

<u>Freigabe von Automatisierten Verfahren</u> gem. § 7, 1 Landesdatenschutzgesetz	Vorblatt
--	-----------------

Angaben zum Verantwortlichen:

Stadt Eutin – Der Bürgermeister – Markt 1, 23701 Eutin

Tel.: 04521 7930

E-Mail: poststelle@eutin.de

Angaben zum Datenschutzbeauftragten:

Behördlicher Datenschutzbeauftragter

Stadt Eutin, Markt 1, 23701 Eutin

Tel.: 04521 793121

E-Mail: datenschutz@eutin.de

Angaben zur verantwortlichen Organisationseinheit für das nachfolgend beschriebene Verfahren

Jugendzentrum Eutin, Lübecker Str. 11, 23701 Eutin

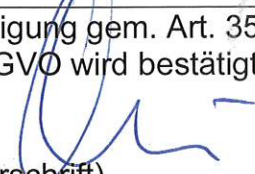
Bezeichnung des Verfahrens:

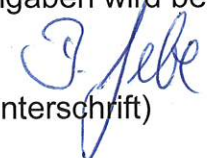
Nupian Ferienprogramm

Angaben zum Verarbeitungsverfahren

Datum der ersten Inbetriebnahme:	03.06.2023
Datum der letzten Änderung:	Entfällt, da Erstbetrieb
Alter Versionsstand	entfällt
Neuer Versionsstand	Nupian Ferienprogramm Version 1
Beschreibung des Verarbeitungszwecks:	Verwaltung und Abwicklung eines Ferienprogrammes: erfasst werden Namen und Kontaktdaten von Eltern und Kindern (incl. Anschrift, Geburtsdatum und Telefonnummern), Veranstaltungen und die Kontaktdaten derer Anbieter
Rechtsgrundlage der Verarbeitung:	Durch vorgegebene Einwilligung bei Registrierung im Ferienpassprogramm erfolgt die Verarbeitung ausschließlich aufgrund von Art 6 Abs. 1 lit. a DSGVO.
Beschreibung der Testumgebung	Keine Testumgebung – wird beim Programmanbieter gehostet
Beschreibung des Tests bzw. aus welchen Gründen kein Test durchgeführt werden konnte	entfällt
Test durchgeführt durch, am	entfällt
Ergebnis des Tests	entfällt
Beschreibung der Installationsumgebung	Hetzner Online GmbH, Industriestraße 25, D-91710 Gunzenhausen,
Zugriffsberechtigte Personen/ Personengruppen in der produktiv Umgebung	Tourismus GmbH: A.Suikat, N. Haack, K.Osowski; Stadt Eutin: B.Mekelnburg, J.Babenhr, B.Jebe, M.Straußfeld, M.Klehs.

Technisch-organisatorische Maßnahmen bei Datenverarbeitung berücksichtigt	Zugriff nur durch Adminanmeldung in der Software, evtl. Akten im erschließbaren Aktenschrank.
Grundsatz der Datenminimierung/ Löschungsfristen	Jedes Jahr nach Ablauf des Ferienpasses werden die Daten der anmeldenden Kinder und Eltern gelöscht.
Risiko-Abwägung vorgenommen, mit folgendem Ergebnis:	entfällt
Aufnahme in IT-Sicherheitskonzept notwendig	entfällt
Datenschutzbeauftragte wurde frühzeitig einbezogen	ja

Volker Hein Datenschutzbeauftragter	21.5.2023 (Datum)	Beteiligung gem. Art. 35 Abs. 2 DSGVO wird bestätigt:  (Unterschrift)
--	----------------------	---

Bärbel Jebe (Name der für die Verarbeitungstätigkeit intern verantwortlichen Leitungskraft)	31.5.23 (Datum)	Die Richtigkeit der o.g. Angaben wird bestätigt:  (Unterschrift)
--	--------------------	---

Einverständnis durch 2 siche amt. E-Mail

Die **FREIGABE** des automatisierten Verfahrens wird hiermit erteilt!

Eutin, den 31. 5. 23


Bürgermeister

Anlage A: Verarbeitungstätigkeit

1. Bezeichnung der Verarbeitungstätigkeit

Der Auftragnehmer verarbeitet personenbezogene Daten innerhalb der Software nupian Ferienprogramm v1, ausschließlich auf Servern in Deutschland. Die personenbezogenen Daten werden systematisiert durch die Software verarbeitet. Die Daten werden ausschließlich durch den Auftraggeber erhoben und in die Software eingepflegt. Der Auftragnehmer betreibt hierfür einen dedizierten Server im Rechenzentrum bei der Firma Hetzner Online GmbH.

Der Auftragnehmer erstellt in regelmäßigen Abständen Backups auf einem Backup-Space bei der Firma Hetzner.

Weiterhin werden in regelmäßigen Abständen verschlüsselte Backups auf einem Server im Büro der nupian GmbH erstellt.

2. Verantwortliche Abteilung

Abteilung zur Entwicklung des Ferienprogramms

Abteilung Server-Ferienprogramm

Support

3. Weitere Verantwortliche

Hetzner GmbH (siehe auch Punkt 12)

4. Zweck der Verarbeitung

Der Zweck der Verarbeitung ist die Bereitstellung der Ferienprogramm-Software für den Auftraggeber.

5. Rechtsgrundlage der Verarbeitung

Die Verarbeitung ist erforderlich zur Erfüllung eines Vertrags mit dem betroffenen Auftraggeber. (Art. 6 Abs. 1 b DSGVO)

6. Betroffene Personengruppen

Der Kreis der Betroffenen besteht aus:

- Benutzer (Eltern), die ein oder mehrere Kinder zu ein oder mehreren Veranstaltungen angemeldet haben.
- Teilnehmern (Kinder), die an Veranstaltungen teilnehmen.
- Die Veranstalter der Veranstaltungen.
- Eigene Betreuer des Auftraggebers.
- Personal beim Auftraggeber für die ein Zugang zur Software angelegt wurde.

7. Kategorien der Daten

Angaben zu Benutzer (Eltern)

Log-in-Status (aktiv/inaktiv), Name (Anrede, Vorname, Nachname), Adress- und Kontaktdaten (Str., PLZ, Ort,

E-Mail, Notfalltelefonnummer), Bankdaten (IBAN, BIC, Kontoinhaber, Mandatsreferenz, Datum SEPA Erteilung), Notiz, Bemerkung, Unterschrift, Verlosung zusammen, Antwort auf Umfrage,

Passwort (verschlüsselt)

Angaben zu Teilnehmer (Kinder)

Name (Geschlecht, Vorname, Nachname), Geburtstag, Ferienpasscode, Bemerkung, ggf. medizinische Daten wie z. B. Allergien, Medikamente oder Behinderungen,

Bemerkung, flexible Teilnehmerfragen 1-13 (durch Auftraggeber einpflegbar)

Angaben zu den Veranstaltungen

Status (aktiv/inaktiv), Nummer, Name, Datum und Uhrzeit (von, bis), Veranstalter, Ort, Kategorie, barrierefrei,

Anmeldungsart, Anzahl Plätze, Altersbeschränkung, Geschlecht, Pflichtfeld, Beschreibung, Treffpunkt, wichtig,

Webseite, Sonstiges, Gebühren, Stornokosten, PDF-Dateien, Bilder,

Angaben zum Veranstalter (E-Mail-Veranstalter, Telefonnr.-Veranstalter), Notiz, Bemerkung

Anmeldungen zu den Veranstaltungen

Status, Gebühr, Datum, Pflichtfeld, Bemerkung, Bezahlstatus

Angaben zu den Veranstaltern

Vertrag Auftragsverarbeitung FP 27.01.2022 mit Anlagen A+B - Seite 6 von 9

Log-in-Status (aktiv/inaktiv), Rechtegruppe, Ansprechpartner (Anrede, Vorname, Nachname, Telefon),

Veranstalter (Name, Straße, PLZ, Ort), E-Mail, Bankdaten (Kontoinhaber, IBAN, BIC), Bemerkung,

Benutzername, Passwort (verschlüsselt), Anzahl Log-in-Fehler

Angaben zu Mitarbeiter

Log-in-Status (aktiv/inaktiv), Benutzername, Passwort (verschlüsselt), Rechtegruppe, Admin-Rechte,

Anrede, Vorname, Nachname, E-Mail, Beschreibung, Anzahl Log-in-Fehler

8. Empfänger der Daten

Die Daten werden von der nupian GmbH nicht weitergegeben.

9. Datenübermittlung in Drittländer

Eine Übermittlung in ein Drittland findet nicht statt und ist auch nicht geplant.

10. Fristen zur Löschung

- Nach Kündigung des Auftraggebers werden dessen Daten in der Software Ferienprogramm gelöscht.
- Aus den Backups werden die Daten nach einem Jahr gelöscht.

11. Art der eingesetzten Datenverarbeitungsanlagen und Software

Software: Linux, Apache, MySQL, PHP, SSL, Mailserver (Postfix, Dovecot), SSH

Hardware: Speicherung der Daten auf einem dedizierten Server der Firma Hetzner Online GmbH sowie auf einem eigenen verschlüsselten Backup-Server in den Räumlichkeiten des Auftragnehmers

Schnittstellen: SEPA (manuell über Datei)

IDEV (manuell über Datei)

Einwohnermeldeamtsabgleich (manuell über Datei)

Excel-Export der Daten (manuell über Datei)

12. Auftragsverarbeiter

Firma Hetzner Online GmbH

Industriestr. 25

91710 Gunzenhausen

Registergericht Ansbach

HRB 6089

Geschäftsführer: Martin Hetzner

Anlage B: Technische und organisatorische Maßnahmen

I. Vertraulichkeit

Zutrittskontrolle

- Die Büroräume werden beim Verlassen abgeschlossen
- Dokumentierte Schlüsselvergabe an Mitarbeiter
- Der Zutritt für betriebsfremde Personen (z. B. Besucherinnen und Besucher) zu den Räumen ist wie folgt beschränkt: nur in Begleitung eines nupian GmbH Mitarbeiters

Zugangskontrolle

- Zugang ist passwortgeschützt, Zugriff besteht nur für berechtigte Mitarbeiter vom Auftragnehmer verwendete Passwörter müssen Mindestlänge haben.

Zugriffskontrolle

- Durch regelmäßige Sicherheitsupdates (nach dem jeweiligen Stand der Technik) stellt der Auftragnehmer sicher, dass unberechtigte Zugriffe verhindert werden.

Datenträgerkontrolle

- Festplatten werden überschrieben (gelöscht). Nach Überprüfung werden die Festplatten entsorgt.
- Defekte Festplatten, die nicht sicher gelöscht werden können, werden zerstört.

Trennungskontrolle

- Daten werden physisch oder logisch von anderen Daten getrennt gespeichert.
- Die Datensicherung erfolgt ebenfalls auf logisch und/oder physisch getrennten Systemen.

Pseudonymisierung

- Die Pseudonymisierung ist im Rahmen der Nutzung der Software nicht möglich. Nach Auftragsabwicklung liegt bei einer weiteren Verarbeitung der Daten durch den Auftraggeber (z.B. Auswerten u.a.) die Verantwortlichkeit der Pseudonymisierung beim Auftraggeber.

II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle

- Alle Mitarbeiter sind i.S.d. Art. 32 Abs.4 DSGVO unterwiesen und verpflichtet, den datenschutzkonformen Umgang mit personenbezogenen Daten sicherzustellen.
- Datenschutzgerechte Löschung der Daten nach Auftragsbeendigung.
- Möglichkeiten zur verschlüsselten Datenübertragung werden im Umfang des Hauptauftrages zur Verfügung gestellt.

Eingabekontrolle

- Die Verantwortung der Eingabekontrolle obliegt dem Auftraggeber.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Verfügbarkeitskontrolle

- bei internen Verwaltungssystemen des Auftragnehmers
- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.

- Sachkundiger Einsatz von Schutzprogrammen (Firewalls, Verschlüsselungsprogramme).
- Monitoring aller relevanten Server

- bei Hauptauftrag

- Backup- und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten.
- Sachkundiger Einsatz von Schutzprogrammen (Firewalls, Verschlüsselungsprogramme).
- Monitoring aller relevanten Server
- Einsatz von Festplattenspiegelung bei allen relevanten Servern.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO);

- Für alle internen Systeme ist eine Eskalationskette definiert, die vorgibt wer im Fehlerfall zu informieren ist, um das System schnellstmöglich wiederherzustellen.

IV. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

- Datenschutzfreundliche Voreinstellungen werden bei Softwareentwicklungen berücksichtigt (Art. 25 Abs. 2 DSGVO).

Auftragskontrolle

- Unsere Mitarbeiter werden in regelmäßigen Abständen im Datenschutzrecht unterwiesen und sie sind vertraut mit den Verfahrensanweisungen und Benutzerrichtlinien für die Datenverarbeitung im Auftrag, auch im Hinblick auf das Weisungsrecht des Auftraggebers. Die AGB enthalten detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Die nupian GmbH hat einen betrieblichen Datenschutzbeauftragten bestellt. (René Rautenberg, Radlkofenstr. 2, 81373 München)