Thema	TOM zur DSGVO
Dokumentenhistorie	Version 1.0 erstellt durch Alexandra Jakubaschk am 16.04.2018 Version 1.1 angepasst durch Christian Kraus 23.05.2018
Verantwortlich	Christian Kraus

Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG

der

Infokom GmbH
Daimlerstraße 5d
76185 Karlsruhe

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Die Systeme auf denen Daten gespeichert werden, werden in zwei Rechenzentren mit Standort in Deutschland betrieben. Zu diesen Rechenzentren haben nur autorisierte Personen Zutritt. Der Zutritt wird 24x7 vor Ort überwacht. Nur Personen, die über eine Chipkarte und entsprechende Berechtigung verfügen, erhalten Zutritt zu den Rechenzentren. Der Zutritt zu den einzelnen Serverräumen wird durch Chipkarten gesteuert. Die Räume, der Eingang, sowie die verbaute Infrastruktur werden durch Kameras überwacht und sind durch Alarmanlagen, Bewegungsmelder, Brandmelder (inkl. Löschanlage), Wassermelder und Einbruchsmelder gesichert.

1. Jeder Zugang zu den Rechenzentren wird mit Datum und Uhrzeit erfasst und gespeichert.
2. Der Zutritt wird nur für autorisierte Zwecke eingeräumt.
3. Kameraüberwachung inkl. Bewegungsmeldern erfassen rund um die Uhr alle Bereiche des Rechenzentrums.
4. Der Zutritt erfolgt über den Ausweis für die einzelnen Sicherheitszonen.
5. Alle Besucher werden begleitet und haben keinen Zutritt zu sensiblen Bereichen.
6. Wartungspersonal wird begleitet und bei der Ausführung beaufsichtigt.

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

1. Für die Mitarbeiter gibt es einen Autorisierungsprozess.
2. Mitarbeitern werden Privilegien durch das Management zugewiesen und auch wieder entzogen.
3. Der Zugriff auf diese Systeme erfolgt ausschließlich über User – ID und Passwort.
4. Die Passwortvergabe erfolgt über eine Sicherheitsrichtlinie, deren Einhaltung regelmäßig überwacht wird.
5. Der Prozess zur Vergabe der Berechtigung ist dokumentiert und geprüft.
6. Alle IT-Systeme sind durch den Einsatz von Firewall- und Anti-Virensystemen geschützt.
7. Nach einer vordefinierten Zeit aktiviert sich ein Bildschirmschoner, der gleichzeitig den Arbeitsplatz sperrt. Die Wiedereingabe des Passworts ist bei Wiederaufnahme der Arbeit notwendig.
8. Arbeitsstationen (z.B. Notebooks), mit denen personenbezogene Daten verarbeitet werden, sind verschlüsselt.

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.

Die Netzwerksicherheit und Sicherheitsrichtlinien sorgen dafür, dass nur vertrauenswürdige Personen oder Organisationen unter Einhaltung allgemeiner Sicherheitsbeschränkungen freigegeben werden. Hierzu greifen folgende Maßnahmen:

1. Sicherheitscheck zur Überprüfung der Netze und Router
2. Einrichtungen von DMZs
3. Der Zugriff von Extern auf das Firmennetz erfolgt ausschließlich per VPN-Tunnel und 2-Faktor Authentifizierung.
4. Die Mitarbeiter mit Zugang zu sensiblen Bereichen, wie z.B. Serverraum, sind entsprechend geschult.
5. Sensible Daten werden durch den Einsatz von Aktenvernichtern entsorgt.
6. Daten/Datenträger werden gemäß DIN 66399 und DIN EN 15713 vernichtet.

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.

Auf allen Systemen, die vertrauenswürdige Daten speichern, wird ausschließlich mit gesicherten Protokollen (SSL, HTTPS, VPN) zugegriffen.

1. Bei der Weitergabe von Daten an Dritte werden vorher notwendige datenschutzrelevante Verträge vereinbart.
2. Der Datenverkehr wird sowohl von intern als auch von extern durch eine Firewall abgesichert.
3. Der Zugriff von extern auf das Firmennetz erfolgt ausschließlich per VPN-Tunnel und 2-Faktor Authentifizierung.
4. Die Weitergabe von personenbezogenen Daten erfolgt verschlüsselt. Zudem werden die Daten soweit möglich, vor der Übermittlung pseudonymisiert und nur die notwendigen Daten übertragen.

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.

1. Alle Systeme, vorbehaltlich der technischen Gegebenheiten bzw. Realisierungsmöglichkeiten, sind in ein umfangreiches Logging- und Monitoring-Konzept eingebunden. Dadurch wird gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem Daten in den jeweiligen DV-Systemen eingegeben, verändert oder entfernt worden sind.
2. Personenbezogene Daten werden ausschließlich über personalisierte Zugänge der autorisierten Person eingegeben, verändert oder gelöscht.
3. Rechte zur Eingabe, Änderung und Löschung von Daten werden auf Basis eines Berechtigungskonzepts vergeben.
4. Alle erfolgreichen und abgewiesenen Zugangsversuche von extern werden protokolliert (verwendete Kennung, Rechner, IP-Adresse).

6. Auftragskontrolle

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

1. Es wird überprüft, ob der Auftragnehmer einen Datenschutzbeauftragten bestellt hat. Entsprechende Auftragnehmer werden bevorzugt.
2. Gegenüber dem Aufragnehmer erfolgt eine schriftliche Weisung (z.B. Auftragsverarbeitungsvertrag).
3. Auftragnehmer sind verpflichtet, Ihre Mitarbeiter auf die Vertraulichkeit zu verpflichten.

7. Verfügbarkeitskontrolle

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

Alle Sicherheitseinrichtungen werden in regelmäßigen Abständen auf Ihre Betriebs- und Ausfallsicherheit hin überprüft.

1. Es existiert ein umfangreiches Backup- und Recoverykonzept.
2. Es ist ein Disaster-Recovery-Konzept, ein Notfallplan und eine Notfallkontaktliste, für die schnelle Wiederinbetriebnahme der Produktivumgebung erstellt worden.
3. Datensicherungen werden an einem sicheren Ort aufbewahrt.
4. Datenwiederherstellungen werden in regelmäßigen Zeitabständen getestet und nach Integrität überprüft.
5. Sämtliche IT-relevante Komponenten sind redundant ausgelegt. Diese Redundanz wird durch Hard- und Softwarelösungen, sowie Virtualisierungs-Lösungen realisiert.
6. Es sind Rauchmelde-, Lösch- und USV-Anlagen, sowie redundante Klimageräte vorhanden.

8. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Personenbezogene Daten können ausschließlich im Rahmen der Ablage durch den Auftraggeber auf dem zur Verfügung gestellten Speicherplatz, für die Nutzung der Dienste durch den Auftraggeber oder in Ausnahmefällen in dem ERP System gespeichert werden. In den ersten beiden Fällen werden die Daten zwar separat gespeichert, jedoch haben zugriffsberechtigte Personen (Administratoren) auf beide Datenspeicher Zugriff. Eine getrennte Erhebung oder Auswertung der Daten ist möglich. Im letzteren Fall haben nur Personen Zugriff auf die Daten, die über entsprechende Berechtigungsstufen im ERP System des Auftragnehmers bzw. seiner beauftragten Dritten verfügen.

1. Zwischen den verschiedenen Kundenbereichen besteht zu keinem Zeitpunkt eine Verbindung.
2. Es besteht eine Trennung zwischen Produktiv- und Testsystemen.
3. Es besteht eine Trennung zwischen dem Produktiv- Test und Gastnetzwerk.

9. Verfahren zur regelmäßigen Überprüfung der Wirksamkeit.

Maßnahmen, zum Sicherstellen und Einhalten der definierten Vorgehensweisen, sowie zu Anpassung der Verfahren an geänderte Gegebenheiten.

1. Alle Server und Clients unterliegen einem automatisierten zentralen Patchmanagement. Somit werden Sicherheitslücken in den Systemen zeitnah behoben.
2. In regelmäßigen Abständen werden externe Dienstleister beauftragt, Penetrationstests auf bei uns eingesetzte Systeme zu fahren. Hierbei sollen Sicherheitslücken aufgedeckt und dann auch geschlossen werden.
3. Jährlich werden in Stichproben die definierten Maßnahmen geprüft und bei Verstößen oder anderen Feststellungen diese angepasst. Hiermit soll ein größtmögliches Maß an Sicherheit der Daten und der Systeme gewährleistet werden.