Datenschutzkonzept

Präambel

Als IT-Dienstleister sind unsere Hauptaufgaben die kompetente Beratung und Implementierung komplexer IT Infrastruktur bei unseren Kunden. Dabei stehen sowohl die Sicherheit der eigenen Infrastruktur, als auch die unserer Kunden an erster Stelle.

Datenschutzpolitik und Verantwortlichkeiten im Unternehmen

- Die Sicherheit und Verfügbarkeit der internen IT, die unserer Kunden und die Umsetzung der Anforderungen nach DS-GVO (Vertraulichkeit, Verfügbarkeit, Integrität) sind unser oberster Anspruch.
- Kontinuierliche Anpassung und Verbesserung unserer Prozesse, Kenntnisse und eingesetzten Systeme sind die Grundvoraussetzung für den Erfolg unseres Unternehmens und unserer Kunden.
- Verantwortlich für die technische und operative Umsetzung nach DS-GVO:
  Norbert Horn, Geschäftsführer

Rechtliche Rahmenbedingungen im Unternehmen

- Für die Ausführung der vereinbarten IT Dienstleistungen beim Kunden vor Ort oder über Fernwartung, gelten für uns die Grundsätze höchster Vertraulichkeit.
- Wir erheben, verarbeiten und speichern ausschließlich Daten, die für die Durchführung unserer Geschäftsziele oder des vertraglich vereinbarten Leistungsumfanges nötig, bzw. vom Gesetzgeber gefordert sind.
- Persönliche Daten werden nur so lange gespeichert, wie notwendig, bzw. vom Gesetzgeber gefordert.
- Generell werden keine Informationen an Dritte, ohne Zustimmung des Betroffenen, weitergegeben.
- Die Datenverarbeitung erfolgt auf Basis der Rechtsgrundlage des Art. 6 Abs. 1 lit. a), b) und c) DS-GVO.

Dokumentation

- Für die Erfüllung der Anforderungen nach DS-GVO führen wir die geforderten Verfahrensverzeichnisse zu unseren Verarbeitungstätigkeiten
- Erhöhte Sicherheitsrisiken und die geeigneten Gegenmaßnahmen dokumentieren wir in der Datenschutzfolgeabschätzung (derzeit keine erhöhten Risiken identifiziert).

Bestehende technische und organisatorische Maßnahmen (TOM)

Zutrittskontrolle:
Der Zugang zu unseren Büroräumen ist nur mit elektronischem Schlüssel möglich. Bei Verlust eines Schlüssels werden alle verbleibenden Schlüssel umprogrammiert und damit wird der verlorene Schlüssel unbrauchbar.
Der Eingangsbereich ist Videoüberwacht.

Zugriffskontrolle:
Wir verwalten den Zugriff auf unsere Systeme über Zugriffsberechtigungen. Diese werden nach Aufgabenbereich angelegt und verhindern unberechtigten Zugriff auf Datenbanken oder Systeme, die nicht für die tägliche Arbeit benötigt werden. Die Passwörter werden regelmäßig erneuert.
Bei Kommunikation mittels eMail mit vertraulichen Inhalten, werden die eMails verschlüsselt gesendet.

Clients:
Unsere Clients sind vom Benutzer mit einem Passwort gesichert. Dieses wird regelmäßig erneuert und besteht aus einer Kombination aus Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen. Bildschirme werden automatisch nach einer eingestellten Zeit von 120 Sekunden gesperrt, des Weitern sind die Benutzer angewiesen die Bildschirmsperre bei Verlassen des Rechners händisch zu aktivieren. Mobiltelefone sind über eine Mobile Device Management Lösung verwaltet und können bei Verlust sofort auf Werkseinstellung zurückgesetzt werden. Ein Verlust ist umgehend mitzuteilen, damit die entsprechenden Maßnahmen ergriffen werden können.

Server:
Unsere Server sind mit einem redundanten Netzteil und einer unterbrechungsfreien Stromversorgung gesichert. Die virtuellen Server sind teils redundant auf ein Zweitsystem ausgelegt.

Backup:
Die Systeme werden täglich auf NAS gesichert. Einmal pro Woche werden sämtliche Sicherungen mit wechselnden Speichermedien gesichert. Alle Sicherungen sind verschlüsselt, dass bei Verlust eines Datenträgers die Daten sicher sind.

Netzwerk:
Sowohl LAN als auch WLAN befinden sich in einem geschützten, passwortgesicherten Bereich.

Weitere Security Komponenten:
Unser Netzwerk und die Kommunikation werden mit einer Firewall mit automatischer Update Funktion, und Virenschutz gesichert. Als Antispam-Lösung kommt ein E-Mail Gateway zum Einsatz.