Technische und organisatorische Maßnahmen der Foto Raabe GmbH nach Art. 32 DSGVO

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

Getroffene Maßnahmen:

Der Zutritt zum Gebäude, von dem heraus auf personenbezogene Daten des Verantwortlichen zugegriffen wird, ist nur befugten Personen gestattet bzw. möglich.

Es erfolgt eine Erfassung des Zutritts per Chip, was softwarebasiert dokumentiert wird.

Das Gebäude, in denen sich Räumlichkeiten der Foto Raabe GmbH befinden, verfügt über eine zentrale Schließanlage. Die Schlüsselvergabe und das Verhalten bei Verlust sind geregelt.

Besucher, die Zutritt zum Gebäude erhalten, in dem personenbezogene Daten des Verantwortlichen verarbeitet werden, werden begleitet oder auf Vertraulichkeit verpflichtet.

Hardware im Büro ist gegen unbefugten Zugang gesichert.

Soweit die Auftragstätigkeit für den Verantwortlichen eine Verarbeitung in einer besonderen Schutzzone erfordert, ist sichergestellt, dass für die zugehörigen Räume dieser Schutzzone besondere Zutrittsmittel nötig sind, die dazu beitragen, dass nur Befugte Zutritt zu diesen Schutzzonen erhalten

Am Standort eingesetztes Fremdpersonal (z. B. Reinigungskräfte, Sicherheitskräfte, Hausmeister) ist auf Vertraulichkeit verpflichtet worden.

Es gibt eine Alarmanlage mit direkter Verbindung zum Sicherheitsdienst, eine Videoüberwachung und Sicherheitsschlösser.

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

Getroffene Maßnahmen:

Die zur Verarbeitung eingesetzten Server befinden sich in einem Serverraum, der als besondere Schutzzone behandelt wird.

Im Serverraum, in dem sich Server befinden, mit deren Hilfe personenbezogene Daten des Verantwortlichen verarbeitet werden, befinden sich keine Wasserleitungen ohne ausreichenden Überlaufschutz und keine unnötigen Brandlasten.

Wartungstätigkeiten durch Fremdpersonal erfolgen im Serverraum nur unter Beaufsichtigung.

Der Serverraum ist immer abgeschlossen. Nur Berechtigte haben Zugang mit einem Schlüssel.

Der Server wird nur mit personalisierten Administratoren-Accounts betrieben.

Bei den eingesetzten Servern und zur Verarbeitung genutzten Netzwerkkomponenten wurden etwaige Standardpasswörter neu gesetzt.

Soweit zur Administration des Servers funktionale Accounts genutzt werden, werden die Kennwörter dieser Accounts neu gesetzt, sobald ein zugangsbefugter Admin aus dem Team ausgeschieden ist.

Der Zugang zu den Datenverarbeitungsanlagen erfolgt ausnahmslos mit Zwei-Faktor Authentifizierung (ist der absolute Idealfall) -Initialpasswörter werden ausnahmslos computergeneriert.

Erforderliche Sicherheitspatches werden zeitnah eingespielt.

Die zur Auftragserledigung genutzte Infrastruktur wird mit tagesaktuellen Virenscannern vor Malware geschützt.

Es besteht eine ausreichende Netzwerksegmentierung und Netzwerksegregation.

Die Durchführung der Auftragsarbeiten wird mindestens einmal pro Jahr hinsichtlich der Wirksamkeit getroffener Maßnahmen kontrolliert.

Wenn das Serversystem insgesamt oder für den Betrieb des Serversystems eingesetzte Komponenten ausgewechselt werden sollen, ist sichergestellt, dass sich auf zu entsorgenden Datenträgern keine lesbaren Daten des Verantwortlichen mehr befinden.

Wenn Datenträger entsorgt werden sollen, die Daten des Verantwortlichen enthalten, welche mittels des eingesetzten Serversystems gespeichert, übertragen oder ausgewertet werden, werden diese Datenträger entweder physisch zerstört oder mittels einer Löschungssoftware so überschrieben, dass eine Rekonstruktion der Daten mit vertretbarem Aufwand nicht mehr möglich ist.

Die Client-Systeme der Personen, die im Rahmen der Auftragserledigung auf personenbezogene Daten des Verantwortlichen zugreifen, weisen einen Bildschirmschutz auf, der nach ausreichend kurzer Zeit der Inaktivität, eine automatische Sperrung auslösen, die nur durch Eingabe eines Kennwortes aufgehoben werden kann. Eine Sperrung des Bildschirms erfolgt nach 5 Minuten.

Mitarbeiter melden sich an ihrer Workstation ab, wenn sie den Arbeitsplatz verlassen, um z.B. in die Pause gehen.

Mitarbeiter fahren ihre Workstation runter, wenn sie das Haus verlassen.

Benutzerpasswörter der zur Auftragserledigung eingesetzten Personen weisen eine hohe Passwortkomplexität mit mindestens acht Zeichen und unter Verwendung von Groß-, Kleinbuchstaben, Zahlen und Sonderzeichen auf.

Zugangsberechtigungen werden mit Ende der Gültigkeit der Berechtigungen unverzüglich gesperrt.

Personen, die personenbezogene Daten des Verantwortlichen verarbeiten, werden über die von ihnen einzuhaltenden Pflichten informiert.

Im laufenden Betrieb festgestellte Sicherheitsvorfälle, die personenbezogene Daten des Verantwortlichen betreffen, werden dem Verantwortlichen unverzüglich gemeldet.

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.

Getroffene Maßnahmen:

Das Anlegen, Ändern und Löschen von Nutzerprofilen erfolgt durch einen auf das Datengeheimnis verpflichteten Systemadministrator. Die Rechtevergabe erfolgt angepasst nach dem Tätigkeitsgebiet des jeweiligen Mitarbeiters.

Zur Erkennung unbefugter Zugriffe von außen werden die Firewall-Protokolldaten regelmäßig nach dem 4-Augen-Prinzip überprüft.

Es bestehen Regelungen zur revisionssicheren Speicherung von Protokolleinträgen und zur Protokollierung unbefugten Einloggens bzw. Überschreitens der Zugriffsbefugnisse wie auch von Fehlermeldungen

Es besteht eine logische Kundentrennung, die gewährleistet, dass jeweils nur auf die Daten eines Auftraggebers zugegriffen werden kann.

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.

Getroffene Maßnahmen:

Sendende und empfangende Stellen werden bei der Datenübertragung protokolliert.

Daten werden ausschließlich verschlüsselt übertragen (SSL oder SSH oder VPN).

Daten auf mobilen Geräten werden ausschließlich verschlüsselt übertragen.

Es bestehen sichere Regelungen zur Löschung von Datenträgern vor der Wiederverwendung bzw. im Fall des Austauschs oder der Aussonderung von Geräten.

MS-Office-Werkzeuge sind so konfiguriert, dass die Erzeugung und Speicherung von Metadaten auf das Notwendigste reduziert ist.

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.

Getroffene Maßnahmen:

Es ist schriftlich dokumentiert, wann welche Person aufgrund welcher Aufgabenstellung personenbezogene Daten in der Datenverarbeitungsanlage eingeben, verändern oder löschen darf. Dies wird protokolliert und die Protokolle werden regelmäßig überprüft.

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

Getroffene Maßnahmen:

Daten des Auftraggebers werden allein von diesem in das System eingegeben und gesteuert.

Der Auftragnehmer unterstützt den Aufraggeber gemäß der vorliegenden Auftragsverarbeitungsvereinbarung und informiert seine Mitarbeiter über die sich daraus ergebenden Pflichten.

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

Getroffene Maßnahmen:

Für die Server besteht eine sichere und ausreichend robuste Default-Einstellung, um einen abgesicherten Wiederanlauf des Serversystems in der vorgesehenen Zeit durchführen zu können.

Für die gespeicherten personenbezogenen Daten besteht eine Datensicherung nach dem Stand der Technik.

Zur Datensicherung eingesetzte Medien werden im Rahmen der Archivierung getrennt von produktiven Servern, mit denen personenbezogene Daten des Verantwortlichen verarbeitet werden, aufbewahrt.

Die Wirksamkeit von Datensicherungen wird regelmäßig durch Wiedereinspieltests überprüft.

Server, auf denen personenbezogene Daten des Verantwortlichen gespeichert werden, verfügen über eine ausreichend dimensionierte unterbrechungsfreie Stromversorgung.

Die gespeicherten personenbezogenen Daten werden nach Ablauf der festgelegten Speicherdauer gelöscht.

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

Getroffene Maßnahmen:

Die Daten unterschiedlicher Auftraggeber werden getrennt voneinander gespeichert, so dass ein isolierter Zugriff auf diese Daten unter Ausschluss der Möglichkeit der Verknüpfung mit anderen Daten gewährleistet ist.

Organisation im Unternehmen

Es besteht ein Datenschutzkonzept mit Richtlinien zum Umgang mit Hard- und Software durch Mitarbeiter, Auskunftsrechten von Nutzern, Regelungen zur Auftragsverarbeitung sowie dem Verhalten bei Datenpannen.

Die Mitarbeiter wurden geschult und sind auf das Datengeheimnis verpflichtet.