F1 GmbH
Mädewalder Weg 2
12621 Berlin

Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 (1) DSGVO

1. Hinweise

Eine Änderung der getroffenen Maßnahmen behält sich die F1 GmbH vor, sofern das Schutzniveau nach DSGVO nicht unterschritten wird.

2. Pseudonymisierung

Bei Datenanalysen werden die Daten pseudonymisiert und anonym verarbeitet.

3. Verschlüsselung

Regelungsgegenstand:

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbefugte Offenlegung von bzw. unbefugten Zugang zu den im Auftrag verarbeiteten Daten ist zu reduzieren.

Technische und organisatorische Maßnahmen:

Einzelne Datenbanken sind verschlüsselt. Der Datenaustausch zwischen den Datenbanken und den Backend-Diensten findet ausschließlich über eine verschlüsselte Kommunikation statt.

Die mobilen Rechner der Mitarbeiter und Datenträger sind standardisiert durch entsprechende Betriebssystemwerkzeuge, jeweils mit dem Verschlüsselungsstandard AES (Advanced Encryption Standard) verschlüsselt.

Das Firmennetzwerk ist durch ein Firewall System abgesichert.

4. Vertraulichkeit

4.1. Physikalische Sicherheit

Regelungsgegenstand:

Unbefugten ist der Zutritt zu den Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten), mit denen Daten im Auftrag verarbeitet werden, zu verwehren. Der Grad der Schutzmaßnahmen richtet sich dabei nach dem Grad der Schutzbedürftigkeit der Daten.

Technische und organisatorische Maßnahmen:

Die Eingangstür zu den Büroräumen der F1 GmbH ist mit einem manuellen Schließsystem und einem automatischen Zuzieher ausgestattet. Die Tür ist während der Geschäftszeiten außer zum Betreten und Verlassen geschlossen. Außerhalb der Geschäftszeiten ist die Türe abgesperrt. Die Fenster sind in allen Lagen außerhalb der Geschäftszeiten geschlossen. Alle Fenstergriffe sind mit einem Schließmechanismus versehen.

Die Geschäftsräume sind außerhalb der Geschäftszeiten durch ein elektronisches System gesichert (Tür- und Fensterkontakte sowie Bewegungsmelder. Alarmierungen werden optisch sowie akustisch signalisiert. Zusätzlich erfolgt eine Benachrichtigung per Telefon in Form einer Meldekette.

Es besteht eine Zugangsbeschränkung für Büro- und Geschäftsräume. Es existiert ein geregelter Ablauf zur Genehmigung, Verwaltung und Löschung von Zutrittsberechtigungen. Die Zutrittsmittel für Mitarbeiter werden ausschließlich an berechtigte Mitarbeiter gegen Nachweis ausgegeben und sofort entzogen, wenn die Berechtigung erlischt. Beim Verlust eines Schlüssels erfolgt der Austausch des Schließsystems. Betriebsfremden Personen ist der Aufenthalt in allen Büroräumen der F1 GmbH nur in Anwesenheit und in Begleitung von Mitarbeitern gestattet.

Für das interne Rechenzentrum gilt die IT-Sicherheitsrichtlinie. Zusätzlich ist das Rechenzentrum durch zwei verschlossene Türen (unterschiedliche Schließungen) sowie eine Videoüberwachung gesichert.

4.2. Authentifizierung

Regelungsgegenstand:

Es muss verhindert werden, dass Datenverarbeitungs-, Datenspeicherungs-, Netzwerk- und Telekommunikationsanlagen (Sprache, Daten) von unbefugten Dritten genutzt werden können.

Technische und organisatorische Maßnahmen:

Alle Rechner verfügen über ein Zugangskontrollsystem (UserID (Benutzername), Passwort). Ein Passwortsystem für den Zugriff auf die Datenverarbeitungssysteme ist eingerichtet. Jeder Berechtigte erhält eine individuelle Benutzerkennung und ein persönliches, geheim zu haltendes Passwort, das nicht an Dritte weitergegeben werden darf. Berechtigungen werden regelmäßig kontrolliert. Das Passwort wird sofort gesperrt, falls die Berechtigung erlischt. Über alle Aktivitäten auf den Datenverarbeitungssystemen werden Protokolle erstellt.

Bildschirmarbeitsplätze werden bei Inaktivität manuell gesperrt.

Interne Netze werden nach dem Stand der Technik gegen Zugriffe von außen durch Firewalls und durch Verschlüsselung abgeschottet. Bestimmungsgemäße Zugriffe von außen werden durch Virtual Private Network (VPN) abgesichert.

Daten / Festplatten von mobilen Endgeräten werden verschlüsselt. Private Speichermedien sind durch Organisationsanweisung verboten. Es sind definierte organisatorische und technische Verfahren und Methoden zum Incident-Management umgesetzt.

4.3. Berechtigungskonzept

Regelungsgegenstand:

Die zur Benutzung von IT-Systemen berechtigten Personen dürfen ausschließlich auf die Daten zugreifen, auf die sie die Berechtigungen haben und die sie für die unmittelbare Ausübung ihrer Arbeit benötigen. Im Auftrag verarbeitete Daten dürfen während der Verarbeitung nicht unbefugt kopiert, verändert oder entfernt werden.

Technische und organisatorische Maßnahmen:

Die eingesetzten IT-Systeme haben ein dediziertes Rechtesystem, welche es ermöglicht, Datenzugriffe und -veränderungen auf Basis von Rollen und individuellen Berechtigungen zu vergeben.

Es existiert ein Berechtigungskonzept. Das Berechtigungskonzept umfasst die Verwaltung der Zugriffsrechte durch Systemadministratoren. Die Beantragung, Genehmigung, Vergabe und Rückgabe von Zugriffsberechtigungen ist in einer Organisationsanweisung geregelt.

Der Zugriff auf Computersysteme und Netzlaufwerke ist auf berechtigte Benutzer beschränkt. Jeder Mitarbeiter kann im Rahmen seiner Aufgabenerfüllung nur auf die für seine Tätigkeit notwendigen Systeme und mit der ihm zugewiesenen Berechtigung auf die erforderlichen Daten zugreifen. Das Erfordernis der Berechtigung wird regelmäßig geprüft.

Die persönliche Verantwortung jedes Mitarbeiters für die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen wird durch Schulungsmaßnahmen und zentral bereitgestellte Informationen gestärkt.

4.4. Weitergabe von Daten

Regelungsgegenstand:

Im Auftrag verarbeitete Daten dürfen bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf den Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden.

Technische und organisatorische Maßnahmen:

Alle Mitarbeiter und Fremdpersonal sind verpflichtet, dass Datengeheimnis zu wahren. Datenschutzschulungen für die Mitarbeiter werden regelmäßig durchgeführt.

Die Verbindung zu den Servern der F1 GmbH findet ausschließlich über eine HTTPS-verschlüsselte Verbindung statt.

Der Transport von benannten Daten per E-Mail erfolgt ausschließlich verschlüsselt.

4.5. Löschen von Daten

Regelungsgegenstand:

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es der Zweck, für den sie verarbeitet werden, erforderlich ist.

Technische und organisatorische Maßnahmen:

Nicht mehr benötigte Datenträger und Fehldrucke werden datenschutzgerecht entsorgt. Datenträger werden ordnungsgemäß durch physische Zerstörung, Papier durch den Schredder vernichtet.

Die Aufbewahrungsfrist der Daten wird im Rahmen der Beauftragung durch die steuerrechtlichen Vorgaben vorgegeben.

4.6. Mandantentrennung

Regelungsgegenstand:

Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können.

Technische und organisatorische Maßnahmen:

Die Daten werden in Datenbanken logisch voneinander getrennt. Entwicklungs-, Test- und Produktionssysteme sind getrennt.

5. Integrität

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten für betroffene Personen durch unbeabsichtigte oder unbefugte Veränderung oder unrechtmäßiges oder fahrlässiges Handeln von im Auftrag verarbeiteten Daten ist zu reduzieren.

5.1. Protokollierung

Regelungsgegenstand:

Es sind Maßnahmen zu wählen, mittels derer nachträglich überprüft und festgestellt werden kann, ob und von wem im Auftrag verarbeitete Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische und organisatorische Maßnahmen:

Die Zugriffe auf die datenverarbeitenden Systeme werden über die Logfiles und Systemlogs kontrolliert.

6. Verfügbarkeit

Hierzu trifft die F1 GmbH im Rechenzentrum Maßnahmen, die dazu dienen, dass im Auftrag verarbeitete Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn der Verantwortliche sie benötigt.

6.1. Sicherstellen der Verfügbarkeit

Regelungsgegenstand :

Im Auftrag verarbeitete Daten sind gegen zufällige oder mutwillig herbeigeführte Zerstörung oder Verlust zu schützen.

Technische und organisatorische Maßnahmen:

Hardwareschutz ist durch unterbrechungsfreie Stromversorgung (USV), Feuerlöschgeräte im oder unmittelbar vor dem Serverraum und die Einhaltung der einschlägigen Brandschutzvorschriften gewährleistet.

Die Ausführung arbeitsplatzfremder Software wird durch Spamfilter, Aktualisierung des Betriebssystems und Sicherheitssoftware (Updates und Patches) und Lizenzüberwachung verhindert. Die Ausführung arbeitsplatzfremder Software wird ferner durch technische Maßnahmen verhindert.

6.2. Zweckbindung

Regelungsgegenstand :

Personenbezogene Daten, die im Auftrag verarbeitet werden, dürfen nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Dies gilt insbesondere auch für die Löschung von Daten.

Technische und organisatorische Maßnahmen:

Die Verarbeitung von Auftragsdaten erfolgt ausschließlich entsprechend den produktbezogenen Leistungsvereinbarungen mit dem Auftraggeber. Weisungen zur Verarbeitung und insbesondere zur Löschung von im Auftrag verarbeiteten Daten werden nur ausgeführt, wenn der Kunde sie in der vertraglich vorgeschriebenen Form erteilt.

7. Belastbarkeit der Systeme

Regelungsgegenstand:

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu im Auftrag verarbeiteten Daten aufgrund von Systemüberlastungen oder -abstürzen ist zu reduzieren.

Technische und organisatorische Maßnahmen:

Um Systemstabilität zu gewährleisten, werden im Rechenzentrum Maßnahmen für eine zuverlässige

und zeitgerechte Verarbeitung der Daten getroffen.

Es werden laufende Überwachungen der Nutzung der Dienste und der Auslastung der Systeme durchgeführt. Speicher-, Zugriffs- und Leistungskapazitäten der Systeme und Dienste werden so ausgelegt, dass sie auch an Tagen planerischer Spitzenleistung ohne merkliche Verzögerung von Zugriffs- und Übertragungszeiten genutzt werden können.

Zusätzlich werden folgende Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Belastbarkeit der Datenverarbeitungssysteme eingesetzt.

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

Regelungsgegenstand:

Das Risiko physischer, materieller oder immaterieller Schäden bzw. das Risiko der Beeinträchtigung der Rechte und Freiheiten auch durch unrechtmäßiges oder fahrlässiges Handeln für betroffene Personen durch Vernichtung , Verlust, Veränderung oder unbefugte Offenlegung von im Auftrag verarbeiteten Daten oder des unbefugten Zugangs zu diesen durch einen physischen oder technischen Zwischenfall ist zu reduzieren.

Hierzu werden für die Verarbeitung von Daten im Auftrag im Rechenzentrum Maßnahmen für die Systemstabilität getroffen, die dem Anspruch der großen Anzahl von Verantwortlichen und betroffenen Personen an zuverlässig zeitgerechte Verarbeitung ihrer Daten gerecht werden.

Technische und organisatorische Maßnahmen:

Regelmäßige Datensicherungen werden durchgeführt. Sicherungskopien werden in geeigneten zeitlichen Abständen erstellt. Der Datenbestand wird mindestens einmal täglich gesichert.

Daten im Rechenzentrum sind durch den jeweiligen Betreiber geschützt. Dazu gehören Brandschutz, unterbrechungsfreie Stromversorgung und redundante Komponenten.

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

Regelungsgegenstand:

Es sind Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung zu betreiben.

Technische und organisatorische Maßnahmen:

Ein interner Datenschutzbeauftragter wurde bestellt. Die Wirksamkeit der Maßnahmen wird

u. a. durch den Datenschutzbeauftragten und durch den Informationssicherheitsbeauftragten der F1 GmbH laufend geprüft. Der Datenschutzbeauftragte oder von ihm oder der Geschäftsleitung beauftragte Mitarbeiter führen regelmäßig interne Kontrollen der Einhaltung der technischen und organisatorischen Maßnahmen der Datensicherheit durch.

Die vorhandenen Dokumentationen der Datensicherheit werden regelmäßig auf Aktualität geprüft. Es erfolgt mindestens jährlich eine technische Überprüfung der Datenverarbeitungssysteme.

Sicherheitsvorfälle werden dokumentiert und ausgewertet. Für die Sicherheitsvorfälle besteht ein geschultes Krisenteam.

Es erfolgen regelmäßige Audits durch den Datenschutzbeauftragten.