Technische und Organisatorische Maßnahmen gem. Art. 32 DSGVO der

Thomas Hirt und Partner GmbH

Stand: 02/2018

Zutrittskontrolle

- Die Geschäftsräume der Thomas Hirt und Partner GmbH können nur durch befugte Personen betreten werden.
- Betriebsfremde Personen werden vom Sekretariat in Empfang genommen und zu ihrem Termin begleitet. Die Räumlichkeiten sind durch eine Schlüsselregelung gesichert.
- Die Server sind in einem abgeschlossenen Raum untergebracht, zu dem nur berechtigte Personen Zutritt erlangen.
- Die Datensicherungsmedien werden in einem zugangsgeschützten Tresor außerhalb der Geschäftsräume aufbewahrt.

Zugangskontrolle

- Der Zugang zur technischen Arbeitsumgebung ist durch Benutzername und Passwort geschützt.
- Es existiert eine Passwort-Richtlinie, welche eine gewisse Komplexität und Länge des Passworts erfordert.
- Der Arbeitsplatzrechner wird nach zehnminütiger Inaktivität automatisch gesperrt.
- Nicht mehr benötigte Zugangsberechtigungen werden taggleich mit Austritt oder Zuständigkeitswechsel entzogen.
- Die Benutzeranmeldungen werden systemseitig protokolliert.
- Die Arbeitsplatzrechner werden durch Anti-Viren-Software geschützt.
- Die Serverlandschaft wird durch eine Firewall geschützt.
- Homeoffice oder Fernwartung ist ausschließlich über gesicherte Verbindungen (VPN) möglich.
- Das Reinigungspersonal wurde auf das Betriebsgeheimnis verpflichtet.

Zugriffskontrolle

- Es bestehen klare Regelungen, dass ausschließlich Personen die mit der Erhebung, Nutzung und Verarbeitung der Daten im Rahmen der vereinbarten Auftragsdatenverarbeitung betraut sind, auch berechtigt sind, die Daten zu lesen, zu ändern und zu kopieren. Die Löschung von Daten ist nur autorisierten Personen erlaubt. Diese Regelungen werden durch differenzierte Vergabe von Zugriffsberechtigungen umgesetzt.

- Sofern Auftragsdatenverarbeiter, welche im Internet im Bereich Datenschutz aufgeführt und aktuell gehalten werden, einen Zugriff auf die technische Infrastruktur erhalten, greifen auch diese über eine gesicherte Verbindung zu.
- Papierunterlagen werden vom Mitarbeiter bei Verlassen des Arbeitsplatzes in abschließbaren Schränken vor unbefugtem dem Zugriff geschützt. Die Mitarbeiter sind angehalten, weitgehendstes papierlos zu arbeiten.

Weitergabekontrolle

- Die Verwendung von Speicherungsmedien mit sensiblen Daten außerhalb der Geschäftsräume ist verboten.
- Die Datenvernichtung in Papierform erfolgt durch Sammlung in einem abgeschlossenen Behältnis und regelmäßiger zertifizierter Entsorgung. Ausrangierte Datenträger werden ebenfalls zertifiziert entsorgt und vernichtet.
- Der E-Mailserver bietet die Möglichkeit der TLS-Verschlüsselung.
- Werden Daten in Form von Listen auf elektronischem Weg weitergegeben, so werden diese zusätzlich als ZIP-Archiv verschlüsselt.
- Werden Daten auf Webseiten bereitgestellt, so werden diese SSL-verschlüsselt.

Eingabekontrolle

- Die Eingaben in die Verwaltungssysteme werden innerhalb dieser protokolliert.
- Administrationstätigkeiten werden ebenfalls protokolliert.

Auftragskontrolle

- Sofern einzelne Prozesse an Dienstleister ausgegliedert werden, bestehen entsprechende Vereinbarungen, welche Art, Umfang und Zweck dieser Tätigkeiten regeln.
- Auftragsdatenverarbeitungen, welche Cloud-Lösungen nutzen, werden in EU Rechenzentren gehostet. Die Kommunikation der Webdienste erfolgt verschlüsselt.

Verfügbarkeitskontrolle

- Die erfassten Daten werden vor Zerstörung oder Verlust geschützt und regelmäßig, i.d.R. stündlich, mindestens aber täglich, gesichert.
- Für die Wiederherstellung des Geschäftsbetriebs im Notfall existiert ein entsprechender Notfallplan.

Trennungsgebot

- Die personenbezogenen Daten der verschiedenen Auftraggeber werden logisch getrennt.