SWOP.

Die Software.

eine Software der

SmartKomm GmbH

Datensicherheitskonzept

Stand März 2024

SmartKomm GmbH :: Rudolf-Breitscheid-Str.34, 14482 Potsdam :: www.smartkomm.de :: kontakt@smartkomm.de
Ust.Nr.: 046 / 118 / 04607 :: Gerichtsstand: Amtsgericht Potsdam :: HRB: 22860 P
Geschäftsführer: Thomas Benke, Jan Kechel :: Prokurist: Björn Engelbrecht

Die SmartKomm GmbH - Hersteller und Betreiber von SWOP - hat zum Schutz personenbezogener Daten des Kunden (Schule) bei der Auftragsdatenverarbeitung nach jeweils geschlossenem Vertrag zur Auftragsdatenverarbeitung (AVV) das nachfolgende Datensicherheitskonzept erstellt:

Allgemeine organisatorische und technische Maßnahmen

Die SmartKomm hat gemäß § 9 BDSG und der Anlage zu § 9 BDSG folgende organisatorischen und technischen Maßnahmen zum Schutz personenbezogener Daten ergriffen:

1. Zutrittskontrolle

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

SmartKomm arbeitet mit den Hosting-Anbietern HostEurope und Hetzner zusammen (Auftragsverarbeiter nach Art. 28 DS-GVO), die beide TÜV Süd ISO 27001 zertifiziert sind. Alle Server mit denen personenbezogene Daten verarbeitet oder genutzt werden befinden sich in Rechenzentren der EWR und sind wie folgt abgesichert ist:

„Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum jeweiligen Data Center nur für autorisierte Personen. Es bestehen Sichtkontrollen und ein Besucherbuch am Empfang. Videokameras sowie Bewegungs-, Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes. Im Alarmfall werden die für das Gebäude verantwortlichen Mitarbeiter automatisch alarmiert. Zusätzlich ist das Hauptgebäude 24/7 durch Personal besetzt. Auch diesem Personal werden die Alarmmeldungen angezeigt. Es besteht eine restriktive Zutrittsregelung. “

(* aus Kontrollziele gemäß Anlage § 9 BDSG und Beschreibung der technischen und/oder organisatorischen Sicherungsmaßnahmen von HostEurope)

2. Zugangskontrolle

(Maßnahmen, die verhindern, dass die Datenverarbeitungssysteme von Unbefugten genutzt werden können):

Benutzer-Accounts

Einen Zugang zu SWOP erhalten nur offiziell mit der Schule assoziierte Personen und Mitarbeiter der SmartKomm GmbH.

Passwörter

Alle Passwörter werden per Zufallsgenerator erstellt und Lehrern, Eltern und Schülern in gedruckter Form persönlich überreicht, oder zugeschickt. Jeder Nutzer kann jederzeit sein Passwort selbst verändern. Eine strenge Passwort-Komplexitäts-Richtlinie sorgt dafür, daß das neu vergebene Passwörter wieder sicher sind.

Wiederholte Zugriffsversuche mit falschen Zugangsdaten führen zu einer automatischen, zeitlich begrenzten, Sperrung des Zugangs.

SSL Zertifikate

Jeder Zugang in interne Bereiche erfolgt über mit SSL-Zertifikaten geschützte Verbindungen. So kann jederzeit überprüft werden das der Zugang direkt erfolgt und nicht über einen Man-in-the-Middle abgefangen wird.

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):

Berechtigungen

Nur Administratoren wird die Möglichkeit eingeräumt, Berechtigungen zu verändern oder zu erstellen.

Mechanismen

Jeder einzelnen Seite werden sogenannte ACLs (Access-Control-Lists) zugeordnet, die für genau diese eine Seite festlegen, welche Gruppe und welcher Benutzer die hier dargebotenen Informationen lesen darf und wer diese Daten verändern darf.

4. 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)

Datenübertragung

Alle sensitiven Daten werden ausnahmslos über Ende-zu-Ende SSL verschlüsselte Internet-Verbindungen übertragen. Sollte versucht werden, Daten unverschlüsselt abzurufen, so bricht SWOP die Verbindung ab.

Datenträger

Die Datenträger mit personenbezogenen Daten liegen ausnahmslos in dem Rechenzentrum des Hosting-Partners HostEurope. SmartKomm verwendet ausschließlich dedizierte Produkte die nicht mit anderen Kunden von HostEurope geteilt werden.

„Die Host Europe GmbH hat bei dedizierten Produkten keinen Zugriff auf durch den Kunden verarbeitete personenbezogene Daten - außer der Kunde beauftragt die Host Europe GmbH mit administrativen Aufgaben auf seinen Systemen."

(* aus Kontrollziele gemäß Anlage § 9 BDSG und Beschreibung der technischen und/oder organisatorischen Sicherungsmaßnahmen von HostEurope)

5. 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):

SWOP führt ein fortlaufendes Änderungs-Logbuch das von Administratoren eingesehen werden kann. Es werden jede An- und Abmeldung am System sowie alle Datenverändernde Aufrufe mit Datum, Uhrzeit und Loginname des Benutzers protokolliert.

6. Auftragskontrolle

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

Alle Änderungen werden durch den Kunden selber durchgeführt. Die SmartKomm kann auf ausdrücklichen Kundenwunsch entsprechend geschulte Mitarbeiter mit der Bearbeitung personenbezogener Daten beauftragen.

7. Verfügbarkeitskontrolle

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

SmartKomm führt regelmäßige Backups durch, die verschlüsselt auf anderen Datenträgern vorgehalten werden. Maßnahmen die physische Verfügbarkeit betreffend obliegen dem Hosting-Partner HostEurope:

„Die autonome Stromversorgung der Data Center erfolgt über eine eigene Trafostation. Die Stromversorgung und Netzersatzanlage

garantieren höchste Ausfallsicherheit. Jedes Serverrack wird über mindestens zwei separate Stromzuführungen versorgt, die je einzeln mit mindestens 16 Ampere abgesichert sind. Die unmittelbare Stromversorgung des Servers ist typenabhänig, so dass bei der Verwendung entsprechender Typen zusätzlich eine redundante Stromversorgung über ein redundantes Netzteil (2 Netzteile) gewährleistet ist. Der gesamte Energieverbrauch der Data Center wird über eine unterbrechungsfreie Stromversorgung (USV) sichergestellt. Im Falle eines Stromausfalls garantiert die USV-Anlage eine unterbrechungsfreie Umschaltung auf eines der Notstrom Dieselaggregate. Daneben filtert die USV vollständig alle Unregelmäßigkeiten oder Störungen des Stromversorgungsnetzes. Eine leistungsstarke Netzersatzanlage (Dieselaggregat) versorgt bei Stromausfall das gesamte jeweilige Data Center und die Kühlsysteme mit konstanter Energie. Der Kraftstoffvorrat ist für mindestens 48 Stunden bei Volllast ausreichend. Eine Auftankung ist während des laufenden Betriebs des Generators möglich. Ein flächendeckendes Wasser- und Brandfrühwarnsystem (VESDA) reagiert bereits bei geringer Überschreitung definierter Grenzwerte, um größere Schäden zu verhindern. Die Brandmeldeanlage verfügt daneben über eine direkte Aufschaltung bei der örtlichen Feuerwehr. Die Gebäudeaußenhaut ist zudem mittels Überspannungsschutz gegen Blitzschlag abgesichert. Sollte es wider Erwarten zu einer Rauchentwicklung oder gar einem Brand kommen, flutet die aufwendige Feuerbekämpfungsanlage mit 150fachen Luftdruck das Data Center innerhalb von nur 60 Sekunden vollständig mit dem Löschgas Argon bzw. Inergen. Hierbei bleibt das Equipment im Data Center vollkommen unbeschädigt. Die Host Europe GmbH bietet allen Dedicated Server Kunden standardmäßig Backup-Möglichkeiten für ihre Systeme an. Für die Einrichtung dieser Backups ist jedoch der Kunde selbst verantwortlich. Er kann dies über das KIS (Kundeninformationssystem) einrichten, verwalten und Restores ausführen. “

(* aus Kontrollziele gemäß Anlage § 9 BDSG und Beschreibung der technischen und/oder organisatorischen Sicherungsmaßnahmen von HostEurope)

8. Trennungskontrolle

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

Jedes SWOP ist eine Einheit für sich mit einer eigenen Datenbank die nur für einen Zweck eingesetzt wird. Übergreifende Datenzugriffe zwischen unterschiedlichen SWOP sind systembedingt ausgeschlossen. Es werden keine Daten für unterschiedliche Zwecke erhoben sondern dienen stets dem Zweck Informationen des Kunden für den Kunden selber abzuspeichern, zu strukturieren diese dann wiederum dem Kunden und

dessen Personenkreis anzuzeigen. Dieser Personenkreis erstreckt sich je nach Produkt bis hin zu Schulleitung, Lehrern, Eltern, Schülern und Erziehungsberechtigten.

9. Datenverarbeitungskontrolle

(Maßnahmen, die gewährleisten, dass Unbefugte keine Zugriff auf Netzwerk, Speicher, Server oder Betriebssystem des Servers der Datenver arbeitungsanlagenerhalten können)

Zugriff wird nur verschlüsselt, passwortgeschützt und zusätzlich mit einem Public/Private-Key Zertifikat abgesichert ermöglicht. Nur benannte und entsprechend technisch befähigte wie datenschutzrechtlich aufgeklärte und verpflichtete Mitarbeiter der SmartKomm GmbH erhalten diese Möglichkeit des Zugriffs. Grundsätzlich kann weder der Datenbank-Server noch der Datei-Server direkt Verbindungen mit dem Internet aufnehmen.

Technische Vorkehrungen auf Netzwerkebene:

Mehrere Firewalls

- Firewall des Hosting-Providers
- Firewall des Host-Servers
- Firewall der Webserver-VM
- Firewall der Dateiserver-VM
- Firewall der Datenbank-VM

Technische Vorkehrungen auf Serverebene

- automatische Sicherheitsupdates des Betriebssystems und aller installierter Komponenten alle 4 Stunden (Sicherheit ist wichtiger als Verfügbarkeit)
- Passwortschutz für Login an Console
- Passwortschutz + zusätzliche Public/Private-Key Authentifizierung auf SSH Netzwerkebene
- Überwachung der Server-Aktivität auf ungewöhnliche Aktivität mit OSSEC von TrendMicro auf dem Ser ver-Host sowie auf jeder VM

10. Dokumentationskontrolle

(Maßnahmen, die gewährleisten, dass technische und organisatorische Vorgänge der Datenhaltung dokumentiert, fortgeschrieben und nachvollziehbar sind)

Es erfolgt serverseitig eine automatische Protokollierung aller administrativer Sitzungen inkl. aller aufgerufener Befehle. Zum Einsatz kommt das Versionsverwaltungs-System Git mit dem ein Rückgriff auf jeden ehemaligen Entwicklungsstand der Software und der Datenbank möglich ist. Eine ausführliche und täglich gepflegte Entwicklungsdokumentation des gesamten Software- und Datenbank-

Frameworks liegt vor. Schulleiter, Schulträger oder Datenschutzbeauftragte können nach Unterzeichnung eines Non-Disclosure-Agreements alle Dokumentationen und Sitzungsprotokolle einzusehen und kontrollieren.

11. Organisationskontrolle

(Maßnahmen, die gewährleisten, dass Zuständigkeiten und Organisationsstrukturen aufseiten der SmartKomm GmbH nur befugten und geschulten Mitarbeitern Zugriff auf Daten von Auftraggebern gewähren)

Die SmartKomm informiert, schult und prüft Mitarbeiter hinsichtlich rechtlicher und datenschutzrechtlicher Kenntnisse im Bezug auf ihr Einsatzgebiet, bevor sie als Support-Mitarbeiter oder als Administrator für Kunden eingesetzt werden. Administratoren, die administrativen Zugriff auf Server mit personenbezogenen Daten erhalten sollen, müssen:

- eine entsprechende fachliche Qualifikation besitzen (z.B. Studium der Informatik)
- über die datenschutzrechtlichen Anforderungen aufgeklärt sein
- eine entsprechende Vertraulichkeitsvereinbarung unterschrieben haben
- sich mit der Protokollierung und Überwachung aller aufgerufener Befehle für einverstanden erklärt haben

Technische „Hürden“ werden implementiert, so das ein tatsächlicher Datenexport nicht „ausversehen“ (z.B. durch einfaches vertippen bei einem Domain-Namen) ausgeschlossen wird, sondern mehrere ansonsten nicht übliche Befehle und Firewall-Einstellungen vorgenommen werden müssten. So ist, wenn ein tatsächlicher Datenexport stattgefunden hat, grundsätzlich „wissentlicher Vorsatz“ und „wissentliche Absicht“ durch den Administrator nachgewiesen.

Grundsätzlich kann weder der Datenbank-Server noch der Datei-Server direkt Verbindungen mit dem Internet aufnehmen. Um dies zu umgehen müsste ein Administrator zuerst die Einstellungen der Firewall verändern, wozu er ausser bei der Ersteinrichtung oder bei Updates die entsprechende neue Protokolle benötigten nicht berechtigt ist.

Administratoren erhalten zusätzlich Informationen über den Zustand der Server, der Server-Software, der Betriebssystem-Parameter, automatische Updates und über ungewöhnliche Aktivitäten auf den Server-Systemen. Keines dieser Systeme ermöglicht den Zugriff auf personenbezogene Daten.

Nagios ist eine Monitoring-Software, mit der Administratoren die funktionsfähigkeit aller Server-Systeme und Dienste überwachen und kontrollieren können. Eine schreibende

Funktion ist nicht möglich und Server-Parameter oder Einstellungen können nicht vorgenommen werden.

12. Sicherheitsvorkehrungen innerhalb der Software-Entwicklung

Die SmartKomm GmbH verwendet modernste und ausgereifte Mechanismen zur regelmäßigen Funktions- und Sicherheits-Testung des Schul - Webportals nach aktuellem Stand der Technik. Neben Black-Box, Gray-Box und White-Box Testing-Verfahren werden auch manuelle Code-Audits, Security-Reviews und viele verschiedene automatische Testverfahren angewendet. Durch stetiges Updaten des zugrunde liegenden Software-Frameworks auf die jeweils neuesten Versionen wird sichergestellt, dass stets die neuesten und aktuellsten Sicherheits-Techniken benutzt werden.

13. Löschung von Daten

Personenbezogene Daten werden nachdem der Nutzer die Schule verlassen hat (Schul-Wechsel, Kündigung, Abschluss), per Default innerhalb eines Jahres anonymisiert, wenn nicht vom Auftraggeber anders gewünscht. Anonymisierte Daten können jederzeit von vom Auftraggeber authorisierten Personen gelöscht werden. Auf Aufforderung werden personenbezogene Daten eines Nutzers innerhalb eines Tages (24h ab Aufforderung) gelöscht. Personenbezogene Daten können von autorisierten Mitarbeitern (Administratoren) des Auftraggebers jederzeit selbts gelöscht werden. Jeder im System eingebundene Nutzer kann jederzeit schriftlich der Verarbeitung seiner personenbezogenen Daten widersprechen.