Technisch-organisatorische Maßnahmen (TOM) der VGF

Version	Datum	Bemerkung	Autor
1.0	01.10.2019	Erstellung	Dr. Michael Reiter
2.0	29.02.2020	Überarbeitung Anmerkungen Datenschutz / Revision	Dr. Michael Reiter

Die Stadtwerke Verkehrsgesellschaft Frankfurt am Main mbH (VGF) die selbst oder im Auftrag personenbezogene Daten verarbeitet, hat die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze insbesondere der Datenschutz-Grundverordnung (DS-GVO) zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Die VGF bedient sich eines IT-Dienstleisters zur Sicherstellung seiner IT-Services für den Bereich der Bürokommunikation und dem Hosting von Applikationen und zugehörigen Systemen. Die technischen und organisatorischen Maßnahmen (TOM) des IT-Dienstleisters gelten grundsätzlich auch für die VGF (bspw. über den IT-Rahmenvertrag). Die hier beschriebenen TOM entsprechen daher denen des IT-Dienstleisters. Dort wo sich Unterschiede ergeben, ist dies entsprechend beschrieben. Weitere IT-Services werden in Eigenregie betrieben und die technischen und organisatorischen Maßnahmen (TOM) gelten entsprechend.

Die VGF erfüllt diesen Anspruch durch folgende Maßnahmen basierend auf den Anforderungen der DS-GVO Artikel 32 (Sicherheit und Verarbeitung) entsprechend der folgenden Anforderungen:

<u>Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)</u>

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Auftragskontrolle
- Trennungskontrolle
- Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO)

<u>Integrität (Art. 32 Abs. 1 lit. b DS-GVO)</u>

- Weitergabekontrolle
- Eingabekontrolle

<u>Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)</u>

- Verfügbarkeitskontrolle

<u>Systemwiederherstellung (Art. 32 Abs. 1 lit. c DS-GVO)</u>

- Verfügbarkeitskontrolle / Systemwiederherstellung

<u>Überprüfung der technischen und organisatorischen Maßnahmen (Art. 32 Abs. 1 lit d DS-GVO)</u>

- Wirksamkeitskontrolle

Im konkreten sind die technischen und organisatorischen Maßnahmen wie folgt umgesetzt:

(1) Schutzmaßnahmen der Zutrittskontrolle:
Kein unbefugter Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Wachdienst bzw. Pförtner, Alarmanlagen, Videoanlagen
<u>Zuständigkeitsbereich der VGF:</u> – Es existiert je nach Liegenschaft ein Pfortendienst, Schließanlage bzw. durchgängig anwesendes Personal vor Ort. – Es erfolgt eine Videoüberwachung verschiedener Liegenschaften.

- Das Verwaltungsgebäude ist teilweise mit Einbruchsmeldeanlage ausgestattet. Das Gebäude selbst ist angemietet und der Pfortendienst wird durch eine externe Firma erbracht. Die vermietende Firma ist selbst in dem Gebäude ansässig.
- Es existiert eine kontrollierte Schlüssel- bzw. Transpondervergabe bzw. Zutrittskontrolle mit Ausweisleser.
- Für das Verwaltungsgebäude existiert eine namensfeine Dokumentation von Besuchern, Gästen und sonstigen firmenfremden Personen und es werden Besucherausweise ausgestellt.
- Es bestehen Regelungen zum Betreten von Räumen der Infrastruktur der DV-Einrichtungen.
- Es bestehen Regelungen hinsichtlich der Vergabe, Änderung und Rücknahme von Zutrittsberechtigungen.
- Es bestehen Regelungen (z.B. Arbeitsanweisung) für die Gebäudesicherheit und Zutrittskontrolle, die z.B. zum offenen Tragen von Dienstausweisen und Abschließen der Bürotüren auch bei nur kurzer Abwesenheit verpflichtet.

<u>Zuständigkeitsbereich des IT-Dienstleisters:</u>

- Die Serversysteme des IT-Dienstleisters befinden sich in dessen Rechenzentrum. Hierfür gelten die diesem Anhang – Technisch-organisatorische Maßnahmen - als Anlage beigefügten Ausführungen.

(2) Schutzmaßnahmen der Zugangskontrolle

Keine unbefugte Systembenutzung, z.B.: (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern

- Sämtliche Mitarbeiter haben nur Zugang zu den Systemen / Software, für deren Nutzung und Betrieb sie im Rahmen ihrer definierten Funktionen und Verantwortlichkeiten auch eine Berechtigung benötigen.
- Für die Vergabe, Änderung und Rücknahme von Zugangsberechtigungen bestehen Regelungen.
- Der Zugriff auf relevante Software und die Anmeldung an den IT-Systemen durch die Mitarbeiter erfolgt mit mitarbeiterspezifischen Anmeldedaten (Usercode und Passwort). Passwörter müssen mindestens 8 Zeichen lang sein und aus einer Kombination von Groß-/ Kleinbuchstaben, Zahlen und Sonderzeichen bestehen (3 von 4 Merkmalen). Nach einer definierten Anzahl fehlerhafter Anmeldeversuche wird ein Benutzer temporär gesperrt.
- Ein Passwortwechsel muss spätestens nach 180 Kalendertagen erfolgen. Die erneute Vergabe eines Kennwortes ist frühestens nach fünf Generationen möglich.
- Nach 15 Minuten Inaktivität wird der Bildschirm systemseitig gesperrt. Der Bildschirm muss durch Eingabe des Passwortes wieder entsperrt werden.
- Das Firmennetz ist durch den Dienstleister gegenüber dem Internet über den Stand der Technik entsprechenden Anwendungen geschützt (Firewall, Intrusion Detection / Intrusion Prevention System (IDS/IPS), mehrstufige Virenscanner, Filterung/Sperrung von nicht vertrauenswürdigen Webseiten).
- Grundsätzlich sind auf Serversystemen und Clients Anti-Viren-Lösungen installiert. Diese werden regelmäßig aktualisiert.

(3) Schutzmaßnahmen der Zugriffskontrolle:

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

- Der Zugriff ist nur mit entsprechenden Zugriffsrechten möglich.

- Es bestehen Berechtigungs-/Rollenkonzepte (differenzierte Berechtigungen nach Zuständigkeitsbereichen).
- Unterschieden werden Lese-, Schreib,- und Löschberechtigungen.
- Alle Mitarbeiter haben nur Zugriff auf die Systeme / Software, die sie zur Erfüllung der ihnen übertragenen Tätigkeiten notwendig sind. Die Systeme / Software sind entsprechend konfiguriert.
- Es ist geregelt, welche Anwender auf welche Datenbestände zugreifen dürfen.
- Zugriffe auf relevante Systeme / Software werden durch den IT-Dienstleister sowie VGF-seitig bei VGF eigenen Systemen und Anwendungen protokolliert.
- Es liegt ein Konzept zur Laufwerksnutzung und - zuordnung vor.
- Bei Programmentwicklungen wird zwischen Test- und Produktionsumgebung unterschieden.

(4) Schutzmaßnahmen der Weitergabekontrolle:

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

- Die lokale Festplatte von allen Clients wird voll verschlüsselt.
- Alle Wechseldatenträger, auf die schreibend zugegriffen werden soll (z.B. USB-Sticks), werden verschlüsselt.
- Es wird sichergestellt, dass eine gezielte Sperrung und/oder Freigabe von austauschbaren Datenträgern und Schnittstellen (z.B. USB Stick, Bluetooth, eSATA) sowie von Teilfunktionen (z.B. schreibender Zugriff auf CD/DVD-RW) gewährleistet wird.
- Für Datenübertragungen zu Auftraggebern oder Dienstleistern werden besondere Verfahren abgestimmt und angewendet.

(5) Schutzmaßnahmen der Eingabekontrolle:

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

- In Ergänzung der Zugriffskontrolle werden je nach Möglichkeiten der Systeme / Software Eingaben und Änderungen mit Usercode und Zeitstempel protokolliert.
- Löschfristen sind abhängig von gesetzlichen oder intern definierten Aufbewahrungsfristen.

(6) Schutzmaßnahmen der Auftragskontrolle:

Keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Nachkontrollen

<u>Zuständigkeitsbereich VGF:</u>

- Für Auftragsverarbeitungen gemäß Art. 28 DS-GVO sind entsprechende Verträge abgeschlossen. Darin sind die Rechte und Pflichten von Auftraggeber und Auftragnehmer eindeutig geregelt.
- Alle Mitarbeiter sind auf die Wahrung der Vertraulichkeit bei Verarbeiten personenbezogener Daten verpflichtet.
- Die Rechte und Pflichten von Auftraggeber und Auftragnehmer sind eindeutig geregelt.
- Die Mitarbeiter erhalten schriftliche Datenschutz-Informationen über das Unternehmenshandbuch und Datenschutz-Infobriefe.

Zuständigkeitsbereich IT-Dienstleister:

- Hierfür gelten die diesem Anhang – Technisch-organisatorische Maßnahmen - als Anlage beigefügten Ausführungen.

(7) Schutzmaßnahmen der Verfügbarkeitskontrolle und Systemwiederherstellung:

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; Rasche Wiederherstellbarkeit

Seitens des IT-Dienstleisters ist sichergestellt, dass während der Vertrags- und Aufbewahrungsdauer gemäß den vereinbarten SLA (Service Level Agreement) die Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der Daten gewährleistet ist und die notwendigen IT-Systeme / Anwendungen zur Verfügung stehen:

- Es liegt ein Notfallkonzept und ein Wiederanlaufkonzept vor. Diese werden regelmäßig auf Aktualität und Angemessenheit überprüft und getestet.
- Es existiert ein Backup-Konzept. Dieses wird regelmäßig überprüft.
- Es besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall.
- Die Datensicherung erfolgt regelmäßig auf geeigneten Datenträgern. Die Datenträger werden sorgfältig aufbewahrt und archiviert.
- Alte oder unbrauchbare Datenträger werden unter Beachtung der DIN 66399 datenschutzgerecht und ordnungsgemäß vernichtet.
- Grundsätzlich erfolgt der Einsatz eines Virenscanners auf Serversystemen und auf Arbeitsplatzrechnern. Die Virenscanner werden regelmäßig aktualisiert.
- Es werden regelmäßig sicherheitsrelevante Softwareupdates und –patches eingespielt.
- Das Firmennetz ist durch den Dienstleister gegenüber dem Internet über den Stand der Technik entsprechenden Anwendungen geschützt (Firewall, Intrusion Detection / Intrusion Prevention System (IDS/IPS), mehrstufige Virenscanner, Filterung/Sperrung von nicht vertrauenswürdigen Webseiten).
- Die IT-Systeme werden auf die Wirksamkeit (Effektivität) eingesetzter Maßnahmen geprüft (Penetrationstest, IT-Revision, Informationssicherheits-Managementsystem).

(8) Schutzmaßnahmen der Trennungskontrolle:

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Testumgebung

- Systemveränderungen an der IT bzw. den eingesetzten Softwareprodukten werden grundsätzlich auf dem Backup System oder eine Entwicklungs- und Testumgebung auf Funktionsfähigkeit geprüft, bevor sie kontrolliert entsprechend des Changeprozesses auf das Produktionssystem übernommen werden.
- Eine erforderliche Mandantentrennung ist in den Systemen eingerichtet.

(9) Schutzmaßnahmen der Pseudonymisierung und Verschlüsselung
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 entsprechenden technischen und organisatorischen Maßnahmen unterliegen
– Die Verwendung von Pseudonymisierungsmaßnahmen erfolgt nur dann, sofern dies technisch möglich und wirtschaftlich vertretbar ist.

(10) Schutzmaßnahmen der Wirksamkeitskontrolle
Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung
Die Wirksamkeit der technischen und organisatorischen Maßnahmen wird durch folgende Aktivitäten überprüft: <u>Zuständigkeitsbereich VGF:</u> – IT-spezifische Prüfungen der internen Konzernrevision – Informationssicherheits- und Datenschutzkoordinatoren <u>Zuständigkeitsbereich IT-Dienstleister:</u> – Informationssicherheitsmanagement gemäß der ISO27001