Technische und organisatorische Maßnahmen nach Art. 32 EU-Datenschutzgrundverordnung

der INSIGMA IT Engineering GmbH Stand 01.11.2022

Präambel

Die INSIGMA IT Engineering GmbH (“INSIGMA”, “Wir”) betreibt in ihren Räumen Server, Netzwerk- und Infrastrukturkomponenten (“Infrastruktur”), die an das Internet angebunden sind. Ebenso entwickelt die INSIGMA Softwarelösungen für Kunden und für Dritte als Subunternehmer (“Kunden”), die sie im Rahmen von Software as a Service (“SaaS”) bereitstellt. INSIGMA stellt ihren Kunden für eigene Zwecke Teile dieser Infrastruktur sowie der Software (gemeinsam “Systeme”) zur Nutzung zur Verfügung. Die Räumlichkeiten zum Betrieb der Systeme sind in Rechenzentren (“RZ”) gemietet. Die Systeme sind ausschließlich im Kundenbesitz oder gehören der INSIGMA.

Wir berücksichtigen laut Art. 32 der EU-Datenschutzgrundverordnung (“DSGVO”) nachfolgende technische und organisatorische Maßnahmen (“TOM”) und bieten unseren Kunden diese Leistungen äquivalent an. Alle getroffenen Maßnahmen können kundenspezifisch gegen Entgelt angepasst werden.

Der Umgang mit Kundendaten im Rahmen der Datenverarbeitung durch INSIGMA selber in eigenen Systemen, unterliegt in jedem Fall den unten angegebenen Maßgaben. Unsere involvierten Mitarbeiter werden anhand einer gesonderten Verpflichtungserklärung zum Datenschutzgeheimnis nach DSGVO verpflichtet.

1. Vertraulichkeit

1. **Zutrittskontrolle** *Hiermit sind Maßnahmen gemeint, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:*

   Alle Serverräume und -schränke sind in Rechenzentren mit Einbruchmeldeanlage und angebundenem Wachdienst untergebracht. Die Zutrittskontrolle zu allen Serverräumen erfolgt durch vorherige telefonische Anmeldung und ausschließlich über personengebundene, zeitgesteuerte Chipkarten sowie PIN-Abfrage an den Türen. In den Serverräumen sind Kameras mit Aufzeichnung vorhanden. Die Serverschränke sind jeweils mit Schlüsseln zusätzlich geschützt.

   Die Geschäftsräume haben ein elektronisches Zutrittskontrollsystem für Mitarbeiter und Gäste, Alarmanlage, Sicherheitsfenster im Erdgeschoss und eine Videoüberwachung. Die sich im Haus befindlichen EDV-Räume sind durch eine zusätzliche Zutrittskontrolle separat abgesichert.

   Regelmäßig erfolgt eine Überprüfung der Notwendigkeit der Zutrittsberechtigungen der Mitarbeiter. Die gesamten Maßnahmen orientieren sich an der DIN/ISO 27002 Punkt 11.1.2.

2. **Zugangskontrolle** *Hiermit sind Maßnahmen gemeint, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:*

Die Zugangskontrolle zu den Systemen orientiert sich an der DIN/ISO 27002 Punkt 9.1.1 bis 9.2.6. Hierunter fallen unter anderem Benutzerverwaltung, Rechtemanagement, Passwortverwendung, Netzzugangskontrolle, Zugriffskontrolle auf Betriebssysteme, Zugangskontrolle zu Anwendungssystemen und Informationen.

Die entsprechenden organisatorischen Anweisungen werden von unseren verantwortlichen Mitarbeitern umgesetzt und regelmäßig geprüft. Daten werden wo notwendig verschlüsselt gespeichert.

Alle Zugänge auf Systeme sind nur mittels individuellem Login und Kennwort möglich. Zusätzlich verwenden wir komplexe Passwortrichtlinien, Multi-Faktor-Authentisierung und eine automatische Sperrung der Clients nach festgelegtem Zeitablauf.

Mögliche Zugriffe von außen werden ausschließlich über verschlüsselte VPN-Verbindungen oder SSL-verschlüsselte Zugriffe und ein gesichertes WLAN erlaubt. Die Verschlüsselung der Festplatten aller Notebooks erfolgt mit Bitlocker. Unsere internen Systeme im Finanzwesen, die Warenwirtschafts- oder Dokumentenmanagementsysteme werden über zusätzliche Kennwörter oder andere Maßnahmen geschützt. Unsere Mitarbeiter erhalten nur Zugriff auf die Daten der Projekte, an denen sie arbeiten.

3. **Zugriffskontrolle** *Hiermit sind Maßnahmen gemeint, 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:*

   Es erfolgt eine kundenindividuelle bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung des jeweiligen Kundensystems.

   Die Maßnahmen zur Sicherstellung der Zugriffe auf INSIGMA-eigene Systeme werden, wie unter Zugangskontrolle beschrieben, von den verantwortlichen Mitarbeitern ergriffen. Es werden durch technische und organisatorische Maßnahmen folgende Punkte umgesetzt: Ausschließlich personalisierte Zugangsberechtigungen, komplexe Passwortrichtlinien, differenzierte Zugriffberechtigungen auf alle Daten, insbesondere auf Kennwortdaten Dritter. Intrusion-Prevention-Systeme sind firewallseitig implementiert. Ein unabhängiges Monitoring überprüft die Wirksamkeit der Maßnahmen kontinuierlich.

   Die Berechtigungen werden nach Personen, Projekten und Geräten strukturiert im Active Directory verwaltet. Alle Systeme sind durch ein redundantes Firewall-Cluster mit regelmäßigen Checks geschützt. Die Zugriffsberechtigungen von Mitarbeitern werden regelmäßig, im Rahmen von Audits, überprüft.

   Für eine sichere Datenvernichtung werden Unterlage und Datenträger nur gemäß DIN 66399 und mit schriftlichem Vernichtungszertifikat entsorgt.

4. **Trennungskontrolle** *Hiermit sind Maßnahmen gemeint, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.*

   Die Systeme verschiedener Kunden sind technisch voneinander getrennt, so dass kein direkter Datenaustausch zwischen diesen möglich ist. Wo anwendbar, werden verschiedene Umgebungen für Entwicklung,

Test und Produktiv (Dev, QA, Live) eingesetzt.

5. **Pseudonymisierung** *Hiermit sind Maßnahmen gemeint, die die Pseudonymisierung von personenbezogenen Daten gewährleisten.*

   Es kann eine kundenindividuelle, bedarfsorientierte Pseudonymisierung von Daten erfolgen.

2. Integrität

1. **Weitergabekontrolle** *Hiermit sind Maßnahmen gemeint, 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:*

   Wie unter Zugriffskontrolle beschrieben, werden die Maßnahmen bei Transport, Übertragung und Übermittlung oder Speicherung auf Datenträger (manuell oder elektronisch) sowie bei der nachträglichen Überprüfung kundenspezifisch gestaltet. Die Weitergabekontrolle im Bereich von Systemen orientiert sich an der DIN/ISO 27002 Punkt 13.2 „Informationsübertragung“.

   Berücksichtigt werden können hierbei folgende Hauptpunkte:

   - Prozeduren für den Schutz sensitiver Informationen durch separate zusätzliche Kennwörter. Lagerung von Backupmedien im Safe in einem separaten Gebäude, Spiegelung wesentlicher Informationen für den Zugriff auf Daten in ein separates RZ.
   - Individuelle Verfahren, um auszutauschende Informationen vor Abhören, Kopieren, Veränderung und Zerstörung zu schützen. Hier kommen gesicherte VPN-Verbindungen, SSL-Verbindungen, WebDAV-Laufwerke, u. a. geschützt durch aktuelle Firewall-Systeme, zum Einsatz.
   - Der Mailaustausch wird mindestens über Transport Layer Security (“TLS”) geschützt. Auf Kundenwunsch richten wir verschlüsselte Verbindungen zwischen den Mailservern ein.

   Die Datenübertragungen werden durch separate Systeme im Rahmen der zulässigen Speicherung protokolliert und automatisch ausgewertet. Fernzugriffe werden ausschließlich über gesicherte und verschlüsselte Verbindungen ermöglicht.

2. **Eingabekontrolle** *Hiermit sind Maßnahmen gemeint, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:*

   Die Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben, verändert oder entfernt (gelöscht) worden sind, orientieren sich an den Möglichkeiten der jeweils eingesetzten Anwendungen/Systeme. Die Aktivitäten INSIGMA-eigener Systeme werden durch Logging der relevanten Änderungen protokolliert.

3. Verfügbarkeit

Hiermit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Die Sicherstellung der Verfügbarkeit von identifizierten, geschäftskritischen Daten orientiert sich an der DIN/ISO 27002 Punkt 17 „Informationssicherheitsaspekte beim Business Continuity Management“. Ein automatisches Monitoring aller IT-Systeme mit abgestuften Meldungsprioritäten und redundanten Meldungswegen per SMS, E-Mail und Wachdienst stellt eine kontinuierliche Verfügbarkeitskontrolle dar. Die Systeme sind RZ-seitig durch unterbrechungsfreie Stromversorgung-Anlagen (“USV”) und Notstrom-Aggregate geschützt.

Die Räume des RZ sind darüber hinaus redundant klimatisiert und verfügen über eine Rauchmelde- und Feuerlöschanlage. Zusätzlich ist das RZ durch einen Blitzschutz gesichert.

4. Verschlüsselung

Hiermit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten vor unberechtigtem Zugang geschützt sind:

Es erfolgt eine kundenindividuelle bedarfsorientierte Ausgestaltung des Berechtigungskonzepts und der Zugriffsrechte sowie deren Überwachung und Protokollierung des jeweiligen Kundensystems. Die Systeme verschiedener Kunden sind technisch voneinander getrennt, so dass kein direkter Datenaustausch zwischen diesen möglich ist. (siehe Zugriffskontrolle) Details werden kundenspezifisch festgelegt. Zudem werden Maßnahmen, wie Bitlocker und das Verschlüsselungsprotokoll TLS verwendet. Auf Kundenwunsch richten wir verschlüsselte Verbindungen und spezielle IP-Filter zwischen den Mail- und anderen Servern ein.

5. Belastbarkeit der Systeme

Hiermit sind Maßnahmen gemeint, die die Belastbarkeit der Systeme dauerhaft gewährleisten:

Wir setzen eine redundante VMWare-Infrastruktur mit mehrfach redundant ausgelegten SSD-/SAS-/SATA-Storages ein.

Für Kundensysteme stellen wir nach Leistungsschein einen Virenschutz bereit. Unsere Systeme sind durch Antivirenschutz sowohl auf der Firewall wie auch auf allen Systemen geschützt.

6. Wiederherstellung der Verfügbarkeit und des Zugangs

Hiermit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten nach Sicherheitsvorfällen schnellstmöglich wieder verfügbar und zugänglich sind:

Basis hierfür sind das Backup- und das Recovery-Konzept. Dies beinhaltet u. a. bewährte Back-Up-Verfahren, USV und Vertretungsregelungen des relevanten Personals. Somit gewährleisten wir die schnelle Wiederherstellung.

Die Aufbewahrung von Sicherungen in einem separaten Brandabschnitt gehören ebenso zu diesen Konzepten wie die Tatsache, dass alle Systeme von INSIGMA entsprechend dem Backup-Konzept mindestens täglich über File to Disk to Tape gesichert werden und die Backups an separaten Standorten für 30 Tage aufbewahrt werden. Systeme werden je vereinbartem Leistungsschein gesichert.

7. Verfahren zur regelmäßigen Überprüfung

Hiermit sind Maßnahmen gemeint, die die regelmäßige Überprüfung der Datensicherungsmaßnahmen gewährleisten:

Durch Prüfroutinen und die Evaluierung von Prüfberichten wird eine regelmäßige Überprüfung gewährleistet. Diese Audits finden im Rahmen der regelmäßigen ISO-Zertifizierungen statt. Der Informationssicherheitsmanagementbeauftragte, der Datenschutzkoordinator und der Datenschutzbeauftragte sind entsprechend involviert.

8. Verarbeitung personenbezogener Daten nur nach Anweisung

Hiermit sind Maßnahmen gemeint, die gewährleisten, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden können:

Unsere Mitarbeiter stehen in der Verpflichtung des Datenschutzgeheimnisses. Im Rahmen der implementierten, unternehmensinternen Datenschutzrichtlinien werden zugriffsberechtigte Mitarbeiter regelmäßig geschult und es erfolgt eine Bestimmung von Ansprechpartnern und verantwortlichen Projektmanagern für den konkreten Auftrag.