CDE Datensicherheitskonzept

Stand: 11/2018

Datenschutzmaßnahmen

CDE – Communications Data Engineering GmbH
Softwarepark 37
A-4232 Hagenberg im Mühlkreis
Tel.: +43 7236 3351 4350
office@cde.at
www.cde.at

CDE - Communications Data Engineering GmbH
A-4232 Hagenberg | Softwarepark 37
+43 7236 3351 4350
http://www.cde.at | office@cde.at

Sehr geehrte Damen und Herren!

Für CDE ist nicht nur der aktuellste Stand der Technik und eine perfekt Hardware- oder Softwareprogrammierung ein Anliegen, sondern auch die Sicherheit Ihrer Daten!

Dieses Dokument zeigt eine Auflistung, welche Maßnahmen wir für Sie durchführen um Ihre Daten optimal zu schützen.

Freundliche Grüße

Ihr CDE-Team

CDE - Communications Data Engineering GmbH
A-4232 Hagenberg | Softwarepark 37
+43 7236 3351 4350
http://www.cde.at | office@cde.at

1. Zutrittskontrolle

Folgende im Unternehmen getroffene Maßnahmen gewährleisten, dass Unbefugte nicht in der Lage sind, sich physisch den Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder gespeichert werden, nähern zu können:

Der Zutritt zu den Büroräumlichkeiten ist nur durch berechtigte Personen möglich. Der Zutritt zum Rechenzentrum ist ebenfalls nur autorisiertem Personal möglich, wobei die Anzahl der Personen mit Zutrittsrechten auf ein Minimum eingeschränkt wird. Um dies zu gewährleisten, existieren neben einem Zutrittssystem zu den Büroräumen auch eine Gebäudeüberwachung. Des weiteren werden alle Zutritte von unternehmensfremden Personen durch den Gebäudebetreiber aufgezeichnet. Alle CDE Mitarbeiter sind weiters dazu angehalten, die Türen zu den Büroräumen geschlossen zu halten und Besucher während des Aufenthalts bei CDE immer zu begleiten.

2. Zugangskontrolle

Folgende bei der CDE getroffenen Maßnahmen gewährleisten, dass Unbefugte nicht in der Lage sind, vorhandene Datensysteme zu nutzen:

Der Zugang zum CDE Netzwerk bzw. dem System ist nur mit einem persönlichen, gültigen und passwortgeschützten Benutzerkonto möglich.
Passwörter unterliegen einer eigenen Policy. Domain-Passwörtern müssen mindestens 8 Zeichen enhalten, davon 1 Großbuchstabe, 1 Kleinbuchstabe, 1 Sonderzeichen und eine Zahl enthalten. Domain-Passwörter müssen alle 2 Jahre geändert werden. VPN-Passwörter werden generiert und müssen mindestens 16 Zeichen, davon 1 Großbuchstabe, 1 Kleinbuchstabe und 1 Zahl enthalten. Server-Passwörter werden automatisch generiert und enthalten 10 bis 20 Zeichen.

Die CDE Mitarbeiter sind dazu angehalten, bei jedem Verlassen ihres Arbeitsplatzes oder längerem Nichtbenutzen des PCs, sich von diesem abzumelden.

3. Zugriffskontrolle

Folgende bei der CDE getroffene Maßnahmen gewährleisten, dass Befugte ausschließlich im Maße ihrer Befugnisse auf Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen oder verändert werden können.

Nur Mitarbeiter von CDE haben Zugang zum System und somit Zugriff auf die Daten. Die Art und Umfang des Zugriffs ist für Mitarbeiter individuell geregelt und auf das nötigste Ausmaß eingeschränkt.

Die Verschwiegenheitspflicht ist bei allen Mitarbeitern in den Dienstverträgen und darüber hinaus durch eine ausdrückliche Erklärung und Verschwiegenheitsvereinbarung zum Datengeheimnis und zur Wahrung von Geschäfts- und Betriebsgeheimnissen verankert. Die CDE Mitarbeiter erhalten regelmäßige Schulungen im Bereich des Datenschutzes.

Es existieren Prozesse für den Eintritt, bei Veränderung oder beim Austritt von Mitarbeitern im Unternehmen.

Die CDE Server sind durch eine Zutrittskontrolle in das Rechenzentrum geschützt, welcher ausschließlich die von CDE definierten Zugriffsmöglichkeiten erlaubt.

4. Weitergabekontrolle

Folgende bei CDE getroffenen Maßnahmen gewährleisten, dass personenbezogene Daten bei Übertragung bzw. während des Transports nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Das CDE System ist ausschließlich über HTTPS erreichbar. Daten und Dokumente werden ausschließlich verschlüsselt an Kunden übermittelt, wobei das Passwort den Kunden per SMS oder Telefon mitgeteilt wird. Datenträger werden in der Regel nicht versendet. Falls doch, werden diese vor der Versendung oder einem Transport nach außen verschlüsselt.

5. Verfügbarkeitskontrolle

Folgende bei CDE getroffene Maßnahmen gewährleisten den Schutz personenbezogener Daten vor zufälliger Zerstörung oder Verlust.

Das Rechenzentrum ist mit einer redundanten, unterbrechungsfreien Stromversorgung gesichert und mit einer Brandmeldeanlage ausgestattet.

Die CDE Server sind von extern und intern durch eine Firewall geschützt, welche ausschließlich die von CDE definierten Zugriffsmöglichkeiten erlaubt. Des weiteren sind wichtige interne Systeme und extern erreichbare Systeme (z.B. CDE-Zeiterfassung oder Demosysteme für Kunden) vollständig durch eigene DMZ getrennt.

Die Server werden laufend gewartet und regelmäßig mit den neuesten Updates und Patches aktualisiert. Bei CDE ist dazu eine Überwachungssoftware eingerichtet, welche alle Systeme überwacht und bei Updates oder Fehlfunktionen sofort die Administratoren per Nachricht informiert. Eine laufend aktualisierte Anti-Viren-Software auf allen PC-Systemen verhindert Computer-Viren. Die Mitarbeiter werden durch die Administratoren regelmäßig über neueste Angriffsmethoden und Viren aufgeklärt. Somit wird präventiv dafür gesorgt, dass die Systeme von CDE nicht infiziert werden.

Mehrstufige gut dokumentierte Backup-Strategien - vom einfachen Server-Stillstand bis zum Ausfall des gesamten Rechenzentrums - ermöglichen höchste Verfügbarkeit und kürzeste Wiederaufnahme der CDE Systeme. Die virtuellen Maschinen der CDE Server werden periodisch gesichert. Die CDE Datenbanken werden zusätzlich jede Stunde gesichert, um den Datenverlust im Ausfall möglichst gering zu halten. Eine monatliche Datensicherung an einem anderen Standort ermöglicht außerdem die Wiederherstellung des Systems (mit einem entsprechenden zeitlichen Offset) selbst dann, wenn die gesamten Server im Rechenzentrum oder das Rechenzentrum selbst irreparabel beschädigt werden würde.

6. Trennungskontrolle

Folgende bei CDE getroffene Maßnahmen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden.

Durch die Mandantsfähigkeit von CDE können zu unterschiedlichen Zwecken erhobene Daten auch getrennt verarbeitet werden.

Desweiteren werden eigene – vom Produktivsystem unabhängige – Systeme für Testzwecke betrieben.