Anlage III
zum Auftragsverarbeitungsvertrag nach Art.28 Abs.3 DSGVOim Rahmen des Jugendhilfeprojektes Babybegrüßungsbesuche (BBB)

zu Pkt. 8: Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

Technische und organisatorische Maßnahmen gemäß § 29 KDG

Die Verarbeitung von personenbezogenen Daten im Auftrag erfolgt im Einklang mit den gesetzlichen Anforderungen des Datenschutzes und gewährleistet den Schutz der Rechte der betroffenen Personen. Im Folgenden werden die zum Schutz der Daten geeigneten und getroffenen technischen und organisatorischen Maßnahmen des Caritasverbandes für Saarbrücken und Umgebung e.V. im Haus der Caritas beschrieben.

1. Wahrung der Vertraulichkeit (§ 29 Abs. 1 lit. b KDG)

Folgende technischen und organisatorischen Maßnahmen werden vom Auftragnehmer zur Wahrung der Vertraulichkeit ergriffen:

1.Zutrittskontrolle - Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

Der Caritasverband für Saarbrücken und Umgebung e.V. hat seinen Geschäftssitz im Stadtzentrum in der Johannisstraße 2, 66111 Saarbrücken. Die Mitarbeiter/Innen verfügen über einen RFID-Chip um Zutritt zu den Geschäftsräumen zu erlangen. Zusätzlich verfügt jede Etage über eine immer verschlossene Etagenzugangstür, sodass der Zugang zu den Büros nur mit einem zusätzlichen Schlüssel möglich ist. Die Ausgabe der Chips und Etagenzugangsschlüssel wird mithilfe eines Schlüsselkonzepts verwaltet. Generalschlüssel sind nur einem begrenzten Personenkreis ausgehändigt.
Im Eingangsbereich ist eine Pforte eingerichtet, die in den Zeiten von 08.00 – 12.30 Uhr und von 13.30 – 16.00 Uhr (Mo – Do) und 08.00 – 12.30 Uhr (Fr.) besetzt ist und an der die Anmeldungsmöglichkeit zu den Diensten und Fachbereichen oder der Erhalt von Informationen möglich ist. Klienten werden entweder in den Wartebereich hinter der Pforte gebeten oder bei den Mitarbeitern/Innen der in den 6 Etagen verteilten Dienste angekündigt, d i e diese an den jeweiligen verschlossenen Etagentüren abholen und zu den Besprechungsräumen geleiten. Einzelne Dienste verfügen jenseits der Etagentüren über weitere Wartebereiche, die jedoch erst nach Öffnung der Etagentüren durch die Mitarbeiterinnen der Dienste erreichbar sind. Klienten erhalten keinen unkontrollierten Zutritt.

Der Serverraum ist verschlossen und verfügt über keine sonstige Zutrittsmöglichkeit. Zutritt ist grundsätzlich nur berechtigten Personen gestattet oder in Ausnahmefällen nur in Begleitung von berechtigten Personen.

2. Zugangskontrolle - **Keine unbefugte Systembenutzung**

Die Mitarbeiterinnen verfügen über individuelle Benutzerkonten und melden sich individuell am System an. Dazu ist zur Benutzeridentifikation die Eingabe eines nach der Komplexitätsrichtlinie gestalteten Kennworts notwendig (regelmäßiger Passwortwechsel: max. Gültigkeit: 90 Tage). Schutzgerecht werden Firewalls je Gateway und Virenschutz eingesetzt. Für Arbeitspausen der Mitarbeiter/Innen ist eine automatische Sperrung der Bildschirme mit Passwortschutz eingerichtet. Mobile Geräte und Datenträger sind nach einem Standardverfahren verschlüsselt.

3. Zugriffskontrolle - **Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems**

Für Schutz gegen unberechtigte Zugriffe sorgen Firewalls, Virenschutz und individuelle Passwörter. Die Zugriffsrechte werden mithilfe einer Rollen- und Rechteverwaltung durch die IT vergeben. Die Datenträger werden verwaltet. Die Datenträger sind entsprechend gekennzeichnet. Sicherungsdatenträger werden ausgelagert. Nicht mehr benötigte Datenträger werden fachgerecht mechanisch vernichtet. Papierakten werden nach Sicherheitsstufe 4 systematisch entsorgt. Der Umgang mit mobilen Datenträgern ist reglementiert. Individuell können Lese- und Schreibrechte vergeben werden.

4.Trennungskontrolle - **Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden**

Für unterschiedliche Verarbeitungszwecke existieren getrennte Dateiebenen bzw. Speicher- bereiche.

5.Pseudonymisierung (§ 26 Abs. 1 lit. a KDG; § 27 Abs. 1 KDG)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen:
Findet im Rahmen dieses Projektes nicht statt.

2. Integrität (§ 26 Abs. 1 lit. b KDG)

Folgende technischen und organisatorischen Maßnahmen werden vom Auftragnehmer zur Wahrung der Integrität ergriffen:

1. Weitergabekontrolle - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

Die Weitergabe von personenbezogenen Daten an Dritte per E-Mail erfolgt nicht in der E-Mail sondern mittels angehängter Dateien, die mit einem Kennwort geschützt sind. Ansonsten findet Datenversandt mittels Post- oder Faxversandt statt. Der Datenträgertransport zur extern hinterlegten Datensicherung erfolgt sicherheitsorientiert und durch zuverlässige Mitarbeiterinnen. Die Datenträger sind nach Sicherheitsstandard verschlüsselt.

2 Eingabekontrolle- Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind

Die Eingabeverfahren mit Festlegung der für die Erstellung von Datenträgern und der Bearbeitung von Daten Befugten werden dokumentiert. Im Rahmen der Backups gesicherte Daten werden zu keinem Zeitpunkt verändert. Systemaktivitäten werden serverseitig protokolliert und kontrolliert.

3. Verfügbarkeit und Belastbarkeit (§ 26 Abs. 1 lit. b KDG)

Folgende technischen und organisatorischen Maßnahmen werden vom Auftragnehmer zur Gewährleistung von Verfügbarkeit und Belastbarkeit ergriffen:

Verfügbarkeitskontrolle - Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

Die notwendigen Brandschutzmaßnahmen sind getroffen. Für den Fall eines Stromausfalls ist im Serverraum eine USV etabliert. Zur Datensicherung existiert ein Backup-Konzept, die Festplatten werden getrennt voneinander aufbewahrt und sind verschlüsselt. Die Speichermedien sind redundant ausgelegt. Ein Notfallplan beschreibt Vorkehrungen nach einem Schadensfall und sorgt für rasche Wiederherstellbarkeit.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (§ 26 Abs. 1 lit. d KDG; § 27 Abs. 1 KDG)

Folgende organisatorischen Maßnahmen werden zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen

Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung ergriffen:

1. Datenschutz-Management

In Teilbereichen existieren schriftliche Regelungen und Verfahrensbeschreibungen zum Betrieb und den Abläufen der Datenverarbeitung und den verschiedenen Datensicherheitsmaßnahmen (IT-Sicherheitskonzept). Die Sicherung der Daten erfolgt nach einem Datensicherungskonzept. Zur IT – Sicherheit wird auf etablierte Standards zurückgegriffen. In Teilbereichen werden Protokolle erstellt. Es finden Audits zur Kontrolle über die Einhaltung von Datenschutz- und Datensicherungsmaßnahmen statt. Mitarbeiterinnen werden systematisch über ein Onlinesystem und –programm geschult. Bei wichtigen bzw. sensiblen Datenverarbeitungsnotwendigkeiten wird das 4-Augen-Prinzip angewandt.

2. Incident-Response-Management

Eine Verfahrensdokumentation beschreibt das Vorgehen einer notwendigen Meldung an die Diözesandatenschutzbeauftragte und die Berücksichtigung der Rechte der Betroffenen.

3. Datenschutzfreundliche Voreinstellungen (§ 27 Abs. 2 DS-GVO)

Bei der Implementierung neuer IT- Technologien oder Software wird der Stand der Technik und die wirksame Umsetzung von Datenschutzgrundsätzen sowie Art, Umfang, Umstände und Zweck der Verarbeitung berücksichtigt unter besonderer Berücksichtigung der mit der Verarbeitung verbunden Risiken zum Schutze der Rechte der betroffenen Personen. Entsprechende Voreinstellungen bzgl. Menge der Daten, Umfang der Verarbeitung, Speicherfrist, Zugänglichkeit orientieren sich an der Erforderlichkeit.

4. Auftragskontrolle - Keine Auftragsdatenverarbeitung im Sinne des § 29 KDG ohne entsprechende Weisung des Auftraggebers

Jede Auftragsverarbeitung geschieht auf der Grundlage eindeutiger Vertragsgestaltung. Dienstleister unterliegen einem kontrollierten und sorgfältigen Auswahlverfahren und Nachkontrollen. Der Caritasverband für Saarbrücken e.V. hat einen Datenschutzbeauftragten bestellt, der im Rahmen seiner Zuständigkeiten datenschutzkonform tätig ist.