Anlage1 zu Auftragsverarbeitungsvereinbarung

Technisch-organisatorische Maßnahmen

ID.on GmbH, Prinzenstrasse 6, 30159 Hannover

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

Zutrittskontrolle
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen;

Technische Maßnahmen zur Zutrittskontrolle bei ID.on
Die Geschäftsräume von ID.on befinden sich in einem Haus in der Prinzenstraße (4 Etagen) mit einem elektronischen Schloss an der Haustür.
Der Serverraum von ID.on, in dem ausschließlich interne Verwaltungssysteme betrieben werden, steht im Keller in einem Raum mit einer verschlossenen Metalltür. Die Schlüssel und damit den Zugang haben nur ausgewählte Mitarbeiter.

Organisatorische Maßnahmen zur Zutrittskontrolle bei ID.on
Jeder Besucher wird von einem Mitarbeiter unmittelbar nach Betreten der Geschäftsräume persönlich in Empfang genommen und darf sich nicht ohne Begleitung im Gebäude bewegen.
Es existiert ein lückenlos protokolliertes Schlüsselbuch.

Zugangskontrolle
Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Verschlüsselung von Datenträgern;

Technische Maßnahmen zur Zugangskontrolle bei ID.on
Zugang zu Datenverarbeitungssystemen erfolgt ausschließlich nach Authentifikation mit Benutzernamen und Passwort oder Public-Key-Authentifizierung.
Es werden Firewall und Antivirensoftware auf Windows Betriebssystemen eingesetzt.
Datenübertragungen wie z.B. Bestellinformationen werden mittels SSL-Technologie verschlüsselt.

Organisatorische Maßnahmen zur Zugangskontrolle bei ID.on
Es findet eine Benutzerberechtigungsverwaltung statt, so dass die Mitarbeiter nur im Rahmen des Projekts bzw. Systems, für welches sie zuständig sind, die erforderlichen Rechte haben.
Es existieren Dienstanweisungen über den sicheren Umgang mit Passwörtern.
Das Reinigungspersonal wurde sorgfältig ausgesucht, zur Geheimhaltung verpflichtet und arbeitet seit mehr als 2 Jahren beanstandungslos mit ID.on zusammen.

Zugriffskontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen;

Technische Maßnahmen zur Zugriffskontrolle bei ID.on
Dokumente werden unter Einsatz von Aktenvernichtern entsorgt.

Zugriffe auf wesentliche Anwendungen ergeben sich aus den Logfiles.
Datenträger werden in aller Regel nicht mehr eingesetzt, sondern in einer betriebssicheren Cloud gespeichert.

Organisatorische Maßnahmen zur Zugriffskontrolle bei ID.on
Es besteht ein Berechtigungskonzept zur Zugriffskontrolle, welches sich an der jeweiligen Projekt- bzw. Systemverantwortung orientiert.
Die Systemadministratoren verwalten entsprechend die Benutzerrechte der Mitarbeiter.

Trennungskontrolle
Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Trennung der Stammdaten von den verknüpften Inhalten.

Technische Maßnahmen zum Trennungsgebot bei ID.on
Es findet eine physikalisch getrennte Speicherung der Daten auf gesonderten Systemen statt.
Produktiv- und Testsysteme werden getrennt.

Organisatorische Maßnahmen zum Trennungsgebot bei ID.on
Datenbankzugriffe erfolgen im Rahmen des jeweiligen Projekts bzw. Systems, woraus sich auch eine logische Mandantentrennung ergibt. Wo das nicht möglich ist, erfolgt die Trennung der Daten softwareseitig durch ein Berechtigungskonzept.
Die Datensätze sind mit Zweckattributen oder sonstigen Datenfeldern versehen.

Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)
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;

- Pseudonymisierung findet bei uns nicht statt.

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

Weitergabekontrolle
Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

Technische Maßnahmen zur Weitergabekontrolle bei ID.on
Datenübertragungen erfolgen SSL-verschlüsselt.

Organisatorische Maßnahmen zur Weitergabekontrolle bei ID.on
Die Empfänger von Daten ergeben sich stets aus der Projekt- bzw. Systembezogenheit der Datenübermittlung.

2.2 Eingabekontrolle
Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Die Eingabe, Änderung und Löschung von Daten ergibt sich nachvollziehbar aus der Projekt- bzw. Systembezogenheit der Benutzerrechte und den Logfiles. Es besteht eine stets aktuelle Übersicht der eingesetzten Applikationen.

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

Verfügbarkeitskontrolle
Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

Technische Maßnahmen zur Verfügbarkeitskontrolle bei ID.on

Der Serverraum verfügt über eine Klimaanlage, Schutzsteckdosenleisten und Geräte zur Wahrung von Temperatur und Feuchtigkeit.

Organisatorische Maßnahmen zur Verfügbarkeitskontrolle bei ID.on

Der Serverraum befindet sich nicht unter einer sanitären Anlage und das Gebäude befindet sich nicht in einem Hochwassergebiet.

Es existiert ein Backup- & Recoverykonzept (Notfallplan) und es wird eine betriebssichere Cloud eingesetzt.

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

- Datenschutz-Management;
  Über den Datenschutzbeauftragten ist ein Datenschutzmanagementsystem integriert, das auch entsprechende TOM im Rahmen der gesetzlichen Regelungen immer wieder auf Datenschutzkonformität prüft. Es wird ein jährliches Datenschutz-Audit bei ID.on durchgeführt.
- Incident-Response-Management; Es existiert ein ausgefeilter Notfallplan bei ID.on.
- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);
  Bei den von ID.on eingesetzten Anwendungen handelt es sich um Standardanwendungen, die von vielen Kunden eingesetzt werden und entsprechend auf Datenschutzkonformität, insbesondere in Bezug auf privacy by design und privacy by default getestet wurden.

Auftragskontrolle
Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

ID.on sucht seine Auftragnehmer unter besonderer Berücksichtigung der datenschutzrechtlichen Sorgfaltspflichten aus. Diese werden auf die Einhaltung der datenschutzrechtlichen Vorschriften

(DSGVO, BDSG) verpflichtet. ID.on setzt nur solche Auftragnehmer ein, die ihre Mitarbeiter auf die Vertraulichkeit verpflichtet haben. Es wird darauf geachtet, dass ID.on wirksame Kontrollrechte dem Auftragnehmer gegenüber zustehen.

Im Rahmen unserer Audits erfolgt eine Überprüfung der Auftragnehmer und deren Tätigkeiten.

Es finden insoweit keine Datenverarbeitungen statt, die eine Vorabkontrolle erforderlich machten.