SCOPEVISIO

Unternehmenssoftware – nur anders

ANHANG 1 ZUR

ADV nach Art. 28 DSGVO

Technisch-organisatorische Maßnahmen zur Einhaltung des Datenschutzes (Stand: 28. Januar 2019)

Einleitung

Das vorliegende Dokument beschreibt die technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes bei Scopevisio AG, im Folgenden Scopevisio genannt.

Als Auftragsdatenverarbeiter verarbeitet Scopevisio Daten im Auftrag ihrer Kunden. Ein Verlust oder unbefugtes Lesen oder Ändern dieser Daten hätte sowohl für unsere Kunden als auch für Scopevisio selber weitreichende negative Konsequenzen. Scopevisio ist sich über die besondere Verantwortung für die Daten ihrer Kunden bewusst. Um dieser Verantwortung gerecht zu werden, hat Scopevisio die erforderlichen technischen und organisatorischen Maßnahmen getroffen, diese Daten nach dem aktuellen Stand der Technik zu schützen.

Die Kunden von Scopevisio haben sich laut Art. 28 DS-GVO von der Einhaltung der technischen und organisatorischen Maßnahmen zur Einhaltung des Datenschutzes zu überzeugen, welche in Art. 32 Abs 1 DS-GVO konkretisiert werden. Grundlage hierfür bildet diese Dokumentation. Die Gliederung dieser Dokumentation richtet sich nach dem Aufbau des Art. 32 Abs. 1 DS-GVO.

1. Vertraulichkeit (Art. 32 Abs. 1 Ziff. b DS-GVO)

1.1 Zutrittskontrolle

1.1.1 Zutrittskontrolle (Bonn)

In den einzelnen Bereichen des Firmengebäudes wird die Zutrittskontrolle durch ein elektronisches Zutrittskontrollsystem geregelt. Im Innenbereich des Firmengebäudes sind unterschiedliche Sicherheitszonen eingerichtet, für die, zeitlich begrenzt, unterschiedliche Berechtigungen eingerichtet werden.

Jeder Mitarbeiter erhält einen Zugangscode, der einer Gruppe zugeordnet ist, die den Zugangsbereich regelt.

Es ist ein Empfang eingerichtet, der den Zutritt von betriebsfremden Personen kontrolliert. Besucher müssen klingeln und sich nach Zutritt zum Gebäude beim Empfang anmelden. Besucher werden nicht registriert. Innerhalb des Firmenbereichs werden die Besucher geführt. Dabei liegt es in der Verantwortung des Empfangs, die Besucher zu den jeweiligen Mitarbeitern zu führen. Jeder Mitarbeiter ist dann für seine Besucher verantwortlich.

Nebenausgänge, Fluchttüren und sonstige Notausgänge können von außen nicht geöffnet werden. Das Parkhaus ist mit einer Schrankenanlage und einem Rolltor gesichert. Der Zugang vom Parkhaus zum Gebäude ist für Betriebsfremde gesondert gesichert.

1.1.2 Zutrittskontrolle (Rechenzentrum Digital Realty, Frankfurt am Main)

Für das Rechenzentrum der Digital Realty, Frankfurt am Main liegt ein ISO 27001:2013 Zertifizierung vor. Diese können Sie auf unserer Website einsehen und herunterladen.

1.2 Zugangskontrolle

Die Zugangskontrolle verhindert, dass Datenverarbeitungsanlagen von Unbefugten genutzt werden können.

Die Server im Rechenzentrum werden ausschließlich von namentlich benannten Mitarbeitern der Scopevisio administriert und verfügen hierzu über entsprechende Benutzerkonten. Die Administration erfolgt über das Internet mittels verschlüsselter Verbindungen. Mitarbeiter des Rechenzentrumbetreibers haben keinen Zugang zu Kundendaten oder der Datenverarbeitungs-software.

Um nicht autorisierten Zugang über das Internet zu verhindern sind die Server durch eine hardwarebasierte Firewall geschützt. Die Datenbankserver sind in ein nur für diesen Zweck eingerichtetes eigenes virtuelles Netzwerk ausgelagert. Zugriffe auf dieses Netzwerk werden über eine zweite, eigene hardwarebasierte Firewall geschützt.
Der Zugang zu Rechnern in den Büroräumen der Scopevisio wird über Benutzerkonten kontrolliert. Hierzu hat jeder Mitarbeiter auf seinem Rechner ein eigenes Benutzerkonto. Der Zugriff auf das bürointerne Netzwerk von außerhalb der Büroräume ist ausschließlich über eine VPN Verbindung (Virtual Private Network) möglich. Das bürointerne Netzwerk wird ebenfalls von einer hardwarebasierten Firewall geschützt.

Der Zugang zu den Datenverarbeitungssystemen ist mit Benutzerkennung und einem sicheren Authentifizierungsverfahren geschützt.

Es sind Regeln zur Bildung eines sicheren Passworts festgelegt. Die Zugänge sind mit einer sicheren „Pausenschaltung“ geschützt.

1.3 Zugriffskontrolle

Die Zugriffskontrolle gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

In den vom Auftragnehmer genutzten Datenverarbeitungssystemen sind Berechtigungsprofile hinterlegt, in denen die zugriffsberechtigten Personen festgelegt sind. Die Rechte werden in einem geregelten Verfahren vergeben, und die Notwendigkeit der bestehenden Rechte wird regelmäßig kontrolliert. Die Einrichtung und Freigabe werden dokumentiert.

Der Auftragnehmer hat die technischen und organisatorischen Maßnahmen getroffen, die sicherstellen, dass ausscheidenden Mitarbeitern sämtliche Unterlagen, Zugangsberechtigungen und Zugriffsrechte entzogen bzw. gelöscht werden um einen unberechtigten Zugriff auf die Daten des Auftraggebers zu verhindern.

Der Zugang zu Daten über Kunden für den Scopevisio Support ist auf ein Mindestmaß beschränkt. Dieser Zugang erfolgt über eine eigene Installation. Damit ist es möglich, Informationen zu den Kunden einzusehen, die für die Aufgaben des Supports notwendig sind.

Diese Rolle muss jedem Supportmitarbeiter individuell zugewiesen werden. Der Zugriff ist auf folgende Daten beschränkt:

- Name, Vorname, Geschlecht und E-Mail-Adresse des Kunden bzw. der Benutzer der Kundeninstanz
- Gebuchte Leistungen bzw. Anwendungen und Abrechnungsdaten

Der Zugriff auf technischer Ebene auf Kundendaten, z.B. über die Datenbank des Kunden, ist ausschließlich eigens dafür benannten Mitarbeitern aus dem Team „Betrieb“ der Scopevisio möglich. In diesem Fall verwenden besagte Mitarbeiter jeweils eigene Benutzerkonten. Der Zugriff ist nur gestattet, wenn eine Supportaufgabe vorliegt, die nicht durch den Kunden oder den Support alleine gelöst werden kann und der Auftraggeber seine Einwilligung zum Zugriff schriftlich erteilt hat. Diese wird im Ticketsystem protokolliert. Sollte die Aufgabe auch durch direkten Zugriff auf die Daten nicht lösbar sein, kann eine lokale Kopie der Daten z.B. für Debuggingzwecke erstellt und dem verantwortlichen Entwickler zugänglich gemacht werden. Nach Abschluss der Arbeiten werden lokale Kopien unverzüglich gelöscht.

1.4 Trennungskontrolle

Mittels der Verwendungszweckkontrolle soll gewährleistet werden, dass „zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können“.

Scopevisio verarbeitet die Daten mehrerer Kunden auf den gleichen Servern. Die strikte Trennung der Daten einzelner Kunden voneinander wird durch eine Reihe von Maßnahmen sichergestellt: Jeder Kunde hat eine eigene logische Datenbank mit einem eigenen Benutzerkonto innerhalb eines Datenbankmanagementsystems (DBMS), das mehrere dieser logischen Datenbanken verwaltet.

Dabei läuft jede Transaktion auf der Datenbank in einem eigenen Betriebssystemprozess ab, so dass jeder Prozess immer nur die Daten eines einzelnen Kunden verarbeitet. Der Applikationsserver, der die Geschäftslogik ausführt, öffnet zum Schreiben oder Lesen der Daten Verbindungen auf die Datenbank des jeweiligen Kunden. Dabei wird durch von Scopevisio vorgenommene Änderungen an dem Datenbanktreiber sichergestellt, dass innerhalb einer Benutzersitzung immer nur Verbindungen zu der dem jeweiligen Kunden gehörenden Datenbank geöffnet werden können. Ein Zugriff auf die Datenbank eines bestimmten Kunden durch Benutzer eines anderen Kunden ist somit ausgeschlossen.

2. Integrität (Art. 32 Abs. 1 Ziff. b DS-GVO)

2.1 Weitergabekontrolle

Die Weitergabe-Kontrolle gewährleistet, 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.

Die Weitergabe-Kontrolle wird durch verschiedene Maßnahmen gewährleistet. Zum einen werden Daten nicht außerhalb des Rechenzentrums gespeichert, mit Ausnahme der in Ziffer 3 genannten Speicherung für Debuggingzwecke. Die Mitarbeiter des Rechenzentrumbetreibers haben grundsätzlich keinen Zugriff oder Zugang zu den auf den Datenträgern gespeicherten Daten und können diese Daten weder lesen noch verändern.

Zum anderen werden Daten grundsätzlich nur über verschlüsselte Verbindungen zwischen dem Server und dem Client des Kunden außerhalb des Rechenzentrums übertragen. Hierbei kommt das SSL verschlüsselte HTTP Protokoll (HTTPS) zum Einsatz. Sollte für besondere Supportaufgaben eine Übertragung von Daten in die Büroräume der Scopevisio notwendig sein, findet diese ebenfalls ausschließlich verschlüsselt statt.

Eine Übertragung außerhalb Deutschlands findet nur dann statt, wenn der Auftraggeber oder seine Mitarbeiter die Scopevisio Unternehmenssoftware im Ausland verwendet.

2.2 Eingabekontrolle

Die Eingabekontrolle gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die Eingabekontrolle wird bei Scopevisio über Protokolleinträge umgesetzt. Die Protokolleinträge sind nicht änderbar oder löschbar.

Darüber hinaus ist es für eine Vielzahl von verschiedenen Datensätzen direkt in der Anwendung ersichtlich, von welchem Benutzer diese zu zuletzt geändert wurden und wann diese Änderung stattfand.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Ziff. b DS-GVO)

Ein mehrstufiges Sicherheitskonzept stellt die Verfügbarkeit der Daten sicher. Alle physikalischen Datenträger (Festplatten) sind als RAID-Verbund ausfallsicher angelegt und jede Komponente des verwendeten Storage Area Network (SAN) ist redundant vorhanden. Der Status der Datenträger wird laufend automatisch überwacht und defekte Festplatten werden unverzüglich ausgetauscht.

Zum anderen werden die Kundendaten jede Nacht im einem getrennten Brandabschnitt gesichert und gespeichert. Es existiert ein schriftlicher Notfallplan, um die Sicherungen bei Verlust oder Zerstörung der physikalischen Datenträger auf andere Datenträger zurück zu spielen.

Das Rechenzentrum bietet durch vollklimatisierte Sicherheitsräume zusammen mit einer Löschanlage weitgehenden Schutz vor Schäden durch äußere Einflüsse wie Feuer, Gas und Wasser.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Ziff. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutzmanagement

Scopevisio ist sich seiner Verantwortung in Bezug auf Datenschutz sehr bewusst. Deshalb wird dem Datenschutzmanagement eine besondere Stellung in unserem Haus zuteil. Wir haben uns schriftlich im Rahmen einer gesonderten Erklärung und im Rahmen einer Vielzahl von Leitlinien und Konzepten zu einem verantwortungsbewussten Umgang mit dem Thema Datenschutz verpflichtet.

Unsere Mitarbeiter sind umfassend mit dem Thema durch Schulungen und andere Sensibilisierungsmaßnahmen vertraut gemacht worden.

Wir sind uns aber auch der Tatsache bewusst, dass Datenschutz und IT-Sicherheit zwei Seiten einer Medaille darstellen und damit untrennbar miteinander verbunden sind. Dem tragen wir in einer Richtlinie zur Informationssicherheit und einer IT-Sicherheitsrichtlinie Rechnung. Deren Umsetzung wird durch sämtliche Mitarbeiter unseres Unternehmens sichergestellt.

Der Aufbau unseres Datenschutz- und IT-Sicherheitsmanagements orientiert sich am BSI Grundschutz.

4.2 Incident-Reponse-Management

Für anerkannte und vermutete Sicherheitsvorfälle haben wir einen Geschäftsprozess erarbeitet, der sowohl mit technischen als auch mit organisatorischen Maßnahmen sicherstellen soll, dass der Geschäftsbetrieb mit minimalen Störungen aufrechterhalten werden kann.

Das Incident-Response-Management der Scopevisio AG ist dazu konzipiert, um mit Vorfällen und Notfällen verschiedener Art zielgerichtet, schadensbegrenzend und lösungsorientiert umzugehen. Dazu ist es vor allem auch notwendig, klare Melde- und Bearbeitungswege sowie Verantwortlichkeiten zu definieren und die Effizienz dieser zu erfassen, zu evaluieren und regelmäßig den aktuellen Gegebenheiten anzupassen und zu verbessern.

Aus dem sich ständig ändernden und neuausrichtenden Umfeld der modernen IT ergibt es sich aber zur gleichen Zeit, dass gerade Lösungswege zu Sicherheitsvorfällen nicht starr definiert werden dürfen, sondern dass eine

Richtlinie zum Incident-Response-Management stattdessen gleichzeitig das notwendige Rüstzeug und die notwendige Flexibilität anbieten muss, die zur Bewältigung aller möglichen denkbaren und auch (noch) nicht denkbaren Sicherheitslagen geeignet ist.

Alle Mitarbeiter, die mit der Entwicklung, der Bereitstellung und der Unterstützung des Dienstes in Kontakt kommen, wurden geschult und haben sich mit ihren Aufgaben in diesem Zusammenhang vertraut gemacht.

4.3 Datenschutzfreundliche Voreinstellungen

Die Art der Daten, die vom Auftraggeber erfasst und verarbeitet werden, liegen rein in der Verantwortung des Auftraggebers. So hat der Auftraggeber das dem Verarbeitungsrisiko angemessene Schutzniveau zu ermitteln und die diesbezügliche Schutzbedarfsklassifizierung zu dokumentieren.

Scopevisio unterstützt Sie in Bezug auf die datenschutzrechtlichen Voreinstellungen mit einer Reihe von Funktionalitäten. So ist es Ihnen als Auftraggeber möglich, in Scopevisio ein Rollen- und Berechtigungskonzept zu hinterlegen und zu dokumentieren.

Im Ergebnis der Einstellungsmöglichkeiten ist es unser Ziel, Scopevisio derart zu entwickeln, dass einerseits die Privatsphäre der Betroffenen durch den Auftraggeber geschützt werden können und andererseits der Auftraggeber die Kontrolle über die von ihm erfassten und verarbeiteten Daten behält.

4.4 Auftragskontrolle

Vor Vergabe der Datenverarbeitung im Auftrag durch den Auftragnehmer an Subunternehmer, stellt der Auftragnehmer sicher, dass beim Subunternehmen eine Kontrolle in Bezug auf die Einhaltung der Anforderungen nach Art. 28 DS-GVO durch Auftraggeber und/oder Auftragnehmer durchgeführt werden kann. Diese Kontrolle stellt sicher, dass beim Subunternehmen die Einhaltung der erforderlichen technischen und organisatorischen Maßnahmen zur Sicherung des Datenschutzes nach Maßgabe dieser Vereinbarung eingerichtet sind.

Über jeden Unterauftrag wird ein Vertrag unter Einhaltung der Vorschriften des Bundesdatenschutzgesetzes abgeschlossen. Dies gilt insbesondere auch für Verträge über Wartungsarbeiten an den Datenverarbeitungssystemen und über Softwarepflege sowie sonstige IT-Unterstützungsverträge, wenn dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Die Datenverarbeitung findet ausschließlich im Rechenzentrum der Digital Realty in Frankfurt am Main statt. Die Nutzung oder Weitergabe der Daten durch Mitarbeiter des Rechenzentrums ist dabei technisch ausgeschlossen. Regelmäßige Updates der Scopevisio Software finden über Fernwartung im Rechenzentrum statt (siehe 1.2). Zu diesem Zweck hat jeder damit beauftragte Mitarbeiter ein eigenes Benutzerkonto, über das er mittels einer verschlüsselten Verbindung arbeiten kann.

Aufträge zum Support oder zur sonstigen Verarbeitung von Kundendaten durch Scopevisio an andere Firmen werden nicht erteilt.

Sonstige Angaben

Die technischen und organisatorischen Maßnahmen können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden. Wesentliche Änderungen sind schriftlich festzuhalten und dem Auftraggeber bekannt zu geben.