Netzdirektion - Gesellschaft für digitale Wertarbeit mbH
Dokumentation der technischen und organisatorischen Maßnahmen

Stand: 10.10.2024

Verantwortlicher:

Netzdirektion - Gesellschaft für digitale Wertarbeit mbH
Adam-Foßhag-Str. 29
65428 Rüsselsheim am Main

Tel.: +496142 9538060
E-Mail: hallo@netzdirektion.de
Webseite: https://netzdirektion.de/

Datenschutzbeauftragter:

Die Netzdirektion hat folgenden Datenschutzbeauftragten benannt:

Jens Engelhardt, sein Stellvertreter ist Sven Kolja Braune
c/o NOTOS Xperts GmbH
Heidelberger Str. 6
64283 Darmstadt

Telefon: +49 6151-52010-0
Telefax: +49 6151-52010-99

Webseite: www.notos-xperts.de
E-Mail: datenschutz@notos-xperts.de

Nachfolgend werden die technischen und organisatorischen Maßnahmen (TOMs) der Netzdirektion - Gesellschaft für digitale Wertarbeit mbH (nachfolgend: Netzdirektion) übersichtlich dokumentiert.

1. Zutrittskontrolle

- Die Zutrittskontrolle liegt im Verantwortungsbereich der Geschäftsführung
- Sicherung von Eingangstüren, Gebäude kann nicht unbemerkt betreten oder verlassen werden
- Besucher werden in den Gebäuden beaufsichtigt
- Türen werden bei Abwesenheit verschlossen
- Türen und Fenster sind gegen Einbruch gesichert
- Serverräume und Rechenzentrum sind nur durch die Geschäftsführung betretbar und besonders geschützt

2. Zugangskontrolle

- IT-Systeme werden durch Passwortvergabe geschützt
- Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort
- Es existieren Richtlinien für die Vergabe von Passwörtern (Mindestlänge, Komplexität, Sonderzeichen)
- Passwörter werden nur verschlüsselt gespeichert
- Es existiert eine Home-Office-Richtlinie
- Administratorpasswörter und Kryptographieschlüssel werden gesichert aufbewahrt
- Sperrung der Anmeldung nach drei erfolglosen Versuchen
- Passwörter der Mitarbeiter sind keinem anderen bekannt
- Aktivitäten an Datenverarbeitungsanlagen werden automatisiert protokolliert
- Auswertung von Protokollen ist bei Bedarf möglich
- Mobile PCs werden außerhalb der Geschäftszeiten weggeschlossen
Identifizierung an IT-Systemen erfolgt durch einen Benutzer und einen VPN
- Authentifizierung erfolgt durch Benutzername, Passwort, SSH-Key und Biometrie
- Dokumentation von Zugangsberechtigungen und Prozess zur Vergabe
- Passwortgeschützter Bildschirmschoner bei Arbeitsunterbrechungen
- Verschlüsselung von Daten auf mobilen IT-Systemen

3. Zugriffskontrolle

- Datenträger werden vor unbefugtem Lesen, Kopieren, Verändern oder Entfernen durch Verschlüsselung und Biometrie geschützt
- Laptops verbleiben über Nacht im abgeschlossenen Büro oder werden von Mitarbeitern mitgenommen
- Es gilt das Need-to-know-Prinzip bzw. Erforderlichkeitsprinzip für Mitarbeiter
- Die differenzierte Zugriffsberechtigung ist aufgeteilt nach Datenfeldern, Anwendungsprogrammen und Servern, bzw. IT-System
- Die differenzierten Verarbeitungsmöglichkeiten sind Lesen, Ändern, Löschen
- Zugriffsrechte werden durch die Geschäftsleitung vergeben
- Zugriffsrechte werden dokumentiert
- Zugriffsrechte werden bei Organisationsänderungen überprüft
- Daten auf Wechseldatenträgern werden verschlüsselt

4. Weitergabekontrolle/Übermittlungskontrolle

- Die elektronische Übertragung ist sicher
- Die Webseite ist SSL/TLS-verschlüsselt
- Die elektronische Kommunikation ist verschlüsselt
- Eine Firewall ist im Einsatz
- Es existiert ein IPS
- Übermittlungen durch unsichere Netzwerke werden durch SSH geschützt
VPNs werden eingesetzt.
- Es erfolgt kein Versand von Datenträgern
- Im Unternehmen gibt es keine unbenutzten Datenträger
- Magnetische Datenträger werden mehrfach durch sicheres Verfahren überschrieben
- Optische Datenträger und defekte Festplatten werden physisch vernichtet
Verändern oder Entfernen der Daten geschützt durch Verschlüsselung und Postversand
- Zum Transport vorgesehene Daten mit sensiblem Inhalt werden verschlüsselt und über eine Standleitung übermittelt
- Prozesse sind im Verzeichnis von Verarbeitungstätigkeiten erfasst
- Jegliche Datenübermittlungen werden protokolliert
- Externe Dienstleister werden schriftlich auf den Datenschutz verpflichtet
- Externe Dienstleister werden bei ihren Aktivitäten beaufsichtigt
- Passwörter werden gewechselt, nachdem sie einem Dienstleister bekannt geworden sind
- Fernwartung erfolgt nur fallbezogen
- Fernwartungen werden nur durch Abteilungsleiter oder Geschäftsleitung genehmigt
- Fernwartungen sind durch eine vertragliche Grundlage geregelt

5. Eingabekontrolle/Plausibilitätskontrolle

- Es existiert eine Verarbeitungskontrolle für Daten in IT-Systemen
- Systeme werden bei jedem Start auf Schadsoftware geprüft
- Updates der Schadsoftware erfolgen automatisch
- Automatische Updates zur regelmäßigen und zeitnahen Installation von sicherheitsrelevanten Updates und Patches
- Daten und Programme werden in unterschiedlichen Verzeichnissen abgespeichert
- Komplettsicherung von Systemen vor größeren Wartungs-, Fernwartungs- und Reparaturarbeiten

6. Auftragskontrolle/Vertragskonformitätskontrolle

- Aktivitätenprotokoll zur Überprüfung und Feststellung der Dateneingabe, -veränderung und -überprüfung
- Schriftliche Weisungen (Weisungsbefugnis) und vertraglich festgelegte Verantwortlichkeiten zur Überprüfung der Weisungsgebundenheit des Auftragnehmers
- Auftraggeber kann Programmfehler selbst einsehen und darauf reagieren
- Fernwartung wird über VPN abgesichert

7. Verfügbarkeitskontrolle

- Diverse Backups (SAN-Snapshots, Festplattenspiegelung) werden in täglichem und wöchentlichem Rhythmus durchgeführt
- Backups werden im Rechenzentrum aufbewahrt
- Allgemeines Backup-Verfahren wird durch Nutzer- und Systemmeldungen regelmäßig kontrolliert
- Datenverarbeitende mobile Endgeräte werden regelmäßig gesichert
- Störende Umwelteinflüsse (z.B. Stromausfall, Stromschwankungen) werden bei der Installation berücksichtigt
- Serverräume sind durch Temperatur-, Luftfeuchtigkeitssensoren, Luftfilter und Brandmelder ausgestattet
- Wartung liegt im Verantwortungsbereich der Geschäftsleitung
- Regelmäßige und automatische E-Mail-Archivierung durch Aufbewahrungsrichtlinie

- Personenbezogene Daten sind vor unbefugtem Zugriff und unbefugter Veränderung, Löschung, Vernichtung etc. geschützt
- Anti-Viren-Programme

8. Datentrennungskontrolle/Mandantentrennungskontrolle

- Produktiv- und Testsysteme werden getrennt
- Produktiv- und Testdaten werden getrennt
- Jeder Auftraggeber hat eigene IT-Systeme
- Mandantentrennung erfolgt softwareseitig

9. Prüfung der Betriebsorganisation und Rechenschaftspflicht

- Maßnahmen der innerbetrieblichen Organisation zur Einhaltung der Vorgaben des Datenschutzrechts:
- Nachweise über Schulungen der Mitarbeiter zum Datenschutz
- Nachweise über Einhaltung der datenschutzrechtlichen Verpflichtungen der - verarbeitenden Mitarbeiter liegen vor
- Datenschutzbeauftragter ist schriftlich bestellt
- Fachkundenachweise des Datenschutzbeauftragten liegen vor
- Richtlinien und Konzepte zum Datenschutz liegen vor
- Datenschutzinformationen (Datenschutzhinweis) auf der Webseite verfügbar
- Verzeichnis von Verarbeitungstätigkeiten liegt vor
- Konzept zur Erfüllung von Betroffenenrechten sowie zugehörige Antwortvorlagen liegen vor
- Mitarbeiterinformationen zur Datenverarbeitung im Beschäftigungsverhältnis liegen vor
- Verpflichtung der Mitarbeiter auf das Datengeheimnis liegt vor
- Dokumentation der rechtlichen Vorgaben in Bezug auf die Speicherung und Aufbewahrung von Unterlagen liegen vor