Richtlinie für den Datenschutz in der Katholischen Kirchengemeinde [St. Petrus, Lastrup…]

Inhalt

Präambel 1
1 Bedeutung, Ziel, Zugänglichkeit 2
2 Geltungsbereich 2
3 Begriffsbestimmungen 2
4 Datenschutzbeauftragter 3
5 Datenschutzorganisation 4
6 Grundsätze für die Verarbeitung personenbezogener Daten 5
7 Besondere Kategorien personenbezogener Daten 5
8 Rechenschaftspflicht 5
9 Auftragsverarbeiter 6
10 Datenübermittlung 6
11 Datenschutzvorfälle 6
12 Rechte von betroffenen Personen 7
13 Beschwerden 7
14 Auskunftsersuchen Dritter über betroffene Personen 7
15 Sensibilisierung und Schulung 8
16 Vertraulichkeit 8
17 Sicherheit der Verarbeitung 8
18 Folgen von Verstößen 8
19 Aktualisierung der Richtlinie 9

Präambel

Seit der Fusion im Jahr 2010 setzt sich die St. Petrus Gemeinde wie folgt zusammen. St. Petrus Lastrup, Herz-Jesu Hemmelte und St. Michael Kneheim. Die Anzahl der Gemeindemitglieder beträgt zur Zeit ca. 5300.

Das Anliegen dieser Datenschutzrichtlinie ist es, im Interesse der betroffenen Personen und auch der Kirchengemeinde in jeder Phase der Informationsverarbeitung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten zu gewährleisten. Um dieses Ziel zu erreichen, sind nicht nur gesetzliche Vorschriften zum Schutz personenbezogener Daten einzuhalten, sondern auch geeignete technische und organisatorische Maßnahmen umzusetzen. Alle Beschäftigten müssen sich der Risiken bewusst sein, die mit technischen

Systemen und Kommunikationstechnologien verbundenen sind, und bei der Verarbeitung personenbezogener Daten die erforderliche Sorgfalt walten lassen.

1 Bedeutung, Ziel, Zugänglichkeit

1.1 Diese Richtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten in der Kirchengemeinde.

1.2 Mit dieser Richtlinie sollen die Persönlichkeitsrechte von Betroffenen gewahrt und geschützt werden.

1.3 Die Richtlinie muss für alle Beschäftigten und leitenden Angestellten jederzeit leicht zugänglich sein.

2 Geltungsbereich

2.1 Diese Richtlinie gilt persönlich für alle Beschäftigten sowie leitenden Angestellten der Kirchengemeinde. Nach § 4 Nr. 24 des Gesetzes über den kirchlichen Datenschutz (KDG) sind Beschäftigte insbesondere

- alle Kleriker und Kandidaten für das Weiheamt,
- Ordensangehörige, soweit sie auf einer Planstelle in einer Einrichtung der eigenen Ordensgemeinschaft oder aufgrund eines Gestellungsvertrages tätig sind,
- in einem Beschäftigungsverhältnis oder in einem kirchlichen Beamtenverhältnis stehende Personen,
- zu ihrer Berufsbildung tätige Personen mit Ausnahme der Postulanten und Novizen,
- Teilnehmende an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobungen (Rehabilitanden),
- in anerkannten Werkstätten für Menschen mit Behinderungen tätige Personen,
- nach dem Bundesfreiwilligendienstgesetz oder dem Jugendfreiwilligendienstegesetz oder in vergleichbaren Diensten tätige Personen sowie Praktikanten,
- Personen, die wegen ihrer wirtschaftlichen Unselbstständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
- sich für ein Beschäftigungsverhältnis Bewerbende sowie Personen, deren Beschäftigungsverhältnis beendet ist.

2.2 Die Gebote und Verbote dieser Richtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, sowohl in elektronischer Form als auch in Papierform. Ebenso beziehen sie alle Arten von Betroffenen (Beschäftigte, Kunden, Interessenten, Lieferanten, Dienstleister, etc.) in ihren Geltungsbereich ein.

3 Begriffsbestimmungen

3.1 Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen,

psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

3.2 Besondere Kategorien personenbezogener Daten sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Die Zugehörigkeit zu einer Kirche oder Religionsgemeinschaft ist keine besondere Kategorie personenbezogener Daten.

3.3 Verarbeitung bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

3.4 Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

3.5 Betroffene Person eine identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten von der Einrichtung oder anderen Stelle verarbeitet werden.

3.6 Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

3.7 „Dritter" eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

3.8 Die Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

4 Datenschutzbeauftragter

4.1 Die Kirchengemeinde hat einen externen Datenschutzbeauftragten (eDSB) nach Maßgabe des Gesetzes über den kirchlichen Datenschutz (KDG) bestellt:

- Stefan Winkel
  Consultant Datenschutz
  Volljurist
  Telefon: +49 40 790235 – 250
  E-Mail: swinkel@intersoft-consulting.de

4.2 Der eDSB unterrichtet und berät die Leitung der Kirchengemeinde und die Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dem KDG und anderen datenschutzrechtlichen Vorschriften.

4.3 Der eDSB überwacht die Einhaltung des KDG, anderer datenschutzrechtlicher Vorschriften sowie dieser Richtlinie und sensibilisiert die Beschäftigten für den Schutz personenbezogener Daten.

4.4 Betroffene Personen können den eDSB zu allen Fragen zu Rate ziehen, die mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte im Zusammenhang stehen. Sämtliche Anfragen werden vertraulich behandelt.

4.5 Die Leitung der Kirchengemeinde stellt sicher, dass der eDSB bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält.

4.6 Die Leitung der Kirchengemeinde unterstützt den eDSB bei der Erfüllung seiner Aufgaben, indem sie die erforderlichen Ressourcen zur Verfügung stellt und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen ermöglicht.

4.7 Der eDSB ist für die Kommunikation mit der Datenschutzaufsicht zuständig.

5 Datenschutzorganisation

5.1 Der eDSB berichtet unmittelbar der Leitung der Kirchengemeinde.

5.2 Die Leitung der Kirchengemeinde hat (einen) Datenschutzkoordinator(en) ernannt, der/die Kontaktperson des eDSB in der Kirchengemeinde ist/sind:

Elisabeth Gänsler
KIrchenprovisorin
Telefon: +4944721302
E-Mail:provisor-st.petrus@ewetel.net

5.3 Leitung der Kirchengemeinde stellt durch die Ernennung des Datenschutzkoordinators und weitere organisatorische Maßnahmen sicher, dass der eDSB insbesondere in den folgenden Fällen so frühzeitig wie möglich eingebunden wird:

- Einführung von wesentlichen Verarbeitungstätigkeiten, insbesondere bei der Einführung von IT-Systemen, die zur Verarbeitung personenbezogener Daten bestimmt sind,
- Beauftragung von Dienstleistern und Lieferanten, die als Auftragsverarbeiter tätig werden,
- Übermittlung personenbezogener Daten an Dritte, insbesondere bei Übermittlungen in Staaten außerhalb der Europäischen Union,
- Verletzung des Schutzes personenbezogener Daten,
- Konsultation der Datenschutzaufsicht, wenn aus einer Datenschutz-Folgenabschätzung gemäß § 35 KDG hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern keine Maßnahmen zur Eindämmung des Risikos getroffen werden.
- Abschluss von Dienstvereinbarungen mit Bezug zum Umgang mit Mitarbeiterdaten,
- Beschwerden betroffener Personen, ggf. im Rahmen eines Eskalationsprozesses (soweit Beschwerden nach einer ersten Reaktion der Kirchengemeinde aufrechterhalten bleiben).

6 Grundsätze für die Verarbeitung personenbezogener Daten

6.1 Rechtmäßigkeit und Transparenz: Personenbezogene Daten müssen auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

6.2 Zweckbindung: Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

6.3 Datenminimierung: Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

6.4 Richtigkeit: Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

6.5 Speicherbegrenzung: Personenbezogene Daten müssen 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.

6.6 Integrität und Vertraulichkeit: Personenbezogene Daten müssen 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.

7 Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogene Daten dürfen grundsätzlich nur mit Einwilligung des Betroffenen oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis verarbeitet werden. Ferner sind zusätzliche technische und organisatorische Maßnahmen (z. B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

8 Rechenschaftspflicht

8.1 Um die Rechtmäßigkeit der Datenverarbeitung und insbesondere die Einhaltung der Grundsätze aus den Ziffern 6 und 7 dieser Richtlinie nachweisen zu können, sind alle datenschutzrelevanten Dokumente so vorzuhalten, dass sie in ihrer Gesamtheit ohne Verzögerung abgerufen werden können.

8.2 Über alle Verarbeitungstätigkeiten, die der Zuständigkeit der Kirchengemeinde unterliegen, wird ein Verzeichnis geführt. Dieses Verzeichnis enthält sämtliche Angaben, die nach § 31 KDG erforderlich sind.

8.3 Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, wird vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchgeführt. Die Datenschutz-Folgenabschätzung wird nach Maßgabe des § 35 KDG erstellt.

9 Auftragsverarbeiter

9.1 Dienstleister und Lieferanten mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Erfolgt eine Verarbeitung im Auftrag der Kirchengemeinde, muss der Auftragsverarbeiter durch geeignete technische und organisatorische Maßnahmen hinreichend Garantien dafür bieten, dass die Verarbeitung im Einklang mit den Anforderungen der KDG erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

9.2 Die Auswahl von Dienstleistern sowie Lieferanten ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

- Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang,
- Technisch-organisatorische Sicherheitsmaßnahmen,
- Erfahrung des Anbieters im Markt,
- Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schließen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten etc.).

9.3 Vor der Beauftragung ist der eDSB zu informieren, sodass er überprüfen kann, ob der erforderliche Vertrag nach § 29 KDG abgeschlossen worden ist.

9.4 Die Vereinbarungen mit Dienstleistern und Lieferanten werden in einem Dokumentenmanagementsystem erfasst, damit der Abschluss von Verträgen nach § 29 KDG nachvollziehbar und der Inhalt der Verträge einsehbar ist.

9.5 Auftragsverarbeiter sind im Hinblick auf die vertraglich vereinbarten technischen und organisatorischen Maßnahmen regelmäßig zu überprüfen. Das Ergebnis ist zu dokumentieren.

10 Datenübermittlung

10.1 Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung des Betroffenen zulässig.

10.2 Befindet sich der Empfänger personenbezogener Daten außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Maßnahmen zur Wahrung von Rechten und Interessen Betroffener. Eine Datenübermittlung ist zu unterlassen, wenn das Drittland, in dem der Empfänger seinen Sitz hat, kein angemessenes Datenschutzniveau bietet oder andere geeignete Garantien nicht vorhanden sind. Eine solche Garantie besteht insbesondere in Standarddatenschutzklauseln, die mit dem Empfänger abgeschlossen werden.

11 Datenschutzvorfälle

11.1 Bei der Verletzung des Schutzes personenbezogener Daten, etwa durch Abfluss von Daten nach einem IT-Vorfall oder durch unbefugten Zugriff auf Daten nach dem Verlust eines Notebooks, ist innerhalb von 72 Stunden eine Meldung an die Datenschutzaufsicht abzusetzen. Soweit die Voraussetzungen des § 34 KDG erfüllt sind, müssen auch die von der Verletzung Betroffenen benachrichtigt werden.

11.2 Vor der Meldung an die Datenschutzaufsicht und der Benachrichtigung der Betroffenen ist der eDSB anzuhören. Der Inhalt von Meldung und Benachrichtigung ist mit ihm abzustimmen.

11.3 Der Bereich der Kirchengemeinde, in deren Verantwortungsbereich der Datenschutzvorfall fällt, schlägt unverzüglich Maßnahmen zur Behebung der Verletzung und zur Abmilderung möglicher nachteiliger Auswirkungen vor. Soweit Maßnahmen

keinen Aufschub dulden, sind sie umgehend zu ergreifen. Sämtliche Maßnahmen werden dokumentiert.

11.4 Wenn von einer Meldung abgesehen werden kann, sind die Gründe dafür gemäß § 33 Abs. 5 KDG zu dokumentieren.

12 Rechte von betroffenen Personen

12.1 Betroffene Personen, insbesondere Beschäftigte, Kunden sowie Ansprechpartner bei Dienstleistern und Lieferanten, haben das Recht auf Transparenz der Verarbeitung (insbesondere Informationspflichten nach den §§ 15 und 16 KDG sowie Auskunftsrecht nach § 17 KDG), auf Richtigkeit der Verarbeitung (insbesondere Recht auf Berichtigung nach § 18 KDG, auf Löschung nach § 19 KDG und auf Einschränkung der Verarbeitung nach § 20 KDG) sowie auf Beschränkung der Verarbeitung (insbesondere Widerspruchsrecht nach § 23 KDG).

12.2 Die betroffenen Personen werden bei der Ausübung ihrer Rechte durch die Kirchengemeinde unterstützt.

12.3 Bei der Bearbeitung von Anträgen ist die Identität der betroffenen Person zweifelsfrei festzustellen.

12.4 Die Leitung der Kirchengemeinde trifft geeignete Maßnahmen, um betroffenen Personen alle Informationen gemäß den §§ 15 und 16 KDG und alle Mitteilungen gemäß den §§ 17 bis 24 und § 34 KDG, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache innerhalb der gesetzlichen Fristen zu übermitteln.

12.5 Die Leitung der Kirchengemeinde trifft geeignete Maßnahmen, um eine weitere Verarbeitung zu unterbinden, wenn eine betroffene Person ihr Recht auf Widerspruch (§ 23 KDG) ausübt.

12.6 Die Erteilung von Auskünften ist zu dokumentieren.

13 Beschwerden

13.1 Betroffene Personen können sich über eine Verarbeitung ihrer personenbezogenen Daten beschweren, sollten sie sich durch die Verarbeitung in ihren Rechten verletzt fühlen. Insbesondere können Beschäftigte Verstöße gegen diese Richtlinie jederzeit anzeigen.

13.2 Die Leitung der Kirchengemeinde stellt sicher, dass Beschwerden in angemessener Zeit beantwortet werden und berechtigten Beschwerden abgeholfen wird.

13.3 Beschäftigte können sich jederzeit an den eDSB wenden (Kontaktdaten unter Ziffer 4.1). Soweit es erforderlich ist, wird für Beschwerden anderer betroffener Personen ein Eskalationsprozess eingerichtet. Im Rahmen dieses Prozesses bearbeitet der eDSB Beschwerden, die nach einer ersten Reaktion der Kirchengemeinde aufrechterhalten werden.

14 Auskunftsersuchen Dritter über betroffene Personen

Sollten Dritte, insbesondere Behörden, Informationen über betroffene Personen fordern, beispielsweise über Kunden oder Beschäftigte der Kirchengemeinde, ist eine Weitergabe von Informationen nur zulässig, wenn

- eine gesetzliche Norm zur Auskunft verpflichtet oder

- die Kirchengemeinde ein berechtigtes Interesse an der Weitergabe der Informationen hat und
- die Identität des anfragenden Dritten zweifelsfrei feststeht.

15 Sensibilisierung und Schulung

15.1 Beschäftigte, die an den Verarbeitungsvorgängen beteiligt sind, werden in geeigneter Weise für den Datenschutz sensibilisiert. Der Inhalt von entsprechenden Schulungen umfasst die gesetzlichen Vorgaben sowie diese Richtlinie. Im Übrigen entscheidet der eDSB über Inhalt, Form und Turnus der Schulungen.

15.2 Die Teilnahme an den Schulungen ist zu dokumentieren.

16 Vertraulichkeit

16.1 Beschäftigten ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Sie sind vor Aufnahme ihrer Tätigkeit gemäß § 5 KDG schriftlich auf das Datengeheimnis zu verpflichten. Die Verpflichtung erfolgt durch die Leitung der Kirchengemeinde unter besonderem Hinweis auf die strafrechtlichen Vorschriften des Datenschutzrechts.

16.2 Unterliegen Beschäftigte besonderen Geheimhaltungsverpflichtungen, insbesondere dem Telekommunikationsgeheimnis nach § 88 Telekommunikationsgesetz, werden sie von der Leitung der Kirchengemeinde darauf ergänzend verpflichtet.

17 Sicherheit der Verarbeitung

17.1 Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen schließen unter anderem Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Datenverarbeitung auf Dauer sicherzustellen,
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

17.2 Die Leitung der Kirchengemeinde führt zu diesem Zweck ein Managementsystem für Informationssicherheit (ISMS) ein, das in einer gesonderten Richtlinie niedergelegt ist. Der eDSB berät bei der Einführung des ISMS.

17.3 Die technischen und organisatorischen Maßnahmen sind fortlaufend zu dokumentieren.

18 Folgen von Verstößen

Ein Verstoß gegen diese Richtlinie kann arbeitsrechtliche Maßnahmen nach sich ziehen, einschließlich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

19 Aktualisierung der Richtlinie

19.1 Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie regelmäßig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

19.2 Änderungen an dieser Richtlinie sind formlos wirksam. Die Beschäftigten und leitenden Angestellten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

Lastrup, den 15.11.18