Dokumentation der technischen und organisatorischen Massnahmen für die Verarbeitung von Personendaten in der Classtime Software

Datum: 11. August 2022

Die vorliegende Liste dokumentiert die getroffenen technischen und organisatorischen Sicherheitsmassnahmen zur Einhaltung der Anforderungen der EU-Datenschutz-Grundverordnung und des schweizerischen Datenschutzrechts in Bezug auf die Verarbeitung von Personendaten in der Classtime Software.

1. Transparenz

Um zu gewährleisten, dass die Verarbeitung von Personendaten für die betroffenen Personen nachvollziehbar ist, wurden die folgenden Massnahmen getroffen:

- Dokumentation der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
- Dokumentation von Datenempfängern und Auftragsverarbeitern
- Dokumentation verbindlicher Löschfristen
- Veröffentlichung der Datenschutzdokumentation (online)
- Bereitstellung der Datenschutzdokumentation auf Antrag der betroffenen Person
- Veröffentlichung der Informationen über die Verarbeitung von Personendaten als Datenschutzerklärung (online)

2. Zweckbindung

Um zu gewährleisten, dass Personendaten nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden, wurden folgende Massnahmen getroffen:

- Darstellung der Verarbeitungszwecke in der Datenschutzdokumentation
- Verpflichtung der Mitarbeiter auf die Beachtung der Datenschutzanforderungen
- Trennung von Produktiv- und Testsystemen

3. Datenminimierung und Speicherbegrenzung

Um zu gewährleisten, dass Datenverarbeitungen dem Zweck angemessen, erheblich und auf das notwendige Mass beschränkt sind, wurden folgende Massnahmen getroffen:

- Datenschutz durch Technikgestaltung (data protection by design), z.B. Möglichkeit zur pseudonymisierten Nutzung der Software durch Lernende
- Vornahme datenschutzfreundlicher Voreinstellungen (data protection by default)
- Beschränkung der Datenerhebung auf das für den jeweiligen Zweck Erforderliche
- Festlegung verbindlicher Löschfristen
- Festlegung automatisierter Löschzyklen
- Regelmässiges manuelles Auslösen der Löschung nicht benötigter Daten.
- Pseudonymisierung der Daten insbesondere bei Weiterverarbeitung oder Übermittlung soweit mit dem Verarbeitungszweck vereinbar und sinnvoll
- Anonymisierung von Daten, wenn Identifikation nicht (mehr) notwendig

4. Richtigkeit

Um zu gewährleisten, dass die verarbeiteten Personendaten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind, wurden folgende Massnahmen getroffen:

- Nachweis der Herkunft von Daten
- Zertifikatsbasierte Authentifizierung der Datenquelle
- Unverzügliche Löschung oder Berichtigung unrichtiger Daten
- Möglichkeit der elektronischen Beantragung einer Berichtigung
- Eigenständige elektronische Berichtigung der Daten durch die betroffene Person

5. Vertraulichkeit

Um zu gewährleisten, dass die verarbeiteten Personendaten vor unbefugter oder unrechtmässiger Verarbeitung und vor unbeabsichtigtem Verlust geschützt sind, wurden folgende Massnahmen getroffen:

- Alarmanlage
- Wachpersonal
- Zugangskontrollsystem
- Unterteilung in Sicherheitszonen
- Sicherheitsschlösser
- Schlüsselregelung
- Schliesssystem mit Chipkarte
- Manuelles Schliesssystem
- Festlegung befugter Personen
- Ausweispflicht
- Personenkontrolle
- Absicherung des Gebäudes, einbruchhemmende Fenster und Türen
- Geräte- und Gehäuseversiegelung
- Auf Datenschutz verpflichtetes Reinigungs- und Wartungspersonal

- Zeitliche Zugangsbeschränkung
- Implementierung eines Rollen- und Berechtigungskonzepts
- Benutzerkonto für jeden Mitarbeiter
- Arbeiten mit individuellen Benutzerkennungen
- Authentifikation mit Passwort
- Authentifikation mit SmartCard
- Authentifikation über Verzeichnisdienste
- Single Sign-on
- Angemessene Passwortrichtlinien
- Kontensperrung nach mehrmaliger Falscheingabe des Passworts
- Automatische Abmeldevorgänge
- Regelungen beim Ausscheiden von Mitarbeitern
- Vergabe von Administratorrechten an minimale Anzahl Personen
- Physikalisch getrennte Speicherung und Verarbeitung
- Trennung von Produktiv- und Testsystemen
- Sicheres Löschen von Datenträgern
- Sicheres Löschen einzelner Dateien
- Datenträgervernichtung nach DIN 66399
- Datenträgerverschlüsselung
- Dateiverschlüsselung
- Verschlüsselung von Datenbanken
- Transportverschlüsselte Datenübertragung
- Durchgängige Transportverschlüsselung bei der Email-Übertragung
- Email-Verschlüsselung mit S/MIME
- Verhinderung nicht-autorisierter Cloud-Synchronisation durch Drittanbietersoftware
- Übermittlung von Daten in pseudonymisierter Form
- Übermittlung von Daten in anonymisierter Form
- Einsatz von Virenschutzlösungen
- Intrusion Detection Systeme
- Application Layer Firewall
- Packet Filter Firewall
- Automatisierte Updateprozesse für Betriebssysteme, Anwendungen und Dienste
- Protokollierung der Datenzugriffe

Die in diesem Abschnitt aufgeführten Massnahmen werden z.T. durch den Cloud-Anbieter umgesetzt, der den Applikationsserver und die Datenbank für Classtime hostet.

6. Integrität

Um zu gewährleisten, dass die verarbeiteten Personendaten vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung geschützt sind, die Daten also vollständig, unverändert und unversehrt sind, wurden folgende Massnahmen getroffen:

- Intrusion Detection Systeme
- Einsatz von Virenschutzlösungen
- Application Layer Firewall
- Packet Filter Firewall
- Überwachung von Fernwartungsaktivitäten
- Anwendung von Prüfsummenverfahren
- Verschlüsselung der Internetpräsenz

- Verschlüsselung von mobilen Datenträgern
- Inhaltsverschlüsselte Datenübertragung
- Automatisierte Updateprozesse für Betriebssysteme, Anwendungen und Dienste
- Differenzierte Berechtigungen für Datenobjekte
- Protokollierung der Datenzugriffe
- Plausibilitätskontrollen bei der Datenverarbeitung
- Signieren elektronischer Dokumente

Die in diesem Abschnitt aufgeführten Massnahmen werden z.T. durch den Cloud-Anbieter umgesetzt, der den Applikationsserver und die Datenbank für Classtime hostet.

7. Verfügbarkeit und Belastbarkeit

Um zu gewährleisten, dass die verarbeiteten Personendaten ihrem Zweck nach jederzeit nutzbar sind bzw. dass die Verfügbarkeit und der Zugang zu den Daten bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden kann, wurden folgende Massnahmen getroffen:

- Automatisiertes Anfertigen von Datensicherungen (Backup)
- Datenträgerspiegelung (RAID)
- Datenreplikation
- Festgelegte Zuständigkeiten für die Datensicherung
- Aufbewahrung der Datensicherung in einem anderen Brandabschnitt
- Regelmässiger Test der Datenwiederherstellung
- Redundante IT-Systeme
- Automatisches Benachrichtigungssystem bei Ausfall
- Notfallplan zur Wiederinbetriebnahme von Servern und Diensten
- Virtualisierte Infrastruktur
- Vermeidung lokaler Datenspeicherung
- IT-Komponenten verfügen über erforderliche Leistungsfähigkeit
- Automatische Skalierung virtueller Systeme
- Lastausgleich (load balancing) der Netzwerkkomponenten, Server und Dienste
- Automatisches Benachrichtigungssystem bei Erreichung der max. Auslastung
- Unterbrechungsfreie Stromversorgung
- Überspannungsschutz
- Eignung der Räumlichkeiten / des Baus
- Sicherung von Datenträgern gegen Elementarschäden
- Klimaüberwachung (Raumtemperatur, Feuchtigkeit) in Serverräumen
- Klimaanlage in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöscher / automatisches Löschsystem
- Schutz vor Wassereinbruch und Hochwasser

Die in diesem Abschnitt aufgeführten Massnahmen werden z.T. durch den Cloud-Anbieter umgesetzt, der den Applikationsserver und die Datenbank für Classtime hostet.

8. Rechenschaftspflicht und Wirksamkeitsnachweis

Um die Einhaltung der Verarbeitungsgrundsätze nachzuweisen und die Wirksamkeit der technischen und organisatorischen Sicherheitsmassnahmen zu überwachen, wurden folgende Massnahmen getroffen:

- Bestellung einer für den Datenschutz verantwortlichen internen Stelle
- Führen eines Verzeichnisses von Verarbeitungstätigkeiten
- Dokumentation über vorhandene IT-Infrastruktur, eingesetzte Programme und Anwendungen
- Dokumentation der getroffenen Sicherheitsmassnahmen
- Zentrale Dokumentation der Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für die Mitarbeiter
- Mitarbeiterschulungen
- Protokollierung der Anmeldevorgänge
- Protokollierung der Datenzugriffe
- Protokollierung gescheiterter Zugriffsversuche
- Protokollierung aller Administratorenaktivitäten