zu verarbeiten und zu lagern, die Schutzbefohlene, Klienten (Kunden), Mitarbeiter, Geschäfts- oder Kooperationspartner und sonstige Dritte identifizierbar machen.

7.4 Daten die nicht unter die in 7.3 genannte Kategorien fallen sind z.B. (anonymisierte) Statistiken, Berichte, Anträge, Projektbeschreibungen, Protokolle etc., immer ohne Personenbezug.

7.5 Ebenfalls ausgenommen ist die Mitarbeiter*in mit arbeitsvertraglich vereinbartem Home-Office (auch zeitweise), dass Art und Umfang der zu erbringenden Tätigkeit und die dafür benötigten Daten(Kategorien) klar beschreibt.

Weitere Vorschriften und Ausnahmen Punkt 11.

8 Telekommunikationssicherheit

8.1 Achten Sie auf die Vertraulichkeit von Telefongesprächen. Führen Sie Telefonate nach Möglichkeit nur in geschlossene Räumen und / oder geschützten Arbeitsabläufen.

8.2 Verwenden Sie nur dienstliche, von der KV zur Verfügung gestellte Anlagen und mobile Endgeräte.
8.3 Stellen Sie Anlagen (Telefone und Anrufbeantworter) so auf, dass ein Mithören bei Aufzeichnungen oder die missbräuchliche Verwendung nicht möglich sind. Verhindern Sie nicht autorisierte Fernabfragen oder Zugriffe von außen (AB).

8.4 Geben Sie grundsätzlich keine Auskunft am Telefon zu pbD, wenn die Identität der Anrufer*in nicht zweifelsfrei (ohne jeden Zweifel) feststeht und nur dann wenn die anrufende Person auch eine berechtigte Person (für den Empfang der Daten) ist.

9 IT-Sicherheit allgemein

9.1 Netzwerke / Internet(Nutzung)

9.1.1 Jede Mitarbeiter*in trägt unabhängig von Leitungs- oder Bereichsverantwortung durch eine stets umsichtige Arbeitsweise auch zur Sicherheit im IT-Bereich bei.

9.1.2 Die vom Arbeitgeber zur Verfügung gestellte IT-Technik (Netzwerktechnik, Server, PCs, Laptops, Smartphones, externe Speicher etc.) ist immer nur bestimmungsgerecht und für dienstliche Zwecke zu verwenden.

9.1.3 Leiter*innen / Projektleiter*innen sind verantwortlich, im Zusammenwirken mit Dienstleistern oder fachkundigen Personen, in den jeweiligen Einrichtungen / Projekten ein Höchstmaß an Netzwerksicherheit herzustellen und zu erhalten. Dazu zählt insbesondere:

- das Stilllegen von nicht benötigten Netzwerkdosen (LAN Dosen), besonders in öffentlichen und teilöffentlichen Bereichen
- die Abschaltung von W-LAN Netzwerken, wenn diese nicht benötigt werden
- bei aktivem W-LAN Netz ist (dauerhaft) die Verschlüsselung WPA2 einzustellen (siehe auch 9.2)
- die Herausgabe von Zugangsdaten zu W-LAN Netzwerken ist nur an berechtigte Personen zulässig, insbesondere darf Kindern und Jugendlichen, Besuchern und betriebsfremden Personen kein Zugang zu Netzwerken gestattet werden

9.1.4 Wenn sich im Einzelfall der Zugang zu Netzwerken für Kinder und Jugendliche, sowie Besucher aus pädagogischen Gründen und / oder für Projekte notwendig macht, ist die betreuende Mitarbeiter*in für die bestimmungsgerechte Nutzung des Netzwerkzugangs verantwortlich. Es ist auszuschließen, dass auf sämtliche Daten, die nicht unmittelbar zum Projekt / zur Aufgabe gehören, zugegriffen werden kann.

9.1.5 Wird Kindern, Jugendlichen und / oder Besuchern der Zugang zum Internet ermöglicht, sind diese auf geeignete Weise zu belehren, dass insbesondere keine illegalen, gesellschaftlich unerwünschte oder dem Leitbild der KINDERVEREINIGUNG® Leipzig e.V. wiedersprechende Aktivitäten gestattet sind. Dies können zum Beispiel sein:

- das Herunterladen oder das zur Verfügung stellen, sowie die Vervielfältigung von urheberrechtlich geschützten Inhalten (Bilder, Videos, Musik, Spielen, Texten, Tonaufnahmen etc.) auf illegalen Plattformen, im sogenannten „Darknet“, aber auch über Clouds (Internetspeicher), in sozialen Netzwerken, über eigene Internetseiten oder auf andere Weise

- der Konsum und / oder die Verbreitung von radikalen politischen oder gesellschaftlichen, pornografischen oder in anderer Weise anstößigen Inhalten bzw. Angeboten
- Aktivitäten die Mobbing, Verleumdung oder üble Nachrede darstellen (könnten) und / oder in anderer Weise geeignet sind Personen zu schmähen, herabzuwürdigen, zu beleidigen oder auszugrenzen

Die Aufzählung ist nicht vollständig. Maßgeblich sind die einschlägigen Gesetze und Vorschriften, das Leitbild der KINDERVEREINIGUNG® Leipzig e.V., pädagogische Grundprinzipien, bestehende Dienstanweisungen, erarbeitete Standards der Fachberatungen und der Q-Teams, der insoweit erfahrenen Fachkräfte nach § 8a.

9.1.6 Jeder Mitarbeiter*in sind die unter 9.1.5 genannten Aktivitäten ebenfalls strikt untersagt.

9.1.7 Ferner wird hier Bezug auf die Dienstanweisung **KVL DA 08-2013** (Sicherheitsrichtlinie für die Internet- und E-Mail-Nutzung) genommen, die parallel zu dieser Dienstanweisung weiterhin Gültigkeit hat.

9.2 Passwörter / Benutzerkonten

9.2.1 Geräte, Konten, Anwendungen etc. mit denen pbD verarbeitet und gespeichert werden, und die einen Passwortschutz zulassen, sind auch durch Passwörter (PW) zu schützen.

9.2.2 Passwörter sind nur berechtigten Personen zugänglich zu machen. Es ist der Sinn von Passwörtern bestimmte Personen oder unbestimmte Dritte „auszusperren“. PW dürfen nicht notiert und für unberechtigte Dritte zugänglich sein. Ein Klassiker wäre zum Beispiel auf einem Klebezettel unter der Tastatur. Diese und ähnliche Vorgehensweisen werden als grob fahrlässig angesehen.

9.2.3 Passwörter müssen mindestens 8 Zeichen lang sein, aus Klein- und Großbuchstaben, Zahlen und / oder Sonderzeichen bestehen. Sie dürfen nicht „leicht zu erraten“ sein. Persönliche Daten (z.B. Geburtstag), einfache Zahlenfolgen (123456…), das Wort „Passwort“ o.ä. sind nicht zulässig.

9.2.4 Das gleiche PW darf nicht für einen oder mehrere andere Zugänge genutzt werden.

9.2.5 PW müssen regelmäßig geändert werden. Vorschrift ist hiermit einmal im Jahr auch ohne Anlass. Unverzüglich (also ohne schuldhaftes Zögern) müssen Passwörter aber geändert werden, wenn:

- der Verdacht besteht, dass diese ausgespäht oder „gehackt“ wurden
- offensichtlich Veränderungen an Daten stattgefunden haben, die nicht anders zu erklären sind
- nach Wiederübernahme der EDV nach einer Vertretung (Urlaub, Krankheit)
- wenn Mitarbeitende den Arbeitsbereich verlassen oder aus der KINDERVEREINIGUNG® ausscheiden und somit nicht mehr zugriffsberechtigt sind

9.2.6 Jede Mitarbeiter*in, insbesondere aber Leiter*innen / Projektleiter*innen sind für die Passwortsicherheit und die Einhaltung vorstehender Regelungen verantwortlich.

9.2.7 Jede Mitarbeiter*in soll generell an dienstlicher EDV mit einem eigenen Benutzerkonto arbeiten. Ausgenommen hiervon sind sich typischer Weise vertretende Mitarbeiter*innen. Diese Situation wird ständig bei Leiter*innen und stellvertretenden Leiter*innen angenommen. Ebenfalls ausgenommen sind Situationen in denen anderenfalls die gestellten dienstlichen Aufgaben nicht oder nicht richtig erledigt werden können, weil der gemeinsame Zugriff auf Daten dafür absolut notwendig ist.

9.2.8 Es muss in der täglichen Arbeit darauf geachtet werden, um den Schutz pbD zu gewährleisten, dass beim Verlassen von Büroräumen und (mobilen) EDV Arbeitsplätzen zu mindestens eine Abmeldung vom Benutzerkonto erfolgt. Unter Umständen ist das Herunterfahren des gesamten Systems durchzuführen. Zudem sind ggf. die Vorschriften unter Punkt 6 (TOM) zu beachten und anzuwenden.

Zugang zu Passwort-geschützten dienstlich Daten siehe auch Punkt 17.4 Verfügbarkeit

9.3 Software- und Hardwaredoktrin

9.3.1 Die Mitarbeiter*in ist verpflichtet auf bestehende Probleme bei dienstlicher EDV-Technik hinzuweisen. Dies gilt insbesondere bei stark veralteten PC bzw. Laptops, bei denen angenommen werden muss, dass diese nicht mehr bzw. nicht mehr lange den Anforderungen für moderne Betriebssysteme, Sicherheitssoftware und Sicherungslösungen entsprechen. Dieser Hinweis soll parallel an den / die direkten Vorgesetzten und den DSB gehen. Ziel ist ein alsbaldiger Austausch der veralteten EDV.

9.3.2 Mit Inkrafttreten dieser Dienstanweisung werden nur noch die Betriebssysteme ab Windows 7 als sicher angesehen und sind zur Nutzung zugelassen. Windows Vista, XP, ME, 98 und 95 dürfen auf keinerlei dienstlichen Systemen verwendet werden, auf denen pbD verarbeitet und / oder gespeichert werden. Ausgenommen hiervon sind Systeme die als reine „Spiele PCs“ für Kinder, Jugendliche und Besucher genutzt werden.

9.3.3 Benutzer (Einzahl und Mehrzahl) sind ausnahmslos als lokale Konten anzulegen. Sprich es erfolgt keine Einrichtung der Benutzer mit einem Microsoft (Online)Konto.

9.3.4 Auf allen dienstlichen EDV Systemen, auf denen pbD verarbeitet und / oder gespeichert werden, ist ausnahmslos eine Firewall zu installieren und zu betreiben (ab Windows 7 im Betriebssystem integriert, aber auch der Betrieb eigenständiger Software ist möglich).

9.3.5 Auf allen dienstlichen EDV Systemen, auf denen pbD verarbeitet und / oder gespeichert werden, sind ausnahmslos Antivirenprogramme zu installieren und zu betreiben. Außerdem müssen die Virendefinitionen ständig aktuell gehalten werden. Dies ist nur mit einer (ständigen bzw. temporären) Internetverbindung zu realisieren.

9.3.6 Jede Mitarbeiter*in ist verpflichtet bei der Nutzung von „fremder Hardware“ wie USB Sticks, externen Festplatten etc. bzw. bei Datenträgern aus fremden Quellen besondere Vorsicht walten zu lassen, um mögliche Infektionen mit Schadsoftware von dienstlichen Systemen zu verhindern.

9.3.7 Die Installation von Software aus unbekannten oder nicht vertrauenswürdigen Quellen ist strikt untersagt. Die Sicherheit dienstlicher Systeme muss zu jeder Zeit gewährleistet sein.

9.3.8 Anwenden (Software / Programme), insbesondere Browser, E-Mailprogramme, Office Anwendungen, Multimediaprogramme, Flashanwendungen etc., sind stets aktuell zu halten und mit den neuesten Sicherheitsfeatures auszustatten. Dies ist über die eingebauten Optionen (auf Updates prüfen / Sicherheitsupdates laden etc.) zu realisieren.

9.3.9 Ermüdungsanzeichen oder erste Ausfallerscheinungen von EDV, die auf technische Ursachen zurückzuführen sein könnten (Festplattendefekte etc.), sind wichtige Alarmsignale und müssen unverzüglich zu Sicherungsmaßnahmen der pbD seitens der verantwortlichen Mitarbeiter*in führen.

10 E-Maildoktrin

10.1 Dienstliche Kommunikation darf ausschließlich nur über dienstliche E-Mailadressen erfolgen!
Die Verwendung von privaten E-Mailadressen für dienstliche Belange ist strikt untersagt. In Einrichtungen / Projekten mit mehreren Mitarbeitenden sind Maßnahmen zu treffen, die es jeder Mitarbeiter*in ermöglichen dienstliche E-Mailadressen zu nutzen, wenn dies für die Erfüllung ihrer Arbeitsaufgaben notwendig ist oder zweckmäßig erscheint.

10.2 Jede ausgehende E-Mail enthält ein korrektes Impressum. Stellen Sie sowohl die entsprechenden Angaben ihrer Einrichtung / Projektes als auch die Angaben der KINDERVEREINIGUNG® Leipzig e.V. zur Verfügung.
Vorgabe:

- IMPRESSUM -

KINDERVEREINIGUNG® Leipzig e.V.
Einrichtung / Projekt ...
Vorname, Name, Funktion
Adresse ...
Tel.: ...
Fax.: ... (wenn vorhanden)
E-Mail: ...
Web: ... (wenn vorhanden)

KINDERVEREINIGUNG® Leipzig e.V.
Frohburger Straße 33c
04277 Leipzig
Tel.: 0341 / 2257440
Fax.: 0341 / 22574410
E-Mail: gs@kv-leipzig.de
Web: www.kv-leipzig.de
VR-Nr.: 1291 Amtsgericht Leipzig
St.-Nr.: 231/140/01023
Geschäftsführer: Matthias Heinz
Vorstandsvorsitzender: Stefan Schaller

10.3 Jede E-Mail enthält einen Vertraulichkeitshinweis in deutscher und optional in englischer Sprache.
Vorgabe:

Diese E-Mail einschließlich ihrer Anlagen ist nur für den Adressaten bestimmt. Die Information in dieser E-Mail ist vertraulich und kann dem Berufsgeheimnis unterliegen. Wenn Sie nicht der vorgesehene Empfänger sind, bitten wir Sie, diese E-Mail mit Anlagen unverzüglich vollständig zu löschen und uns umgehend zu benachrichtigen. Jede Veröffentlichung, Vervielfältigung oder Weitergabe ist untersagt.

This e-mail and its attachements are intended solely for the attention of the person to which it is addressed. The information in this e-mail is strictly confidential and may be legally privileged. If you are not the intended recipient of this e-mail, please delete this message including its attachements immediately and inform us accordingly. Any disclosure, copying or distribution is prohibited and may be unlawful.

10.4 Aus jeder E-Mail in der Außenkommunikation geht hervor wer die Verfasser*in der Nachricht ist. Dies soll, durch die Nennung des vollständigen Namens und der Funktion im Verein, in der Nachricht bei der Grußformel erfolgen. Dies gilt insbesondere für den Fall, dass sich Mitarbeiter*innen E-Mailadressen teilen. Ist die Verfasser*in der Nachricht identisch mit der mit vollständigem Namen und Funktion genannten Mitarbeiter*in im Impressum kann hier in sinnvoller Weise abgewichen werden.

10.5 Es soll stets darauf geachtet werden, dass E-Mails nur die gewünschten Adressaten erreichen. Von daher ist zur Vorsicht bei der Autovervollständigungsfunktion von Adressen zu raten. Verteilerlisten sind stets aktuell zu halten, so dass keine nicht mehr berechtigten Empfänger angesprochen werden.

10.6 Wenn auf Nachrichten geantwortet wird bzw. sie sollen weitergeleitet werden, ist zu überprüfen ob die Empfängerliste (einzelne Person oder mehrere Empfänger) so gewollt ist, oder ob Anpassungen hinsichtlich der Adressaten und / oder die Entfernung von (Teil)Inhalt sinnvoll erscheint.
Gegeben falls ist auch die Funktion Bcc (Blindkopie) des Mailprogrammes einzusetzen, wenn nicht ersichtlich sein soll wer zur Empfängerliste gehört.

10.7 Jede Mitarbeiter*in ist verpflichtet, insbesondere die „Viren-Freiheit“ ausgehender Dateianhänge zu gewährleisten (Einstellung im Virenprogramm). Überdies ist jede Mitarbeiter*in angehalten besondere Obacht bei eingehenden E-Mailanhängen bzw. Links in Nachrichten walten zu lassen, um die Sicherheit dienstlicher Systeme nicht zu gefährden. Verdächtige Nachrichten, Absender oder offensichtlicher Spam ist sofort zu löschen. Im Zweifelsfall sollen fachkundige Personen zu Rate gezogen werden.
10.8 Geben Sie grundsätzlich keine Auskunft zu pbD per E-Mail, wenn die Identität und die Berechtigung der schreibenden Person nicht zweifelsfrei (ohne jeden Zweifel) feststehen.

10.9 Ferner wird hier Bezug auf die Dienstanweisung **KVL DA 08-2013** (Sicherheitsrichtlinie für die Internet- und E-Mail-Nutzung) genommen, die parallel zu dieser Dienstanweisung weiter Gültigkeit hat.

11 Besondere Vorschriften zu IT und Smart Technik, Applikationen, Clouds, Datenspeichern, Providern, Internetangeboten und Internetdiensten, sowie Presse- und Öffentlichkeitsarbeit

11.1 Ortsbindung dienstlicher EDV

11.1.1 Es ist nicht gestattet, dienstlich zur Verfügung gestellte EDV Technik aus den Betriebsstätten der KINDERVEREINIGUNG® Leipzig e.V. zu entfernen und an andere Orte zu verbringen. Eventuell notwendige Reparaturen an der EDV sollten immer im Haus und unter Aufsicht stattfinden. Ist dies im Einzelfall nicht möglich, sind aber besondere Vorsichtsmaßnahmen zu treffen, die den unberechtigten Zugriff auf pbD verhindern. Zum Beispiel der Ausbau der Festplatte (wenn dies sinnvoll ist), die vorherige Sicherung der Daten (wenn dies noch möglich ist) und die Mitgabe des Systems ohne kritische Inhalte oder beaufsichtigte Reparaturen außer Haus. Im Übrigen sollen nur vertrauenswürdige Dienstleister / Fachwerkstätten mit Reparaturen betraut werden.

11.1.2 Wie unter Punkt 7 genannt, verlassen dienstliche pbD den Einflussbereich der KV nicht. Dies gilt auch für auf mobiler EDV (Laptops / Tablets) gespeicherte Daten. Das heißt, die Mitnahme auch von Laptops / Tablets mit personenbezogenen Inhalten ist erst einmal grundsätzlich nicht gestattet. Ausgenommen sind Mitarbeiter*innen mit arbeitsvertraglich vereinbartem Home-Office.

11.1.3 Ausgenommen vom Mitnahmeverbot sind auch Systeme auf denen keine pbD gespeichert sind.

11.1.4 Ausgenommen vom Mitnahmeverbot sind auch Systeme auf denen zwar pbD gespeichert sind, dies aber nur **(A)** wenn die Erfüllung dienstlicher Aufgaben anders nicht möglich wäre und die Daten auf das Maß für die im konkreten Einzelfall zu erledigende Arbeitsaufgabe beschränkt sind **und** nur in Verbindung mit den Tatsachen, dass **(B)** die Mitnahme lediglich in Ausnahmefällen stattfindet und **(C)** der Einsatzort entweder zum Einflussbereich der KV gehört, bei Kooperationspartnern, Projektpartnern oder für die Arbeit einschlägigen Ämtern und Behörden ist, bzw. die Privatadresse der Mitarbeiter*in ist.

11.1.4.1 Diese Vorschrift wird nur zu erfüllen sein, wenn sich der komplette (Arbeits)Bestand an pbD auf einem externen Speichermedium (Festplatte, NAS o.ä.) befindet, dass in der Einrichtung / Projekt verbleibt und die pbD die auf dem Laptop mitgenommen werden sollen auf das Maß beschränkt sind, dass der konkrete dienstliche Anlass rechtfertigt und der Einsatzort ansonsten nicht im „öffentlichen Raum“ liegt. Eine weitere (die Beste) Möglichkeit ist, dass ein verschlüsseltes Gerät zum Einsatz kommt, dies stellt den wirksamsten Schutz von pbD im Falle eines Verlustes des Gerätes dar!

11.1.5 Jede Mitarbeiter*in ist überdies verpflichtet, wenn eine Mitnahme von EDV erfolgt, geeignete Sicherheitsmaßnahmen zu treffen, die den Verlust von pbD verhindern. Als Mindestanforderungen gelten hierbei:

- der gesicherte Transport und Betrieb, sprich es muss verhindert werden, dass die Hardware während des Transportes oder am Einsatzort gestohlen wird
- dass die Einsichtnahme oder der Diebstahl von pbD durch unberechtigten Dritten während des Arbeitens verhindert wird
- dass die Systemintegrität gewährleistet ist, sprich es darf nicht möglich sein, dass das Gerät in irgendeiner Weise von unberechtigten Dritten manipuliert oder mit Schadsoftware infiziert wird
- dass das Gerät passwortgeschützt ist
- und unmittelbar nach Beendigung bzw. bei Unterbrechung der Arbeit heruntergefahren wird (damit der Passwortschutz greift)

11.1.6 Jede Mitarbeiter*in ist verpflichtet, dienstliche EDV nach dem außer Haus Einsatz schnellstmöglich wieder in den Einflussbereich der KV zu verbringen.

11.1.7 Mitarbeiter*innen die dienstliche EDV häufiger oder regelmäßig*(2) außerhalb des Einflussbereiches der KV benutzen, sind zusätzlich zu den voranstehenden Punkten unter 11 verpflichtet, das entsprechende Gerät oder die Bereiche mit pbD auf geeignete Weise zu verschlüsseln und beim DSB zur Abnahme vorzustellen.

**(2) alle Mitarbeiter*innen die im Datenschutzfragebogen 2017 bei der Frage 11 den Punkt „häufiger oder regelmäßig" angekreuzt haben*

11.1.8 Bestandsmitarbeiter*innen und neue Mitarbeitende sind verpflichtet, wenn sie nach Inkrafttreten dieser Dienstanweisung, ebenfalls häufiger oder regelmäßig dienstliche EDV (mit pbD) außer Haus nutzen oder nutzen wollen, Punkt 11.1.7 zu erfüllen.

11.1.9 Unabhängig von der Häufigkeit möglicher außer Haus Einsätze von EDV, wird für Laptops und stationäre PCs allgemein eine Verschlüsselung empfohlen. Auch dann ist Punkt 11.1.7 zu erfüllen.

*Jedes Jahr findet eine Schulung des DSB zum Thema Verschlüsselung statt. Alle Mitarbeiter*innen, die mit dienstlicher EDV (mit pbD) arbeiteten, können an der Schulung (Arbeitszeit) teilnehmen. Ziel ist die kontinuierliche Erhöhung verschlüsselter Systeme innerhalb der KV.*

11.1.10 Es ist Vorschrift, dass bei verschlüsselten Geräten der entsprechende Schlüssel und der Wiederherstellungsschlüssel beim DSB hinterlegt sind. Jede Mitarbeiter*in die ein verschlüsseltes dienstliches Gerät betreibt ist verpflichtet dieser Vorschrift nachzukommen. Dies soll sicherstellen, dass auf die dienstlichen Daten, auch nach einem möglichen Personalwechsel bzw. bei längeren Abwesenheitszeiten der Mitarbeiter*in, zugegriffen werden kann. Ausgenommen von dieser Vorschrift sind die Systeme der Geschäftsführung, von leitenden Angestellten (im Sinne des Gesetzes), die EDV des Betriebsrates in dessen Büro und die Systeme des Datenschutzbeauftragten selbst.

11.1.11 Jede Mitarbeiter*in die dienstliche EDV mit pbD außerhalb des Einflussbereiches der KV nutzt, muss im Falle eines Verlustes oder der unberechtigten Kenntnisnahme von pbD (Datenschutzverstöße) den Nachweis führen oder glaubhaft versichern können, dass der Einsatz der EDV außer Haus entsprechend den Vorgaben dieser Dienstanweisung war.

11.2 Mobile Datenspeicher (USB-Sticks / externe Festplatten etc.), die pbD enthalten, sind nur dann außerhalb des Einflussbereiches der KV mitzuführen, wenn dies im Rahmen eines Dienstganges, Dienstweges, einer Dienstreise oder eines sonstigen triftigen dienstlichen Anlasses geschieht. Die auf dem externen Speichermedium gespeicherten Daten sind auf das für die Erfüllung der konkreten Arbeitsaufgabe nötige Maß zu beschränken.

11.2.1 Das ständige Mitführen von größeren Mengen an Daten oder gar von kompletten Datenbeständen auf externen Speichermedien ist strikt untersagt. Dies meint auch sogenannte (Voll- oder Teil-) Backups von Systemen. Die Menge an transportierten Daten auf externen Speichermedien darf nie das notwendige Maß überschreiten, das der konkrete dienstliche Anlass oder eine zielführende Arbeitsweise rechtfertigen.

11.2.2 Jede Mitarbeiter*in ist verpflichtet, wegen der erhörten Wahrscheinlichkeit eines Verlustes von externen Speichermedien bei „losem" Transport, besondere Vorsichtsmaßnahmen zu treffen. Dies meint z.B. die Sicherung mit Bändern, die Anbringung an entsprechende Möglichkeiten in Taschen oder Kleidungsstücken oder die Verwahrung in Etuis die dann wiederum sicher verstaut werden.

11.2.3 Es ist Vorschrift, dass externe Speichermedien die dem Transport von Daten dienen, regelmäßig auf die weitere Notwendigkeit der Speicherung von Daten hin überprüft werden. Das heißt, Daten sollen vom Transportmedium gelöscht werden, wenn die Arbeitsaufgabe erfüllt ist bzw. der Grund für eine weitere Speicherung (auf diesem Medium) weggefallen ist.

11.2.4 Es wird hier ausdrücklich empfohlen, externe Speichermedien zudem zu verschlüsseln und die Zugangsbeschränkung konsequent anzuwenden. Dies stellt den wirksamsten Schutz von pbD im Falle eines Verlustes des Speichermediums dar!

11.3 Der Transport / das Mitführen von analogen Daten (Papieren, Dokumenten etc.) ist sinngemäß der Vorschriften 11.2 - 11.2.3 zu handhaben.

11.4 Clouddienste / Onlinetools

11.4.1 Die Nutzung von Clouddiensten und Internetspeichern wie Google Drive, Dropbox, Microsoft OneDrive oder ähnlichen Diensten ist für dienstliche pbD nicht gestattet. Es dürfen also keinerlei Dokumente oder Dateien in der „Wolke" abgelegt werden, die einen Personenbezug haben.

Siehe auch Punkt 7.

11.4.2 Die Nutzung von Onlinetools zur (reinen) Terminvereinbarung wie z.B. Doodle ist zulässig, solange es sich um Mitarbeiter*innen der KV handelt und dienstliche E-Mailadressen verwendet werden.

11.4.2.1 Wenn unter Nutzung dieser Onlinetools Termine mit unseren Kunden (Zielgruppe) oder mit Eltern bzw. Kooperations- und Geschäftspartnern vereinbart werden sollen, so ist auf geeignete Weise ein grundsätzliches Einverständnis der Betroffenen einzuholen. Liegt dieses Eiverständnis nicht vor oder wird wiederrufen, hat die Kontaktaufnahme mit dieser Möglichkeit zu unterbleiben.

11.5 Dienstliche Smartphones dienen in erster Linie als sprachliche Kommunikationsmittel. Sie sind nicht als Datenspeicher oder EDV Systeme im herkömmlichen Sinne zu verstehen! Die Verwendung als solche (Datenspeicher oder EDV System) soll nur im Ausnahmefall und sinngemäß der Vorschriften 11.2 - 11.2.3 erfolgen. Besonderer Augenmerk soll hierbei auch auf E-Mail Verläufen und Kontaktlisten liegen, die es besonders abzusichern gilt (Vorsicht daher ggf. bei einer möglichen Synchronisation).
Mindestanforderung ist aber eine Sperre des mobilen Endgerätes mit einer PIN die nach dem Bootvorgang und nach kurzer Zeit der Nichtbenutzung des Gerätes aktiv eingegeben werden muss.

11.5.1 Die Verwendung von Messengern wie WhatsApp, Threema oder ähnlichen Applikationen ist für die Verarbeitung von dienstlichen Daten mit Personenbezug nicht gestattet. Das heißt, die Übermittlung von Dokumenten, Dateien, Fotos, Videos, Tonaufnahmen oder anderer Inhalte und Diskussionen über identifizierbare Kunden, Klienten, Schutzbefohlene, deren Eltern und Kolleg*innen hat ausnahmslos zu unterbleiben. Die Übermittlung von pbD über diese Dienste wird als nicht sicher angesehen.

11.5.2 Zur Terminvereinbarung ist die Verwendung von Messengern zulässig, wenn es sich um Mitarbeiter*innen der KV handelt und dienstliche E-Mailadressen verwendet werden. Gleiches gilt für die Verwendung in Zusammenhängen die als dienstlich sinnvoll und arbeitserleichternd anzusehen sind, aber nur, wenn keine pbD über die Namen und dienstlichen E-Mailadressen der Mitarbeiter*innen hinaus verarbeitet (verbreitet) werden.

11.5.3 Der Beitritt zu einer Gruppe oder die Herausgabe einer privaten E-Mailadresse, wenn keine dienstliche E-Mailadresse vorhanden ist (dies ist regelmäßig bei den Erzieher*innen in der Kita der Fall) ist ausnahmslos freiwillig und kann zu keinem Zeitpunkt durch Kolleg*innen oder Vorgesetzte verlangt werden. Auch ist es kategorisch ausgeschlossen, dass die Arbeitsorganisation an sich und in wichtigen Teilen ausschließlich über diese Dienste erfolgt. Erst nach der persönlichen Ansprache, der Team- oder Dienstberatung, dem Aushang und der Kommunikation per dienstlicher E-Mail und auf dem Postweg (für Einreichungen) sind Messenger als nachgeordnetes und lediglich ergänzendes Mittel anzusehen.
Dies gilt im Besonderen für die Bekanntgabe von Dienstplänen, jeglichen Dienst- und arbeitsorganisatorischen Anweisungen, Beantragungen, Krank- oder Gesundmeldungen, pädagogischen Diskussionen oder Kommunikation die zwingend im geschützten Rahmen des Arbeitsumfeldes stattzufinden hat.

11.5.4 Die Verwendung von Messengern zur Terminvereinbarung und zu organisatorischen Zwecken mit unseren Kunden (Zielgruppe) oder mit Eltern bzw. Kooperations- und Geschäftspartnern ist erlaubt, wenn die Ansprache seitens der KV Mitarbeiter*in über eine dienstliche E-Mailadresse erfolgt. Ferner gelten die Bestimmungen hinsichtlich des Einverständnisses von 11.4.2.1 hier gleichlautend.

11.6 Die Nutzung von sogenannten „Smart Speakern“ wie Amazon Echo, Google Home oder ähnlichen Produkten ist in den Einrichtungen der KINDERVEREINIGUNG® Leipzig e.V. nicht gestattet.

11.7 Es ist jeder Mitarbeiter*in untersagt selbstständig und ohne Abstimmung mit dem / der direkten Vorgesetzten und dem DSB **Verträge zum Hosting von Internetseiten** und / oder Blogs etc. abzuschließen und entsprechenden Webspace zu mieten. Hintergrund ist, dass ein Hosting-Anbieter im Sinne des Gesetzes ein sogenannter „Auftragsverarbeiter“ ist. Mit diesen müssen zusätzlich zum Hauptvertrag auch noch gesonderte Verträge zur Auftragsdatenverarbeitung geschlossen werden, die vor allem datenschutzrechtliche Bestimmungen besonders würdigen. Solche Verträge bestehen derzeit mit:

- der Strato AG (Hoster einiger Projektwebseiten und unser E-Mail Anbieter)
- der Mittwald GmbH (Hoster der zentralen Internetseite des Vereins)
- der WebhostOne GmbH (Hoster der Internetseite des Ferienbereiches)
- der Webgo GmbH (Hoster der Internetseiten der Internationalen Arbeit)

11.8 Soziale Medien, Blogs und Internetseiten (Webseiten) der KINDERVEREINIGUNG® Leipzig e.V. dienen als öffentlichkeitswirksame Kommunikationsplattformen des Vereines. Alle Verlautbarungen und Veröffentlichungen müssen im Einklang mit dem Leitbild der KINDERVEREINIGUNG® Leipzig e.V., pädagogischer Grundprinzipien, bestehenden Dienstanweisungen und erarbeiteten Standards der Fachberatungen stehen. Ferner ist stets auch das Corporate Design und die Corporate Identity zu berücksichtigen.

11.8.1 Auf allen Internetseiten, bei allen Blogs und in sozialen Medien ist ein korrektes Impressum (siehe auch 10.2) vorgeschrieben. Darüber hinaus sind auf Webseiten und Blogs die Informationen zum Haftungsausschluss, zum Datenschutz und zum Streitschlichtungsverfahren zu veröffentlichen. Als Vorlage gilt hier das Impressum der zentralen Webseite der KINDERVEREINIGUNG® Leipzig e.V.

11.8.2 Ferner sind auf Webseiten und Blogs die Kontaktdaten des Datenschutzbeauftragten, analog der rechten Seite „Adresse“ unter dem Link Datenschutz auf der zentralen Webseite der KV, zu veröffentlichen.

11.8.3 Insbesondere ist jede Mitarbeiter*in aber verpflichtet die Datenschutzleitlinie der KV zu beachten und auch auszuschließen, dass z.B. Verletzungen von Persönlichkeitsrechten und / oder Verletzungen von Urheberrechten stattfinden.

Siehe auch weiter Punkt 12 Veröffentlichungen und 14 Einwilligung

11.9 Bei öffentlichen **Verlautbarungen in der Presse und den Medien**, sowie bei von der KV herausgegebenen **Drucksachen**, ist darauf zu achten, dass keine pbD „mitveröffentlicht" werden, die nicht Gegenstand der Berichterstattung (Veröffentlichung) sein sollen und / oder für die keine Einwilligung zur Veröffentlichung vorliegt. Ferner gilt Punkt 11.8 hier gleichlautend.
11.9.1 Ferner wird hier auf die Dienstanweisung **KVL DA 01-2016** „Umgang mit der Presse und den Medien" in Bezug genommen, die parallel zu dieser DA Gültigkeit hat.

12 Veröffentlichungen / Abfragen im Haus

12.1 Bei Aushängen, Veröffentlichungen und Informationen im Haus ist stets darauf zu achten, dass die veröffentlichten Inhalte relevant, aktuell und auf das tatsächlich notwendige Maß beschränkt sind. Ferner dürfen Aushänge nur einem berechtigten Personenkreis zugänglich gemacht werden. Dies gilt z.B. auch für Dienstpläne, Urlaubslisten etc.

12.2 Die Veröffentlichung von Angaben zu Kindern (z.B. Geburtstage, Adressen, [Telefonnummern, E-Mail der Eltern]) hat nur in einem pädagogisch und inhaltlich sinnvollen Umfang (Hauskonzept) und mit der allgemeinen Zustimmung der Eltern zu erfolgen. Über die üblichen Formen in den entsprechenden Einrichtungen sollten Eltern im Rahmen von Aufnahmegesprächen (Kita) informiert werden und ihr Einverständnis erklären können. Gleiches gilt für Werke (Arbeiten) der Kinder und die mögliche Veröffentlichung von Tagesdokumentationen oder ähnlichen Einschätzungen (über Kinder). Sinngemäß ist unter Berücksichtigung der entsprechenden Rahmenvereinbarungen in allen Einrichtungen der KV so zu verfahren.

12.3 Keinesfalls dürfen jedoch Angaben zu Kindern **allgemein zugänglich** (für Eltern, Besucher, Dienstleister etc.) ausgehängt werden, die Informationen zu Krankheiten, persönlichen Vorlieben, Essgewohnheiten, religiöser oder weltanschaulicher Zugehörigkeit sind. Von daher ist insbesondere in den Essensräumen der Kitas darauf zu achten, dass diesbezügliche Informationen zwar den Erzieher*innen, Servicekräften und ggf. Vertretungskräften unbedingt zugänglich sind, eine Kenntnisnahme von Unberechtigten aber, soweit dies arbeitsorganisatorisch mit vertretbarem Aufwand zu bewerkstelligen ist, verhindert wird.

12.4 Auch hausinterne und ggf. öffentlichkeitswirksame Veröffentlichungen von Angaben zu Mitarbeiter*innen (vollständiger Name, Fotos, Werke etc.) sollen, so diese nicht zwingend zur Erfüllung von dienstlichen Aufgaben notwendig oder vorgeschrieben sind, auf Freiwilligkeit beruhen.

12.5 Abfragen (und damit verbundene Aushänge bzw. Umlaufpapiere) für z.B. Feste, Teilnehmerlisten und sämtliche Erhebungen die organisatorischen Zwecken dienen, sind so zu gestalten, dass nur aktuell notwendige Angaben abgefragt werden. Jede betreuende Mitarbeiter*in ist verantwortlich sicherzustellen, dass die auf diesem Wege erfassten pbD nicht unberechtigten Dritten zur Kenntnis gelangen (siehe auch 12.2 / 12.3). Im Zweifels- bzw. Bedarfsfall ist von der listenmäßigen Erfassung abzusehen und eine Einzelblatterfassung zu verwenden.

13 Sonderfall Fotoentwicklung außer Haus

13.1 Zur Beauftragung von Entwicklungen / Abzügen von Fotos (mit Personenbezug), ist der Transport von Daten via Datenträger / USB Stick zulässig (siehe 11.2). Die Sicherheitsregeln wie unter 11 beschrieben sind einzuhalten.

13.2 Besonderer Augenmerk muss in diesem Zusammenhang aber auf der Art des Verfahrens liegen. Wenn möglich sollten „Sofortabzüge“ mitgenommen werden. Die Bestellung von Abzügen am Automaten über ein Labor sollte nach Möglichkeit mit der Zusendung der Fotos in die Einrichtung beauftragt werden. Die Bestellung von Abzügen in die Filiale (Drogeriemarkt etc.), die dann dort in offenen Fächern (tagelang) gelagert werden und im Prinzip jedermann zugänglich sind, ist sehr kritisch zu sehen. Hier besteht potentiell die Gefahr von Diebstahl und missbräuchlicher Verwendung.

13.3 Nach Möglichkeit sollte daher zukünftig auf die Onlinebestellung von Fotos ausgewichen werden, die dann auch direkt in die Einrichtung geliefert werden.

14 Einwilligungen

14.1 Grundsätze der informierten Einwilligung *(Auszüge aus dem Gesetzestext EU DS-GVO)*

- Der Einwilligende muss über Identität des Verantwortlichen und möglicher Empfänger, Art, Umfang, Zweck und Rechtsgrundlage, sowie das jederzeitige Widerrufsrecht informiert werden.
- Eine Einwilligung muss in informierter Weise, klarer Sprache, unmissverständlich und frei von Zwängen abgegeben werden (können).
- Die Kopplung der Erbringung vertraglicher Leistungen oder sonstiger Vorteile mit der Erteilung einer datenschutzrechtlichen Einwilligung stellt die Freiwilligkeit in Frage. Dies wird maßgeblich daran gemessen, ob die Vertragserfüllung von der Einwilligung zur Verarbeitung pbD abhängig ist, die für die Erfüllung des Vertrages nicht notwendig sind.
- Die Einwilligung muss sich daher auf sämtliche Verarbeitungszwecke erstrecken und ggf. getrennt voneinander möglich sein.
- Einwilligungen können im Rahmen von AGB erteilt werden, wenn diese klar abgetrennt oder hervorgehoben und allgemein verständlich zur Verfügung gestellt werden.

14.2 Jede Mitarbeiter*in ist verpflichtet, die internen Formulare für Einwilligungen mit der Kennzeichnung **KVL-EW-xx/2018** zu verwenden.

14.3 Einwilligungen haben nach den allgemeinen Archivierungsfristen (Löschfristen, siehe Punkt 18) der KV im Original in der Einrichtung aufbewahrt zu werden.

15 Datenübermittlung an Dritte (Wir = Erste, Betroffene = Zweite, jede andere Stelle / Person = Dritte)

15.1 Die Datenübermittlung an Dritte hat immer nur bei Vorliegen von triftigen Gründen zu erfolgen. Diese Gründe können z.B. sein:

- **A)** die Übermittlung an Dritte ist zur ordnungsgemäßen Vertragserfüllung absolut notwendig
- **B)** es gibt andere (begründbare) berechtigte Interessen der KV (Interessensabwägung)
- **C)** wir sind durch ein Gesetz oder durch eine andere Vorschrift zur Übermittlung und / oder Mitwirkung verpflichtet

15.2 Muss das Einverständnis der Betroffenen eingeholt werden, sind die internen Formulare (siehe 14.2) zu verwenden.

15.3 Im Übrigen gelten unverändert die Vorschriften in Fällen von (möglicher) Kindeswohlgefährdung wie von unseren insoweit erfahrenen Fachkräften nach § 8a aufgestellt.

16 Bewerbungsunterlagen / Personalakten

16.1 Unterlagen zu Bestandsmitarbeiter*innen (Personalakten, Zeugnisse, Einschätzungen etc.), in digitaler und analoger Form, unterliegen einer besonderen Vertraulichkeit. Der Zugriff auf diese Dokumente ist nur einem begrenzten Personenkreis gestattet. Das ist in der KV die Geschäftsleitung, die Fachbereichsleiter*in Kindertagesstätten und die Personalsachbearbeiter*in.
Alle anderen Mitarbeiter*innen, die aus triftigen dienstlichen Gründen Informationen aus diesen Unterlagen erhalten wollen, weil dies zur Erfüllung ihrer Arbeitsaufgaben notwendig ist, müssen auf dem Dienstweg die entsprechenden Informationen anfordern und bekommen diese dann von den berechtigen Personen zur Verfügung gestellt. Ein nichtautorisierter Zugriff auf Personalakten, Teilen davon bzw. Unterlagen die der Personalakte typischer Weise zuzuordnen sind, ist strikt untersagt.
Das Einsichtsrecht in die eigene Personalakte (auf dem Dienstweg zu beantragen) bleibt hiervon unberührt.

16.2 Wird in einzelnen Einrichtungen / Projekten eine „Zweitakte“ zu Mitarbeiter*innen geführt, hat einzig die Leiter*in und im Vertretungsfall die Stellvertreter*in eine Zugriffberechtigung.

16.3 Bewerbungsunterlagen sind der Personalakte als gleichrangig anzusehen. Aus arbeitsorganisatorischen Gründen ist hier aber die Berechtigung für einen erweiterten Personenkreis notwendig. Zugriffberechtigt sind neben dem unter 16.1 benannten berechtigten Personenkreis auch die Fachkoordinator*innen Projekte, die stellvertretende Fachbereichsleiter*in Kita, Einrichtungs- und Projektleiter*innen, die Fachberatungen Kita und SSA und der Betriebsrat im Rahmen seiner Aufgaben und Befugnisse.

16.4 Ausnahmslos haben aber Daten und Unterlagen zu Bewerber*innen in einer Weise verarbeitet zu werden, die dem besonderen Vertrauensvorschuss von potentiell neuen Mitarbeiter*innen an die KINDERVEREINIGUNG® Leipzig e.V. gerecht werden.

16.5 Die Verteilung wird in der Regel von der Personalsachbearbeiter*in vorgenommen. Berechtigte Personen (16.3) haben stets darauf zu achten, dass die Daten der Bewerber*innen nur ihnen zur Kenntnis gelangen und die Unterlagen (digital und analog) stets angemessen zu schützen. Arbeitsorganisatorisch unnötige Umläufe oder Vervielfältigungen sind untersagt, ebenso wie die Weiterleitung an eine Vielzahl von Empfänger*innen innerhalb der KV ohne redaktionelle Auswahl.

16.6 Nach einer Entscheidungsfindung zur Besetzung einer Stelle sind analoge Unterlagen umgehend in den Verantwortungsbereich der Personalsachbearbeiter*in zurück zu überstellen. Elektronische Unterlagen (Doppel) sind zu löschen.

16.7 Die Personalsachbearbeiter*in ist verantwortlich, Bewerbungsunterlagen nach den gesetzlichen Fristen für Einsprüche zu archivieren, an die Bewerber*innen zurück zu geben, dauerhaft zu löschen oder ggf. der Personalakte zuzuordnen. Eine weitere Speicherung von Bewerberdaten für (mögliche) spätere Stellenbesetzungen ist vom Einverständnis der Bewerber*in abhängig, aber auf die Dauer von höchstens 12 Monaten begrenzt.

17 Sicherung / Backups / Verfügbarkeit

17.1 Personenbezogene Daten müssen, solange die Zweckbindung vorliegt, auch stets verfügbar gehalten werden. Jede Mitarbeiter*in hat daher ihrem Verantwortungsbereich dafür zu sorgen, dass von den Daten neben dem Arbeitsbestand auch immer eine Sicherungskopie oder ein Backup vorhanden ist.
Als zweckmäßigste Variante gilt hierbei die Sicherung auf ein externes Speichermedium (Festplatte oder USB Stick mit größerer Kapazität), das wiederum sicher innerhalb des Einflussbereiches der KV zu verwahren ist.

17.2 Sicherungen müssen stets aktuell sein und die Wiederherstellung des überwiegenden Datenbestandes ermöglichen, der vor dem (möglichen) Verlust der Daten gespeichert war! Je nach Arbeitsumfeld und Aufgabe sind hier unterschiedliche Sicherungsintervalle sinnvoll. **Mindestanforderung für alle Einrichtungen und Projekte ist aber 1 x im Quartal!**

17.3 Unverzüglich müssen aber Daten gesichert werden, wenn der Verdacht besteht, dass durch Soft- oder Hardwareprobleme (Ermüdungserscheinungen von Festplatten oder externen Speichern etc.) Datenbestände verloren gehen könnten. Gleiches gilt für analoge Datenbestände (Papiere) wenn geeignete Maßnahmen eine (weitere) Schädigung oder den Verlust der Daten verhindern, beenden oder abmildern können.

17.4 Unterbleiben Sicherungen und ist die (mögliche) Wiederherstellung von Datenbeständen nicht, nur teilweise und / oder nur mit erheblichem Erhebungsaufwand möglich, stellt dies eine grobe Fahrlässigkeit der verantwortlichen Mitarbeiter*in dar.

17.5 Kann auf dienstliche pbD nicht mehr zugegriffen werden, weil die Mitarbeiter*in Zugangsdaten (Passwörter) für einen möglichen (längeren) Vertretungsfall oder für ihr Ausscheiden aus der KV nicht auf geeignete Weise bereitstellt, wird ebenso ein schweres Versäumnis angenommen.

18 Löschvorschriften

18.1 Wie unter **3 e** beschrieben erlischt die Berechtigung zur weiteren Speicherung / Verarbeitung von pbD, wenn der Zweck der Erhebung / Verarbeitung erfüllt oder weggefallen ist. Der Zweck kann für eine bestimmte Frist fortbestehen, wenn korrespondierende Gesetze und Vorschriften eine weitere Speicherung der Daten oder Teilen davon vorschreiben (z.B. Finanzgesetze, Steuerrecht, Handelsgesetzgebung, Sozialgesetze, zivilrechtliche Verjährungsfristen etc.).
Dennoch gilt: **Eine unbegrenzte Speicherung von Daten ist unzulässig, auch in der KV!**

18.2 Daher ist jede Mitarbeiter*in verpflichtet ihrem Verantwortungsbereich dafür zu sorgen, dass regelmäßig Daten (analog und digital) gelöscht werden, für die keine Zweckbindung mehr besteht. Maßgeblich dafür sind die Dokumente (Listen) Aufbewahrungs- und Löschfristen Kita bzw. Projekte, die hier ausdrücklich in Bezug genommen werden und Bestandteil dieser Dienstanweisung sind.

18.3 Alltägliche Arbeitspapiere und digitale Daten die nicht spezieller in den Löschlisten aufgeführt sind, können, wenn der Zweck zu dem sie erstellt wurden erfüllt ist, gelöscht werden. Besteht dahingehend Unsicherheit, ist jede Mitarbeiter*in verpflichtet sich bei den Leiter*innen, den direkten Vorgesetzten und / oder beim DSB darüber zu informieren, ob und wann diese Daten gelöscht werden können.
In diesem Zusammenhang ist es besser einmal mehr zu fragen als unvorsichtig zu löschen.

18.4 Mindestanforderung ist aber für alle Einrichtungen, Projekte und die Geschäftsstelle **1 x im Jahr alle Datenbestände zu überprüfen (digital und analog) und ggf. zu löschen / zu vernichten**.

18.5 Digitale Daten sollen von allen EDV Systemen und ggf. auch aus Sicherungen und auf externen Datenträgern sowie als CDs / DVDs etc. gelöscht werden. Dazu ist es zwingend notwendig, dass bei jeder EDV mit dienstlichen pbD, neben dem inhaltlich logischen Ordnungssystem auch ein zeitliches Ordnungssystem existiert. Anderenfalls ist eine gezielte Löschung nach Inhalt und spezieller Frist gar nicht möglich. Die Mitarbeiter*in ist verpflichtet solche Strukturen zu schaffen und funktionstüchtig zu halten.

Siehe auch Punkt 20 Betroffenenrechte

18.6 Müssen aufgrund von Defekten, technischen Anforderungen oder Löschvorschriften ganze EDV Systeme vernichtet (entsorgt) werden, sind auf jeden Fall die Festplatten auszubauen. Keinesfalls dürfen Festplatten mit pbD, auch wenn sie vermeintlich defekt sind, in die allgemeine Verwertungskette für Wertstoffe gelangen. Die ausgebauten Festplatten, auch ggf. aus Servern oder von NASs, sind dem DSB zu übergeben. Dieser veranlasst dann eine zertifizierte Vernichtung.

18.7 Analoge Daten (Papiere, Akten etc.) mit pbD müssen dauerhaft vernichtet werden. Einfaches, mehrfaches Zerreißen ist nicht zulässig, ebenso wie die Vernichtung in Aktenvernichtern mit einfachem Streifenschnitt. Aktenvernichter müssen Papiere im Partikelschnitt vernichten (Partikel in ca. 5 x 50 mm oder kleiner). Genaue Schutzklassen und Sicherheitsstufen können beim DSB erfragt werden.

18.8 Die unzerkleinerte Entsorgung über sogenannte „Papiersammler“ (meist kostenlos von Verwertern aufgestellte Tonnen) oder über den normalen Papiermüll ist nicht zulässig.

18.9 Verbrennen von Papieren ist grundsätzlich zulässig, wenn sichergestellt ist, dass alle Unterlagen rückstandslos, in jedem Fall aber vollkommen unleserlich, verbrannt sind. Im Übrigen sind in diesem Zusammenhand die Vorschriften des Arbeitsschutzes, sowie ordnungs- und umweltpolitische Auflagen zu beachten.

18.10 Übersteigt die zu vernichtende Menge an Papieren ein Maß, dass nicht mehr sicher in der Einrichtung vernichtet werden kann, sollen die Akten gesammelt einmal im Jahr der zentralen Vernichtung über den DSB / Geschäftsstelle zugeführt werden. Diese Aktion findet immer Ende Januar / Anfang Februar eines jeden Jahres statt und wird rechtzeitig angekündigt. Dieser Termin fällt in die Zeit, in der regelmäßig Datenbestände verfallen, siehe Erklärung in den Löschlisten.

18.11. Müssen zwischendurch größere Datenmengen vernichtet oder Archive (teil)aufgelöst werden, ist individuell mit dem DSB ein Termin für eine Sondervernichtung zu vereinbaren. Dieser beauftragt einen zertifizierten Vernichter.

18.12 E-Mail Verläufe (lokal auf dem PC und ggf. parallel auch online im Strato Account und / oder auf synchronisierten mobilen Endgeräten) sind in der Regel häufiger (als 1 x im Jahr) auf die Notwendigkeit der weiteren Speicherung von pbD hin zu überprüfen. Es sollen keine unnötigen „Historien“ der Kommunikation entstehen.

19 Neue Verfahren

19.1 Mit Inkrafttreten dieser Dienstanweisung ist der DSB ausnahmslos vor der Installation von neuen Verfahren*(3) zu informieren und seine verbindliche Genehmigung zur geplanten Maßnahme abzuwarten. Als Verfahren ist jedwede Erhebung pbD anzusehen, egal ob dies mit einer neuen Software, per Direkterhebung (analog) oder über technische Erfassungssysteme geschehen soll.

Beispiele (nicht abschließend):

- geplante Einführung von Zeiterfassungs- oder Personenerfassungssystemen, Videoüberwachung
- mögliche Personalbefragungen / Erhebungen über die Zielgruppe(n) oder andere nat. Personen
- geplante Einführung neuer Software für Personaldatenverarbeitung, Lohnberechnung oder sonstiger Datenverarbeitungssysteme mit Personenbezug
- geplante Erschließung neuer Geschäftsfelder mit neuer Erhebungen von Daten
- geplante Ansprache neuer Zielgruppen oder geplante neue Projekte
- geplante Nutzung neuer Technologien und neuer Medien
- geplante Aufstellung von Servern, Massenspeichern oder Netzwerktechnik
- geplante Erstellung und Nutzung von Datenbanken

- geplante Nutzung neuer Telekommunikationstechnik oder sozialer Plattformen
- geplante Dienstleistungen für Dritte, die mit der Erhebung von pbD verbunden sind
- neuartige Reise- und / oder Ferienkonzepte
- geplante Angebote im Bereich Fort- und Weiterbildung
- neue Übermittlungsverfahren an Städte-, Gemeinden oder Fördermittelgeber
- geplante Datenverarbeitungen im Auftrag / Dienstleistungserträge
- geplanter Datenaustausch mit Dritten oder die Übermittlung in Drittländer (nicht EU)

**(3) Als neu gilt hierbei der Umstand, dass die geplanten Maßnahmen in gleicher oder sehr, sehr ähnlicher Weise nicht schon vor dem 01.01.2018 und über einen ununterbrochenen Zeitraum von mindestens 3 Jahren stattgefunden haben. Das heißt, dass die tägliche Arbeit in den Kitas, den Projekte und der Geschäftsstelle, wie seit Jahren praktiziert wird (es wird hier auch auf den Datenschutzfragebogen 2017 Punkte 29 - 32 verwiesen) nicht darunterfällt.*

19.2 Diese Vorschrift ist bindend für alle Bereiche der KV inklusive Geschäftsleitung, Fachbereichsleitung(en), Fachkoordination, Fachberatung(en), allen Kitas und Projekten und der Verwaltung.

19.3 Verfahren die länger als 3 Jahre nicht im Vollzug / in der Anwendung waren oder Verfahren in denen grundlegende Veränderungen vorgenommen werden sollen sind neue Verfahren und müssen durch den DSB (neu) genehmigt werden.

19.4 Werden pbD in neuen Verfahren erhoben und / oder verarbeitet ohne das der DSB ordnungsgemäß eingebunden wurde, lastet die volle datenschutzrechtliche Verantwortung auf den Verantwortlichen.

Hintergrund dieser Vorschriften ist die gesetzlich vorgeschriebene Notwendigkeit einer Datenschutzfolgeabschätzung für (neue) Verfahren der Datenerhebung.

20 Betroffenenrechte / Verfahren dazu

20.1 Die europäische Datenschutzgesetzgebung räumt jedem Betroffenen umfassende Auskunfts-, Berichtigungs-, Widerspruchs- und Übertragungsrechte zu seinen pbD ein. Zu diesem Zweck kann sich der Betroffene in jeder Form an den Verantwortlichen (die KINDERVEREINIGUNG® Leipzig e.V.) wenden. Das heißt fernmündlich, persönlich oder schriftlich (per Post, Fax oder E-Mail).

20.2 Von daher ist im Prinzip jede Mitarbeiter*in verpflichtet, entsprechende persönliche Anfragen eines Betroffenen auf dessen Ersuchen entgegenzunehmen. In Kitas, dem Hort und allen Einrichtungen mit mehreren Mitarbeitern*innen soll zweckmäßiger Weise an die jeweilige Leiter*in oder ggf. Stellvertreter*in verwiesen werden, wenn diese anwesend ist / sind. In keinem Fall dürfen aber diesbezügliche Anfragen abgewiesen werden oder der Eindruck beim Betroffenen erweckt werden -Anfragen sind nicht erwünscht oder werden nicht ernsthaft behandelt-!

20.3 Wenn die Umstände es zulassen, soll der Betroffene gebeten werden, sich mit seinem Ersuchen schriftlich (per E-Mail oder per Post) an die Eirichtungsleiter*in / Projektleiter*in zu wenden.
Zweite und angestrebte Variante ist, direkt an den DSB zu verweisen. Dazu müssen die Kontaktdaten des DSB schnell verfügbar gehalten werden (z.B. die Visitenkarten des DSB). Es soll dem Betroffenen nicht zugemutet werden diese selbst zu recherchieren (nach dem Prinzip „schauen Sie mal auf unsere Webseite, da steht das irgendwo“).

20.4 Alle Anfragen die in der Einrichtung / im Projekt gestellt werden, sind unverzüglich (also ohne schuldhaftes Zögern) und ohne Ausnahme an den DSB weiterzuleiten! Verantwortlich ist die einzelne Mitarbeiter*in, die die Anfrage tatsächlich entgegengenommen hat. Die Einbeziehung des DSB soll im ersten Schritt nach Möglichkeit immer persönlich erfolgen. Das heißt, unmittelbar nach einer Anfrage eines Betroffenen soll der DSB angerufen werden und über die Anfrage informiert werden. Schriftliche Anfragen sind parallel zum Anruf(versuch) an den DSB weiterzuleiten.

20.5 In jedem Fall muss aber sichergestellt sein, dass der DSB schnellstmöglich in den Prozess eingebunden wird und dies gegenüber der Mitarbeiter*in schriftlich bestätigt. Erst mit dieser Bestätigung gilt der Vorgang als ordnungsgemäß gemeldet. Bleibt diese Bestätigung aus, wird von einem Versäumnis der Mitarbeiter*in ausgegangen.

20.6 Im Falle längerer urlaubs- oder krankheitsbedingter Abwesenheit des DSB wird diesbezüglich per Rundmail informiert. Die Meldung (Weitergabe) von Anfragen muss daher in diesem Fall ohne Verzögerung an die direkte Fachvorgesetzte gehen. Abweichend von Punkt 4.5 gilt hier auch keine stillschweigende Fristverlängerung, sondern die Bestätigung an die Mitarbeiter*in und die Erstansprache des Betroffenen soll, je nach Zuständigkeit, ersatzweise durch die Fachbereichsleiter*in Kita oder die Fachkoordinator*innen Projekte erfolgen. Diese sind nach Arbeitsaufnahme des DSB verpflichtet, diesen über den Vorgang zu unterrichten.

20.7 Im Regelfall wird der DSB gegenüber dem Betroffenen den Eingang der Anfrage erklären und die angeforderten Auskünfte oder Maßnahmen, nach interner Rücksprache, erteilen, treffen oder treffen lassen. Dazu gibt es gesetzmäßige Fristen zu wahren, von daher sind die voranstehenden Vorschriften zu verstehen.

20.8 Damit überhaupt eine qualifizierte Aussage zu Art und Umfang sowie den Speicherorten und Speicherfristen gegenüber Betroffenen gegeben werden kann, ist jede Mitarbeiter*in verpflichtet, pbD in ihrem Arbeitsumfeld und ihren Arbeitsaufgaben entsprechend so systematisch zu speichern (analog und digital), dass ein gezieltes Auffinden, Auswerten, die Änderung, die Begrenzung des Zugriffs oder der Verarbeitung bis hin zur Löschung der Daten zu jedem einzelnen Betroffenen jederzeit möglich ist! Dies meint auch Sicherungen und Backups und ggf. parallele Speicherorte.

Dieser Grundsatz stellt einen der wichtigsten Gesichtspunkte dieser DA und der Arbeit nach moderner Datenschutzgesetzgebung dar!!!

21. Vertragsgestaltung

20.1 Im Verantwortungsbereich der Geschäftsführung, der Fachbereichsleiter*in Kita und der Fachkoordinator*innen Projekte liegt es, alle Verträge, bei denen pbD erhoben werden, nach den Vorgaben der EU DS-GVO hinsichtlich der Information der Betroffenen, rechtssicher auszugestalten.

20.2 Arbeitsorganisatorisch nachgeordnete Stellen, an denen typischer Weise regelmäßig Verträge mit Betroffenen geschlossen und / oder ausgereicht werden, sind jedoch verpflichtet die Vorgaben der Artikel 13 und 14 der EU DS-GVO dahingehend zu kennen und zielführend bei deren Umsetzung im Vertragswesen mitzuwirken. Diese Stellen sind:

- der Fachbereich Kindertagespflege
- die Verwaltungsbereiche Elterngeld und Kita allgemein
- die Personalabteilung
- der Bereich Ferienfahrten
- die internationale Arbeit
- die Kitaleitungen

- alle Projektleitungen die sich mit Angeboten an die Zielgruppe(n) richten, zu deren Umsetzung Verträge unterzeichnet werden müssen
- alle Stellen die AGB verwenden

Die entsprechenden Artikel 13 und 14 stellt der DSB als Auszüge aus dem Gesetzestext zur Verfügung.

22 (mögliche) Datenschutzverstöße / Verfahren dazu

22.1 Ziel, unter anderem dieser Dienstanweisung und ihrer Umsetzung in der täglichen Arbeit in der KINDERVEREINIGUNG® Leipzig e.V. ist es, Verstöße gegen den Datenschutz unbedingt zu vermeiden.

22.2 Der DSB überwacht die Einhaltung der einschlägigen Gesetze. Im Rahmen von Kontrollen in den Einrichtungen und Projekten wird zudem auf mögliche Risiken im Datenschutz aufmerksam gemacht und es werden gemeinsam mit den Mitarbeiter*innen Lösungen erarbeitet.

22.3 Bei Fragen zur Anwendung dieser DA oder anderer Datenschutzvorschriften, beim Problemen in der Durchsetzung von Datenschutzbelangen im Innen- und im Außenverhältnis, bei Risiken oder dem Verdacht auf mögliche (auch minderschwere) Datenschutzverstöße ist immer der DSB zu Rate zu ziehen. Er wird nach Prüfung der Umstände geeignete Maßnahmen empfehlen und ggf. weitere Schritte einleiten.

22.4 Für den (hoffentlich) unwahrscheinlichen Fall, dass es zu (potentiell) schweren Datenschutzverstößen kommt oder gekommen ist gilt zu allererst die wichtigste Regel: **Jede Mitarbeiter*in ist verpflichtet, unmittelbar bei Eintritt oder mit Bekanntwerden eines (potentiellen) Datenschutzproblems, geeignete Erstmaßnahmen zu treffen die den Missbrauch von pbD verhindern, beenden und / oder mögliche Folgen abmildern, sofern dies noch möglich ist.**

22.5 In jedem Fall ist aber der DSB definitiv und unverzüglich (also ohne schuldhaftes Zögern) zu informieren! In diesen Fällen gibt es auch keinen Büroschluss oder ein Wochenende. Es muss versucht werden den DSB sofort telefonisch (z.B. über die dienstliche Mobilfunknummer) zu erreichen und der Vorfall / das Problem zu melden! Ist der DSB nicht erreichbar muss der Kontaktversuch via Telefon mindestens zweimal in Abständen wiederholt werden.

22.6 Spätestens aber mit dem Beginn eines regelmäßigen Arbeitstages des DSB (Mo. - Fr.) muss telefonisch oder persönlich informiert werden.

22.7 Darüber hinaus muss jede Mitarbeiter*in, in deren Verantwortungsbereich das Datenschutzproblem aufgetreten ist, den Vorfall im Anschluss an die persönliche Information dem DSB sehr zeitnah zusätzlich schriftlich melden. Der DSB bestätigt schriftlich die Meldung des Vorfalls in der Frist. Bleibt diese Bestätigung aus, wird von einem schweren Versäumnis der Mitarbeiter*in ausgegangen.

Hintergrund ist die gesetzlich verankerte Meldepflicht von Datenschutzverstößen (mit möglichen Folgen für Betroffene) an die Aufsichtsbehörde mit extrem kurzer Frist von nur 72 Stunden.

22.8 Der DSB ist nach 22.5 / 22.6 mindestens über folgende Datenschutzprobleme zu informieren:

- den Diebstahl / Verlust von PCs, Laptops, Servern, externen Festplatten oder Speichern, USB-Sicks, Speicherkarten, Kameras, Datenträgern wie CDs oder DVDs auf denen pbD gespeichert waren
- den Verlust von Datenbanken mit pbD (auf ext. Servern oder in z.B. Webseiten eingebunden)
- den Diebstahl / Verlust von Telefonen oder Smartphones mit pbD
- Diebstahl / Verlust von Akten oder Papieren und Dokumenten mit pbD
- den Virenbefall, die Infektionen mit Erpressersoftware oder Trojanern von EDV Systemen
- bei Bekanntwerden des Verlustes von pbD bei Stellen die berechtigt für uns Daten verarbeiten

- gezielte Hackerangriffe oder Systemmanipulationen von innen und außen
- den technischen Totallausfall von EDV Systemen (dienstliche Hauptrechner mit dem wesentlichen Bestand an pbD)
- das (klassische) Ausspähen von pbD durch Unberechtigte in einem ernst zu nehmendem Ausmaß
- über Fälle in denen abgehört oder unerlaubt überwacht wird oder wurde
- Einbrüche in Betriebsstätten der KV, wenn Folgen für pbD erkennbar oder auch nur möglich sind
- den Verlust von Schlüsseln oder größere (andauernde) Defekte von Schließanlagen die den Zugang zu pbD für Unberechtigte ermöglicht haben oder ermöglichen könnten
- andauernder Ausfall von Alarmsystemen
- über Wassereinbrüche, Feuer oder Havarien, wenn pbD betroffen sind oder sein könnten
- über Umwelteinflüsse wie Licht, Hitze, Feuchtigkeit, starker Wind o.ä. die pbD vernichtet haben, dies noch tun oder zu mindestens eine erhebliche Gefahr dazu besteht
- wiederholte minderschwere Datenschutzverstöße einzelner Personen (durch Mitarbeiter*innen, oder auch durch Dritte)

Diese Aufzählung ist nicht abschließend. Entscheidend ist, dass mit Maßgabe dieser DA, der Datenschutzleitlinie der KV und einem normalen Rechtsempfinden, durch die Mitarbeiter*in ein Verstoß gegen geltende Datenschutzvorschriften zu mindestens angenommen hätte werden können, bei dem die Rechte des einzelnen Betroffenen oder einer Gruppe von Betroffenen in erheblichem Maß gefährdet sind oder sein können. Hier ist es ratsam den DSB „lieber einmal zu viel als zu wenig zu informieren“!

22.9 Unterbleibt die Benachrichtigung des DSB ganz oder innerhalb angemessener Frist (siehe 22.5/22.6), stellt dies einen schweren Verstoß im Sinne dieser DA und geltender Datenschutzgesetzgebung dar.

22.10 Es liegt einzig in der Entscheidungsbefugnis des DSB den (potentiellen) Datenschutzverstoß zu klassifizieren und die weiteren Maßnahmen zu treffen oder treffen zu lassen.

22.11 Im Falle längerer urlaubs- oder krankheitsbedingter Abwesenheit des DSB wird diesbezüglich per Rundmail informiert. Die Meldung von Datenschutzverstößen muss daher in diesen Fällen ohne Verzögerung ersatzweise an die direkte Fachvorgesetzte gehen. Die Bestätigung der fristgerechten Meldung des Vorfalls an die Mitarbeiter*in soll je nach Zuständigkeit von der Fachbereichsleiter*in Kita oder den Fachkoordinatorinnen Projekte kommen. Diese sind ihrerseits verpflichtet umgehend den Geschäftsführer einzubeziehen und gemeinsam nach einem internen Notfallplan über die weitere Vorgehensweise zu entscheiden. Mit Arbeitsaufnahme des DSB ist dieser unverzüglich in den Vorgang einzubinden.

23 Diese DA bleibt in der **Urheberschaft** des DSB. Jedwede Veröffentlichung und Verbreitung außerhalb der KINDERVEREINIGUNG® Leipzig e.V. ist untersagt.

Diese Dienstanweisung tritt am 01.02.2018 unbefristet in Kraft.

KINDERVEREINIGUNG® Leipzig e.V.

Matthias Heinz, Geschäftsführer

Eckhart Gottschling, Datenschutzbeauftragter

Kontaktdaten des Datenschutzbeauftragten der KINDERVEREINIGUNG® Leipzig e.V.
Herr Eckhart Gottschling, Bernhard-Göring-Straße 161, 04277 Leipzig
Tel.: +49 (0)341 30 68 0541 - **Mobil:** +49 (0)157 83 30 0601 - **E-Mail:** gottschling.e@kv-leipzig.de / dsb@kv-leipzig.de