NFON
Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. b DSGVO

Die Telefonanlage einer neuen Generation.

NFON

Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. b DSGVO der NFON AG

Version 1.2

NFON AG
Machtlfinger Str. 7
81379 München
Tel.: + 49 89 45 3000
www.nfon.com

© 2022 NFON AG – Alle Rechte vorbehalten

Änderungen bleiben vorbehalten
Version 1.2 / 01.2022 (DE)
gültig ab dem 01.01.2022

NFON

Technische und organisatorische Maßnahmen nach Art. 32 Abs. 1 lit. b DSGVO der NFON AG

1 Inhaltsverzeichnis

© 2022 NFON AG – Alle Rechte vorbehalten Änderungen bleiben vorbehalten. Version 1.2 / 01.2022 (DE)

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

2 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

2.1 Zutrittskontrolle

Bei der Zutrittskontrolle handelt es sich um Maßnahmen, die geeignet sind, „Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren“.

Es ist zu unterscheiden zwischen dem Zutritt zu den Rechenzentren und Zutritt zu den Büroräumen.

2.2 Grundsätzliche Maßnahmen zur Zutrittskontrolle – Zutrittskontrolle Bürobereich

- Definition von Sicherheitsbereichen einschl. Festlegung individueller Maßnahmen

Davon abhängig:

- Schließanlage (physische Schlüssel, Chipkarten, Token)
- Kamera- und Alarmüberwachung
- Berechtigungsvergabe (Schlüsselverwaltung und grundsätzliche Zutrittsberechtigungen)
- Besucherregelung
- Regelungen für Arbeiten in Sicherheitsbereichen

Unabhängig von den Sicherheitsbereichen

- Clear-Desk Regelungen
- Regelung zu An- und Ablieferung
- Besucherbuch
- Schutz von Betriebsmitteln, auch außerhalb des Gebäudes

© 2022 NFON AG – Alle Rechte vorbehalten Änderungen bleiben vorbehalten. Version 1.2 / 01.2022 (DE)

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

2.3 Zutrittskontrolle Rechenzentren

Die NFON betreibt bewusst keine eigenen Rechenzentren, sondern hat Flächen in den Rechenzentren großer Anbieter angemietet. Diese Rechenzentren erfüllen verschiedene Zertifizierungen wie ISO 27001, ITIL, eco Datencenter Five Star.

Bei der Beauftragung der Rechenzentren handelt es sich um Colocation-Services.

Die grundsätzlich von der NFON festgelegten Maßnahmen zur Zutrittskontrolle sind auch beim Rechenzentrumsbetreiber umgesetzt.

Die Zutrittsberechtigungen zu den Rechenzentren sind personalisiert und auf einen dokumentierten Personenkreis eingeschränkt. Die Authentifizierung erfolgt per (Personal-) Lichtbildausweis.

Die Datenverarbeitungsanlagen befinden sich innerhalb des Rechenzentrums in eigenen verschlossenen Racks, die nur mit einem Passwort seitens der NFON geöffnet werden können.

Die Rechenzentren werden ausschließlich in Deutschland und mit deutschen Vertragspartnern betrieben.

3 Zugangskontrolle

Bei der Zugangskontrolle handelt es sich um Maßnahmen, die geeignet sind „zu verhindern, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden“.

Es ist zu unterscheiden zwischen dem Zugang in den Rechenzentren, Zugang in den Offices, Zugang über das Internet und generelle Zugangskontrollen.

3.1 Zugangskontrolle generell

- Zugangsberechtigungen sind nach Notwendigkeit eingerichtet. - Minimalprinzip
- Unterscheidung „normaler-“, „privilegierter Accounts“ und „externer Accounts“ - Rollenkonzept
- Vergabe- und Entzugsprozess von Berechtigungen
- Regelmäßige Kontrolle der vergebenen Berechtigungen
- Es gibt eine Richtlinie für das Sperren der Arbeitsplatzrechner; Clear-Desk Policy
- Entsprechend der technischen Möglichkeiten werden Timeouts konfiguriert.

© 2022 NFON AG – Alle Rechte vorbehalten Änderungen bleiben vorbehalten. Version 1.2 / 01.2022 (DE)

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

- Mobile Datenträger, sowie die Datenträger von Laptops / Notebooks, werden verschlüsselt.
- Sämtliche Zugänge sind mit Benutzernamen und Passwort gesichert.
- Anforderungen an die Passwortkomplexität
- Nutzeraktivitäten werden protokolliert.
- Elektronische und papiergebundene Informationen werden datenschutzkonform vernichtet. Über die Vernichtung wird ein Protokoll erstellt.

3.2 Zugangskontrolle Rechenzentren

- Der Zugang zu den Datenverarbeitungsanlagen ist – nach Öffnen des Racks – weiterhin zusätzlich durch Benutzername und Passwort geschützt.
- Der Personenkreis mit Zugang im Rechenzentrum (Racks und Anlagen) ist gegenüber dem Personenkreis mit Zutritt zum Rechenzentrum weiter eingeschränkt (Rollenvergabe).

3.3 Zugangskontrolle Internet

- Der Zugang zu den Datenverarbeitungssystemen ist mittels Benutzernamen und Passwörtern geschützt.
- Der Zugang zu den Rechnersystemen der NFON erfolgt mittels VPN-Technologie und personenbezogenen Zugangsdaten.
- Der Login zu den Rechnersystemen der NFON in den Rechenzentren erfolgt mittels SSH (Secure Shell; verschlüsselt) und personenbezogenen Zugangsdaten.
- Der Zugang zu den Datenverarbeitungssystemen ist generell mit Hardware-Firewalls gesichert.
- Das Setup der Rechnersysteme der NFON in den Rechenzentren ist minimalistisch, um Gefahren durch fehlerhafte Software zu minimieren – Systemhärtung.
- Die Rechnersysteme der NFON in den Rechenzentren werden regelmäßigen, turnusmäßigen System- und Security-Updates unterzogen. Die Durchführung wird durch Monitoring-Systeme überwacht und protokolliert.

© 2022 NFON AG – Alle Rechte vorbehalten Änderungen bleiben vorbehalten. Version 1.2 / 01.2022 (DE)

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

4 Zugriffskontrolle

Zugriffskontrolle sind Maßnahmen, die „gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“.

Die Zugriffsberechtigungen sind in der Praxis oft an die Zugangsberechtigungen gekoppelt, sodass die Maßnahmen zum Zugang auch indirekte Auswirkungen auf den Zugriff haben.

- Zugriffsberechtigungen sind nach Notwendigkeit eingerichtet. - Minimalprinzip
- Unterscheidung „normaler-“, „privilegierter Accounts“ und „externer Accounts“ - Rollenkonzept
- Vergabe- und Entzugsprozess von Berechtigungen
- Regelmäßige Kontrolle der vergebenen Berechtigungen
- Zugriffe sind mit Passwort gesichert, gemäß Schutzbedarf.
- Anforderungen an die Passwortkomplexität
- Nutzeraktivitäten werden protokolliert.
- Elektronische und papiergebundene Informationen werden datenschutzkonform vernichtet. Über die Vernichtung wird ein Protokoll erstellt.

5 Trennungskontrolle

Maßnahmen, die „gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können“.

- Trennung von Test- und Produktivsystemen
- Getrennte Speicherung
    - der ERP-/CRM-Daten
    - der Netzwerkprofile/Konfigurationsdaten
    - Service-/Supportdaten der Kunden
- Ein mehrstufiges Berechtigungskonzept sorgt dafür, dass unterschiedliche Benutzer unterschiedliche Rechte zur Eingabe, Änderung und Löschung von Daten in der Portaloberfläche haben.

© 2022 NFON AG – Alle Rechte vorbehalten Änderungen bleiben vorbehalten. Version 1.2 / 01.2022 (DE)

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

- Logische Mandantentrennung
- Festlegung von Datenbankrechten

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
- Zentrale Speicherung der Zuordnungsinformationen

7 Integrität

7.1 Weitergabekontrolle

Unter Weitergabekontrolle versteht man Maßnahmen, die geeignet sind „zu 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".

- Alle Mitarbeiter sind vertraglich auf das Datengeheimnis verpflichtet.
- Alle Mitarbeiter sind vertraglich auf § 88 des TKG verpflichtet.
- Mobile Datenträger, sowie die Datenträger von Laptops / Notebooks werden verschlüsselt.
- Der Zugang zu den Rechnersystemen der NFON in den Rechenzentren erfolgt mittels VPN-Technologie und personenbezogenen Zugangsdaten.

© 2022 NFON AG – Alle Rechte vorbehalten Änderungen bleiben vorbehalten. Version 1.2 / 01.2022 (DE)

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

- Der Login zu den Rechnersystemen der NFON in den Rechenzentren erfolgt mittels SSH (Secure Shell; verschlüsselt) und personenbezogenen Zugangsdaten.
- Der Zugang zu den Datenverarbeitungssystemen der NFON ist generell mit Hardware-Firewalls gesichert.
- Die Zugriffe auf die Portaloberfläche per Internet erfolgen über gesicherte Verbindungen (SSL/TLS) mit Schlüssellängen, die dem Stand der Technik entsprechen.
- Die Löschfristen der überlassenen Daten entsprechen den gesetzlichen Vorgaben.
- Bei Kommunikation mit externen Geschäftspartnern, Kunden und Diensten werden Verschlüsselungen nach dem Stand der Technik eingesetzt, sofern der Kommunikationspartner dies unterstützt.
- Die bei der Verschlüsselung verwendeten Signaturen werden gegen die Zertifizierungsstelle validiert.
- Informationsklassifizierung, ab wann verschlüsselt werden muss.
- Protokollierung der Übertragung
- Geschützter physischer Transport

7.2 Eingabekontrolle

Unter Eingabekontrolle versteht man Maßnahmen, die geeignet sind „zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind“.

- Festlegung, was protokolliert wird, insbesondere die Eingabe, Änderung und Löschung von Daten werden protokolliert und sechs Monate gespeichert.
- Sichere Aufbewahrung von Protokollinformationen
- Ein mehrstufiges Berechtigungskonzept sorgt dafür, dass unterschiedliche Benutzer unterschiedliche Rechte zur Eingabe, Änderung und Löschung von Daten in der Portaloberfläche haben.
- Der Zugriff auf die Portaloberflächen erfolgt mittels individueller Benutzernamen und Passwörter.

© 2022 NFON AG – Alle Rechte vorbehalten Änderungen bleiben vorbehalten. Version 1.2 / 01.2022 (DE)

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

8 Verfügbarkeit und Belastbarkeit

8.1 Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit

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

- Die Rechenzentren erfüllen verschiedene Zertifizierungen wie ISO 27001, ITIL, eco Datacenter Five Star, welche sich mit der Thematik der Verfügbarkeit auseinandersetzen.
    - Brandschutzeinrichtungen (Feuerlöscher, Rauch- oder Brandmelder), Rauchverbot, Wasserschutzeinrichtungen
    - Unterbrechungsfreie Stromversorgung (USV)
    - Klimaanlage
    - Redundante Stromzuführung
    - Löschanlage
- Redundante Internet-Anbindung der Serversysteme
- Verwendung von USVs
- Brandmeldeanlagen
- Einsatz von Monitoring-Systemen zum Erkennen von Fehlern oder Ressourcen-Engpässen und zur Bedarfsplanung.
- Einsatz von Alerting-Systemen im Fehlerfall, mit SMS und E-Mail Benachrichtigung und Eskalationsstufen bis hin zu telefonischer Benachrichtigung über einen externen Anbieter.
- Verwendung eines Virenschutzes
- Rufbereitschaft 24/7 (mit Stellvertreterregelung bei Nichterreichbarkeit)
- Live-Datensicherung durch Replikation der Daten an verschiedene Standorte.
- Ausfallsicherheit durch Replikation der Daten und automatische Failover-Mechanismen im Fehlerfall.
- Redundante Rechenzentren mit entsprechender Planung von Überkapazitäten, so dass der Ausfall eines Rechenzentrums durch die anderen vollständig kompensiert werden kann.
- Verwendung von RAID Systemen in den Servern.
- Automatische tägliche Datensicherung mit anschließender Replikation auf ein Zweitsystem in einem anderen Rechenzentrum. Der Vorhaltezeitraum beträgt 12 Tage.

© 2022 NFON AG – Alle Rechte vorbehalten Änderungen bleiben vorbehalten. Version 1.2 / 01.2022 (DE)

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

- Es existiert ein Notfallplan / -handbuch.
- Dokumentation der Systeme an zentraler Stelle außerhalb unserer eigenen Infrastruktur.
- Die Software und Konfiguration wird über ein Versionierungssystem verwaltet, dies erlaubt schnelle Rollbacks.
- Die Rechnersysteme der NFON in den Rechenzentren werden regelmäßigen, turnusmäßigen System- und Security-Updates unterzogen. Die Durchführung wird durch Monitoring-Systeme überwacht und protokolliert.
- regelmäßige Durchführung von Wiederherstellungsübungen
- Verschlüsselung der Datensicherung

Erstellung von Wiederherstellungsplänen gemäß den intern festgelegten Anforderungen.

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
- Maßnahmenplanung
- Reporting bzw. Berichterstattung
- Risikomanagement und -Analyse
- Prozess zur Behandlung von Datenschutzvorfällen
- Bildung und Auswertung von DS-relevanten KPI
- Datenschutzfreundliche Voreinstellungen

© 2022 NFON AG – Alle Rechte vorbehalten Änderungen bleiben vorbehalten. Version 1.2 / 01.2022 (DE)

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com

10 Auftragskontrolle

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

- Die Unterauftragnehmer sind sorgfältig ausgewählt
- Sorgfältige Vertragsgestaltung (z.B. SLA, Kontrollrechte, Verpflichtung Mitarbeiter, AV-Verträge, relevante Aspekte des TKG, etc.)
- Durchführung von Kontrollen
- Einholen von Nachweisen (z.B. Zertifikate)

© 2022 NFON AG – Alle Rechte vorbehalten Änderungen bleiben vorbehalten. Version 1.2 / 01.2022 (DE)

NFON AG · Machtlfinger Str. 7 · 81379 München · Tel.: + 49 89 45 3000 · nfon.com