Technische und organisatorische Maßnahmen
nach Art. 32 Abs. 1 lit. b DSGVO der Sprengnetter Unternehmensgruppe

Sprengnetter Real Estate Services GmbH
Sprengnetter-Campus 1
53474 Bad Neuenahr-Ahrweiler
Telefon 02641 9130 0
Fax 02641 9130 1010
www.sprengnetter.de
info@sprengnetter.de
datenschutz@sprengnetter.de
Version 1.43 / 21.11.2022

INHALTSVERZEICHNIS

2 VERTRAULICHKEIT (ART. 32 ABS. 1 LIT. B DS-GVO)

2.1 Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

2.2 Grundsätzliche Maßnahmen zur Zutrittskontrolle:

Zutrittszonen:	Die Räumlichkeiten der Sprengnetter Immobilienbewertung sind in folgende Zutrittsbereiche unterteilt: 1. Server- und IT-Bereich **(Zone 1)**. 2. Büro- und Geschäftsräume **(Zone 2)**. 3. Eingangsbereich **(Zone 3)**.
Zutrittsberechtigt sind:	1. **Zone 1** Zutritt nur für die zentrale Systemadministration, die Abteilungsleitung der Systemadministration, die Gebäudeverwaltung und die Geschäftsführung. 2. **Zone 2** Zutritt für alle Mitarbeiter der Sprengnetter Immobilienbewertung. 3. **Zone 3** Zutritt für alle o.g. Personen und für Gäste/Besucher.
Zutrittskontrolle durch:	1. **Zone 1 (eigenständig gesicherter Bereich der Alarmanlage)** Zylinder-Sicherheits-Schließsystem mit personalisiertem Chip zum aktivieren/deaktivieren der Alarmanlage. Sowie abgeschlossene Serverschränke. 2. **Zone 2** Zylinder-Sicherheits-Schließsystems mit personalisiertem Chip zum aktivieren/deaktivieren der Alarmanlage. 3. **Zone 3** Der während den Geschäftszeiten dauerhaft besetzte Empfang gewährleistet, dass unbefugte Personen die Räumlichkeiten nicht betreten können. Gäste müssen sich in eine Besucherliste eintragen und erhalten einen Besucherausweis. Erst dann können Sie dort abgeholt werden.
Außerhalb der Geschäftszeiten:	Für die gesamten Räumlichkeiten der Sprengnetter Immobilienbewertung gibt es ein Zylinder-Sicherheitsschließsystem, sowie ein Alarmanlagensystem. Das Alarmanlagensystem verfügt über ein protokolliertes Aktivierungs-, Deaktivierungs- sowie Alarmkonzept, sowie ein 24/7 besetzte Leitstelle mit Interventionsfahrern.

3 ZUGANGSKONTROLLE

3.1 Zugangskontrolle generell

Maßnahmen, die verhindern, dass unbefugte Personen Datenverarbeitungssysteme nutzen können, auf denen personenbezogene Daten gespeichert sind.

- Zugang zu den Server-Systemen der Sprengnetter Immobilienbewertung nur über passwort-geschützte gesicherte Verbindung.
- Zugang zu Client-Systemen der Sprengnetter Immobilienbewertung erhalten Nutzer nur dann, wenn sie sich mit Benutzername und Passwort legitimiert haben.
- Folgende Passwortanforderungen für Client- und Serversysteme sind umgesetzt:
  - Das Passwort muss aus mindestens 8 Zeichen bestehen.
  - Sie müssen Zeichen aus drei der vier folgenden Kategorien enthalten:
    - Großbuchstaben von A bis Z
    - Kleinbuchstaben von a bis z
    - Ziffern der Basis 10 (0 bis 9)
    - Nicht-Alphanumerische Zeichen (z. B. !, $, #, %)
  - Es darf keines der vorherigen 5 Passwörter verwendet werden.
  - Ein Passwort kann nur einmal pro Tag geändert werden.
  - Keine Worte aus einem Wörterbuch, keine Namen oder Geburtsdaten, keine KFZ-Kennzeichen, keine Geburtsnamen und keine Haustiernamen (durch Arbeitsanweisung im Intranet festgelegt)
- In der Benutzerverwaltung ist ein erzwungener Passwortwechsel nach 90 Tagen eingerichtet.
- Bei privilegierten Nutzern beträgt die Passwortlänge 12 Zeichen bei gleicher Komplexitäts-anforderung.
- Nach 5 fehlerhaften Anmeldeversuchen ist das Benutzerkonto für 10 Minuten gesperrt.
- Vergessene Passwörter können nur vom Systemadministrator zurückgesetzt werden.
- Eindeutige Vergabe von Benutzerkonten zu Benutzern
- Das automatische Sperren des EDV-Systems nach 5 Minuten bei Verlassen oder nicht Nutzung des Arbeitsplatzes ist umgesetzt (Eine Arbeitsanweisung, die das manuelle Sperren verlangt ist ebenso im Intranet umgesetzt).

3.2 Zugangskontrolle Internet

- Der interne Zugang zu den Datenverarbeitungssystemen ist mittels Benutzernamen und Passwörtern geschützt.
- Der externe Zugang zu den Datenverarbeitungssystemen erfolgt mittels VPN-Technologie und personenbezogenen Zugangsdaten sowie Zwei-Wege-Authentifizierung. Externen Zugang hat nur ein begrenzter Benutzerkreis.
- Der Login zu den Datenverarbeitungssystemen in den Rechenzentren erfolgt mittels SSH (Secure Shell verschlüsselt) und VPN vom Unternehmensstandort Bad Neuenahr mit personenbezogenen Zugangsdaten. Jeder Zugriff wird per Sprungserver Aufzeichnung dokumentiert.
- Der Zugang zu den Datenverarbeitungssystemen ist generell mit Hardware-Firewalls gesichert.
- Die Rechnersysteme in den Rechenzentren werden regelmäßigen, turnusmäßigen System- und Security-Updates unterzogen. Die Durchführung wird durch Monitoring-Systeme überwacht und protokolliert.

4 ZUGRIFFSKONTROLLE

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten, ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten, Programme und Server zugreifen können und dass personenbezogene Daten nach erfolgter Speicherung nicht von Unbefugten gelesen, kopiert, verändert oder entfernt werden können.

- Zugriff auf Netzlaufwerke nur für berechtigte Benutzergruppen mit Hilfe von Rollenprofilen.
- Einsatz von Firewalls.
- Einsatz von Mac-Filtern
- Verbindliches Verfahren zur Berechtigungsvergabe der Rollen (Freigabe durch Management bzw. Geschäftsführer mit Dokumentation im Ticketsystem) nach dem „Need-To-Known-Prinzip“.
- Jährliche Benutzer-Rezertifizierung der vergebenen Rechte/Rollen.
- Verbindliches Verfahren zur Wiederherstellung von Daten (Freigabe durch Management bzw. Geschäftsführer mit Dokumentation im Ticketsystem).
- Verbindlicher ticketbasierter Prozess für Joiner, Mover und Leaver.

5 TRENNUNGSKONTROLLE

Personenbezogene Daten, die zu unterschiedlichen Zwecken gespeichert werden, müssen getrennt verarbeitet werden.

- Trennung von Produktiv- und Testdaten
- Auf Wunsch (und Produktspezifisch) physikalisch getrennte Server-Systeme möglich
- Die in den Systemen verwendeten Berechtigungsmechanismen ermöglichen eine exakte Umsetzung der Vorgaben.

6 PSEUDONYMISIERUNG

Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

- Erzeugung von Pseudonymen bei gegebener Verhältnismäßigkeit und Umsetzbarkeit
- Umsetzung der hier genannten TOMs zum Schutz der Zuordnungsinformationen

7 INTEGRITÄT

7.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern 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.

- Bei jeder Übermittlung von Daten werden sichere Verschlüsselungsmethoden verwendet.
- Zugriff auf personenbezogene Daten nur über verschlüsselte und gesicherte Kanäle.
- Sperrung von USB Ports
- Verschlüsselung von Notebook-Festplatten
- Kein unverschlüsselter Versand personenbezogener Daten via Email.
- Einsatz von Firewalls

7.2 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.

- Beschränkung der Arbeit mit personenbezogen Daten des Auftraggebers auf die im Zusammenhang mit Leistungen aus dem Vertrag tätigen Mitarbeitern des Auftragnehmers

8 VERFÜGBARKEIT UND BELASTBARKEIT

8.1 Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Vollständiges Back-Up und Recovery-Konzept mit täglicher Sicherung und katastrophensicherer Aufbewahrung der Sicherung an verschiedenen physikalisch Standorten.
- Einsatz von Schutzprogrammen wie Virenscanner, Firewalls, Verschlüsselungsprogramme und Spamfiltern.
- Einsatz von Storage-Systemen mit Redundanz (RAID).
- SAN-System mit Serversystemen in unterschiedlichen Brandabschnitten.
- Einsatz unterbrechungsfreier Stromversorgung für alle Serversysteme.
- Klimatisierte Serverräume.
- Feuer-/Rauchmeldeanlage in den Geschäftsräumen sowie Feuer-/Rauch-/Temperatur- und Wassereinbruchmeldeanlage in den Serverräumen.
- Automatisierte Standardroutinen zur Wartung und Durchführung von Updates auf Servern und Clients (Virensoftware, Windows-Updates etc.).
- Ticket-System für den optimalen Workflow bei Wartungs- und Störungsmeldungen.
- Überwachung der Server- und Kommunikationslandschaft durch ein professionelles Monitoring-System.

9 VERFAHREN ZUR REGELMÄßIGEN ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

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

- Auditplanung und Durchführung von internen- und externen Audits
- Durchführung von Sensibilisierungsmaßnahmen in Form von halbjährlichen Sensibilisierungsmaßnahmen sowie Einzel- und Teamschulungen.
- Reporting bzw. Berichterstattung

- Risikomanagement und -Analyse
- Prozess zur Behandlung von Datenschutzvorfällen
- Datenschutzfreundliche Voreinstellungen

Alle beim Auftragnehmer eingesetzten Beschäftigten sind und werden auf das Daten-, Geschäfts-, Privat- und Bankgeheimnis verpflichtet und entsprechend zum Datenschutz sensibilisiert. Ein Datenschutzbeauftragter ist zur Wahrung der datenschutzrechtlichen Anforderungen bestellt. Es finden regelmäßige Kontrollen durch den Datenschutzbeauftragten statt, wobei in diesem Rahmen regelmäßige Hinweise erfolgen, um das Problembewusstsein zu fördern. Schließlich finden gelegentliche unvermutete Kontrollen der Einhaltung von Datenschutz- und Datensicherheitsmaßnahmen statt.

- Incident-Response-Management

Im Rahmen der datenschutzrechtlichen Mitarbeiterschulung werden die mit der Verarbeitung eingesetzten Beschäftigten über den Umgang mit jeglichen Anfragen zum Datenschutz unterrichtet. Aufgrund der flachen Hierarchien im Unternehmen des Auftragnehmers werden jegliche Anfragen im Zusammenhang mit dem Datenschutz unverzüglich an den Datenschutzbeauftragten und ggfs. an die Geschäftsleitung weitergeleitet. Eine entsprechende Bearbeitung jeglicher datenschutzrelevanten Anfragen erfolgt zeitnah.

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Die zur Verfügung gestellten Produkte enthalten datenschutzfreundliche Voreinstellungen. Zudem werden die Mitarbeiter in Schulungen hierauf sensibilisiert, so dass bei der Entwicklung auf die Grundsätze Privacy by Default und Privacy by Design geachtet wird.

10 AUFTRAGSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

- Detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers durch schriftlich formulierten Auftrag
- Detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch Sprengnetter Immobilienbewertung außerhalb des schriftlich formulierten Auftrags
- Sprengnetter Immobilienbewertung hat einen betrieblichen Datenschutzbeauftragen bestellt und sorgt für dessen angemessene und effektive Einbindung in die relevanten Prozesse.
- Auf Kundenwunsch kann im Vertrag eine verantwortliche Person beim Auftraggeber benannt werden, die in Bezug auf die vereinbarte Auftragsdatenverarbeitung gegenüber Sprengnetter Immobilienbewertung weisungsbefugt ist.
- Mündliche Aufträge müssen schriftlich bestätigt werden.
- Dem Auftraggeber können Kontrollrechte eingeräumt werden.
- Sorgfältige Vertragsgestaltung (z.B. SLA, Kontrollrechte, Verpflichtung Mitarbeiter, AV-Verträge)
- Die Unterauftragnehmer sind sorgfältig ausgewählt.
- Durchführung von Kontrollen
- Einholen von Nachweisen (z.B. Zertifikate)