Technische und organisatorische Maßnahmen

Im Folgenden werden die technischen und organisatorischen Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit festgelegt, die der Auftragsverarbeiter zur Einhaltung der datenschutzrechtlichen Vorgaben einzurichten und laufend aufrecht zu erhalten hat. Die technischen und organisatorischen Maßnahmen betreffen die Produkte evasys, evaexam und qurricula.

Sofern ein Softwareprodukt durch die evasys GmbH gehostet wird, sind Maßnahmen eingerichtet, die ebenfalls aus diesem Schriftstück hervorgehen.

Relevante Informationen:

- Support: Der Auftragnehmer führt nach Auftrag durch den Verantwortlichen (Supportanfrage) Live-Support mittels TeamViewer aus. TeamViewer wird für die Produkte evasys und evaexam eingesetzt.
- Für qurricula gilt: Der Support wird mithilfe des Projektmanagementtools Jira abgewickelt.
- Die evasys GmbH betreibt das Cloudkonzept „IaaS“, „Infrastruktur as a Service“

1. Sicherstellung der Vertraulichkeit

1.1. Zugangskontrolle

1.1.1. Verantwortlicher

Die Tätigkeiten, die durch den Auftragsverarbeiter beim Support durchgeführt werden, sind durch den Verantwortlichen kontrollierbar. Die Tätigkeit des Auftragsverarbeiters kann an einem Kontrollbildschirm in Echtzeit verfolgt werden. Grundsätzlich werden beim Support notwendige Passwörter durch den Verantwortlichen eingegeben, der die Arbeiten am Kontrollbildschirm verfolgt.

Der Verantwortliche stellt durch entsprechende Infrastruktur (Hardware/Software) und einer dementsprechend sicheren Konfiguration und Rechtevergabe sicher, dass durch den Zugriff für Support nur auf die Rechner, Netzwerkabschnitte und Ressourcen zugegriffen werden kann, die für Support zwingend erforderlich sind.

1.1.2. Auftragsverarbeiter

Die für die Supporttätigkeiten verwendeten Rechner sind im Eigentum des Auftragsverarbeiters und sind nur für den rein dienstlichen Gebrauch zugelassen. Es ist ausschließlich Software für den dienstlichen Gebrauch installiert.

Das Betriebssystem auf den Rechnern, die für Support und Hosting-Administration genutzt werden, verfügt über eine Benutzerverwaltung, so dass mittels eines Rollen- und Rechtekonzepts die Zugriffsmöglichkeiten eingeschränkt sind und ohne gültige Authentifizierung verhindert werden.

evasys GmbH, Konrad-Zuse-Allee 13, 21337 Lüneburg

Die Zugriffsmöglichkeiten können nach Daten, Programmen und Art des Zugriffs differenziert werden.

Die Rechteverwaltung der Datenträger ist abgestuft auf der Ebene der Laufwerke, Verzeichnisse, Unterverzeichnisse, Dateien und Freigaben. Dabei sind die Rechte restriktiv vergeben.

Das Betriebssystem ist auf dem aktuellen Stand der Technik. Verfügbare Sicherheitsaktualisierungen für das Betriebssystem und der installierten, sicherheitsrelevanten Software werden regelmäßig durchgeführt. Täglich erfolgt eine Prüfung auf eine Verfügbarkeit von Sicherheitsaktualisierungen sowie deren unverzügliche Installation. Die Rechner verfügen über eine aktuelle Sicherheitssoftware (Antiviren-Software). Sobald die Signaturupdates für die Antiviren-Software verfügbar sind, wird diese nach Kenntnisnahme durch den Client installiert. Die Prüfaktivität wird im internen IT-Support des Auftragsverarbeiters dokumentiert.

Die Datenträger werden regelmäßig (mindestens einmal wöchentlich vollständiger Scan, jedoch dauerhaft in Echtzeit per Echtzeitscanner) mit der Sicherheitssoftware auf schädliche Software überprüft. Sollte eine Infizierung festgestellt werden, so wird dieses Gerät erst dann wieder in Betrieb genommen, wenn zweifelsfrei festgestellt wurde, dass der oder die Schädlinge vollständig entfernt wurden. Ggfs. wird eine Neuinstallation des Systems vorgenommen.

Sollte das Gerät vor der Entdeckung einer Schadsoftware bereits für Support oder Hosting-Administration beim Verantwortlichen eingesetzt worden sein, so wird diesem der Vorfall unverzüglich angezeigt.

Das System wird bei einer Inaktivität vom mehr als 5 Minuten automatisch gesperrt und kann nur durch Eingabe des gültigen Passwortes wieder entsperrt werden.

Alle Tätigkeiten für den Support oder Hosting-Administration erfolgen ausschließlich von Geräten, die der Auftraggeber bereitstellt und dauerhaft verwaltet.

Sollten personenbezogene Daten, die während des Supportprozesses anfallen, nach Beendigung des Supports noch zur Supportfallbearbeitung beim Auftragsverarbeiter gespeichert werden müssen, so werden diese auf einem getrennten dedizierten Laufwerk gespeichert. Dieses Laufwerk hat restriktive Zugriffsbeschränkungen, sämtliche Schreib- und Löschvorgänge werden protokolliert. Die Daten werden unmittelbar nach Wegfall des Zwecks datenschutzkonform protokolliert gelöscht. Zu Nachweiszwecken kann die Löschung bis maximal 8 Wochen nach Ende des Supportfalls verlängert werden.

Regelmäßig (monatlich) erfolgt eine Überprüfung durch die Abteilungsleitung, ob alle Daten entsprechend den Regeln (spätestens 8 Wochen nach Ende des Supportfalls) gelöscht wurden. Die Verantwortlichkeit für die Löschvorgänge liegt beim Abteilungsleiter der Abteilung Support oder dessen Vertreter. Der Löschvorgang selbst wird durch einen eingewiesenen Mitarbeiter vorgenommen oder automatisiert durchgeführt.

Werden Daten zu Supportzwecken übertragen, so ist der Übertragungsweg Ende-zu-Ende nach Stand der Technik verschlüsselt.

Nach Beendigung des Supportvertragsverhältnisses werden sämtliche Daten des Auftraggebers gelöscht. Die Daten werden unmittelbar nach Wegfall des Zwecks datenschutzkonform protokolliert gelöscht.

Sollte es nötig sein, die Daten auf einem System einzuspielen, um Fehlersituationen nachzustellen und zu analysieren oder um eine (Rück-)Migration vorzunehmen, so ist dieser Rechner für die Dauer dieser Aufgabe exklusiv zur Verfügung gestellt. Nach Erledigung der Aufgabe können die Daten noch für maximal 2 Wochen vorgehalten werden. Danach werden die Daten datenschutzgerecht gelöscht. Die Protokollierung der Löschung erfolgt in dem für diese Dienstleistung geführten Protokoll.

Hosting:

Zur Erbringung der Dienstleistung sind per VNet-Konfigurationen innerhalb von Azure auf Netzwerkebene lediglich die für den Betrieb benötigten Netzwerkports (80, 443, in manchen Fällen auch 3306, wenn benötigt) freigegeben. Zudem kommen weitere, infrastrukturbedingte Netzwerkports hinzu (z.B. für das Monitoring oder unserer Automationslösung).

Die Verbindungen sind über eine Firewall gesichert. Der administrative Zugriff wird basierend auf IP-Filterung eingeschränkt, konkret:

IP-Sperre auf Netzwerkebene (TCP), nur Zugriff aus dem evasys-Netzwerk heraus möglich.

Zugangskontrollen über die verwendete Remotedesktopsoftware (jeder Art Zugriff wird namentlich per Benutzerkürzel protokolliert).

Server-Passwörter, sowie das Passwort zur Administrationsoberfläche sind nur dem Auftragsverarbeiter bekannt und entsprechen der Passwortrichtlinie (siehe Passwortrichtlinie).

Das Server-Betriebssystem ist auf dem aktuellen Stand der Technik. Verfügbare Sicherheitsaktualisierungen für das Betriebssystem und der installierten, sicherheitsrelevanten Software werden regelmäßig durchgeführt.

Das Hosting wird über Microsoft Azure auf einem Windows-Betriebssystem bereitgestellt. Microsoft veröffentlicht Update-Pakete am zweiten Dienstag eines jeden Monats (Microsofts "Patch Tuesday").

Das Update wird am Samstag nach dem zweiten Dienstag eines jeden Monats auf die evasys-Produktionsserver aufgespielt.

Die Serversysteme verfügen über eine aktuelle Sicherheitssoftware (Antiviren-Software).

Sobald die Signaturupdates für die Antiviren-Software verfügbar sind, wird diese nach Kenntnisnahme durch den Server installiert.

Die Serverdatenträger werden regelmäßig (mindestens einmal wöchentlich vollständiger Scan, jedoch dauerhaft in Echtzeit per Echtzeitscanner) mit der Sicherheitssoftware auf schädliche Software überprüft.

Sollte eine Infizierung festgestellt werden, so wird dieses Gerät erst dann wieder in Betrieb genommen, wenn zweifelsfrei festgestellt wurde, dass der oder die Schädlinge vollständig entfernt wurden. Ggfs. wird eine Neuinstallation des Systems vorgenommen.

1.2. Zutrittskontrolle

1.2.1. Verantwortlicher

Die Verbindung für Support ist so gestaltet, dass diese jederzeit durch den Verantwortlichen unterbrochen werden kann.

Nach Abschluss des Supports stellt der Verantwortliche sicher, dass die Verbindung wieder abgebaut ist.

1.2.2. Auftragsverarbeiter

Die Arbeitsplatzrechner, die für Support oder Hosting-Administration genutzt werden, stehen in einem nicht öffentlich zugänglichen Büroraum. Bei längerer Abwesenheit, zum Beispiel für Termine oder nach Arbeitsende, ist der Zugang verschlossen. Die Schlüsselvergabe unterliegt einer klaren Regelung, so dass der Kreis der Zutrittsberechtigten zu jeder Zeit klar und eindeutig feststeht.

Sollte Support oder Hosting-Administration außerhalb der Büroräume stattfinden, gilt die firmenweite Richtlinie. Zusätzlich bedarf es im Fall des Supportes einer expliziten Zustimmung des Kunden.

Erläuterung:

- Dokumentierte Schlüsselvergabe an Beschäftigte.
- Durchgehende Eingangskontrolle während der Geschäftszeiten.
- Alarmanlage mit Alarmierung eines Wachdienstes außerhalb der Geschäftszeiten.
- Begleitung und Kennzeichnung von Gästen.

Hosting-Server:

Die Hosting-Server stehen in separaten Rechenzentren mit entsprechenden Sicherheitsvorkehrungen und Regelungen. Die evasys GmbH beauftragt für Hosting Dienstleistungen ausschließlich Anbieter, die eine ISO-Zertifizierung 27001 vorweisen. Die entsprechenden Nachweise über die Zertifikate werden dem Verantwortlichen auf Nachfrage zur Prüfung bereitgestellt.

Erläuterung:

- Elektronisches Zutrittskontrollsystem mit Protokollierung.
- Hochsicherheitszaun um das gesamte Rechenzentrum.
- Dokumentierte Schlüsselvergabe an Mitarbeiter.
- Begleitung und Kennzeichnung von Gästen.
- 24/7 personelle Besetzung des Rechenzentrums.
- Videoüberwachung an den Ein- und Ausgängen, Sicherheitsschleusen und Serverräumen.

1.3. Pseudonymisierung

1.3.1. Verantwortlicher

Sofern es für die Bearbeitung eines Supportfalls erforderlich ist, personenbezogene Daten beim Auftragsverarbeiter zu speichern, so ist vor jeder Übertragung an den Auftragsverarbeiter durch den Verantwortlichen zu prüfen, ob für die Bearbeitung unter Umständen auch pseudonymisierte oder anonymisierte Echtdaten oder Testdaten genutzt werden können. Dies kann in Rücksprache mit dem Auftragsverarbeiter erfolgen.

Bei der Pseudonymisierung muss darauf geachtet werden, dass die Daten derart transformiert werden, dass auch durch die Kombination der einzelnen Merkmale und das Hinzuziehen von weiteren Quellen für den Auftragsverarbeiter kein Personenbezug herstellbar ist. Weitere Quellen sind in diesem Zusammenhang öffentlich zugängliche Quellen, insbesondere Daten, die zum Beispiel auf dem Webauftritt des Verantwortlichen oder in anderen öffentlich zugänglichen Datenbeständen publiziert sind

1.3.2. Auftragsverarbeiter

Sofern für die Aufgabenerfüllung - sei es als Ausnahme oder als Regelfall - die Übertragung von personenbezogenen Daten des Verantwortlichen an den Auftragsverarbeiter zwingend erforderlich ist, müssen die Punkte 2.2.1 (Maßnahmen zur Übertragungskontrolle) und 2.3.2 (Maßnahmen zur Eingabekontrolle) erfüllt sein.

1.4. Verschlüsselung

1.4.1. Auftragsverarbeiter

Mobile Rechner oder Geräte

Die Datenträger in den mobilen Rechnern, sofern diese für Support oder Hosting-Administration eingesetzt werden, sind mit anerkannt starken kryptografischen Algorithmen, Verfahren und Software vollständig verschlüsselt und mit einem Passwort gesichert (siehe hierzu die Passwortrichtlinie und für die Mindestanforderungen, Punkt 2.2).

Hosting-Server

Bei der Speicherung von Daten auf den Serversystemen kommt Encryption at Rest zum Tragen.

1.5. Datenträgerkontrolle

1.5.1. Auftragsverarbeiter

Defekte oder ausgemusterte Festplatten werden mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Der Löschvorgang wird protokolliert. Das Verfahren orientiert sich am aktuellen Stand der Technik.

Im Anschluss werden die Festplatten durch einen zertifizierten Dienstleister vernichtet.

Hosting-Server:

Festplatten werden nach Kündigung mit einem definierten Verfahren mehrfach überschrieben (gelöscht). Das Verfahren orientiert sich am aktuellen Stand der Technik. Nach Überprüfung werden die Festplatten wiedereingesetzt. Der Hostingdienstleister befolgt die NIST 800-88-Richtlinien (Löschen, Löschen und Zerstören) und bewahrt Aufzeichnungen über die Zerstörung auf.

2. Sicherstellung der Integrität

2.1. Übertragungskontrolle

Der Verantwortliche und der Auftragsverarbeiter stellen durch starke Verschlüsselung sicher (siehe 2.2), dass keine personenbezogenen Daten im Rahmen des Supports oder der Hosting-Administration an einen fremden Dritten übermittelt werden.

2.2. Verschlüsselung

Die Verbindung, die zum Zweck des Supports zu den Systemen des Verantwortlichen aufgebaut wird (Online-Verbindung), hat eine kryptografisch starke Verschlüsselung.

Derzeit bedeutet dies mindestens:

- AES mit mindestens 256 Bit Schlüssellänge als Blockchiffre,
- SHA2 als Hash-Algorithmus,
- RSA mit einem mindestens 4096 Bit langen Schlüssel, und
- TLS in aktuell als sicher anerkannten Version als Protokoll oder ein anerkannt äquivalent sicheres.

Die Verschlüsselung von personenbezogenen Daten auf mobilen Datenträgern, in Containern (z.B. verschlüsselte Dateien, Archive, E-Mail o.ä.) oder die Verschlüsselung von Datenträgern in mobilen Rechnern genügt mindestens folgenden derzeitigen Anforderungen:

Derzeit bedeutet dies mindestens:

- AES mit mindestens 256 Bit Schlüssellänge als Blockchiffre,
- SHA2 als Hash-Algorithmus,
- RSA mit einem mindestens 4096 Bit langen Schlüssel, und
- TLS in aktuell als sicher anerkannten Version als Protokoll oder ein anerkannt äquivalent sicheres.

2.2.1. Verantwortlicher

Der Verantwortliche stellt einen geeigneten Zugang zur Verfügung, der genügend stark verschlüsselt ist und sowohl die Authentizität der Kommunikationspartner als auch die Integrität der Verbindungsdaten sicherstellt. (für die Mindestanforderungen siehe 2.2)

Dies gilt sowohl für Online-Verbindungen als auch für den Transport personenbezogener Daten mit mobilen Datenträgern oder Containern.

Für evasys und evaexam gilt:

Der Support wird wie folgt realisiert:

Auf dem Arbeitsplatzrechner beim Verantwortlichen läuft eine lokale Firewall, die die statischen IP-Adressen des Auftragsverarbeiters für Port 443 und für das Protokoll UDP bei Bedarf freischaltet.

Wenn Transport von personenbezogenen Daten an den Auftragsverarbeiter außerhalb der Online-Verbindung erforderlich ist:

Die personenbezogenen Daten werden vom Verantwortlichen stark verschlüsselt, bevor diese an den Auftragsverarbeiter versendet werden (für die Mindestanforderungen siehe 2.2).

Bei dem Versand mit einem Datenträger oder Container genügt das Passwort der Passwortrichtlinie für verschlüsselte Datenträger (siehe Passwortrichtlinie) und wird auf einem anderen Weg zum Auftragsverarbeiter versandt als die verschlüsselten Daten selbst.

Erläuterung:

Wird es im Rahmen eines Supportfalls nötig, Dateien mit personenbezogenen Daten zum Auftragsverarbeiter zu übertragen, so erfolgt diese Übertragung per Online Support System (OSS) oder mit FTP over TLS verschlüsselt (Schlüssellänge 4096 bit, SHA256RSA) zu einem speziell für diesen Zweck vorgesehene Server des Auftragsverarbeiters. Dateien, die auf diesen Server geladen werden, werden nach 48 Stunden vollautomatisch datenschutzkonform gelöscht.

Für qurricula gilt:

Supportanfragen reicht der Verantwortliche in einem Ticketsystem ein: (Erläuterung)

- Kunden erhalten bei Vertragsabschluss Zugang zum Ticketsystem,
- Zugang ist entsprechend der oben genannten Rahmenbedingungen gesichert,
- Kunden platzieren Supportanfragen,
- Wird es im Rahmen eines Supportfalls nötig, Dateien mit personenbezogenen Daten zum Auftragsverarbeiter zu übertragen, so erfolgt diese Übertragung per Online Support System (OSS) oder mit FTP over TLS verschlüsselt (Schlüssellänge 4096 bit, SHA256RSA) zu einem speziell für diesen Zweck vorgesehene Server des Auftragsverarbeiters. Dateien, die auf diesen Server geladen werden, werden nach 48 Stunden vollautomatisch datenschutzkonform gelöscht.
- Die Verantwortlichen haben jederzeit die Steuerung von Übergabe, Zurverfügungstellung und Löschung im Ticketsystem inne.

Der Zugriff auf die zu wartenden Systeme ist durch den Verantwortlichen auf die statische IP-Adresse durch technische Maßnahmen, z.B. an der Firewall, beschränkt.

2.2.2. Auftragsverarbeiter

Sollte die Tätigkeit zum Support nicht unmittelbar aus dem Firmennetz des Auftragsverarbeiters heraus erfolgen, so ist zuerst eine VPN-Verbindung oder eine äquivalent sichere Verbindung in das Firmennetz des Auftragsverarbeiters aufzubauen.

Sofern die technischen Voraussetzungen beim Verantwortlichen vorhanden sind, erfolgt die Verbindung für Support ausschließlich stark verschlüsselt von Punkt zu Punkt (für die Mindestanforderungen siehe 2.2), so dass zwischen dem Rechner des Auftragsverarbeiters, auf dem der Support erfolgt, und dem Endpunkt beim Verantwortlichen keine Komponente liegt, die den Datenstrom im Klartext einsehen oder manipulieren kann.

Für evasys und evaexam gilt:

Die Personen, die Live-Support durchführen, sind dem Verantwortlichen auf dessen Anforderung namentlich zu nennen.

Sollte Support oder Hosting-Administration außerhalb der Büroräume stattfinden, gilt die firmenweite Richtlinie. Zusätzlich bedarf es im Fall des Supportes einer expliziten Zustimmung des Kunden.

Für qurricula gilt:

Der Support erfolgt über statische IP-Adressen.

Die Verschlüsselung von personenbezogenen Daten auf mobilen Datenträgern, in Containern (z.B. verschlüsselte Dateien, Archive, E-Mail o.ä.) oder die Verschlüsselung von Datenträgern in mobilen Rechnern genügt mindestens folgenden derzeitigen Anforderungen:

- AES mit mindestens 256 Bit Schlüssellänge als Blockchiffre,
- SHA2 als Hash-Algorithmus,
- RSA mit einem mindestens 4096 Bit langen Schlüssel.
- einem Passwort entsprechend der Richtlinie für verschlüsselte Datenträger oder einem RSA-Schlüsselpaar mit mindestens 4096 Bit. Der private Schlüssel ist dabei mit einem Passwort entsprechend der Passwortrichtlinie für verschlüsselte Datenträger (siehe Passwortrichtlinie) gesichert.

Die Personen, die Support durchführen, sind dem Verantwortlichen auf dessen Anforderung namentlich zu nennen.

Sollte Support oder Hosting-Administration außerhalb der Büroräume stattfinden, gilt die firmenweite Richtlinie. Zusätzlich bedarf es im Fall des Supportes einer expliziten Zustimmung des Kunden.

Live-Support für evasys und evaexam erfolgt über eine Direktverbindung wie folgt:

Wird die Software TeamViewer beim Verantwortlichen eingesetzt, können Zugriffe "Peer to Peer" ohne Nutzung der IP-Adressen des Anbieters der Fernwartungssoftware "TeamViewer" erfolgen. Dazu übermittelt der Verantwortliche die statische IP-Adresse des Computers, über die eine Verbindung aufgebaut werden soll, an den Auftragsverarbeiter (Supporter). Verbindungen werden nur im "LAN-Modus" des TeamViewers aufgebaut.

Sollte es im Rahmen eines Supportfalls notwendig sein, Dateien zum Download o.ä. bereitzustellen, werden diese Ende zu Ende verschlüsselt über die laufende TeamViewer-Verbindung zur Verfügung gestellt.

Der Zugriff auf die zu wartenden Systeme ist durch den Verantwortlichen auf die oben genannten IP-Adressen durch technische Maßnahmen, z.B. an der Firewall, beschränkt.

Hosting:

Die gesamte Kommunikation ist über https abgesichert (TLS 1.2). Wartungen der virtuellen Maschinen erfolgen ebenso per TLS abgesicherter RDP-Verbindung. Grundsätzlich ist sämtliche Kommunikation durch aktuelle Transportverschlüsselungsverfahren abgesichert.

2.3. Eingabekontrolle

2.3.1. Verantwortlicher

Support:

Der Verantwortliche hat nur die Programme geöffnet, die zur Behebung des Problems zwingend erforderlich sind. Er verfolgt die Tätigkeiten des Auftragsverarbeiters am Kontrollbildschirm und wird ggf. die Verbindung unterbrechen.

Der Zugriff des Auftragsverarbeiters auf das System des Verantwortlichen erfolgt nur nach persönlicher anlassbezogener Einwilligung des Verantwortlichen.

Grundsätzlich wird der Zugriff auf personenbezogene Daten durch den Verantwortlichen verhindert, sofern dieser nicht zur Aufgabenerfüllung erforderlich ist.

2.3.2. Auftragsverarbeiter

Rechner, die einen Netzanschluss haben, der direkten Zugang zu einem öffentlichen Netz hat (Internet, Firmennetz, o.ä.), d.h. ohne vorgeschaltete Firewall betrieben werden, verfügen selbst über eine eigene Firewall. Dies gilt zwingend für mobile Rechner.

Die Firewall, vorgeschaltet oder auf dem Rechner selbst, ist so konfiguriert, dass nur das freigeschaltet ist, was explizit erlaubt ist, und dass Verbindungen nur erlaubt sind, die vom Rechner selbst initiiert werden.

Auf dem Rechner des Auftragsverarbeiters für den Support oder Hosting-Administration werden grundsätzlich keine personenbezogenen Daten des Verantwortlichen gespeichert. Sollte dies zur Erfüllung der Tätigkeit zwingend erforderlich sein, werden folgende Bedingungen erfüllt:

- Nach Beendigung des Supports oder der Hosting-Administration werden alle personenbezogenen Daten, die im Rahmen der Tätigkeit verarbeitet und gespeichert wurden, unverzüglich datenschutzgerecht gelöscht oder dem Verantwortlichen datenschutzgerecht übergeben.
- Sollten Ausdrucke angefertigt worden sein, so werden diese unverzüglich nach Beendigung der Tätigkeit datenschutzgerecht vernichtet. Ferner wird durch den Auftragsverarbeiter zumindest durch dienstliche Anweisungen ausgeschlossen, dass Kopien der Ausdrucke bei weiteren Systemen (Druckserver, Multifunktionsgerät o.ä.) angefertigt und gespeichert wurden. Sollte dies trotzdem der Fall sein, so werden auch diese Kopien unverzüglich datenschutzgerecht gelöscht oder dem Verantwortlichen datenschutzgerecht übergeben.

Falls die Speicherung personenbezogener Daten beim Auftragsverarbeiter über Online-Verbindung hinaus erforderlich ist.

Im Rahmen des Supports kann es zwingend erforderlich sein, dass personenbezogene Daten über den Zeitraum der Online-Verbindung hinaus beim Auftragsverarbeiter gespeichert werden müssen.

Diese Daten werden in einem stark kryptografisch gesicherten Container (für die Mindestanforderungen siehe 2.2) oder gleichwertig gespeichert. Die Daten werden unverzüglich datenschutzgerecht gelöscht oder dem Verantwortlichen datenschutzgerecht übergeben, sobald diese für die Bearbeitung nicht mehr erforderlich sind. Die Dauer der Speicherung und Löschung ist dem Verantwortlichen anzuzeigen.

Das Betriebssystem, das auf den Rechnern für Support installiert ist, erzwingt eine Benutzerauthentifizierung mit Benutzername und Passwort (siehe Passwortrichtlinie).

Für die Tätigkeit des Supports werden durch den Auftragsverarbeiter der Zeitpunkt, der Auftrag und die beteiligten Personen schlüssig und nachvollziehbar dokumentiert.

Hosting

Die Daten werden von dem Verantwortlichen selbst eingegeben bzw. erfasst.

3. Sicherstellung der Verfügbarkeit, Belastbarkeit und Resilienz

3.1. Zugangsdaten

Auftragsverarbeiter

Für den Support an den Systemen des Verantwortlichen werden Zertifikate, SSH-Schlüssel oder ähnliche Zugangsdaten für Systeme des Verantwortlichen durch den Auftragsverarbeiter verwendet. Diese sind gesondert gesichert aufbewahrt. Dabei wird ein stark verschlüsselter Container

(für die Mindestanforderungen siehe 2.2 und die Passwortrichtlinie) oder eine gleichwertige Sicherung verwendet.

Der Auftragsverarbeiter stellt durch interne Regelungen sicher, dass der Zugriff auf die Zugangsdaten auch durch einen benannten Stellvertreter möglich ist, sollte ein Vertretungsfall eintreten.

Es ist zu jeder Zeit technisch und/oder organisatorisch nachvollziehbar, auf welchen Medien die Zugangsdaten für Hosting-Systeme gespeichert sind, wie diese gesichert sind und von wem diese genutzt werden.

3.2. Verfügbarkeit, Belastbarkeit, Resilienz

3.2.1. Hosting-Server

Der Auftragsverarbeiter gewährleistet durch Regelungen eine hohe Verfügbarkeit des Hosting-Servers und der installierten Software, sowie eine rasche Wiederherstellbarkeit im Fehlerfall.

3.2.2. Backup- und Recoverykonzept:

Wie im Hosting-Vertrag angegeben werden die Benutzerdaten 30 Tage lang täglich mit dem Azure Backup abgesichert. Ein Restore ist jederzeit möglich, auch z.B. in ein temporäres weiteres System. Integritätstests werden von Azure selbst durchgeführt.

Wiederhergestellte Daten können innerhalb von 8 Stunden der Geschäftszeiten der evasys GmbH zur Verfügung gestellt werden.

Erläuterung:

- Backup und Recovery-Konzept mit täglicher Sicherung aller relevanten Daten (siehe oben).
- Monitoring des Hosting-Servers.
- Sachkundiger Einsatz von Schutzprogrammen (Virenscanner, Firewall).
- Einsatz von Festplattenspiegelung.
- Einsatz unterbrechungsfreier Stromversorgung, Netzersatzanlage.
- Dauerhaft aktiver DDoS-Schutz.
- Definierte Eskalationskette im Fehlerfall zur schnellstmöglichen Wiederherstellung eines Systems.

4. Regelmäßige Überprüfung, Bewertung und Evaluierung der TOM

4.1. Verantwortlicher

Der Verantwortliche prüft regelmäßig, ob die von ihm zu treffenden technischen und organisatorischen Maßnahmen umgesetzt und eingehalten werden.

4.2. Auftragsverarbeiter

Der Auftragsverarbeiter prüft regelmäßig selbständig, ob die von ihm zu treffenden technischen und organisatorischen Maßnahmen umgesetzt und eingehalten werden.

Der Auftragsverarbeiter gewährleistet, dass er die zur Verarbeitung der personenbezogenen Daten des Verantwortlichen befugten Personen zur Vertraulichkeit und Verschwiegenheit verpflichtet hat und es ihnen untersagt ist, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Unabhängig von einer gesetzlichen Verpflichtung informiert er sie regelmäßig über das Datengeheimnis und Dienstanweisungen zum Datenschutz.

Die Beschäftigten des Auftragsverarbeiters werden regelmäßig verpflichtet, die entsprechenden Anforderungen an den Datenschutz und die Informationssicherheit im Homeoffice entsprechend dem Stand der Technik einzuhalten.

Der Auftragsverarbeiter trifft Regelungen zur Löschung oder Vernichtung personenbezogener Daten, die beim Support gespeichert oder gedruckt wurden.

Erläuterung:

Alle sensiblen Daten, die während des Supportprozesses anfallen, werden auf einem getrennten dedizierten Laufwerk gespeichert. Dieses Laufwerk hat restriktive Zugriffsbeschränkungen, sämtliche Schreib- und Löschvorgänge werden protokolliert.

Regelmäßig (monatlich) erfolgt eine Überprüfung, ob alle Daten entsprechend den Regeln (spätestens 8 Wochen nach Ende des Supportfalls) gelöscht wurden.

Anlage 1:

Tabellarische Darstellung der technischen und organisatorischen Maßnahmen der evasys GmbH

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

Zutrittskontrolle:

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Technisch	Alarmanlage	x
Technisch	Klingelanlage mit Kamera	x
Technisch	Lichtschranken / Bewegungsmelder	x
Technisch	Manuelles Schließsystem	x
Organisatorisch	Personenkontrolle beim Pförtner / Empfang	x
Organisatorisch	Protokollierung der Besucher / Besucherbuch	x
Organisatorisch	Schlüsselregelung / Schlüsselbuch	x
Technisch	Sicherheitsschlösser	x
Organisatorisch	Tragepflicht von Mitarbeiter- / Gästeausweisen	x (Gäste)
Technisch	Videoüberwachung der Zugänge	x

Zutrittskontrolle:

Keine unbefugte Systembenutzung

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Organisatorisch	Sorgfältige Auswahl des IT-Dienstleisters	x
Technisch	Authentifikation mit Benutzer-Passwort	x
Organisatorisch	Benutzerberechtigungen verwalten	x
Organisatorisch	Definierte Passwortregeln	x
Technisch	Einsatz automatischer Bildschirmschoner, Spamfiltern	x
Technisch	Einsatz von Antiviren-Software	x
Technisch	Einsatz von Firewalls	x
Technisch	Einsatz von Mobile Device Management	x
Technisch	Einsatz von VPN-Technologie	x
Organisatorisch	Erstellen von Benutzerprofilen	x
Organisatorisch	jährliche Überprüfung der Berechtigungen	x
Organisatorisch	Sorgfältige Auswahl des Fernwarters	x
Organisatorisch	Sorgfältige Auswahl von Reinigungspersonal (Vertraulichkeitsverpflichtung)	x
Organisatorisch	Sorgfältige Auswahl von Sicherheitspersonal (Vertraulichkeitsverpflichtung)	x
Technisch	Zwei-Faktor-Authentifizierung	x

Zugriffskontrolle:

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Organisatorisch	Anzahl der Administratoren auf das "Notwendigste" reduzieren	x
Technisch	Einsatz von Aktenvernichtern (siehe BSI- Anforderungen)	x
Organisatorisch	Einsatz von Dienstleistern zur Akten- und Datenvernichtung (nach Möglichkeit mit Zertifikat)	x (DIN EN ISO/IEC 27001:2017)
Organisatorisch	Erstellen eines Berechtigungskonzepts	x
Technisch	Minimierung der Berechtigungen nach Erforderlichkeit	x
Technisch	Ordnungsgemäße Vernichtung von Datenträgern (DIN 66399)	x
Organisatorisch	Passwortrichtlinie inkl. Länge und Wechsel	x
Technisch	Physische Löschung von Datenträgern vor deren Wiederverwendung	x
Technisch	Protokollierung der Vernichtung von Daten	x
Technisch	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	x
Organisatorisch	Sichere Aufbewahrung von Datenträgern	x
Technisch	Verschlüsselung von Datenträgern	x
Technisch	Verschlüsselung von Smartphones	x
Organisatorisch	Verwaltung der Benutzerrechte durch Systemadministratoren	x
Organisatorisch	Vier-Augen-Prinzip	x

Trennungskontrolle:

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Technisch	Anonymisierung von Datensätzen	x
Technisch	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System	x
Organisatorisch	Festlegung von Datenbankrechten	x
Organisatorisch	Logische Mandantentrennung (softwareseitig)	x
Technisch	Trennung von Produktiv- und Testsystem	x

Pseudonymisierung:

(Artikel 32 Abs. 1 lit. a DSGVO und 25 Abs. 1 DSGVO)

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Organisatorisch	Anweisungen / Regelungen zur möglichst frühzeitigen Verfremdung von Datensätzen	x
Organisatorisch	Erstellung von Verfremdungskonzepten	x
Organisatorisch	Festlegung von Verfremdungsregeln	x
Technisch	Verfremdung von identifizierbaren Merkmalen durch Eigen- oder Fremdsoftware	x

Integrität (Artikel 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle:

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Organisatorisch	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen	x
Technisch	Einrichtung von VPN-Tunneln	x
Technisch	E-Mail-Verschlüsselung	
Technisch	Ende-zu-Ende-Verschlüsselung	x
Technisch	Inhaltsverschlüsselung	x
Organisatorisch	Sorgfältige Auswahl von Transportunternehmen	x
Organisatorisch	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form	x

Eingabekontrolle:

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Organisatorisch	Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	x
Technisch	Protokollierung der Eingabe, Änderung und Löschung von Daten	x

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

Verfügbarkeitskontrolle und rasche Wiederherstellbarkeit (Artikel 32 Abs. 1 lit. c) DSGVO)

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust und Vorkehrungen, um möglichst schnell die Daten wiederherzustellen

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Organisatorisch	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	x
Organisatorisch	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort	x
Technisch	Doppelte IT-Infrastruktur (Redundanz)	x
Technisch	Eingerichtetes Business Continuity Management (BSI)	x
Organisatorisch	Erstellen eines Backup- & Recovery-Konzepts	x
Organisatorisch	Erstellen eines Notfallplans	x
Organisatorisch	Festlegung von Meldewegen	x
Technisch	Feuer- und Rauchmeldeanlagen	x
Technisch	Feuerlöschgeräte in Serverräumen	x
Technisch	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	x
Technisch	Klimaanlage in Serverräumen	x
Technisch	Regelmäßige Belastungstests	x
Organisatorisch	Regelmäßige Durchführung von Krisen- / Notfallübungen	x
Technisch	Schutzsteckdosenleisten in Serverräumen	x
Organisatorisch	Serverräume nicht mit Wasserführenden Leitungen	x
Organisatorisch	Testen von Datenwiederherstellung	x
Technisch	Unterbrechungsfreie Stromversorgung (USV)	x

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

Datenschutz-Management

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Technisch	Regelmäßige Penetrationstests	x
Technisch	Regelmäßige Prüfung der Hardware (Lifecycle, Performance)	x
Organisatorisch	Bestellung eines Datenschutzbeauftragten	x
Organisatorisch	Bestellung eines IT- / Informationssicherheits-beauftragten	x
Organisatorisch	Datenschutz-Management-Konzept	x
Organisatorisch	Eskalationsverfahren für Notfälle	
Organisatorisch	Evaluierung der Dienstleister	x
Technisch	Incident-Response-Management	
Organisatorisch	Informations- / IT-Sicherheitskonzept	x
Organisatorisch	Regelmäßige interne Überprüfung / Aktualisierung der getroffenen Maßnahmen gemäß dem Stand der Technik (durch DSB, IT-Revision etc.)	x
Organisatorisch	Regelmäßiges Berichtswesen an die Geschäftsführung	x

Auftragskontrolle: Auftragsverarbeitung im Sinne von Artikel 28 DSGVO

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Organisatorisch	Abschluss von Verträgen zur Auftragsverarbeitung unter Berücksichtigung aller gesetzlichen Anforderungen gemäß Artikel 28 DSGVO	x
Organisatorisch	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	x
Organisatorisch	Regelmäßige Überprüfung des Auftragnehmers hinsichtlich Datenschutz/Datensicherheit	x
Technisch	Überprüfung aller vertraglich zugesicherten technischen Maßnahmen (ggf. vor Ort)	x
Organisatorisch	Vorherige Prüfung der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen und entsprechende Dokumentation mit Nachweisen	x

Einhaltung der Betroffenen-Rechte

Art der Maßnahme	Maßnahme	Maßnahme vorhanden bei evasys GmbH
Organisatorisch	Auskunft über Verarbeitung personenbezogener Daten, Zwecke, Kategorien, Speicherdauer, Berichtigung, Löschung, Einschränkung, Widerspruch, Beschwerde-Recht,	x
Organisatorisch	Beschwerde bei zuständiger Aufsichtsbehörde	x
Organisatorisch	Datenportabilität	x
Organisatorisch	Differenzierte Einwilligungs- und Widerspruchsmöglichkeiten	x
Organisatorisch	Einrichtung eines single point of contact für Betroffene	x
Organisatorisch	Einschränkung der Verarbeitung	x
Organisatorisch	Löschung der Daten	x
Organisatorisch	Unverzügliche Berichtigung	x
Organisatorisch	Widerruf der Einwilligung	x

Anlage 2:

Passwortrichtlinie

Das Passwort besteht aus mindestens zwölf Zeichen; bei administrativen Benutzerkonten oder Passwörter für verschlüsselte Datenträger, Container oder Dateien aus mindestens 20 Zeichen.

1. Das Passwort besteht mindestens aus drei der vier Zeichenklassen Groß-, Kleinbuchstaben, Ziffern oder Sonderzeichen (z.B. Satzzeichen).

2. Das Passwort ist nicht im Klartext und auch nicht reversibel verschlüsselt gespeichert. Entweder wird hierfür die Methode unter Punkt 4 oder eine qualitativ äquivalente verwendet.

3. Zur irreversiblen Speicherung des Passwortes wird derzeit mindestens SHA2 oder besser verwendet. Dabei wird auf die Erhöhung der Entropie entweder durch ein kryptografisches „Salt“ oder einem „rehashen“ oder durch eine qualitativ äquivalente Methode bei der Speicherung geachtet.

4. Das Passwort wird durch den jeweiligen Benutzer eigenständig gewählt und eingegeben.

5. Das Passwort darf nicht leicht zu erraten sein. Insbesondere dürfen nicht verwendet werden:

    1. triviale Zeichenfolgen wie „1234“, „qwertz“, „asdf“, usw.,

    2. Wörter, Begriffe oder Namen aus dem privaten oder beruflichen Umfeld oder auch Teile hiervon,

    3. Daten, die man sich als Außenstehender leicht erschließen kann, wie Geburtsdatum, Ort, Straße, usw. zu denen die Person einen Bezug hat, keine Wörter, keine Namen/Kürzel.

6. Die generische Änderung der Passwörter wird alle 90 Tage erzwungen, auch bei einfachen Nutzer*innen. Das neue Passwort muss sich mindestens an drei Stellen von allen Passwörtern der letzten 18 Monate unterscheiden. Dies entfällt bei verschlüsselten Datenträgern, Containern oder Dateien.

7. Sofern möglich oder erforderlich kann eine Zwei-Faktor-Authentifizierung mittels OTP- bzw. Token-Generatoren oder Chipkarte oder biometrischen Verfahren in Kombination mit einem Passwort, das den obigen Richtlinien genügt, verwendet werden. Dies bietet eine erhöhte Sicherheit für die Zugangskontrolle. Biometrische Identifizierungsverfahren sowie die OTP- bzw. Token-Generatoren oder Chipkarte allein sind keine ausreichende Authentifizierung, da diese nur über Besitz funktionieren.