Vereinbarung zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen i.S.d. Art 32 DSGVO

Stand 25.05.2018

Allgemeines

Personenbezogene Kundendaten werden nur auf den genannten Anlagen gespeichert. An anderen Orten, auch in den Büroräumen, befinden sich regelmäßig keine Kundendaten. Einzige Ausnahme ist eine temporäre Kopie einzelner Datensätze für spezielle Aufgaben (z.B. Bearbeitung einer Kundenanfrage). Alle Mitarbeiter des Auftragnehmers werden vor Aufnahme der Tätigkeit auf die DSGVO verpflichtet. Darüber hinaus wird mit allen Mitarbeitern des Auftragnehmers eine verbindliche Arbeitsanweisung zu den relevanten datenschutzrechtlichen Bereichen getroffen. Mit den Mitarbeitern ist hierbei insbesondere Folgendes vereinbart:

a) Auf den PCs der Mitarbeiter dürfen keinerlei personenbezogenen Kundendaten gespeichert werden. Alle personenbezogenen Kundendaten dürfen ausschließlich für aktuelle Anfragen oder Geschäftsabläufe abgerufen und eingesehen werden.

b) Alle personenbezogenen Kundendaten müssen von den Mitarbeitern nach Verwendung von dem PC gelöscht werden.

c) Bei dem Verlassen des Arbeitsplatzes müssen die Mitarbeiter sich am PC abmelden und den PC über ein selbst zu vergebendes Kennwort sperren bzw. den PC ausschalten. Die Mitarbeiter dürfen keine personenbezogenen Kundendaten am Arbeitsplatz zurücklassen, wenn sie Ihren Arbeitsplatz verlassen. Da in den allgemeinen Büroräumen keine Kundendaten gespeichert werden, wäre für diese Räume keine spezielle Zutrittskontrolle erforderlich. Es erfolgt jedoch eine kontrollierte und protokollierte Zutrittskontrolle per Fingerscan Türöffner.

1. Pseudonymisierung

Auf den dem Auftraggeber zur Verfügung gestellten Systemen werden per Grundeinstellung IP Adressen in Logfiles die z.B. zur Erstellung von Besucherstatistiken verwendet werden, durch die Ersetzung des letzten Oktetts der IP-Adresse anonymisiert.

2. Verschlüsselung

Datenübertragungswege werden verschlüsselt. Dabei kommen unterschiedliche Verfahren zum Einsatz (u.a. SSH, TLS, SFTP, SSL, Tunnel) um Übertragungen vor Fremdzugriff zu schützen.

3. Gewährleistung der Vertraulichkeit

Die personenbezogenen Daten des Auftraggebers werden von dem Auftragnehmer auf Server-Systemen auf Linux Basis im Rechenzentrum der Dogado GmbH, Saarlandstr. 25, D-44139 Dortmund betrieben. Dort erfolgen die folgenden Maßnahmen zur Zutrittskontrolle: Elektronische Zutrittskontrolle bei Betreten des Rechenzentrums als auch in den jeweiligen Sicherheitsbereich. Elektronisch: Zutritt ist durch ein materielles (RFID-Chip) und ein geistiges (PIN) Identifikationsmerkmal gesichert. Physikalisch: Jedes Rack verfügt über eine eigene Schließung. Die Außenhaut des Rechenzentrums und der Zutritt zu Sicherheitsbereichen im Rechenzentrum wird mit Videotechnik überwacht. Das Rechenzentrum wird regelmäßig innerhalb vorgegebener Zeitfenster durch einen Wachdienst begangen.

Der Auftragnehmer hostet sein Verwaltungssystem (u.a. Bestellverwaltung, Domainregistrierung, Newsletterversand) in den eigenen Räumlichkeiten. Die Daten werden in gesondert verschlossenen Räumlichkeiten aufbewahrt, zu denen nur eine begrenzte Personengruppe Zutritt hat. Die Räumlichkeiten sind vor Zugriff von Dritten physikalisch gesichert und werden zudem durch einen 24/7-Kamera-Alarm laufend überwacht. Die Server sind nur mit Konsolenpasswort oder über eine geschützte, verschlüsselte VPN-Verbindung administrierbar. Der Schutz erfolgt durch ein Passwort oder durch eine Authentifizierung mit Hilfe eines Schlüsselpaares (Private Key und Public Key). Der Zugang zur „Administrationsumgebung“ (Verwaltungsprogramm des Auftragnehmers) erfolgt ausschließlich Passwort geschützt über eine SSL-verschlüsselte Verbindung. Die Einhaltung der SSL-Verschlüsselung wird durch technische Maßnahmen sichergestellt. Der Zugriff zur webbasierten „Administrationsumgebung“ (Verwaltungsprogramm des Auftragnehmers) erfolgt durch persönliche Benutzer-Konten der einzelnen Mitarbeiter. Die Mitarbeiter legen das Passwort für Ihren persönlichen Zugang selbst fest, wobei eine Mindest-Stärke des Passwortes zwingend erforderlich ist. Über eine feste IP-Adresse wird sichergestellt, dass der Zugriff nur von dort aus möglich ist. Einzelne Mitarbeiter können dann für einen externen Zugriff freigeschaltet bzw. wieder gesperrt werden. Regelmäßig vorgesehen ist dies lediglich für die Geschäftsführung und technische Mitarbeiter, die auch außerhalb der Bürozeiten für Störungsbeseitigungen zur Verfügung stehen sollen. Weiteren Mitarbeitern kann im Einzelfall ein externer Zugriff temporär eingerichtet werden. Eine separate Administrationsumgebung wird für gesonderte Aufgaben genutzt. Für diese gilt: Passwörter zur Administration sind ausschließlich der

Celeros Online KG
Billstr. 87
20539 Hamburg
Germany

Geschäftsführer:
Christian Bruns
Unternehmenssitz:
Barsbüttel

Registergericht: Lübeck
HRA: 5793 HL
Steuer-Nr.: 30/280/53503
USt-ID: DE264341806

Bankverbindung:
IBAN: DE63200800000323821000
BIC: DRESDEFF200
Commerzbank AG

Geschäftsführung und einem technischen Mitarbeiter als Administrator bekannt und auf den PCs der Mitarbeiter gespeichert. Darüber hinaus sind alle PCs mit einem persönlichen Kennwort des jeweiligen Mitarbeiters geschützt. Der Zugang zu den Räumlichkeiten ist durch eine kontrollierte und protokolliertes Fingerscan Türschloss gesichert. Zugang zu den Administrationsumgebungen erhalten nur die Mitarbeiter, die ihn im Rahmen ihrer regelmäßigen Tätigkeit brauchen. Die unterschiedlichen Datenarten werden in unterschiedlichen Systemen gespeichert und verarbeitet.

4. Gewährleistung der Integrität

Die Nutzung der Online-Administration erfolgt über eine SSL gesicherte Verbindung. Die Übertragung der Daten an den Auftraggeber erfolgt standardmäßig durch Download über eine SSL gesicherte Verbindung. Falls in der Hauptvereinbarung eine andere Art der Weitergabe vereinbart ist, erfolgt dies auf ausdrücklichen Wunsch des Auftraggebers. Der Auftraggeber ist gehalten, in diesen Fällen einen Übertragungsweg zu wählen, der die Anforderungen des Datenschutzes ebenfalls angemessen erfüllt. Die Eingabe der Daten erfolgt durch den Internet-Nutzer selbst. Dafür stellt der Auftragnehmer online Formulare zur Verfügung, in denen einzelne Datenfelder mit Plausibilitäts-Prüfungen versehen sind. Bei der Erhebung des Datensatzes werden Datum und Uhrzeit sowie die IP-Adresse des Nutzers festgehalten.

5. Gewährleistung der Verfügbarkeit

Zusätzlich zu den technischen Maßnahmen, die bereits durch die Dogado GmbH im Rahmen der Infrastruktur bereitgestellt werden (z.B. unterbrechungsfreie Stromversorgung), hat der Auftragnehmer BackupRoutinen eingerichtet. Das Hauptbackup wird auf einen Speicher gesichert, der vom Auftragnehmer zur Verfügung gestellt wird. So ist sichergestellt, dass die Übertragung und nötigenfalls die Rückspielung über eine sehr schnelle Verbindung möglich ist. Der Auftragnehmer stellt klar, dass mit dieser Backup-Erstellung keine vertragliche Leistungsübernahme gewollt ist. Vielmehr ist der Auftraggeber - wie auch vertraglich in der Hauptvereinbarung vereinbart - für die ordnungsgemäße Sicherung seiner Daten selbst verantwortlich.

6. Gewährleistung der Belastbarkeit der Systeme

Die Räumlichkeiten der Datenverarbeitungsanlagen sind mit Feuer- und Rauchmeldeanlagen, Klimatisierung sowie USV Einrichtungen ausgestattet.

7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Es existiert eine zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz sowie Recovery mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung.

8. Verfahren regelmäßiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

Der Auftragnehmer verpflichtet seine Mitarbeiter auf das Datengeheimnis und der Vertraulichkeit. Hierzu erfolgt auch eine regelmäßige Sensibilisierung. Neben der Sicherheitszertifizierung nach ISO 27001 wird mindestens jährlich eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen durchgeführt.

Celeros Online KG
Billstr. 87
20539 Hamburg
Germany

Geschäftsführer:
Christian Bruns
Unternehmenssitz:
Barsbüttel

Registergericht: Lübeck
HRA: 5793 HL
Steuer-Nr.: 30/280/53503
USt-ID: DE264341806

Bankverbindung:
IBAN: DE63200800000323821000
BIC: DRESDEFF200
Commerzbank AG