Technische und organisatorische Maßnahmen
gem. Art. 32 Abs. 1 DSGVO für Verantwortliche (Art. 30 Abs. 1 lit. g)
und Auftragsverarbeiter (Art. 30 Abs. 2 lit. d)

Zum Schutz der personenbezogenen Daten, die die IundS AG von ihren Kunden zum Zweck der Auftragsdatenverarbeitung im Sinne von Art. 28 DSGVO erhalten hat, hat diese die nachfolgend dargestellten technische und organisatorische Maßnahmen im Sinne von Art. 32 DSGVO getroffen.

A. Vertraulichkeit (Art. 32 Abs. 1lit. b DSGVO)

1. Zutrittskontrolle

- Physische, technische und personelle Sicherheit sind im Rechenzentrum Berlin Spandau durch ein 6-stufiges Sicherheitssystem gewährleistet, das mit der Überwachung des Rechenzentrumsgeländes und der jeweiligen Gebäude beginnt und mit der Kontrolle der Colocationfläche und der einzelnen Systeme abschließt:
  - ISO 27001 zertifiziertes Rechenzentrum
  - Videoüberwachungsanlage für das Gelände und die Gebäude in Kombination mit einer Gefahrenmeldeanlage
  - Gesicherte Grundstücksgrenzen durch Sicherheitszaunanlage mit Übersteig- und Unterkriechschutz
  - Zufahrt durch Schrankenanlage mit Sicherheitstoren und Durchfahrsperren
  - Geschlossene Videoüberwachung von Türen und Zugängen mit automatischem Intrusionsalarm
  - Diverse Sensoren innerhalb und außerhalb der Gebäude zur Intrusionserfassung
  - 24/7 Notruf- und Betriebs-Leitstelle (NSL und BSL)
  - Zu- und Ausgänge des Gebäudes sind von außen nicht zu öffnen
  - Sicherung der Fenster, Kellerfenster, Lichtschächte
  - Besondere Sicherung der Türen
  - Kartendokumentation
  - Schlüsseldokumentation
  - Sichere Verwahrung von Ersatzkarten/Ersatzschlüsseln

2. Zugangskontrolle (Datenverarbeitungsanlagen auf Netz- und Serverebene)

- Zugangskontrollen per berührungsloser Chipkarte und persönlicher PIN
- Verschlüsselte) Identifikation und Authentifikation von Benutzern (User-ID und Passwort etc.)
- Passwortregeln vorhanden (Mindestlänge, Zeichensatz, Gültigkeitsdauer, Ausschluss Trivialkennworte etc.)
- Vorläufig vergebene Passwörter werden unverzüglich durch sichere Individualpasswörter ersetzt
- Sperrung bei wiederholter Fehleingabe von Passwörtern, Freigabe nur nach Zeitablauf
- Hardware-Firewall vorhanden
- Updates für Firewall werden regelmäßig manuell installiert

- Anti-Virus-Software vorhanden
- Updates für Anti-Virus-Software werden regelmäßig automatisch installiert
- Regelmäßiges automatisches/manuelles Einspielen von Sicherheitspatches und/oder -updates bei Browsern
- Protokollierung von Internetnutzung
- Sicherheitsmaßnahmen WLAN (Standardeinstellungen, Standardbenutzernamen und Standardpasswörter durch sichere individuelle Einstellungen ersetzt, Verschlüsselungsverfahren, Log-Dateien werden regelmäßig ausgewertet, MAC-Adressfilter aktiviert, regelmäßige Sicherheitschecks etc.)
- Sicherungsmaßnahmen bei Zugang von extern zum Firmennetz (Virtual Private Network (VPN), Protokollierung der externen Kommunikation, regelmäßige Sicherheitschecks von mobilen Endgeräten etc.)

3. Zugriffskontrolle (Datenverarbeitungsanlagen)

- Zugang zu den Systemen nur über personalisierte X509 Zertifikate und RSA Schlüssel.
- Sowohl die Zertifikate als auch die Schlüssel werden beim Erlöschen der Berechtigung zurück gezogen (Revocation).
- Aktive Netzkomponenten (Switches etc.) sind zugriffssicher untergebracht
- Deaktivierung nicht benötigter Anschlussdosen
- Rollenbasierte Berechtigungen wie Kategorien von Rollen und Rechte der Rollen, insbesondere nach „Lesen, Schreiben, Ausführen“
- Rollen- und Rechtekonzept mit einer Festlegung und Dokumentation der Rollen und Rechte der berechtigten Personen
- Prozess zur Aufhebung nicht mehr benötigter Rollen und Rechte
- Dokumentation der Änderung von Rollen und Rechten
- Regelmäßige Überprüfung der Erforderlichkeit der vergebenen Rollen und Rechte
- Kein Zugriff durch Benutzer auf Systemebene möglich

4. Trennungskontrolle

- Logische/physikalische Trennung von verschiedenen speichernden Stellen (Unternehmen)
- Trennung unabhängiger Anwendungen innerhalb eines Unternehmens (durch Zugriffssteuerung/physikalisch eigenständige Datenträger/logische Datentrennung)
- Trennung von Test- und Produktionsdaten (getrennte Programmbibliotheken etc.)
- Trennung der DV-Anlagen und Datenträger für besonders sensible Daten (durch Zugriffssteuerung/physikalisch eigenständige Datenträger/logische Datentrennung)
- Trennung nach Zwecken (durch Zugriffssteuerung/physikalisch eigenständige Datenträger/logische Datentrennung)

5. Pseudonymisierung

- Verschlüsselung
  - Kommunikation: Ja (ausschließlich), alle für die Verschlüsselung möglichen Protokolle HTTPS/SMTPS/IMAPS/SSH

- Daten: Die Daten der Applikation/lokale Daten sind nicht per Freigabe o.ä. zu erreichen. Die Backups erfolgen über DRBD-Snapshots. Die daraus entstehenden Binärdaten werden nicht zusätzlich verschlüsselt.

B. Integrität (Art. 32 Abs. 1 lit b DSGVO)

- Monitoring auf das störungsfreie Funktionieren von
  - Hardware,
  - Betriebssystem und Software

1. Weitergabekontrolle

- Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.
  - Einrichtungen von Standleitungen bzw. VPN-Tunneln Weitergabe von Daten in anonymisierter oder pseudonymisierter Form
  - Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen
  - Regelmäßiges automatisches Einspielen von Sicherheitspatches und/oder -updates bei E-Mail-Programmen
  - Kein Einsatz von Web-Mail-Angeboten
  - Protokollierung des E-Mail-Verkehrs und regelmäßige Auswertung auf abweichendes und verdächtiges Mailverhalten
  - Geeignete Sicherungsmaßnahmen für den Transport von Datenträgern (Sicherungsbehälter, Sicherung der Daten durch Duplizierung, Verschlüsselung etc.)
  - Prozess zur sicheren Löschung/Vernichtung von Datenträgern/Unterlagen (Protokollierung der Vernichtung etc.)
  - Einsatz von Aktenvernichtern

2. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Protokollierung der Eingabe, Änderung und Löschung von Daten Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Protokollierung der Einrichtung und des Betriebes von IT-Systemen
- Protokollierung der Einrichtung/Änderung von Benutzern und Rechten (Dokumentation aller berechtigten Nutzer, Rechteprofile der berechtigten Nutzer, Dokumentation von

Änderungen von Nutzern/Rechten, Dokumentation, wer die Benutzer und Rechte angeordnet/eingerichtet hat, Historie über die eingerichteten Nutzer und Rechte etc.)

- Protokollierung von Systemänderungen (Dokumentation von funktionalen Systemänderungen/Erweiterungen einschließlich Testfälle, Testung, Testergebnisse und Freigabe, Dokumentation von Versionsänderungen oder Änderungen der technischen Umgebung des IT-Systems, Änderungen der Dateiorganisation oder des Dateiverwaltungssystems etc.)
- Protokollierung von Eingaben und Veränderungen (Datum und Uhrzeit von Zugriffen mit Kennung des Benutzers, Ausgeführte Aktionen, insbesondere Lösch- und Kopiervorgänge, Zugriff auf Dateien mit personenbezogenen oder vertraulichen personenbezogenen Inhalten, unbefugte und abgewiesene Zugriffsversuche, wiederholte Eingabe von fehlerhaften Passwörtern zu einem Login, unbefugtes Einloggen und Überschreiten von Befugnissen, Benutzung von Admin-Accounts, Warnungen über unbefugtes Eindringen etc.)
- Systemüberwachung (Protokollierung von benutzten Programmen, Systemstart und -stopp, Anmeldung/Abmeldung von Benutzern, Anmelde-Fehlversuche, Anschluss und Entfernung von Ein- und Ausgabegeräten, Aktivitäten im Zusammenhang mit Fremdwartung und Fernwartung, Systemwarnungen oder Systemfehler, Konsolwarnungen und Konsolmeldungen, am Paketfilter wegen Regelverstoß abgewiesene Pakete, Änderungen und Änderungsversuche von Gateway- und Firewallpolicies, Systemprotokollausnahmen, Zugriffe auf die Server-Registry, Konfigurations- und Statusänderungen, Systemfehler, Regelverstöße, Maßnahmen zur System- und Datenwiederherstellung, wie Restore- und Back-up-Maßnahmen, Änderungen von Konfigurationseinstellungen etc.)
- Überwachung von Routern und Switches
- Protokollierung von Verbindungs- und Gesprächsdaten
- Protokollierung der Entfernung von Datenträgern
- Protokollierung des Exports, Downloads und Versands von vertraulichen Dokumenten und Daten
- Gewährleistung der Sicherheit von Protokolldateien (Kein Abschalten der Protokollfunktionen möglich, kein Bearbeiten/Löschen der Protokolldateien möglich, Protokollierung der Abschaltung von Protokollfunktionen, Protokollierung der Bearbeitung/Löschung von Protokolldateien, Protokollierung von Zugriffen auf die Protokolldateien, verschlüsselte Speicherung der Protokolldateien etc.)
- Regelmäßige/Anlassbezogene automatische/manuelle Auswertung der Protokolle auf Normabweichungen, Sicherheitsverletzungen und Angriffe

C. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

1. Verfügbarkeitskontrolle

- Stromversorgung
    - Die gesamte Stromversorgung des Rechenzentrums Berlin Spandau wird als duale Strom- und Notstromversorgung mit einer unterbrechungsfreien A- und B-Versorgung und mit einer zusätzlichen redundanten Versorgung für alle kritischen technischen Gebäudeanlagen wie Klima-, Kälte-, Lüftungs- und Sicherheitsanlagen ausgeführt.

Darüber hinaus verfügt das Rechenzentrum Berlin Spandau über zwei Einspeisungen auf der 10 kV-Ebene.

- USV-Anlagen und zugehörige Batterieanlagen sind je A- und B-Versorgung redundant aufgebaut und können auf A- oder B- Versorgung für mindestens 15 Minuten die Stromversorgung bei 100 % Maximallast überbrücken. Die Steuerung der Generatoren erfolgt automatisch, so dass bei einem Ausfall der Stromversorgung durch einen Stromlieferanten die Generatoren selbsttätig starten. Der vorgehaltene Kraftstoff reicht aus, um die gesamte Stromversorgung des Standortes für 72 Stunden ununterbrochen sicherzustellen.
  - Redundante 10 kV-Einspeisung
  - Separate USV-Systeme (getrennte, vollredundante A- und B-Versorgung)
  - Redundant ausgelegte Netzersatzanlagen mit Dieselgeneratoren
  - Der Strom wird zu 100% aus erneuerbaren Energien gewonnen

- Klimatisierung

  - Energieeffiziente, redundante Umluft-Kühlungssysteme in Klimaspangen
  - Redundante Klimaschränke und Pumpen der Kälteversorgung
  - Kältemaschinen mit integrierter Freier Kühlung und übergeordneter Gruppensteuerung
  - Redundante, USV-gestützte Gebäudeleitsysteme (GLT) zur Überwachung aller technischen Anlagen und Systeme
  - Raumlufttechnische Anlagen mit zentraler Be- und Entlüftung sowie Be- und Entfeuchtung

- Brandschutz

  - Für den Innenausbau der Colocationfläche im Rechenzentrum Berlin Spandau wurden ausschließlich spezielle, nicht-brennbare oder nur schwer entflammbare Materialien verwendet. Die einzelnen RZ-Flächen sind in separate Brandschutzzonen unterteilt. Innerhalb jedes Bereiches sind umfassende Brandbekämpfungs- und Brandschutzsysteme installiert.
    - Gebäudebrandabschnitte der Feuerwiderstandsklasse F 90 A
    - Alle Technik- und Hardwareräume als F 90 A-Brandbekämpfungsabschnitte
    - Gesicherte Trassen mit F 30 /90 A Brandschotts
    - Flächendeckende Überwachung aller Räume und Ebenen
  - Automatische, digitale Brandmelder und –anlagen

    - Brandfrühesterkennung mit VESDA Systemen
    - Automatische Gaslöschanlage zur Flutung der Rechnerräume

- Notfallhandbuch
- Alarmierungsplan
- Wiederanlaufplan

2. Rasche Wiederherstellbarkeit

- mehrstufige Backups für die Wiederherstellung der Daten (Snapshots und Dumps der Datenbanken) und der virtuellen Maschinen (ReaR Backup)
- Regelmäßige Bestandskontrollen
- Regelmäßige automatisierte Datensicherungen
- Überwachung der Sicherungsdatenträger bezüglich ihrer Haltbarkeit/Anzahl der zulässigen Schreibzyklen
- Prüfung der Rekonstruierbarkeit der Datenbestände durch regelmäßige Tests
- Sichere Lagerung von Datensicherungen (anderer Brandabschnitt/externe Lagerung, Tresor, Verschlüsselung der Datensicherungen etc.)
- Notfallhandbuch
- Alarmierungsplan

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO, Art. 25 Abs. 1 DSGVO)

- Der Scope der Zertifizierung nach ISO 9001:2015 der IundS AG liegt auf Systemadministration und Softwareherstellung.
- Es existieren umfangreiche Verfahrensanweisungen zu allen Bereichen der Datensicherheit und des Datenschutzes. Im Rahmen des QM werden alle Mitarbeiter regelmäßig zum Umgang mit Fremddaten geschult und belehrt.
- Diese Bereiche werden durch den TÜV Nord jährlichen externen Audits unterzogen.
- Die genannten Verfahren sind Bestandteil des QMS und durch den Auftraggeber auf Verlangen einzusehen.

- Dazu ergänzend:
  - interne Verhaltensregeln;
  - Risikoanalyse;
  - Datensicherheitskonzept;
  - Wiederanlaufkonzept (Worst Case)

- Datenschutz-Management (Datenschutz-Richtlinie, IT-Sicherheits-Richtlinie, Datenschutz-Verfahrensanweisungen, Incident-Response-Management etc.)
- Verpflichtung der Beschäftigten zur Vertraulichkeit
- Verpflichtung der Beschäftigten auf das Fernmeldegeheimnis
- Verpflichtung von externen Dienstleistern auf das Datengeheimnis, sofern es sich nicht um Auftragsverarbeiter handelt
- Abschluss eines Vertrages oder eines anderen Rechtsinstruments nach Art. 28 DSGVO und Einhaltung dieser Regularien
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Vertraglich festgelegte Verantwortlichkeiten
- Sofern Verantwortlicher auch Auftragsverarbeiter ist: Vertragliche Regelungen mit Subunternehmern, dass der Auftraggeber seine Rechte aus AV- Vertrag (insbesondere seine Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann

Berlin, 21.09.2023

Datum Unterschrift