Technisch-organisatorische Maßnahmen
Status: 10/10/2022

1. Vertraulichkeit

Die Speicherung & Verarbeitung findet bei ausgewählten Providern in Rechenzentren statt, die hohe Sicherheits- und Verfügbarkeitsstandards garantieren.

Zutrittskontrolle: Der Auftragsverarbeiter verhindert den Zutritt nicht autorisierter Personen zu datenverarbeitenden Einrichtungen, mit/in denen personenbezogene Daten verarbeitet oder verwendet werden durch folgende Maßnahmen: Schlüssel, elektrische Türöffner

In den Rechenzentren:

- Unterbringung der Serverräumlichkeiten in einer eigenen Zone
- Zutritt ist durch eine Zutrittskontrolle abgesichert
- Videoüberwachungsanlage
- Ausschließlich berechtigte Personen erhalten Zutritt (Zugangsprotokolle)

Zugangskontrolle: Der Auftragsverarbeiter verhindert die Nutzung von datenverarbeitenden Systemen durch nicht autorisierte Personen durch folgende Maßnahmen: sichere Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern, Remote-Zugriff über Virtual Private Network (VPN), SSH-Schlüssel

Zugriffskontrolle: Der Auftragsverarbeiter gewährleistet, dass Personen, die autorisiert sind, ein datenverarbeitendes System zu benutzen, nur auf diejenigen Daten Zugriff haben, zu denen sie zugelassen sind und dass weder bei der Verarbeitung noch nach der Speicherung personenbezogene Daten ohne entsprechende Autorisierung gelesen, kopiert, geändert oder entfernt werden können, durch folgende Maßnahmen: Berechtigungsprofile, Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen soweit möglich & zulässig, periodische Überprüfung der vergebenen Berechtigungen, insbesondere von administrativen Benutzerkonten.

In den Rechenzentren:

- Berechtigungssystem - es werden ausschließlich „named-User“ verwendet. Die Zugriffsberechtigungen werden jährlich auf deren Angemessenheit geprüft.
- Die Zugriffsberechtigungen ergeben sich aus den Auftragsverarbeiterverträgen.
- Multi-Factor-Authentication (MFA)

- Pseudonymisierung: Sofern für die jeweilige Datenverarbeitung möglich und sinnvoll, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.
- Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).
- Zwecktrennung: Der Auftragsverarbeiter gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten, insbesondere verschiedener Auftraggeber, getrennt verarbeitet werden können, durch folgende Maßnahmen: getrennte Speicherung und Verarbeitung von Daten nach Auftrag, Berechtigungskonzept, Minimalprinzip bei Berechtigungsvergabe.

2. Integrität

- Weitergabekontrolle: Der Auftragsverarbeiter gewährleistet, dass personenbezogene Daten ohne Genehmigung während der elektronischen Datenübertragung oder -speicherung nicht gelesen, kopiert, geändert oder entfernt werden können und dass es möglich ist, zu überprüfen und festzustellen, an welchen Stellen die Übertragung personenbezogener Daten mittels Datenübertragungseinrichtungen vorgesehen ist, durch folgende Maßnahmen: Verschlüsselung der Verbindung, VPN, elektronische Signatur
- Eingabekontrolle: Der Auftragsverarbeiter gewährleistet, dass es möglich ist, nachträglich zu prüfen und festzustellen, ob und durch wen personenbezogene Daten in Datenverarbeitungssysteme eingegeben, geändert oder entfernt worden sind, durch folgende Maßnahmen: Protokollierung, Dokumentenmanagement
- In den Rechenzentren: durch das Führen eines „Secure-Logs“ oder durch die Protokollierung im Event-Log. Diese Log-Files dienen zur Erkennung einer rechtswidrigen Datenverwendung und zur Abwehr von Angriffen. Die Protokolle werden vom Chief Information Security Officer (CISO) entsprechend dem Auditplan geprüft.

3. Verfügbarkeit und Belastbarkeit

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust: Backup, unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne, Security Checks auf Infrastruktur- und Applikationsebene, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
- Rasche Wiederherstellbarkeit
- Löschungsfristen: Sowohl für Daten und Backups selbst als auch Metadaten wie Logfiles, etc.

In den Rechenzentren:

- redundante Führung des Rechenzentrumsbetriebs

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiterschulungen
- Incident-Response-Management
- Datenschutzfreundliche Voreinstellungen
- Datenschutzfreundliche Softwareentwicklung (Privacy bei Design)
- Durchführung von Penetration Testing in regelmäßigen Intervallen
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, Vorabüberzeugungspflicht, Nachkontrollen.

5. Supplementary Measures seitens Active Campagin / Postmark

Zusätzlich wurden die Standardvertragsklauseln durch weitere (begleitende) Zusicherungen und Klarstellungsmöglichkeiten seitens des US Sub Dienstleister ergänzt, um die die vom EuGH festgestellten Nachteile für das Datenschutzniveau auszugleichen.

- Pflicht zur Prüfung, ob staatliche Maßnahmen erforderlich sind.
- Verpflichtung, sich bis zur Ausschöpfung des Rechtsweges gegen den staatlichen Zugriff auf Daten von EU- Bürgern zu wehren.
- Verpflichtung zur Zahlung einer Vertragsstrafe bei schuldhafter Verletzung von Pflichten aus den Standardvertragsklauseln.