METANET AG, Josefstrasse 218, 8005 Zürich
Telefon 044 310 87 66
Telefax 044 310 87 69
www.metanet.ch

Technisch-organisatorische Massnahmen

Allgemeines

Der Auftraggeber und der Auftragnehmer haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Massnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Sowohl der Auftragnehmer als auch die einzelnen von diesen beauftragten Rechenzentren haben insbesondere die folgenden Massnahmen getroffen. Grundsätzlich ist eine Nutzung der Datenverarbeitungssysteme durch den Betreiber des Rechenzentrums **nicht** vorgesehen. Der Auftragnehmer nutzt eigene Hardware, so dass weder Zugriffsrechte, Zugänge, Weitergaben, Eingaben der Daten des Auftraggebers durch die Rechenzentren stattfinden.

Der Auftragnehmer gewährleistet, dass die Leistungserbringung in Schweizer Rechenzentren erfolgt. Die Leistungen von METANET orientieren sich zudem soweit möglich an den Vorgaben der Normen der ISO 27001 Zertifizierung. Der Workflow zur Annäherung und Erfüllung der Normen richtet sich nach dem im ITIL Framework.

Der Auftragnehmer hat geeignete Massnahmen zur Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung implementiert.

1. Zugangskontrolle

Ziel: Verwehrung des unbefugten Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird

- Die Büroräumlichkeiten der METANET AG befinden sich in einem ausschliesslich geschäftlich genutzten Haus. Sämtliche Zugänge sind ausreichend gegen den unbefugten Zutritt abgesichert, das bedeutet, dass:
- jegliche Aussentüren mit einem manuellen und technischen Schliesssystem (Sicherheitsschlösser) versehen sind,
- die den Mitarbeitern zur Verfügung gestellten Schlüssel personengebunden registriert sind,
- der Zugang zu Serverräumen nur einer begrenzten Anzahl von Personen gestattet wird,
- Mitarbeiter ausschliesslich mit den personalisiert angelegten Benutzerprofilen arbeiten,
- VPN-Technologie (SSL/TLS) eingesetzt wird,
- Datenträger (soweit möglich und relevant) verschlüsselt sind,
- Besucher nur in Begleitung eines Mitarbeiters sich in den Räumlichkeiten bewegen können,
- Personal von Dritten, insbesondere für Reinigungs- und Wartungsaufgaben sorgfältig ausgewählt wird und Geheimhaltungsvereinbarungen bestehen.

Unter anderem im Rahmen des Rechenzentrumsbetriebes wird darauf geachtet, dass:

- der Zutritt zum Rechenzentrum nur autorisierten Personen gestattet ist,
- der Zutritt durch ein materielles (RFID- Chip) und ein geistiges (PIN) Identifikationsmerkmal gesichert ist. Es wird zwischen fest zugewiesenen und beim Sicherheitsdienst zur Abholung hinterlegten Zutrittsberechtigungen unterschieden. Bei Zutrittsberechtigungen, die zur Abholung hinterlegt sind, wird die Autorisierung durch Kontrolle des Personalausweises sichergestellt. Die Daten werden bei einem Sicherheitsdienst hinterlegt , so wird gewährleistet, dass nur berechtigte Personen das Rechenzentrum betreten können,
- der Zutritt zu den einzelnen Kundenschränken oder -flächen ausschliesslich durch den Kunden und durch das zuständige Personal möglich ist,
- die Zutrittskontrollsysteme sowie die Alarmanlagen über USV und Netzersatzanlage gegen Stromausfall gesichert sind,
- das Rechenzentrum, insbesondere der Zutritt zu Sicherheitsbereichen mit Videoüberwachung ausgestattet ist,
- das Rechenzentrum regelmässig innerhalb vorgegebener Zeitfenster durch einen Wachdienst begangen wird. Die zu überprüfenden Punkte, welche der Wachdienst in den Rechenzentren zu kontrollieren hat, sind festgelegt. Auffälligkeiten werden berichtet. Die vorgegebenen Laufwege des Wachdienstpersonals werden protokolliert.

2. Datenträgerkontrolle

Ziel: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern

Der Auftragnehmer gewährleistet, dass

- Datenträger (soweit möglich und relevant) restriktiv einzusetzen sowie verschlüsselt sind,
- Hardware von der IT des Auftragnehmers geprüft und herausgegeben wird,
- die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren,
- ausgesonderte Datenträger datenschutzkonform gelöscht oder physikalisch gelöscht werden,
- der Zugriff auf Anwendungen (Eingabe, Veränderung und Löschung) protokolliert sowie Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls besteht.

3. Speicherkontrolle

Ziel: Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten

Im Rahmen der Speicherkontrolle gilt Nachfolgendes:

- die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) orientieren sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen (Berechtigungskonzept nach dem Need-To-Know-Prinzip),
- der Zugriff auf Anwendungen (Eingabe, Veränderung und Löschung) wird protokolliert und kann ausgewertet werden,
- Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls besteht,
- freigegebene Speicherbereiche werden vor Neuzuweisung überschrieben (genullt).

4. Benutzerkontrolle

Ziel: Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte

Die Benutzerkontrolle bedingt, dass

- die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren (Berechtigungskonzept nach dem Need-To -Know-Prinzip),
- der Zugriff auf Anwendungen (Eingabe, Veränderung und Löschung) protokolliert wird sowie,
- Remote-Access auf Infrastruktursysteme über verschlüsselte, Passphrase -gesicherte Services erfolgen.

5. Zugriffskontrolle

Ziel: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschliesslich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben

Die unerlaubte Tätigkeit in Verarbeitungssysteme ausserhalb eingeräumter Berechtigungen wird verhindert durch:

- die Zugriffsrechte (sowohl für Anwender, wie auch für Administratoren) sich an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren (Berechtigungskonzept nach dem Need-To-Know -Prinzip),
- Passwortrichtlinien inkl. Passwortlänge und Passwortwechsel vorgegeben werden,
- der Zugriff auf Anwendungen (Eingabe, Veränderung und Löschung) protokolliert wird,
- Schutz gegen unberechtigte interne und externe Zugriffe durch Verschlüsselung und Firewalls besteht,
- eine IT -Security Policy für das ITSM existiert und
- dedizierte Aufbewahrungspflichten bestehen.

6. Übertragungskontrolle

Ziel: Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können

Die Aspekte der Weitergabe personenbezogener Daten wird hierdurch umgesetzt, dass:

- VPN-Technologie (SSL/TLS) zur Datenkommunikation eingesetzt wird,
- E-Mail -Nachrichten bzw. sonstige Informationen grundsätzlich verschlüsselt bzw. pseudonymisiert versendet werden können und beim physischen Transport geeignete Transportpersonen sorgfältig ausgewählt werden.

7. Transportkontrolle

Ziel: Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird

Die Transportkontrolle erfordert, dass

- die Auswahl von Dritten sorgfältig erfolgt (insb. bzgl. Datensicherheit) in Zusammenarbeit mit dem Datenschutzbeauftragten (soweit möglich nur ISO 27001 zertifizierte Unternehmen/ Rechenzentren),
- detaillierte vertragliche Regelungen zum Auftragsverhältnis existieren,
- wirksame Kontroll - und oder Zugriffs - bzw. Löschungsrechte (ggf. Vertragsstrafen) vereinbart werden und
- eine regelmässige Kontrolle durch den Datenschutzbeauftragten erfolgt.

Die Aspekte der Weitergabe personenbezogener Daten wird hierdurch umgesetzt, dass:

- VPN -Technologie (SSL/TLS) zur Datenkommunikation eingesetzt wird
- E-Mail -Nachrichten bzw. sonstige Informationen grundsätzlich verschlüsselt versendet werden können und
- beim physischen Transport, geeignete Transportpersonen und -fahrzeuge sorgfältig ausgewählt werden und eine Festlegung der Wege stattfindet. Die Kontrolle von Eingaben, erfolgt durch:
- Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles) sowie
- die Zugriffsrechte, welche sich (sowohl für Anwender, wie auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren.

8. Wiederherstellbarkeit

Ziel: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können

Zur Wiederherstellbarkeit verpflichtet sich der Auftragnehmer

- zur Erstellung eines Backup -& Recovery-Konzepts,
- die Datenwiederherstellbarkeit zu testen,
- RAID-Controller zu verwenden,
- Protokollierung und Auswertung von Störungsvorfällen.

9. Zuverlässigkeit

Ziel: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und Fehlfunktionen gemeldet werden

Die Zuverlässigkeit erfordert, dass

- Eskalationsfälle prozessual gemeldet werden (Anzeige von Fehler- und Störmeldungen in den IT-Systemen),
- externe/interne technische Sicherheitsanalysen durchgeführt werden,
- Test - und Freigabeverfahren z. B. bei Einführung neuer Soft - oder Hardware bestehen und
- Sensibilisierungen der Mitarbeiter zum Datenschutz und/oder - sicherheit vorgenommen werden.

10. Datenintegrität

Ziel: Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

Im Rahmen der Datenintegrität orientiert sich der Auftragnehmer

- an einem Managementsystem für Informationssicherheit (ISMS) bzw. kann
- die Verarbeitung personenbezogener Daten im Einzelfall in Abstimmung mit dem Auftraggeber in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Es erfolgt eine authentifizierte Benutzeridentifikation, insbesondere dadurch, dass:
- alle technischen Systeme (zentral und dezentral), sowohl Hard -, als auch Software durch eine Firewall geschützt sind und Protokollierung und Nachvollziehbarkeit von Eingaben, Änderungen und Löschung von Daten (durch Logfiles) als auch, die Zugriffsrechte, welche sich (sowohl für Anwender, wie auch für Administratoren) an den aufgabenbedingten und datenschutzrechtlichen Erfordernissen orientieren.

11. Verfügbarkeitskontrolle

Ziel: Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind

Zur Durchsetzung der Verfügbarkeit, hat der Auftragnehmer veranlasst, dass:

- eine Backup-Strategie existiert,

- eine unterbrechungsfreie Stromversorgung besteht (USV),
- Räumlichkeiten in Brandabschnitten versehen mit einzelnen Brandschutzeinrichtungen eingeteilt sind,
- Klimaanlagen vorhanden sind,

Im Rahmen des Rechenzentrumsbetriebes wird insbesondere darauf geachtet, dass:

- die Stromversorgung durch Redundanzen sichergestellt wird (Notstromaggregate sowie USV-Anlagen mit n+1 Redundanz; Überbrückungszeit mindestens 15 min. bis die Notstromaggregate die Stromversorgung wieder sicherstellen - Anlaufzeit inkl. Lastübernahme 1-2 min.);
- das Rechenzentrum mit einer Raumklimatisierung ausgestattet ist (redundant ausgelegt (n+1),
- das Rechenzentrum über baulich getrennte Brandabschnitte verfügt. In den Räumlichkeiten ist eine Brandmeldeanlage und eine Brandfrühersterkennung installiert;
- die Hochwasser- und Erdbebenkritikalität DIN-gerecht geprüft wurde.

12. Trennbarkeit

Ziel: Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können

Die getrennte Datenverarbeitung wird gewährleistet durch:

- fehlende Möglichkeit eines physikalischen Zugriffs durch dedizierte Rechte und Pflichten,
- klare Trennung und Nachvollziehbarkeit von Kundenzugriffen (logische Trennung durch individuelle Benutzerprofile mit Passwortschutz / Trennung von Produktiv - und Testinfrastruktur),
- getrennte Verarbeitung zweckgebundener Daten.

Anpassung der innerbetrieblichen Organisation an die besonderen Anforderungen des Datenschutzes

Der Auftragnehmer richtet sich nach den folgenden datenschutzrechtlichen Standards:

- Erarbeitung eines IT-Sicherheits- und Datenschutzkonzepts,
- Fertigung von internen Datenschutz- und Sicherheitsrichtlinien sowie Arbeitsanweisungen,
- Regelmässige Kontrolle durch den Datenschutzbeauftragten,
- Regelmässige Hinweise und Ermahnungen, um das Problembewusstsein zu fördern,
- Gelegentliche unvermutete Kontrolle der Einhaltung von Datenschutz- und Datensicherungsmassnahmen.