Anlage III
zum Auftragsverarbeitungsvertrag nach Art.28 Abs.3 DSGVO im 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 § 27 DSG-EKD

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 Diakonischen Werkes an der Saar gGmbH beschrieben.

1. Wahrung der Vertraulichkeit (§ 27 Abs. 2 DSG-EKD)

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

1. Zutrittskontrolle - Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

Das Diakonische Werk an der Saar gGmbH hat seinen Geschäftssitz in der Rembrandtstraße 17-19, 66540 Neunkirchen-Wiebelskirchen.
Die Serverräume in der Geschäftsstelle in Neunkirchen-Wiebelskirchen sind verschlossen und verfügen über keine sonstige Zutrittsmöglichkeit (elektronische Zutrittskontrolle). Zutritt ist grundsätzlich nur berechtigten Personen gestattet oder in Ausnahmefällen nur in Begleitung von berechtigten Personen. Die Serverräume sind Alarmgesichert. Der Zutritt erfolgt ausschließlich durch berechtigte Personen mit entsprechend konfigurierten Zugangschips.
Die Geschäftsräume in den betreffenden Einrichtungen, die die Einladungen an die Eltern verschicken sollen (Stadtteilbüro Malstatt, BürgerInnenzentrum Brebach, GemeinWesenArbeit Burbach, Gemeinwesenarbeit Dudweiler-Mitte, Gemeinwesenarbeit Völklingen-Mitte) können nur über einen entsprechenden Schlüssel betreten werden. Der Zugang zu den einzelnen Büros ist nur mit einem entsprechenden Schlüssel möglich. Klienten erhalten keinen unkontrollierten Zutritt.

2. Zugangskontrolle - **Keine unbefugte Systembenutzung**

Die Mitarbeitenden 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: 182 Tage). Schutzgerecht werden Firewalls je Gateway und Virenschutz eingesetzt. Die Bildschirme der Mitarbeitenden werden automatisch nach 4 Minuten gesperrt und können nur durch Eingabe des Benutzerkennwortes entsperrt werden.

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 Abteilungsleitungen vergeben und durch die Mitarbeitenden in der IT umgesetzt. Die Datenträger werden verwaltet. Nicht mehr benötigte Datenträger werden fachgerecht mechanisch vernichtet. Es besteht die Möglichkeit, Papierakten nach Sicherheitsstufe 3 systematisch durch einen zertifizierten Entsorger zu vernichten. Mobile Datenträger sind nicht zugelassen.

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

Für unterschiedliche Verarbeitungszwecke existieren getrennte Dateiebenen bzw. Speicherbereiche.

5. **Pseudonymisierung (§ 27Abs. 1.1 DSG-EKD)**
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 (§ 27 Abs. 1.2 DSG-EKD)

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**

Eine elektronische Übertragung außerhalb des VDI-Systems findet nicht statt.

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

Im Rahmen der Backups gesicherte Daten werden zu keinem Zeitpunkt verändert.

3. Verfügbarkeit und Belastbarkeit (§ 27 Abs. 1.3 DSG-EKD)

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

1. Verfügbarkeitskontrolle - Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust

Die notwendigen Brandschutzmaßnahmen sind getroffen. Für den Fall eines Stromausfalls sind in den Serverräumen USVs etabliert. Zur Datensicherung existiert ein Backup-Konzept. Die Storages sind redundant in zwei getrennten Serverräumen in verschiedenen Brandabschnitten installiert. Die Speichermedien sind redundant ausgelegt. Ein Notfallkonzept beschreibt Vorkehrungen nach einem Schadensfall und sorgt für rasche Wiederherstellbarkeit.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (§ 27 Abs. 1.4 DSG-EKD)

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 Verfahrens-beschreibungen 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.

Mitarbeitende werden vor Beginn der Maßnahme geschult.

2. Incident-Response-Management

Das Vorgehen bei Offensichtlichwerden eines Datenschutzvorfalls regelt die Meldeketten. In einem solchen Fall meldet der Datenschutzbeauftragte der Diakonie Saar mittels eines standardisierten Verfahrens diesen Vorfall an den Beauftragten für Datenschutz der Evangelischen Kirche Deutschland (EKD) mit Sitz in Hannover.

3. Datenschutzfreundliche Voreinstellungen (§ 28Abs. 2 DSG-EKD)

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 § 30 DSG-EKD ohne entsprechende Weisung des Auftraggebers

Jede Auftragsverarbeitung geschieht auf der Grundlage eindeutiger Vertragsgestaltung. Dienstleister unterliegen einem kontrollierten und sorgfältigen Auswahlverfahren und Nachkontrollen. Das Diakonische Werk an der Saar gGmbH hat einen Datenschutzbeauftragten bestellt, der im Rahmen seiner Zuständigkeiten datenschutzkonform tätig ist.