Datenschutzkonzept

Version 1.0 vom 01.08.2018

Leben wie Zuhause e. V.
Pützdorfer Str. 50
52457 Aldenhoven
Tel. 02464 2059
info@lebenwiezuhause.de
www.lebenwiezuhause.de

Datenschutzkonzept
nach Datenschutzgrundverordnung (DSGVO)

1. Ziel und Geltungsbereich des Datenschutzkonzeptes

Unser Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen z. B. durch Auftraggeber im Rahmen der Auftragsverarbeitung genutzt werden. Dadurch soll die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) nicht nur gewährleistet, sondern auch der Nachweis der Einhaltung geschaffen werden.

Das Datenschutzkonzept legt unsere Mindestanforderung an den Datenschutz und die Datensicherheit fest und umfasst alle Tätigkeiten von Leben-wie-zuhause e.V., die im Zusammenhang mit Personenbezogenen Daten stehen. Hierbei handelt es sich um bindende Vorgaben zum Datenschutz. Diese Vorgaben sind verbindlich für alle Mitarbeiter und für externe Vertragspartner

2. Datenschutzpolitik und Verantwortlichkeiten

Wir legen für uns und unsere Mitarbeiter klare Datenschutzziele fest, die sich an den Datenschutz-Grundsätzen orientieren. Es ist uns wichtig, die Verarbeitung personenbezogener Daten transparent zu gestalten. Dazu gehört die detaillierte Auflistung der Art der gespeicherten Daten, die Herkunft der Daten und deren Weiterleitung.

Wir stellen den Betroffen, deren Daten wir verarbeiten, Möglichkeiten zur Verfügung, die ermöglichen, diese Daten vollständig einzusehen, zu bearbeiten und zu löschen.

Unsere obersten Datenschutzziele sind:

- Festlegung der Rollen und Verantwortlichkeiten (z. B. Datenschutzbeauftragte, verantwortliche Vertreter des Unternehmens und operativ Verantwortliche).
- Verpflichtung zur kontinuierlichen Verbesserung eines Datenschutzmanagementsystems.
- Schulung, Sensibilisierung und Verpflichtung der Mitarbeiter

Gemeinsam verantwortlich für die Umsetzung des Datenschutzes im Unternehmen ist die Einrichtungsleitung, der Datenschutzbeauftragte und jeder einzelne Mitarbeiter.

2.1 Verantwortlichkeiten

Geschäftsführung, Einrichtungsleitung :

- ➢ Gesamtverantwortung zum Datenschutz
- ➢ Bestellung des Datenschutzbeauftragten
- ➢ In Kraft setzen von DS-Richtlinien
- ➢ Bereitstellen der notwendigen technischen, finanziellen und personellen Ressourcen für den Datenschutz
- ➢ Technische und organisatorische Maßnahmen zum Datenschutz

Datenschutzbeauftragter:

Erfüllung seiner gesetzlich vorgeschriebenen Aufgaben nach Artikel 39 DSGVO

Dazu gehören:

- ➢ Beratung bei der Durchführung der Datenschutzfolgeabschätzung
- ➢ Ansprechpartner bei DS-relevanten Projekten und Einführung neuer Software und IT-Systeme
- ➢ Sicherstellung eines durchgängigen Berichtwesens
- ➢ Zentraler Ansprechpartner für betroffene Personen, das Unternehmen und dessen Beschäftigten und der Aufsichtsbehörde
- ➢ Schulung und Beratung der Geschäftsleitung und der Mitarbeiter hinsichtlich der geltenden Datenschutzvorschriften
- ➢ Überwachung der Einhaltung der geltenden Datenschutzvorschriften

Mitarbeiter:

- ➢ Wahrung des Datengeheimnisses
- ➢ Beachtung und Umsetzung aller sie oder ihre Tätigkeit betreffenden Maßnahmen und Regelungen zum Datenschutz.
- ➢ Melden von Datenschutzvorfällen

3. Rechtliche Rahmenbedingungen

Neben den rechtlichen Grundlagen die sich aus der DSGVO und dem BDSG(neu) ergeben, liegen unserem Datenschutzkonzept noch weitere Regelungen zu Grunde, z.B.:

- Branchenspezifische gesetzliche Regelungen oder Verhaltensregeln für den Umgang mit personenbezogenen Daten.
- Anforderungen interner und externer Parteien.
- Anwendbare Gesetze mit ggf. lokalen Sonderregelungen.

4. Dokumentation

Besonderen Wert legen wir auf die Datenschutzdokumentation. Wir haben den Schutzbedarf der Daten bezüglich Vertraulichkeit, Integrität und Verfügbarkeit festgelegt und klassifizieren die Daten mit „normal“, „hoch“ und „sehr hoch“.

Da es sich bei den personenbezogenen Daten des Leben wie Zuhause e.V. in der überwiegenden Zahl um Gesundheits- oder Sozialdaten handelt, ist der Schutzbedarf der zu verarbeitenden Daten in der Regel als „sehr hoch“ einzuschätzen und die Daten werden von uns dementsprechend behandelt.

Durch regelmäßige interne Prüfungen stellen wir sicher, dass die Vorgaben zum Datenschutz flächendeckend eingehalten werden, dass Datenschutz-Risiken frühzeitig erkannt werden und das im Falle von Datenschutzpannen umgehend und richtig gehandelt wird.

Zur durchgängigen Kontrolle und Nachweisbarkeit wurden DS-Richtlinien zur Dokumentation und Kommunikation erstellt, welches aus wiederkehrenden Gesprächen, regelmäßigen Fragebögen und geplanter Kommunikation besteht. Ein kontinuierliches Berichtswesen rundet die Dokumentation ab.

5. Technische und organisatorische Maßnahmen (TOM)

Wir treffen geeignete technische und organisatorische Maßnahmen, die unter Berücksichtigung u. a. des Zwecks der Verarbeitung, des Stands der Technik und der Implementierungskosten festzuglegen und nachzuweisen sind.

Anforderungen an die Sicherheit der Datenverarbeitung gemäß § 64 BDSG-neu:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (**Zugangskontrolle**)
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (**Datenträgerkontrolle**)
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (**Speicherkontrolle**)
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (**Benutzerkontrolle**)
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben (**Zugriffskontrolle**)
6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (**Übertragungskontrolle**)
7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (**Eingabekontrolle**)
8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (**Transportkontrolle**)
9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (**Wiederherstellbarkeit**)
10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (**Zuverlässigkeit**)
11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (**Datenintegrität**)
12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (**Auftragskontrolle**)
13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (**Verfügbarkeitskontrolle**)
14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (**Trennbarkeit**)

Eine detaillierte Auflistung der umgesetzten technischen und organisatorischen Maßnahmen findet sich in der Datenschutzdokumentation.

Neben den oben aufgezeigten Maßnahmen ergeben sich auch aus anderen Vorschriften der DSGVO eine Reihe weiterer Forderungen.

Z.B. muss durch Schulung, Anweisung oder Unternehmens-Richtlinien sichergestellt werden, dass

- nur auf zulässige Art und Weise personenbezogene Daten erhoben, verarbeitet und genutzt werden,
- die Rechte des Betroffenen auch im Hinblick auf die Transparenzpflichten z.B. bei der Erhebung gewahrt werden,
- die Formalien z.B. bei Auftragsdatenverarbeitung und bei automatisierten Abrufverfahren eingehalten werden,
- die Kontrollen durch die Aufsichtsbehörden ordnungsgemäß vorgenommen werden können,
- das vorgesehenen Meldepflichten korrekt erfüllt werden

Alle DS-Richtlinien für den Umgang mit personenbezogenen Daten sind für alle Mitarbeiter (inkl. Führungsebene) verbindlich.

Eine Auflistung der Arbeitsanweisungen, Richtlinien und Festlegungen findet sich unter **Punkt 9 Mitgeltende Dokumente** oder in der Datenschutzdokumentation.

6. Verzeichnis der Verarbeitungstätigkeiten (DSGVO)

Wir führen ein Verzeichnis der Verarbeitungstätigkeiten nach der DSGVO. Das Verzeichnis unterliegt der regelmäßigen Überprüfung und Kontrolle durch den Datenschutzbeauftragten.

In Zusammenarbeit mit den Bereichsverantwortlichen Mitarbeitern werden neue Verfahren umgehend in dieses Verzeichnis aufgenommen bzw. nicht mehr verwendete Verfahren werden ausgetragen.

Das Verzeichnis der Verarbeitungstätigkeiten findet sich in der Datenschutzdokumentation.

7. Datenschutz-Unterweisungen und Schulungen

Es finden regelmäßig geplante, strukturierte und dokumentierte Unterweisungen für alle Mitarbeiter des Leben wie Zuhause e.V. durch den Datenschutzbeauftragten bzw. den verantwortlichen Mitarbeiter statt.

Ebenso ist durch einen festen Aufnahmeprozess von neuen Mitarbeitern geregelt, dass diese vor Arbeitsantritt auf die Verschwiegenheit und das Datengeheimnis verpflichtet werden und eine Initial-Schulung zum Thema Datenschutz erhalten.

Bei Bedarf können darüber hinaus jederzeit Sonder-Schulungstermine anberaumt werden.

8. Regelmäßige Datenschutz-Kontrollen und Audits

Es finden regelmäßige Datenschutz-Kontrollen durch den Datenschutzbeauftragten statt. Jede Änderung der Verarbeitungsweise wird dem Datenschutzbeauftragten angezeigt. Hier findet wieder das durchgängige Kommunikationskonzept Anwendung.

Regelmäßig, mindestens alle zwei Jahre, wird ein internes Datenschutzaudit durchgeführt. Hierzu werden die entsprechenden Abteilungen durch den Datenschutzbeauftragten auditiert. Die Auditergebnisse werden mit der Einrichtungsleitung und allen verantwortlichen Mitarbeitern besprochen. Ggf. werden Maßnahmen zur Verbesserung eingeleitet und umgesetzt. Dabei muss ein wesentlicher Bestandteil der Umsetzungsphase sein, mit dem betroffenen Personenkreis ins Gespräch zu kommen, um Verständnisdefizite zu erkennen und in einem beratenden Gespräch zu beheben. Hierdurch ist es möglich, nicht nur Lücken im Konzept zu schließen, sondern auch die Akzeptanz für die vorgesehenen Maßnahmen zu fördern.

9. Mitgeltende Dokumente

9.1.1 DS-Richtlinien für Mitarbeiter

9.1.1.1 Allgemein

Die Mitarbeiter sind ein zentraler Faktor für die Implementierung und Aufrechterhaltung des Datenschutzes. Es ist deshalb notwendig, auch in diesem Bereich die Anforderungen des Datenschutzes zu berücksichtigen.

a) Personenbezogenen Daten werden nicht eigenmächtig verarbeitet. Es werden ausschließlich die vom Unternehmen bereitgestellten Programme und Möglichkeiten zur Verarbeitung genutzt.

b) Der Bedarf weiterer Verarbeitung wird der zuständigen Stelle (Leitung, Personalabteilung etc.) gemeldet.

c) Mitarbeiter halten alle sie oder ihre Tätigkeit bestreffenden Maßnahmen und Regelung zur Sicherheit personenbezogener Daten ein, bzw. setzen diese um.

d) Mitarbeiter melden alle möglichen Datenschutzvorfälle an die zuständige Stelle (Leitung, Datenschutzkoordinator, Datenschutzbeauftragter)

9.1.1.2 Einstellung und Beendigung der Anstellung

a) Mitarbeiter verpflichten sich mittels einer schriftlichen Erklärung zur Vertraulichkeit, die Erklärung definiert auch die Pflichten in Bezug auf Datenschutz, die nach Beendigung oder Veränderung des Arbeitsverhältnisses fortbestehen.

b) Neue Mitarbeiter werden in sämtliche, für sie verbindliche DS-Richtlinien und sonstige verbindliche Regelungen zum Datenschutz eingewiesen.

c) Neue Mitarbeiter werden im Umgang mit den für sie relevanten Mechanismen für die Umsetzung im Datenschutz geschult.

d) Bei Beendigung oder Veränderung des Arbeitsverhältnisses werden die Zugriffsmöglichkeiten des Mitarbeiters auf personenbezogenen Daten umgehend überprüft und angepasst

e) Soweit erforderlich werden Mitarbeiter, Kunden sowie Zuarbeiter und sonstige Auftragnehmer über Änderungen im Personal- und betrieblichen Ablauf informiert.

2. DS-Richtlinien für die Verarbeitung personenbezogener Daten

a) Personenbezogenen Daten werden nur aufgrund einer wirksamen Einwilligung des Betroffenen oder einer anderen Rechtsgrundlage verarbeitet. (Rechtmäßigkeit)

b) Personenbezogene Daten werden nur für festgelegte und eindeutige Zwecke verarbeitet. Wenn der Verwendungszweck von personenbezogenen Daten geändert werden soll, wird im Vorfeld die rechtliche Zulässigkeit geprüft und ggf. die Einwilligung des Betroffenen eingeholt (Zweckbindung)

c) Die Verarbeitung personenbezogener Daten ist für die Erreichung ihres Zwecks geeignet, erforderlich und angemessen (verhältnismäßig). (Fairness, Treu und Glauben)

d) Die Betroffenen werden über die Verwendung ihrer personenbezogenen Daten umfassend und verständlich informiert (Transparenz)

e) Es werden nur die unbedingt benötigten personenbezogenen Daten verarbeitet (Datenminimierung)

f) Es werden Maßnahmen etabliert, um unrichtige personenbezogene Daten zu vermeiden und zu erkennen. Wenn personenbezogene Daten im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, werden diese korrigiert oder gelöscht (Richtigkeit)

g) Nicht mehr benötigte personenbezogene Daten werden gelöscht, sofern dem keine Aufbewahrungspflichten entgegenstehen. Personenbezogene Daten werden anonymisiert oder pseudonymisiert, wenn deren Personenbezug nicht benötigt wird. (Speicherbegrenzung)

h) Die Maßnahmen zur Sicherstellung der Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten werden im Zuge einer nachvollziehbaren Risikoanalyse und -behandlung ermittelt und umgesetzt (Vertraulichkeit, Integrität und Verfügbarkeit)

i) Für jede Datenkategorie sind Bedingungen definiert, wie und in welchem Rhythmus nach zu löschenden Daten gesucht wird und wie eine Löschung zu erfolgen hat. Dabei werden der aktive Datenbestand und die archivierten Daten berücksichtigt.

j) Ein Suchlauf, das Löschen sowie auftretende Fehler werden, sofern technisch möglich, protokoliert.

k) Die Einhaltung der DS-Richtlinien wird dokumentiert.

3. DS-Richtlinien für die Auftragsverarbeitung (AV)

Nutzen und Anbieten von Auftragsverarbeitungen setzen bei Kunden und Anbietern ein strukturiertes Vorgehen voraus.

Wenn Verarbeitungen personenbezogener Daten ausgelagert werden, ist es notwendig, die Anforderungen des Datenschutzes zu berücksichtigen. Eine korrekte Vertragsgestaltung ist wichtig um Haftungsrisiken vorzubeugen.

a) Wir überwachen das betriebliche, gesetzliche und vertragliche Bestimmungen in Bezug auf den Datenschutz der ausgelagerten Verarbeitungen erfüllt werden.

b) Das Unternehmen muss sicherstellen und dokumentieren, dass der Auftragsverarbeiter über die notwendige Eignung und die erforderliche Vertrauenswürdigkeit verfügt. Auftragsverarbeiter können ihre Einigung auch durch entsprechende Zertifizierungen nachweisen.

c) Wenn Verarbeitungen ausgelagert werden sollen, muss mit dem Auftragsverarbeiter ein Vertrag geschlossen werden (AV-Vertrag). Dieser Vertrag enthält Regelungen zu folgenden Punkten:

   - Gegenstand und Dauer der Verarbeitung
   - Zweck der Auftragsverarbeitung und Art der Daten und Datenkategorien
   - Sicherstellung der Vertraulichkeitsverpflichtung der Mitarbeiter des AV
   - Umsetzung der Technischen und organisatorischen Maßnahmen beim AV
   - Vereinbarungen zu Sicherheitsmaßnahmen zum Schutz der personenbezogenen Daten
   - Informationspflichten des AV bei Datensicherheitsvorfällen
   - Vereinbarungen zu Dokumentationspflichten und Inspektionen und Überprüfungen
   - Verpflichtung zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten
   - Verpflichtung zur Bestellung eines Datenschutzbeauftragten.

4. DS-Richtlinien bei Datenschutzvorfällen

Die angemessene Reaktion auf Datenschutzvorfälle ermöglicht es einem Unternehmen, Schäden schnell einzudämmen und beheben zu können sowie gesetzliche Anforderungen zu erfüllen. Deshalb ist es notwendig, angemessen auf Datenschutzvorfälle vorbereitet zu sein.

a) Der Begriff des Datenschutzvorfalls wurde klar definiert und wird den Mitarbeitern im Rahmen der jährlichen Datenschutz-Unterweisung erklärt.

b) Jeder Mitarbeiter meldet mögliche Datenschutzvorfälle an die entsprechende Stelle (Leitung, Datenschutzkoordinator, Datenschutzbeauftragter)

c) Die verantwortliche Stelle untersucht in Zusammenarbeit mit dem DSB (ggf. mit dem IT-Verantwortlichen, dem Administrator etc.) den Datenschutzvorfall.

d) Bei Datenschutzvorfällen, die ein Risiko für den Betroffenen bergen, oder die mit Sanktionen geahndet werden könnten, wird die Einrichtungsleitung über den Vorfall informiert.

e) Es ist festgelegt, wir intern und nach außen über akute und bewältigte Datenschutzvorfälle kommuniziert wird.

Vorgehen im Fall eines Datenschutzvorfalles

a) Es wird ein Überblick über die Situation gewonnen

b) Es werden alle erforderlichen Maßnahmen getroffen, um Leib und Leben von Personen zu schützen

c) Der Vorfall wird durch Sofortmaßnahmen eingedämmt

d) Der Vorfall wird dokumentiert, insbesondere

    a. Welche Daten von welchen Personenkategorien betroffen sind

    b. Wie hoch die Anzahl der Betroffenen und der Datensätze ist

    c. Eine Beschreibung der wahrscheinlichen Folgen des Vorfalls

    d. Eine Beschreibung der ergriffenen oder vorgesehenen Maßnahmen

    e. ggf. Maßnahmen für die Abmilderung der möglichen negativen Folgen

e) Beweismittel werden gesichert

f) Der Schaden wird behoben und die regulären Geschäftsprozesse wieder aufgenommen.

g) Es findet eine Nachbereitung statt, bei der die Ursachen ermittelt werden und konkrete Verbesserungen erarbeitet werden.

h) Es wird ermittelt, ob eine Meldepflicht besteht und welche Vorgaben und Fristen hierbei eingehalten werden müssen.

i) Es wird geprüft, ob das Unternehmen die Betroffenen benachrichtigen oder eine öffentliche Bekanntmachung veranlassen muss.

5. DS-Richtlinien zur Risikoanalyse und -behandlung

Das Unternehmen muss eine Risikoanalyse durchführen und erkannte Risiken zeitnah und angemessen behandeln.

a) Die Dokumentation der Risikoanalyse beinhaltet das Vorgebe für das Identifizieren und Bewerten von Risiken

b) Die von uns gewählte Vorgehensweise gewährleistet, dass Bedrohungen und Schwachstellen zuverlässig erkannt werden können

c) Die Bewertung von Risiken erfolgt auf Basis der potentiellen Schäden für das Unternehmen und deren Eintrittswahrscheinlichkeit

d) Das Ergebnis der Risikoanalyse ermöglicht eine Priorisierung bei der Risikobehandlung.

e) Risikoanalysen müssen jährlich auf ihr Aktualität geprüft und bei Bedarf wiederholt werden

f) Risikoanalysen müssen zeitnah überarbeitet werden, wenn der Gegenstand der Risikoanalyse oder der Einsatzzweck des untersuchten Gegenstandes sich wesentlich verändert oder die Gefährdungslage sich erhöht hat.

6. DS-Richtlinie zur Datenschutzfolgeabschätzung (DSFA)

Es besteht die Pflicht, für die Verarbeitung personenbezogener Daten eine Datenschutz-Folgeabschätzung durchzuführen. Dazu muss die Organisation sicherstellen, dass die Prüfung den gesetzlichen Vorgaben entspricht.

Die DSFA sollte folgende Anforderungen erfüllen:

- Der DSB begleitet die DSFA beratend
- Die identifizierten Risiken der Risikoanalyse werden nochmal überprüft
- Es wird eine Dokumentation erstellt, die folgende Informationen beinhaltet:
    a. Beschreibung der beabsichtigten Verarbeitung
    b. Zweck der beabsichtigten Verarbeitung
    c. Interessen des Verantwortlichen an der Verarbeitung
    d. Zweckgebunde Notwendigkeit und Verhältnismäßigkeit der Verarbeitung
    e. Risikobewertung für die persönlichen Rechte und Freiheiten der betroffenen Personen, die mit der Verarbeitung verbunden sind.
    f. Maßnahmen zur Abhilfe der identifizierten Risiken
    g. Notwendigkeit zur Einbindung des Betroffenen

Wenn die DSFA trotz der beabsichtigten Abhilfemaßnahmen mit hohen Risiken für die persönlichen Rechte und Freiheiten der betroffenen Personen verbunden ist, muss die entsprechende Aufsichtsbehörde konsultiert werden.

Ergänzung des Leben wie Zuhause e.V.:

Gemäß Auffassung der Datenschutzbehörden unterschiedlicher Länder unterliegt eine Kita bzw. ein Verein keiner Verpflichtung, eine DSFA durchzuführen.

Begründung der Aufsichtsbehörden:
Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgenabschätzung durchgeführt werden. Ein solch hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.
→ DSK-Kurzpapier Nr. 5: www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf

Hier folgen wir der Auffassung der Behörden und haben festgelegt, daß in unserer Einrichtung keine DSFA durchzuführen ist. Diese Festlegung wird 1x Jährlich bzw. bei Bedarf überprüft und dazu die jeweils gültige Meinung der Aufsichtsbehörden dazu gehört.

7. DS-Richtlinie zur Dokumentation und Kommunikation, inkl. Anfragen von Betroffenen

Das Unternehmen hat festgelegt, in welcher Art und Weise die interne und externe Kommunikation und die Dokumentation zum Thema Datenschutz durchgeführt wird und wie auf Anfragen von Betroffenen reagiert werden muss.

7.1.Dokumentation

a) Die Bearbeitung sämtlicher Datenschutzvorfälle inkl. ergriffener Folge- und Schutzmaßnahmen wird dokumentiert.

b) Der Datenschutzbeauftragte erstellt 2x/Jahr einen Tätigkeitsbericht. Der Bericht beinhaltet den aktuellen Status im Datenschutz, aufgetretene Datenschutzvorfälle, durchgeführte Tätigkeiten, erforderliche Maßnahmen, Ergebnisse von Kontrollen und Analysen, Hinweise zur Verbesserung.

c) Zur generellen Analyse des aktuellen Status wird 1x im Quartal der aktuelle Status durch eine Checkliste abgefragt, die dem Datenschutzbeauftragten ausgefüllt gesendet werden muss.

d) Alle Anfragen von Mitarbeitern oder der Geschäftsleitung sowie von Betroffenen werden vom Datenschutzbeauftragten vertraulich dokumentiert.

7.2.Kommunikation

a) Die verantwortliche Stelle (Leitung, Datenschutzkoordinator) wird von ihren Mitarbeitern umgehen über mögliche Datenschutzvorfälle informiert.

b) Der Datenschutzbeauftragte wird umgehen von der verantwortlichen Stelle über mögliche Datenschutzvorfälle informiert.

c) Mitarbeiter und Einrichtungsleitung wenden sich bei Fragen zum Datenschutz umgehend an den Datenschutzbeauftragen.

d) In Zweifelsfällen ist der Datenschutzbeauftragte berechtigt, Auskunft bei der Datenschutzbehörde zu ersuchen.

e) Auskunftsersuchen von Betroffenen werden umgehend beantwortet und bearbeitet. Der Datenschutzbeauftragte wird bei Bedarf hinzugezogen. Anfragen sind zu dokumentieren.

f) Personenbezogene Daten werden nur an Betroffene kommuniziert, niemals an Dritte. Dazu wird die Identität des Betroffenen (Anfragenden) überprüft.

g) Jede Auskunftserteilung erfolgt nachweislich und innerhalb der gesetzlichen Fristen von vier Wochen.

h) Wenn eine Auskunft über ein unsicheres Medium wie z.B. E-Mail erfolgt, wird zuvor das Einverständnis des Betroffenen eingeholt.

8. DS-Richtlinie zum privaten Umgang mit dienstlichen Kommunikationsmedien

Es wird festgelegt, daß dienstliche Kommunikationsmedien wie z.B. Telefon, Fax, Email oder Internet aus Gründen der Sicherheit ausschließlich zu dienstlichen Zwecken genutzt werden dürfen. Eine private Nutzung dieser Geräte ist ausdrücklich untersagt.