netfiles

Technische und organisatorische Maßnahmen

Im Folgenden werden die wichtigsten organisatorischen und technischen Maßnahmen beschrieben, die netfiles unternimmt, um die Anforderungen der Datenschutzgrundverordnung (DSGVO) umzusetzen.

0. Organisation

Organisatorische Maßnahmen zur Umsetzung des Datenschutzes nach DSGVO:

- Zur Wahrnehmung der Beratungs- und Kontrollfunktionen aus der DSGVO wird folgender externer Datenschutzbeauftragter eingesetzt:
  Christian Volkmer, Projekt 29 GmbH
  Ostengasse 14, 93047 Regensburg
  Telefon +49-941-2986930
- Das Schulungskonzept beinhaltet sowohl eine Datenschutzunterweisung bei Beginn der Tätigkeit, als auch eine konstante Sensibilisierung durch monatliche Datenschutznewsletter, fachbezogene Webschulungen, persönliche Sensibilisierung durch den Geschäftsführer und externen Datenschutzbeauftragten, sowie eine jährliche, umfassende Nachschulung. Zusätzlich werden alle Mitarbeiter und Unterauftragnehmer auf den Datenschutz verpflichtet.
- Im Rahmen des internen Verfahrensverzeichnisses sind die Datenströme dokumentiert und die Zulässigkeit der Verarbeitung und Nutzung nach BDSG nachgewiesen. Eventuell notwendige Vorabkontrollen werden schon im Planungsstadium integriert.
- Der Auftragnehmer hat ein ISO 27001 konformes, vom TÜV Süd zertifiziertes Informationssicherheitsmanagementsystem (ISMS) in Betrieb, dessen Scope den Betrieb von netfiles enthält und dessen Erklärungen zur Anwendbarkeit (Scope of Applicabillity - SOA) um die Controls von ISO 27017 (Cloud Security) und ISO 27018 (Personally Identifiable Information) erweitert wurden.

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

1.1 Zutrittskontrolle

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

- Auf den in den Büroräumlichkeiten befindlichen Datenverarbeitungsanlagen werden keine Daten des Auftraggebers verarbeitet. Die Durchführung der Verarbeitung erfolgt ausschließlich auf Servern von netfiles in hochsicheren Rechenzentren. Die Rechenzentren sind durch elektronische Zutrittskontrollanlagen entsprechend Klasse B nach VdS 2367 gegen den Zutritt Unbefugter gesondert gesichert. Überwachung der Rechenzentren erfolgt rund um die Uhr durch eine externe Sicherheitsfirma.

- Alle Server befinden sich in verschlossenen Serverschränken in separat abgesicherten Serverräumen. Diese Räume sind einbruchhemmend geschützt und mindestens gemäß den Vorgaben der Sicherungsklasse SG1 nach VdS 2333 ausgeführt.
- Beim Betreten und für jeweils einen Zeitraum von 90 Tagen nach Betreten der Räumlichkeiten werden die Zutritte zu diesen Räumlichkeiten protokolliert.
- Der Zutritt zu den Serverräumen ist auf das Personal zur Wartung und Instandsetzung beschränkt. Besuchern und Fremdpersonal werden immer begleitet.
- Die Vergabe von Zutrittsberechtigungen und von Schlüsseln, Magnetkarten, Ausweisen sowie anderen den Zutritt ermöglichenden Identitätsmerkmalträgern ist nachvollziehbar in Form einer aktuellen Auflistung der ausgegebenen Schließmittel und Zutrittsberechtigungen dokumentiert.
- Im Rahmen der regelmäßigen Lieferanten-Audits werden auch die Zutrittskontrollmaßnahmen überprüft.

1.2 Zugangskontrolle

Maßnahmen die verhindern, dass Datenverarbeitungssysteme, mit denen die Verarbeitung und Nutzung personenbezogener Daten erfolgt, von Unbefugten genutzt werden können:

- Die zur Verarbeitung eingesetzten Server in den Rechenzentren sind durch eigene Netze, elektronische Zertifikate sowie Benutzernamen und Kennwörter mehrfach geschützt.
- Benutzerzugänge werden auf die notwendige Anzahl reduziert und nur nach Genehmigung durch die Geschäftsleitung an fachlich und persönlich geeignetes Personal vergeben. Die Anlage und Veränderung von Benutzerzugängen wird im firmeneigenen Ticketsystem dokumentiert.
- Soweit technisch möglich werden alle Benutzerzugänge ausschließlich personenspezifisch vergeben. Ist eine gruppenspezifische Verwendung von Zugängen unvermeidbar, wird die Zuordnung auf eine natürliche Person durch die zeitgenaue Zuordnung in den Logfiles sichergestellt.
- Elektronische Zertifikate, Benutzernamen und Kennwörter sind ausschließlich persönlich.
- Alle Passwörter werden vom jeweiligen Mitarbeiter selbst vergeben. Durch entsprechende Systemeinstellungen werden die vorgegebenen Kennwort Richtlinien erzwungen. Passwörter nicht außerhalb der genehmigten Kennwortmanager gespeichert werden. Die Rücksetzung „vergessener“ Kennwörter erfolgt über ein revisionssicheres, verbindliches Verfahren. Alle Mitarbeiter sind auf die internen Richtlinien zum sicheren, ordnungsgemäßen Umgang mit Kennwörtern verpflichtet worden.
- Zugänge sind ausschließlich über verschlüsselte Verbindungen möglich. Bei Inaktivität erfolgt eine automatische Abmeldung. Bei mehr als drei fehlerhaften Anmeldeversuchen erfolgt eine automatische Zugangssperre. Zusätzlich können alle Zugänge manuell gesperrt werden. Alle Zugänge werden protokolliert.
- Eine Fernwartung ist mit entsprechend elektronisch gesicherten Geräten möglich.

1.3 Zugriffskontrolle

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:

- Es existiert ein abgestuftes und granulares Rechtesystem. Es erfolgt eine detaillierte Vergabe von Zugriffsrechten nach Personen. Der Zugriff wird ausschließlich auf Basis der vergebenen Rechte gewährt. Hierdurch ist sichergestellt, dass alle Mitarbeiter nur Zugriff auf die Daten haben, die sie zur Erfüllung ihrer Aufgaben zwingend benötigen.
- Eine regelmäßige Revision der vergebenen Rechte ist Teil des internen Audits und wird zusammen mit dem internen Sicherheitsbeauftragten durchgeführt und von diesem dokumentiert.
- Alle Dokumente werden ausschließlich verschlüsselt gespeichert.
- Es existiert ein revisionssicheres, verbindliches Verfahren zur Wiederherstellung von Daten aus dem Backup (Restore ausschließlich auf Anweisung der Geschäftsleitung / Geschäftsführung).
- Alle Datenzugriffe werden protokolliert. Es erfolgt eine sporadische Durchsicht der Protokolle. Diese werden in der Regel 12 Monate aufbewahrt.

1.4 Trennungskontrolle

Maßnahmen die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Alle Kundendaten werden in logisch unterschiedlichen Bereichen mit unterschiedlichen Zugriffsrechten gespeichert und mit einem kundenspezifischen Schlüssel verschlüsselt. Dadurch können die Daten des Auftraggebers getrennt von anderen Kunden bearbeitet und gelöscht werden.
- Die von Kunden in netfiles gespeicherten Daten können von netfiles ohne explizite Rechtevergabe durch den Auftraggeber nicht eingesehen werden. Jede weitere Verarbeitung von Daten durch netfiles, z.B. das Erstellung eines Archivdatenträgers, erfolgen nur auf schriftliche Anforderung durch den Auftraggeber.
- Die Daten des Auftraggebers und anderer Mandanten werden soweit möglich von unterschiedlichen Mitarbeitern des Dienstleisters verarbeitet.

1.5 Pseudonymisierung (Art.32 Abs. 1 Lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Organisatorische Maßnahmen, damit die Verarbeitung personenbezogener Daten gesetzeskonform aufbewahrt und verarbeitet werden:

- Alle mit der Verarbeitung von personenbezogenen Daten betrauten Personen wurden auf das unternehmensinterne Datenschutz- und Sicherheitskonzept sowie einen gesetzeskonformen Umgang mit

den Daten verpflichtet. Die Mitarbeiter werden bei Beginn ihrer Tätigkeit und anschließend laufend geschult (sie auch 0. Organisation).

- netfiles Mitarbeiter haben keinen direkten Kontakt bzw. Umgang mit personenbezogenen Daten.

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

2.1 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:

- Es erfolgt keine Weitergabe personenbezogenerer Daten durch den Auftragnehmer. Ausgenommen hiervon ist die Archivierung und Weitergabe der Inhalte eines Datenraums auf explizite Anforderung durch den Kunden an ihn selbst oder einen von ihm bestimmten Empfänger. Hierzu muss der Kunde die Weitergabe schriftlich beauftragen und netfiles Zugang zu diesem Datenraum gewähren. Die Archivierung der Daten erfolgt in der Regel verschlüsselt, es sei denn der Kunde wünscht explizit eine unverschlüsselte Ausfertigung. Der Versand erfolgt in der Regel nachvollziehbar über den Paketdienst DHL. Dieser unterliegt als Tochter der Post dem Fernmeldegeheimnis. Jede Versandaktion wird von netfiles protokolliert. Es erfolgt keine inhaltliche Sichtung des Datenraums. Die Inhalte werden verschickt, wie sie zum Zeitpunkt der Anforderung auf dem System abgelegt waren.
- Alle Daten werden ausschließlich verschlüsselt zwischen allen Systemen übertragen (Client/Server und Server/Server) und nur verschlüsselt gespeichert.
- Für die Verschlüsselung wird mindestens AES-256, als Hash Verfahren mindestens SHA-256, für Schlüssellängen von mindestens 2048 Bit und für den Verbindungsaufbau ECDHC eingesetzt.
- Es werden keine Daten auf Bänder oder andere transportable Datenträger kopiert. Festplatten mit Daten werden nicht transportiert.
- Es erfolgt eine Risikominimierung durch Netzseparierung und eine Implementation von Sicherheitsgateways an den Netzübergabepunkten.

2.2 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:

- Die Nutzung aller Applikationen und aller Eingaben werden personenspezifisch protokolliert.
- Durch entsprechende Rollen-/Rechtekonzepte ist nachvollziehbar welcher Benutzer wann welche Aktivitäten durchgeführt hat.

- Mitarbeiter von netfiles können nur nach expliziter Rechtevergabe durch den Auftraggeber auf dessen Daten zugreifen und sie verarbeiten.
- Unterauftragnehmer haben keinen Zugang zu den personenbezogeneren Daten des Auftraggebers.

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

3.1 Verfügbarkeitskontrolle

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

- Alle Kundendaten sind ausschließlich in den netfiles Rechenzentren und dort in den abgeschlossenen Serverschränken der separat gesicherten Serverräume gespeichert.
- Alle Serversysteme werden durch Intrusion Detection / Intrusion Prevention Systeme (IDS/IPS) sowie Firewalls und eigene Administrationsnetze gegen nicht betriebsnotwendige Zugriffe gesichert. Die Serversysteme selbst sind gehärtet, d.h. auf die betriebsnotwendigen Komponenten, Dienste und Schnittstellen beschränkt und werden laufend aktualisiert. Insbesondere werden alle Sicherheitsupdates des Betriebssystems und der verwendeten Komponenten zeitnah eingespielt.
- Alle Änderungen an den Einstellungen den Softwarekomponenten, den Einstellungen der Firewall oder IDS/IPS werden in einem Ticketsystem revisionssicher dokumentiert.
- Die Sicherheitseinstellungen der Systeme und der verschlüsselten Verbindungen werden regelmäßig (mindestens einmal im Monat) intern überprüft.
- Mindestens zweimal im Jahr werden externe Unternehmen beauftragt einen sog. PEN-Test durchzuführen, bei dem versucht wird Sicherheitslücken beim Auftragnehmer zu entdecken.
- Alle Daten werden mehrfach redundant gespeichert (mehrfach gespiegelte Platten, Speicherung in infrastrukturell getrennten Rechenzentren).
- Alle Daten, die auf den netfiles Servern gespeichert werden, werden automatisch auf Viren untersucht. Die Virenscanner werden mindestens einmal am Tag aktualisiert.
- Alle Backup Daten werden physisch getrennt in einem anderen Rechenzentrum von den Produktivdaten gespeichert.
- Die Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.
- Defekte Festplatten werden vor der Entsorgung mechanisch zerstört. Es werden keine defekten Festplatten zum Hersteller zurückgeschickt, auch nicht bei Garantiefällen. Nicht mehr benötigte Festplatten

werden entweder gelöscht und in anderen netfiles Servern weiterverwendet oder ebenfalls mechanisch zerstört und entsorgt.

3.2 Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Maßnahmen die gewährleisten, dass personenbezogene Daten bei Ausfällen kurzfristig wiederhergestellt werden können:

- Es existiert ein Backup Konzept mit folgenden Stufen:
  - alle Daten liegen auf gespiegelten Festplatten
  - alle Daten werden in Echtzeit auf einem zweiten System im gleichen Rechenzentrum dupliziert
  - alle Daten werden in Intervallen von 15 Minuten in ein Cold-Standby Rechenzentrum kopiert;
  - alle Daten werden einmal täglich auf ein Backupsystem in einem anderen Rechenzentrum gesichert.
- Es werden alle Backups der letzten 30 Tage gespeichert und anschließend zyklisch überschrieben. Alle Backups und Kopien der Daten werden nach den identischen Sicherheitskriterien wie die Originaldaten behandelt.
- Zur Verifikation des Backups wird täglich der Backup des letzten Tages auf einem Testsystem wiederhergestellt und auf seine Funktionsfähigkeit überprüft.
- Das Umschalten vom Live-System auf die Hot-Stand-By und Cold-Stand-By Systeme wird mindestens einmal im Monat getestet.
- Es existiert ein dokumentiertes Notfallkonzept, in dem genau festgelegt ist, was bei welchen Problemen zu machen ist. Mindestens einmal im Jahr wird ein vollständiger Ausfall des primären Rechenzentrums simuliert und das Notfallkonzept überprüft. Das Ergebnis wird im internen Informationssicherheitsmanagementsystem dokumentiert.

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

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

4.1 Datenschutz Management

Maßnahmen zur regelmäßigen Bewertung/Überprüfung der Datenschutz Maßnahmen, um die Sicherheit der Datenverarbeitung zu gewährleisten:

- Der externe Datenschutzbeauftragte überprüft regelmäßig und teilweise auch unangekündigt, die Einhaltung der technisch-organisatorischen Maßnahmen.
- Mindestens einmal im Jahr findet ein internes Audit der Datenschutzmaßnahmen durch die Geschäftsleitung und den Informationssicherheitsbeauftragten statt.
- Der Auftragnehmer ist ISO 27001 zertifiziert. Der Betrieb der Anwendung netfiles ist explizit im Scope des Zertifikates enthalten. Die Erklärungen zur Anwendbarkeit (Scope of Applicabillity - SOA) wurde um die Controls von ISO 27017 (Cloud Security) und ISO 27018 (Personally Identifiable Information) erweitert.
- Im Rahmen der jährlichen Audits der ISO 27001 Zertifizierung findet auch eine Überprüfung der Einhaltung der Controls aus ISO 27018 durch den Auditor des TÜV Süd statt.

4.2 Incident-Response-Management

Maßnahmen die gewährleisten, dass auf Anfragen bzw. Probleme schnell und umfassend reagiert werden kann:

- Alle Systeme des Auftragnehmers werden durch ein internes System (Nagios) rund um die Uhr überwacht. Bei Problemen wird das rund um die Uhr (24/365) verfügbare Betriebsteam automatisch alarmiert.
- Zusätzlich werden die von außen erreichbaren Systeme ebenfalls rund um die Uhr von zwei unabhängigen, externen Dienstleistern auf deren Verfügbarkeit überprüft. Das Ergebnis dieser Prüfung kann von den Kunden im Rahmen der SLAs permanent und in Echtzeit eingesehen werden. Bei Problemen wird das Betriebsteam sofort und automatisch alarmiert.
- Im netfiles Informationssicherheitssystem (ISMS) gibt es ein detailliertes Incident Management System, in dem alle Rollen, das Vorgehen sowie die Ziele bei Vorfällen verbindlich definiert sind.
- Alle Vorfälle und Maßnahmen werden in einem Ticket System dokumentiert.
- Zusätzlich steht den Kunden eine Telefonhotline und Support per E-Mail zur Verfügung.

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Maßnahmen die gewährleisten, dass nur die unbedingt notwendigen personenbezogenen Daten erhoben und gespeichert werden:

- Es müssen nur die personenbezogenen Daten zwingend eingegeben werden, die zur Funktionsfähigkeit von netfiles notwendig sind (z.B.: E-Mail Adresse).
- Es gibt keine automatischen Vorbelegungen von Optionen.
- Alle Benutzer müssen ihre Anmeldeinformationen selbst eintragen. Ein automatisches Ausfüllen, bzw. Vervollständigen wird unterbunden.

4.4 Auftragskontrolle

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

- Für die Verarbeitung personenbezogener Daten setzt der Auftragnehmer ausschließlich persönlich und fachlich geeignete Mitarbeiter ein, die geschult sind und auf den Datenschutz verpflichtet wurden (siehe auch 0. Organisation und 1.5 Pseudonymisierung).
- Der Auftragsverarbeitungsvertrag wurde entsprechend den Richtlinien der DSGVO gestaltet. Er enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers.
- Der Auftragsverarbeitungsvertrag enthält detaillierte Angaben über die Zweckbindung der personenbezogenen Daten des Auftraggebers sowie ein Verbot der Nutzung durch den Dienstleister außerhalb des schriftlich formulierten Auftrags
- Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt. Dieser nimmt entsprechende Beratungs- und Kontrollpflichten wahr und sorgt für eine angemessene und effektive Einbindung des Schutzes personenbezogener Daten in alle relevanten betrieblichen Prozesse
- Auf Kundenwunsch kann im Vertrag eine verantwortliche Person beim Auftraggeber benannt werden, die in Bezug auf die vereinbarte Auftragsdatenverarbeitung gegenüber dem Dienstleister weisungsbefugt ist.

4.5 Löschung

Maßnahmen die gewährleisten, dass alle personenbezogenen Daten des Auftraggebers vollständig und dauerhaft von den Systemen des Auftragnehmers gelöscht werden:

- Zwei Wochen nach rechtswirksamer Beendigung eines Vertrages löscht der Auftragnehmer alle Daten des Kunden von allen seinen produktiven Systemen.
- Hierdurch werden diese Daten automatisch innerhalb von spätestens 24 Stunden von allen nicht produktiven Systemen gelöscht.

- Spätestens nach 30 Tagen wird die letzte Kopie der Kundendaten aus dem Backupsystem gelöscht und überschrieben.
- Das Löschen der Daten erfolgt automatisiert und wird entsprechend protokolliert.

netfiles GmbH
Marktler Strasse 2b
D-84489 Burghausen
Tel. +49 8677 91596-10

www.netfiles.com
sales@netfiles.com