KVJS
Kommunalverband
für Jugend und Soziales
Baden-Württemberg

Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO (Verfahrensverzeichnis)

lfd. Nr.: 02

☐ Erstmalige Beschreibung der Verarbeitungstätigkeiten personenbezogener Daten – Wahrnehmung der Aufgaben zum Schutz der Kinder und Jugendlichen in (teil-) stationären Einrichtungen (§§ 45 bis 48a SGB VIII)
Datum: 12.07.2018 (Programm Heime-BW erstmalig 30.07.2010)

☒ Änderung der Beschreibung vom
Datum: 12.07.2018 Datum 16.10.2024
Aktenzeichen: AZ

1. Angaben zur verarbeitenden Stelle

1.1 Bezeichnung des Dezernats oder der Einrichtung des KVJS:
Dezernat 4, Jugend - Landesjugendamt, Referat 43.

1.2 Name, Telefonnummer, Mail-Adresse des/der Verantwortlichen, in der Regel Referatsleiter/in:
Michael Riehle, Telefon 0711/6375-430,
E-Mail: michael.riehle@kvjs.de.

1.3 Name; Telefon-Nr., Mail-Adresse des Vertreters/ Vertreterin des/der Verantwortlichen:
Gudrun Mittner, Telefon 0711/ 6375-435, E-Mail: gudrun.mittner@kvjs.de.

1.4 Kontaktdaten der/des Datenschutzbeauftragten:
Unsere/n Datenschutzbeauftragte/n erreichen Sie per E-Mail unter:
datenschutz@kvjs.de. Alternativ postalisch unter folgender Adresse:

Kommunalverband für Jugend und Soziales Baden-Württemberg
z.Hd. Datenschutzbeauftragte/r
Lindenspürstraße 39
70176 Stuttgart

2. Zweck der Verarbeitung der personenbezogenen Daten

2.1 Verarbeitendes Referat: Referat 43 Hilfe zur Erziehung

2.2 Konkrete Beschreibung der Aufgabe, für die die personenbezogenen Daten benötigt werden:

Durchführung des Betriebserlaubnisverfahrens mit Bescheid nach § 45 SGB VIII.
-Prüfung des Antrags des Trägers auf Betriebserlaubnis nach § 45 SGB VIII, ob die Voraussetzungen für den Betrieb einer Einrichtung erfüllt sind.
Einholung der Stellungnahmen zum vorgelegten Antrag des Trägers auf Erlaubnis beim örtlich zuständigen Jugendamt, Baurechts- und in der Regel auch beim Gesundheitsamt. Bei Einrichtungen der Eingliederungshilfe nach SGB IX wird der örtliche Sozialhilfeträger bzw. die örtliche Heimaufsicht beteiligt.
-Erlass eines Bescheids.

2.3 Rechtsgrundlage:

Erlaubnis für den Betrieb einer Einrichtung nach § 45 SGB VIII.

3. Betroffener Personenkreis und Daten

3.1 Beschreibung der Kategorien betroffener Personen, zum Beispiel Antragsteller, externe oder interne Personengruppen, Bewerber, Zahlungsempfänger usw.:

Trägervertreter, Leitungspersonal, Fachdienstpersonal, Betreuungspersonal. Bei Angeboten in häuslicher Gemeinschaft auch Vertretungskräfte des Betreuungspersonals im Urlaubs- und Krankheitsfall.

3.2 Beschreibung aller Datenkategorien, die erhoben werden:

Antragstellender Trägervertreter: Name, Vorname, Telefonnummer, Mail-Adresse,
Einrichtungsleitung: Name, Vorname, Geburtsdatum, Qualifikation, Beschäftigungsverhältnis, Telefon-Nr., Mail-Adresse,
Fachdienst: Name, Vorname, Geburtsdatum, Qualifikation, anteiliger Beschäftigungsumfang, Beschäftigungsverhältnis,
Betreuungsdienst: Name, Vorname, Geburtsdatum, Qualifikation, anteiliger Beschäftigungsumfang, Beschäftigungsverhältnis, Zuordnung Einrichtung/steil.

4. Empfängerkategorien

4.1 Beschreibung der Empfänger, die diese personenbezogenen Daten erhalten:

Beim Betriebserlaubnisverfahren mit den Antragsunterlagen des Trägers:
Örtlich zuständiges Jugendamt,
Örtlich zuständiges Baurechtsamt,
Ggf. örtlich zuständiges Gesundheitsamt,
Ggf. örtlich zuständiger Sozialhilfeträger bzw. zuständige Heimaufsicht,
Bemerkung: Im Bescheid sind keine personenbezogenen Daten enthalten.

4.2 Beschreibung zukünftiger Empfänger der personenbezogenen Daten:

Erfolgt nicht.

4.3 Empfänger innerhalb unserer Behörde nach Funktionsbezeichnung/ OE:

Referat 43: zuständiger Sachbearbeiter mit Eingabe in das Programm Heime-BW des KVJS, ggf. Stellvertreter, Sekretariat zur Aktenanlage, ggf. Referatsleitung und stellvertretende Referatsleitung.
Ggf. Dezernent für Jugend – Landesjugendamt.
Zuständiger Sachbearbeiter mit Eingabe in das Programm Heime-BW des KVJS.

4.4 Auftragsdatenverarbeitender (Name des Dritten, der die Daten für den KVJS im Auftrag verarbeitet):

Service-Provider Bringe Informationstechnik GmbH in Karlsruhe.

4.5 Drittländer; konkrete Benennung des Konsulats oder ähnliche Angaben:

Erfolgt nicht.

5. Löschungsfristen

5.1 Regelfrist für die Sperrung und Löschung:

Speicherdauer: Die Daten werden nach Ablauf von zehn Jahren gelöscht.

5.2 Fristen für die regelmäßige Überprüfung der Sperrung und Löschung:

6. Beschreibung der technischen und organisatorischen Maßnahmen

6.1 Verschlüsselung der personenbezogenen Daten: Erfolgt nicht.

6.2 Pseudonymisierung: Erfolgt nicht.

6.3 Sicherstellung der Fähigkeiten von Systemen und Diensten:

Die Aktenführung erfolgt in Papierform. Die Aktenbände werden datensicher aufbewahrt.

- Vertraulichkeit/ Schutz vor unbefugter Preisgabe der Informationen:

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle Rechenzentrum/ Provider: Der Zutritt zu den Datenverarbeitungsanlagen in den Rechenzentren des Auftragnehmers sind durch technische Einrichtungen nach dem Stand der Technik gegen physischem Zugriff durch unautorisierte Dritte geschützt: Das Betreten der Gelände und Gebäude wird durch Codeschlösser mit 2 Faktoren (Chipkarte + PIN), Alarmanlagen und VIDEO-Überwachung gesichert. Die eigentlichen Sicherheitsbereiche sind jeweils durch Schleusen und weitere elektronische Schlösser abgetrennt. In den Sicherheitsbereichen findet ebenfalls eine ständige VIDEO-Überwachung statt. Nur eine bekannte und kleine Zahl von Personen hat zu den inneren Sicherheitsbereichen Zutritt. Aktuell muss an vier Stationen (Gelände, Gebäude, Brandabschnitt, Cage) eine erfolgreiche Authentifizierung erfolgen, bevor der Zugriff auf den inneren Sicherheitsbereich möglich ist.

Zugangskontrolle Rechenzentrum/ Provider: Neben der physischen Absicherung der DV-Anlagen, ist eine elektronische Sicherung des Zugriffs auf die Systeme durch Verwendung von sicheren Zugangsprozeduren (2-Faktor-Authentifizierung, Anmeldesperre nach wiederholter Fehlanmeldung, Public-Key-Verfahren und sichere Kennwörter gewährleistet. Nach Möglichkeit werden Daten nur verschlüsselt abgelegt. Eine interne Password-Policy ist vereinbart und wird regelmäßigen Audits (IS027001) unterworfen. Im Rahmen einer möglichen Fernwartung wird diese in den Räumen des Auftraggebers nur mit seiner Zustimmung und unter seiner Kontrolle durchgeführt. Insbesondere wird auch sichergestellt, dass der Zugriff auf die IT-Systeme während der Fernwartung nur über verschlüsselten Weg (VPN, SSL) erfolgt.

Zugriffskontrolle

Durch Vergabe minimaler Rechte in einem Rollenmodell wird die Zahl der jeweils berechtigten User auf ein System und seine Daten klein gehalten. Zugriffe werden protokolliert und einem regelmäßigen

Review unterzogen. Regelmäßige Schulungen der betreffenden Mitarbeiter in Datenschutzfragen und im Rahmen der IS027001-Audits finden ergänzend statt.

Software – Heime-BW: Die Melde- und Statistiksoftware für Heime der Jugendhilfe in Baden-Württemberg im Weiteren kurz „Heime-BW“ genannt, verfügt über ein eigenes, differenziertes Berechtigungskonzept. Dieses basiert auf klar unterschiedenen, auf die jeweilige Aufgabe eines Nutzers hin limitierten Rechten. Das geschieht in Heime-BW mittels Autorisierung und Vergabe von Zugriffsrechten mit Benutzerkennung und Passwort. Dabei wird unterschieden nach Leserecht bzw. Schreib- und Leserecht. Ferner wird damit der Zugriff auf die Daten restriktiv geregelt und entsprechend der Rolle eines Nutzers eingeschränkt. Nutzerkennungen, d.h. Nutzername und Passwort sind an den jeweiligen Nutzer gebunden und dürfen nicht weiter gegeben werden.

Trennungskontrolle

Provider/Rechenzentrum: Der Zugriff auf spezifische Datenbereiche ist durch technische Maßnahmen (Netzwerksegmentierung, Verschlüsselung, Sandboxing) nur dem jeweils Berechtigten möglich. Servercluster werden jeweils in eigenen, durch Firewalls abgetrennten Subnetzen betrieben. Zugriffe werden protokolliert. Überwachung des aus- und eingehenden Datenverkehrs an den jeweiligen Netzwerkgrenzen.

Heime-BW: Verwendet werden eigene Datenbanken, die ausschließlich für Heime-BW zur Verfügung stehen. Datenbestände werden nicht in Entwicklungs- und Testumgebungen verarbeitet. Produktiv- und Testsystem sind strikt getrennt.

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Insofern von uns personenbezogene Daten im Rahmen unserer Aufgaben verarbeitet werden (User-Zugriffe, IP-Adressen, Zugriffszeit und -Dauer in Firewall- und Serverlogs), werden diese nach angemessener Zeit (4 Wochen) wieder gelöscht. Eine Weitergabe erfolgt nicht. Eine Auswertung dieser Daten erfolgt nur zur Klärung technischer oder datenschutzrechtlicher Fragen (Ausschluss von Missbrauch der DVA (Datenverarbeitungsanlage), SLA (Service-Level-Agreement)-Überwachung).

- Verfügbarkeit des IT-Systems:

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
Verfügbarkeitskontrolle

Durch die Unterbringung der Serversysteme in

- Hochsicherheitsbereichen mit mehrfach redundanter Stromversorgung (Redundanz auf 20kV-Ebene, redundante Diesel- und USV-Anlagen,
- Sicherung der Daten über Backupverfahren (täglich, wöchentlich, monatlich),
- Schutz gegen Feuer (automatisches Gas-Schnüffelsystem und Brandmeldesystem; Inert-Gas-Löschsystem),
- Schutz gegen physikalischen Zugriff,
- Schutz gegen Schadsoftware,
- mit Firewalls und durch

ein umfassendes Monitorsystem

- werden die Daten gegen Umweltschäden und oder Zerstörung durch Dritte geschützt
- und die Verfügbarkeit im Rahmen eines 24/7-SLAs gewährleistet. Dazu gehört auch

- eine mehrfach redundante Anbindung im Backbone (aktuell 5 x 10 GB/s) über vier unabhängige Carrier
- redundante Gestaltung des Providerbackbones.

Die genauen Details sind im Hostingvertrag geregelt.

- Integrität/ Sicherstellung der Unversehrtheit und Korrektheit der Daten:

Integrität (Art. 32 Abs. 1 lit b DS-GVO)

Weitergabekontrolle

Es erfolgt keine Weitergabe der Daten ohne expliziten Auftrag bzw. Weisung durch den Auftraggeber. Auftragsgemäßer Zugriff auf die Daten erfolgt über verschlüsselte Wege (VPN, SSL).

Heime-BW - Übermittlungskontrolle: Der Kommunikationsweg zwischen Anwender und System wird nach dem heute üblichen Standard per SSL verschlüsselt. Es handelt sich dabei um ein SAN- bzw. UCC-Zertifikat mit einer 256-Bit-Verschlüsselung für das Produktivsystem und das Testsystem. Sicherung durch Firewall und VPN (s. a. Verfügbarkeitskontrolle).

Eingabekontrolle

Provider/Rechenzentrum: Zugriff auf die DVA werden protokolliert und Eingabe, Änderung oder Löschung personenbezogener Daten nur im Rahmen des Hauptauftrags bzw. nach Weisung und Kontrolle des Auftraggebers durchgeführt.

Heime-BW: Automatische Protokollierung der Eingaben in Logfiles. Elemente sind:

- der betroffene Datensatz, ·
- Art der Aktivität (Anlage, Veränderung, Löschung des Datensatzes) ·
- Zeitpunkt der Aktivität bzw. des Ereignisses ·

- ausführende Person (Benutzerkennzeichen)

Auftragskontrolle
Zwischen dem Auftraggeber und dem Provider gibt es entsprechende Vereinbarungen. Der Provider ist nach ISO 27001 zertifiziert und gegenüber dem KVJS-Landesjugendamt weisungsgebunden.

- Fähigkeit der raschen Wiederherstellung der Verfügbarkeit und des Zugangs der Daten im Störfall:
Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
wird durch ein umfassendes Backupsystem, Redundanz in der RZ-Architektur und Vorhalten von Ersatzsystemen gewährleistet. Die Details sind in den jeweiligen Hostingverträgen näher geregelt.

6.4 Verfahren zur Überprüfung der Gewährleistung der Sicherheit der Verarbeitung:

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Regelmäßige Audits im Rahmen der IS027001/2013 zur Überprüfung des Datenschutz-Status;
- Engmaschiges Monitoring der Systeme und ihrer Umgebung auf abnormales Verhalten mit Ampelsystem (ok/warn/Error) und zusätzlichem Metering (Dokumentation) wichtiger Systemstatik zur Überwachung der Systemdaten im zeitlichen Verlauf. Dokumentation der Analyse und gegebenenfalls durchgeführter Entstörmaßnahmen (Abhilfe; Incident-Reports);
- Incident-Response-Management;
- Regelmäßige Risikoanalyse zur Ermittlung von HotSpots (Systemen an der Belastungsgrenze) und/oder Systemen, die allein für eine wichtige Funktion stehen (SPOF's);
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);
- Auftragskontrolle.
  Es findet keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftragsgebers statt.
    - Falls Unterauftragnehmer erforderlich sind, erfolgt Ihre Auswahl nach den Kriterien der DS-GVO.
    - In regelmäßigen Abständen wird überprüft, dass die Rahmenbedingungen der DS-GVO eingehalten werden.
    - Weisungen/Aufträge werden auf mögliche Kollisionen mit dem Datenschutz überprüft und diese dem Auftragnehmer mitgeteilt.

6.5 Wenn ein Datenschutzkonzept vorliegt, welches das vorliegende Verfahren erfasst, bitte dieses beifügen.

Liegt nicht vor.

Datum:

Telefon-Nummer:

Fax-Nummer:

E-Mail-Adresse: