Datenschutzkonzept

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Wir verarbeiten personenbezogene Daten stets transparent auf einer rechtlichen Grundlage und werden betroffene Personen fair darüber informieren, zu welchen Zwecken wir diese Daten erheben. Wir werden außerdem immer nur die Daten erheben und verarbeiten, die für die jeweilige Leistung benötigt werden. Mitarbeiter haben nur zu den Daten Zugang, zu dem sie diesen zur Erfüllung ihrer Aufgaben benötigen. Die uns anvertrauten Daten schützen wir wirksam vor Verlust und Diebstahl.

Unser Datenschutzkonzept ist das Erste, womit sich neue Mitarbeiter bei uns befassen müssen.

Datenschutzkonzept
(Öffentliches Verfahrensverzeichnis)

Verantwortlicher:
Stadtservice Oranienburg GmbH
Geschäftsführer Kay Duberow
André-Pican-Straße 42
16515 Oranienburg

Präambel

Die Stadtservice Oranienburg GmbH betreibt im Rahmen der kommunalen Daseinsvorsorge ein sport- und gesundheitsorientiertes Familienfreizeitzentrum. Die Idee einer „Badewanne für Oranienburg“ existierte schon seit den 1920er Jahren. Heute ist die TURM ErlebnisCity ein wichtiger und wertvoller Standortfaktor, wenn es um die Bewertung der Lebensqualität in Oranienburg geht. Durch die TURM ErlebnisCity ist es Oranienburg, nicht zuletzt durch die Lage vor den Toren der Bundeshauptstadt Berlin, gelungen, eine höhere Außenwahrnehmung zu erzielen. Oranienburg wird durch das Familienfreizeitzentrum auch von außen, das heißt auch touristisch wahrgenommen.
In Ergänzung dieses Angebotes steht in unmittelbarer Nachbarschaft die Sport-Kindertagesstätte unter dem Namen Falkennest.

Das SOG-Datenschutzkonzept besteht aus folgenden Elementen:

Die SOG fühlt sich dem Ziel verpflichtet, so wenig personenbezogene Daten wie möglich zu verarbeiten. Es werden personenbezogene Daten erhoben, um Mitarbeiter, Auftraggeber, Mittler, Lieferanten und Kunden in der EDV zu erfassen. Dies erfolgt mit dem Ziel, die tägliche Zusammenarbeit so effizient wie möglich zu gestalten.

Benennung eines Datenschutzbeauftragten
Gem. Artikel 37 Europäische Datenschutz-Grundverordnung (DS-GVO) sind Unternehmen, deren Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Artikel 9 besteht zur Benennung eines Datenschutzbeauftragten verpflichtet. Die SOG hat die

PersCert TÜV zertifizierte
Regina Braun
André-Pican-Straße 42
16515 Oranienburg
Telefon: 03301 – 57381000
datenschutz@erlebniscity.de

benannt.

Technische und organisatorische Maßnahmen
Unternehmen, die personenbezogene Daten verarbeiten müssen technische und organisatorische Maßnahmen treffen, um den Bestimmungen der DS-GVO zu entsprechen. Die SOG erfüllt diesen Anspruch durch folgende Maßnahmen:

Technische und organisatorische Maßnahmen

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

- Zutrittskontrolle

  Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

  - Bereiche sind in verschiedene Sicherheitsbereiche unterteilt
  - Zugänge sind gegen unbefugten Zugang gesichert
  - Alarmanlage (Einbruchmeldesystem)
  - Zugangsauthentisierung (Schlüsselregelung, Chipkartensystem)
  - Sicherheitsschlösser
  - Sicherheits- und Wachdienst (Nachts und am Wochenende);
- Zugangskontrolle
- Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.
  - Zugangsschutz zu allen DV-System durch Benutzerauthentifizierung
  - Es existieren Passwortkonventionen
  - Authentisierung mit Benutzername / Passwort
  - Zuordnung von Benutzerrechten
  - Erstellung und Zuordnung von Benutzerprofilen
  - Einsatz von Anti-Viren-Software
  - Einsatz einer Hard- und Software-Firewall
  -
- Zugriffskontrolle

  Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

  - Anzahl der Administratoren auf das „Notwendigste“ reduziert
  - Regelungen und Verfahren zum Anlegen, Ändern und Löschen von Berechtigungsprofilen

- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Einsatz von Aktenvernichtern
- Sichere Aufbewahrung von Datenträgern
- Ordnungsgemäße Vernichtung von Datenträgern;

- Trennungskontrolle

  Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

  - Es werden nur solche Daten erhoben, gespeichert und verarbeitet die unmittelbar dem eigentlichen Zweck dienen.
  - Technische und Operative Regelung und Maßnahmen zur Sicherstellung der getrennten Verarbeitung;

2. Integrität (Art. 32 Abs. 1 Buchstabe b DSGVO)

- Weitergabekontrolle

  Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

  - Es findet eine Protokollierung statt
  - Die Verbindung zu den Backendsystemen ist geschützt
  - Es existiert eine Verfahrensregelung über den Einsatz von Datenträgern
  - Datenträgerverwaltung – Durchführung regelmäßiger Bestandskontrollen
  - Es gibt Regelungen zur datenschutzkonformen Vernichtung von Datenträgern.
  - Die Vernichtung wird dokumentiert.
  - Bei Übertragungen werden dem Stand der Technik entsprechenden Verschlüsselungsverfahren eingesetzt;

- Eingabekontrolle

  Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

  - Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (Protokollierung)
  - Es existiert eine Dokumentation der Eingabeberechtigungen;

3. Verfügbarkeit **und Belastbarkeit** (Art. 32 Abs. 1 Buchstabe b DSGVO)

- Verfügbarkeitskontrolle

  Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

  - Es existiert ein Backup-Konzept
  - Verantwortliche Personen und Vertreter sind benannt
  - Unterbrechungsfreie Stromversorgung (USV)
  - Klimaanlage im Serverraum
  - Regelmäßige Prüfung von Notstromaggregat und Überspannungsschutzeinrichtung sowie permanente Überwachung der Betriebsparameter

- Lagerung von Datensicherungen in feuer- und wassergeschützten Datensicherheitsschränken, bzw. zusätzlich extern;

- **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchstabe d DSGVO; Art. 25 Abs. 1 DSGVO)**
  - **Datenschutz-Management;**
  - **Vorfalls-Reaktionsplan;**
  - **Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);**
  - **Auftragskontrolle**

Verpflichtung der Mitarbeiterinnen und Mitarbeiter auf die Einhaltung der datenschutzrechtlichen Bestimmungen

Sämtliche Mitarbeiterinnen und Mitarbeiter werden in auf ihre Verpflichtungen zur Wahrung des Datengeheimnisses hingewiesen und bezeugen dies mit Ihrer Unterschrift in der Verpflichtungserklärung gemäß Artikel 13 der DS-GVO. Ihnen wird das Merkblatt „Erläuterungen zu den Datenschutzgesetzten ausgehändigt. Außerdem wird ihnen der wesentliche Inhalt der Vorschriften des DS-GVO, erläutert. Sie bekommen zudem eine schriftliche Zusammenfassung der wichtigsten Regelungen ausgehändigt.

Fassung vom: 14.05.2018