Hectronic

Hectronic GmbH

Technische und organisatorische Maßnahmen im Sinne des Art. 32 Abs. 1 DSGVO

Stand: Mai 2023

Technische & organisatorische Maßnahmen im Sinne des Art. 32 Abs. 1 DSGVO

Hectronic

Smart solutions for parking and refuelling

Inhaltsverzeichnis

Hectronic

Smart solutions for parking and refuelling

1 Einleitung

Die EU-Datenschutzgrundverordnung (DSGVO) enthält Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar.

Gesetzlich geregelt sind die Anforderungen an die Datensicherheit in Art. 32 Abs. 1 DSGVO. Diese Vorschriften fordern, dass solche technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.

Das Gesetz nennt verschiedene Kontrollbereiche, die jeweils noch verschiedene Unterpunkte beinhalten:

(1) Vertraulichkeit

(2) Integrität

(3) Verfügbarkeit und Belastbarkeit

(4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(5) Pseudonymisierung und Verschlüsselung

Diese Maßnahmen stellen wir in der Folge vor, um Art. 28 Abs. 3 lit. c) DSGVO nachzukommen.

2 Organisatorisches

Das HectronicGmbH gewährleistet die schriftliche Dokumentation des aktuellen Datenschutzniveaus sowie der schriftlichen Arbeitsanweisungen, Richtlinien und Merkblätter für Mitarbeiter. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis bzw. auf die Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b), 29, 32 Abs. 4 DSGVO verpflichtet.

Einige diesen Bereich betreffenden Sicherungsmaßnahmen der folgenden Prüfliste sind nicht gesondert ausgewiesen, da sie in die Verantwortung etwaiger Unterbeauftragten fallen oder aus Gründen der Aufrechterhaltung der Sicherheit nicht detailliert veröffentlich werden.

3 Datenschutz-Management

Maßnahmen, die gewährleisten, dass personenbezogene Daten und Personen, die mit diesen arbeiten, organisatorisch auf den Umgang hingewiesen bzw. verpflichtet wurden.

Folgende Maßnahmen wurden im Unternehmen getroffen:

- Die Rollen DSKO, (e)DSB im Bereich Datenschutz sind benannt und über den Umfang ihrer jeweiligen Aufgaben informiert.
- Die Fachkunde des (e)DSBs wird sichergestellt.
- Es existiert ein on-boarding Prozess für neue Beschäftigte in dem Datenschutzthemen berücksichtigt werden und die Vergabe der Rechte durch die IT-Abteilung geregelt ist.
- Alle Beschäftigten haben eine Verpflichtung zur Einhaltung der Vertraulichkeit unterschrieben
- Alle neuen Beschäftigten erhalten bei der Verpflichtung zur Vertraulichkeit Informationen zum Datenschutz. Des Weiteren sind die Beschäftigten auf das Datengeheimnis verpflichtet worden.
- Die Beschäftigten werden regelmäßig durch Datenschutzschulungen/Awarenessmaßnahmen auf datenschutzgerechtes Verhalten geschult.
- Es existiert ein off-boarding Prozess zum Umgang mit ausscheidenden Beschäftigten und dem Entzug der erteilten Rechte/Betriebsmittel.

4 Schutzmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der Hectronic GmbH betrieben werden.

4.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1.1 Zutrittskontrolle

Die Zutrittskontrolle umfasst Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (bspw. automatisches Zutrittskontrollsystem, manuelles Schließsystem, Videoüberwachung, Wachpersonal etc.).

Das Unternehmen setzt unterschiedliche physische Zutrittsbeschränkungen ein. Die eingesetzten Zutrittsbeschränkungen verhindern den Zutritt für Unbefugte zu den Geschäftsräumen sowie zum Serverraum/Rechenzentrum. Es werden folgende Zutrittsbeschränkungen eingesetzt:

- Bebauungsart:
  - Es ist ein freistehender Gebäudekomplex, das Grundstück ist umzäunt
  - Es existiert eine Besucherverwaltung und alle Besucher des Unternehmens müssen sich am zentralen Empfang anmelden und dürfen die nicht-öffentlichen Bereiche nur in Begleitung betreten. Zusätzlich findet eine Erfassung der Besucher im Besucherbuch statt.
- Das Unternehmen setzt ein automatisches Zugangskontrollsystem ein, die berechtigten Personen verwenden zur Verifizierung Chipkarten / Token.
- Im Unternehmen werden teilweise Sicherheitsschlösser eingesetzt.
- Das Unternehmen hat ein manuelles Schließsystem.
- Es existiert eine dokumentierte Schlüsselvergabe für die Schlüssel / Token / Chipkarten.
- Die Verwaltung und Wartung der maschinellen Zutrittskontrollsysteme ist geregelt und dokumentiert.
- Die protokollierten Daten werden regelmäßig oder aufgrund besonderer Anlässe, wie z.B. nach (versuchten) Sicherheitsverletzungen, ausgewertet.
- Für Firmengelände und -gebäude wird eine Videoüberwachung eingesetzt.
- In den Zutrittskontrollanlagen werden personenbezogene Daten gespeichert, sodass nachvollziehbar ist, wer wann einen bestimmten räumlichen Bereich betreten und ggf. auch wieder verlassen hat (eventuell inkl. Auswertung bei Sicherheitsverletzungen).
- Die Verteilerräume oder -bereiche (Gebäudetechnik) sind gegen unbefugten Zutritt gesichert.
- Es sind Sicherungsmaßnahmen gegen Überfälle im Einsatz (bspw. Gegensprechanlagen, elektrische Türöffner, Lichtschranken, Überfallmelder, Videoüberwachung).
- Der Gebäudekomplex ist außerhalb der Geschäftszeiten geschlossen und kann nur von berechtigten Personen manuell geöffnet werden.
- Die Büroräume des Unternehmens sind separat über Bereichstüren mit elektrischem Sicherheitsschloss gesichert. Besonders sensible Bereiche sind zusätzlich manuell abschließbar.
- Entsprechende Regelungen für den Zutritt von externen Personen (Wartungsdienst; Reinigungsdienst; Besucher) sind implementiert. Externe Personen, die Zutritt zum Rechenzentrum benötigen, halten sich ausschließlich in Beisein der IT-Administration im Rechenzentrum auf.
- Serverraum:
  - Berechtigungsprüfung des Zutritts zu sensiblen Bereichen des Serverraums/Rechenzentrum durch Ausweiskontrolle und Abgleich mit Listen von autorisierten Personen.
  - Die Unternehmensserver werden in einem abgeschlossenen und zutrittsgesicherten Raum betrieben; zu diesem Serverraum haben nur befugte Personen Zutritt.
  - Es sind Maßnahmen zur Raumüberwachung des Serverraums/Rechenzentrums getroffen (Videokameras/Bewegungsmelder) worden.

4.1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (bspw. Maßnahmen zur Authentifikation, VPN-Verbindungen)

- Der Zugang zu den EDV-Systemen ist nur mit individuellen Benutzernamen und Kennwörtern möglich.

- Der Zugang zu den EDV-Systemen ist nur den Beschäftigten des Unternehmens möglich, welche hierfür die Zugangsberechtigung erhalten haben.
- Es ist mit der Geschäftsführung ein Vergabeprozess für die Zugangsrechte definiert und die Freigabe erfolgt nach diesem definierten Prozess.
- Es erfolgt eine Protokollierung der Benutzeranmeldungen und des jeweiligen Zeitpunktes der Anmeldung.
- Es gibt für alle Informationssysteme und Dienste eine formale Benutzer-Registrierung und Deregistrierung zur Vergabe und Rücknahme von Zugangsberechtigungen.
- Es ist sichergestellt, dass nur berechtigte Personen logischen Zugang zu den Netzwerkkomponenten haben.
- Erfolgt ein (Fern-) Wartungsvorgang wird dieser überwacht und protokolliert. Der Anwender hat jederzeit die Möglichkeit die Verbindung zu beenden.
- Der Zugriff auf das Unternehmensnetzwerk von außerhalb erfolgt über verschlüsselte Verbindungen (bspw. VPN) und einer separaten Authentisierung.
- Im Unternehmen erfolgt die Zuordnung von Benutzerrechten zu den jeweiligen IT-Systemen.
- Im Unternehmen werden auf allen IT-Systemen Anti-Viren-Lösungen eingesetzt.
- Es existiert ein verbindliches Verfahren zur Rechtevergabe.
- Alle Geräte werden von der IT-Abteilung mit einer automatischen Bildschirmsperre (passwortgeschützt) zur Verfügung gestellt.
- Das Unternehmen schützt die IT-Infrastruktur durch Software- und Hardware-Firewalls.
- Die Authentifikation erfolgt mit Benutzername / Passwort.
- Das Unternehmen setzt Intrusion-Detection-Systeme ein.
- Es findet eine Reduktion zugriffberechtigter Personen auf ein Minimum statt.
- Es wird ein separates Gäste-WLAN eingesetzt, so dass ein Zugang über dieses zum Firmennetzwerk nicht möglich ist.

4.1.3 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 (bspw. automatische Prüfung der Zugriffsberechtigung mittels Passwort, differenzierte Zugriffsberechtigungen auf Anwendungsprogramme).

- Es existiert ein Rollen- und Berechtigungskonzept; die Berechtigungsprüfungen erfolgen auf Basis dieses Konzeptes.
- Die Berechtigungsvergabe basiert auf dem «need-to-know-Prinzip»
- Es existiert eine Anweisung an die Benutzer, wie mit den DV-Systemen bei Verlassen des Arbeitsplatzes (Sperren) umzugehen ist.
- Personenbezogene Daten können nur im Rahmen des Berechtigungskonzepts gelesen, kopiert, verändert oder entfernt werden.
- Eine Verwendung fortlaufend aktualisierter Virenschutzsoftware ist technisch durch die IT-Abteilung sichergestellt.
- Eingehender E-Mail-Verkehr wird durch ein zentrales Virenschutz- und Spamfiltersystem auf Viren und Spam überprüft.
- Es existiert eine Passwortrichtlinie, welche die aktuellen Empfehlungen des BSI berücksichtigt. Die Mindestkriterien sind systemseitig festgelegt.
- Auf den IT-Systemen findet eine Protokollierung von Datenänderungen statt.

- Es ist ein softwareseitiger Ausschluss (Berechtigungskonzept) etabliert.
- Die Zugriffsmöglichkeiten der Benutzer sind auf den benötigten Umfang eingeschränkt.
- Es sind restriktive Zugriffsberechtigung/projektbezogene Zugänge etabliert.
- Es existiert ein Konzept zur Laufwerksnutzung/-zuordnung.
- Es existiert ein abgestimmtes Berechtigungsvergabeverfahren.
- Es existieren abgestufte Zugriffsrechte mit Logging/Protokollierung.
- Die IT-Abteilung hat IT-Sicherheitsrichtlinien/Policies erstellt und die Beschäftigten darauf geschult.
- Es existiert eine Anweisung an die Mitarbeiter, wie mit nicht mehr benötigten Datenträgern (Festplatten, USB-Sticks, Papierform) umzugehen ist.
- Es existiert eine Anweisung über die Entsorgung von Geräten inkl. Speichermedien.

4.1.4 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (bspw. Trennung Test- und Produktivumgebung, Trennung Managementnetz von Produktionsnetz, logische Trennung etc.).

- Im Unternehmen erfolgt die Trennung der Produktiv- von der Test- und Entwicklungsumgebung.
- Es erfolgt eine logische Trennung der Systemlandschaft gemäß dem Rollen- und Berechtigungskonzept.

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

4.2.1 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 (bspw. Vernichtung, Löschung und Verschlüsselung von Datenträgern, VPN-Verschlüsselung, Hardwareverschlüsselung).

- Bei der Weitergabe von Daten werden nur freigegebene Verschlüsselungslösungen / Nutzung von VPN-Tunneln bei Übertragungen eingesetzt.
- Der Zugriff auf die Daten und Dateien über das Web erfolgt über eine SSL-verschlüsselte Verbindung.
- Regelung des Systemkommunikationsverkehrs (zentrale Firewall, exklusive WAN-Verbindungen (Wide Area Network) mit Zugriffkontrollen), Protokollierung (Userauthentifizierung, Zeitpunkt).
- Die Beschäftigten können nur über VPN-Zugänge von ihren mobilen Arbeitsplätzen/ Heimarbeitsplätzen auf das Unternehmensnetzwerk zugreifen.
- Es ist ein Verbot für den Einsatz privater Datenträger vorhanden und wird technisch erzwungen.
- Die Beschäftigten können Dienste nur nutzen, die von der IT freigegebenen wurden.
- Es findet eine kontrollierte Vernichtung von Datenträgern und Papierdokumenten nach DIN 66399 statt.

4.2.2 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 (bspw. Benutzerprofile, Protokollierung eingegebener Daten (Verarbeitungsprotokoll), gescheiterte Anmeldeversuche, administrative Tätigkeiten über ein Ticketsystem).

- Im Bedarfsfall kann nachträglich festgestellt werden, ob und von wem Kundenstammdaten in DV-Systeme eingegeben, verändert oder entfernt worden sind (Protokollierung).
- Es ist ein Rollen- und Berechtigungskonzept vorhanden.
- Alle Beschäftigten haben auf deren Berechtigungsumfang angepasste Benutzerprofile.
- Im Unternehmen erfolgt eine Protokollierung der eingegebenen Daten (Verarbeitungsprotokoll).
- Für (Fern-) Wartungstätigkeiten findet eine Zugriffsprotokollierung statt.
- In den EDV-Systemen sind Benutzeridentifikationen etabliert.
- Es findet eine Firewall-Protokollierung (TCP/IP) statt.
- Die Systeme sind so konfiguriert, dass eine Protokollierung der gescheiterten Anmeldeversuche stattfindet.
- Es findet eine Protokollierung der Eingabe, Änderung und Löschung von Daten statt.
- Im Active Directory ist die Protokollierung der Benutzer aktiviert.
- Die kompletten protokollierten Daten sind gegen unbefugte Einsicht und/oder Manipulation gesichert.

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

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können (bspw. USV und Notstromaggregat, Alarmanlage, redundante Datenspeicherung (RAID-Festplattensysteme), Firewalls, Virenschutzprogramme, mehrfache inkrementelle Datenbank- und Systembackups, Datensicherungskonzepte).

- Die personenbezogenen Daten sind ständig verfügbar und durch regelmäßige Datensicherungen gegen zufällige Zerstörung oder Verlust geschützt.
- Es ist ein Datensicherungskonzept mit regelmäßigen Backups aufgebaut. Die Backups werden in getrennten Bereichen sowie in verschlüsselter Form aufbewahrt.
- Es ist ein Backup-/Recoverykonzept ausgearbeitet und etabliert.
- Es ist ein Notfallhandbuch implementiert und wird regelmäßig aktualisiert.
- Die Serverräume/Rechenzentren sind über ein getrenntes Zutrittskontrollsystem besonders geschützt.
- Das Unternehmen verwendet Brandschutzvorrichtungen im Gebäude zur Sicherung der EDV-Systeme.
- Die Serverräume / Rechenzentren verfügen über redundante Stromzuführungen, sowohl georedundant als auch doppelte Netzteile.
- Die Serverräume / Rechenzentren haben eigene Überwachungs- und Meldesysteme, welche direkt in der IT-Abteilung auflaufen.
- Es kommen unterbrechungsfreie Stromversorgung inkl. Überspannungsschutz und Notstromaggregat zum Einsatz.
- Im Serverraum gibt es eine Feuer-/Rauchmeldeanlage.
- Im Serverraum / Rechenzentrum kommt eine Klimaanlage zum Einsatz. Die Klimatechnik ist beim Unternehmen dokumentiert.
- Die Netzwerkkomponenten zum Zweck der Risiko-/Ausfallminimierung ist auf mehrere geschützte Bereiche verteilt.
- Es findet eine Überwachung der Raumtemperatur und Leckage statt.
- Es ist ein Überspannungsschutz integriert.
- Die eingesetzte Alarmanlage hat eine direkte Weiterleitung an die Leitstelle und die Feuerwehr
- Im Serverraum / Rechenzentrum werden keine brennbaren Materialien/Gegenstände gelagert.
- Das Unternehmen hat einen IT-Sicherheitsbeauftragten bestellt, der die Sicherheitsmaßnahmen regelmäßig prüft.
- Die Serversysteme setzen RAID-Festplattensystemen ein, um eine Ausfallsicherheit zu gewährleisten.

4.3.1 Rasche Wiederherstellbarkeit

Anforderung: Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können. (Art. 32 Abs. 1 Hs. 2 lit. c) DSGVO)

- Es ist ein Backup vorhanden
- Es ist ein Backup-/Recoverykonzept ausgearbeitet und etabliert.

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

4.4.1 Datenschutz-Management

Die Hectronic GmbH betreibt ein Datenschutzmanagement-System (DSMS) nach den Vorgaben des Art. 5 Abs. 2 DSGVO. Es orientiert sich an dem PDCA-Zyklus und unterliegt damit einer dauerhaften Wirksamkeitsüberwachung.

4.4.2 Incident-Response-Management

Ein prozessualisierter Umgang mit Sicherheitsvorfällen ist implementiert. Im Falle eines Vorfalls informieren die Mitarbeiter die IT bzw. ihren Vorgesetzten unverzüglich. Im Anschluss erfolgt die Abstimmung mit dem Datenschutzbeauftragten. Die Bearbeitung von Vorfällen ist durch entsprechende Vertretungsregelungen sichergestellt.

4.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftstätigkeiten zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden können.

4.4.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (bspw. Verpflichtung auf die Vertraulichkeit bzw. Datengeheimnis, insbesondere der IT-Administratoren, Vertrag zur Auftragsverarbeitung nach Vorgabe des Art. 28 DSGVO, Sperrung der Zugriffe nach außen bspw. bei Fernwartung durch Externe, Vergabe restriktiver Zugriffsberechtigungen, Einbindung des Datenschutzbeauftragten/Informationssicherheitsbeauftragten etc.).

Voraussetzungen für das Eingehen eines Unterauftragsverhältnisses:

- Vertrag zur Auftragsdatenverarbeitung nach Vorgabe des Art. 28 Abs. 3 DSGVO.
- Deutsche Dienstleister haben einen betrieblichen Datenschutzbeauftragten bestellt und sorgen durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
- Beschreibung Prüfungen und Audits.
- Vergabe von Einzelaufträgen. Bestätigung von mündlichen Aufträgen.
- Auf die betreffenden technischen Umgebungen werden nur restriktive Zugriffsberechtigungen vergeben. Bei externem Zugriff auf das System wird der Zugang nach Beendigung der Zusammenarbeit deaktiviert oder gesperrt.
- Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsdatenverarbeitung zur Verfügung, die entsprechende Regelungen zur Kontrolle enthält.

4.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

4.5.1 Pseudonymisierung

Sofern eine direkte Personenbeziehbarkeit nicht erforderlich ist, wird von der Pseudonymisierung Gebrauch gemacht, wenn dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (Datensparsamkeit).

4.5.2 Verschlüsselung auf Dateiebene:

(Bspw. Verschlüsselung von vertraulichen Dokumenten, verschlüsselte Übertragungswege via VPA, Aufbau Transportverbindung nur zwischen definierten und durch Zertifikate gesicherten Systemen, Datenübertragung von der Website erfolgt über eine SSL-Verschlüsselung).

- Es werden Verschlüsselungstechnologien nach dem aktuellen Stand der Technik eingesetzt. Das bedeutet, es kommen TLS(SSL)-Verschlüsselungen, Hash-Verschlüsselungen etc. zum Einsatz.

5 Kooperation

Zur Einhaltung der datenschutzrechtlichen Vorgaben nach der DSGVO, arbeitet die Hectronic GmbH mit der DDSK GmbH zusammen. Neben der Erstellung von Richtlinien und Handlungshilfen berät die DDSK GmbH die Hectronic GmbH in allen Fragen rund um den Datenschutz und stellt mit Herrn Stefan Fischerkeller den externen Datenschutzbeauftragten nach Art. 37 DSGVO des Unternehmens.

Stefan Fischerkeller

Diplomverwaltungswirt (FH), geprüfter fachkundiger Datenschutzbeauftragter (DESAG)

DDSK GmbH

Dr. Klein-Straße 29, 88069 Tettnang

Tel. 07542 / 949 21 01

E-Mail: fischerkeller@ddsk.de

Web: www.ddsk.de

DEUTSCHE DATENSCHUTZ KANZLEI