

Technische und organisatorische Maßnahmen zur Datensicherheit

Bei der constancy GmbH wurden nachfolgende technische und organisatorische Maßnahmen zur Datensicherheit im Sinne des Art. 32 DSGVO getroffen.

Vertraulichkeit

Zutrittskontrolle

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

1. Die Büroräume der constancy GmbH befinden sich in einem Mietobjekt in der August-Bebel-Straße 27b in Jena.
2. Der Hauptzugang wird von mehreren Mietern geteilt und ist meist nicht verschlossen.
3. Der Eingang zu den Büroräumen in der ersten Etage ist verschlossen. Zugang zu den Räumlichkeiten haben nur Mitarbeiter:innen der Firma.
4. Für Besucher:innen gibt es am Eingang eine Klingel. Die Tür wird durch jemanden aus der Belegschaft geöffnet und Besucher:innen werden zu ihrem jeweiligen Ansprechpartner begleitet.
5. Die Eingangstür ist von den Büroräumen einsehbar. Diese schließt automatisch.
6. In Zeiten, in denen die Büros voraussichtlich nicht besetzt sind, findet eine Videoüberwachung statt. Die Kamera ist u.a. auf die Eingangstür ausgerichtet und reagiert auf Bewegung. Damit soll der unberechtigte Zutritt protokolliert werden.
7. Neben der zentralen Eingangstür gibt es eine zweite Tür. Diese befindet sich im Treppenhaus rechts neben der Eingangstür. Die Tür endet in den Büroräumen, welche tagsüber regelmäßig besetzt sind. Die Tür soll immer verschlossen gehalten werden und dient lediglich als Fluchtweg. Allerdings wird beim Betätigen der Tür das Schloss geöffnet und die Tür ist danach von außen offenbar. Die Mitarbeiter:innen sind angehalten in dem Falle die Tür wieder zu verschließen. Beim abendlichen Verlassen der Büroräume wird kontrolliert, ob diese Tür verschlossen ist.
8. Über den Parkplatz existiert ein Aufgang zu einem gemeinsam genutzten Balkon. Vom Balkon aus gibt es eine Balkontür, durch die Personen Zutritt zu den Räumen erhalten können. Diese Tür ist entweder über den Türgriff verschlossen oder offen, wenn auch die Büroräume besetzt sind. Fenster und Türen werden durch eine zweite Kamera überwacht.
9. Angrenzend zu der obigen Balkontür befinden sich Fenster. Diese sind ggf. einfach zugänglich. Alle weiteren Fenster liegen oberhalb der Straße und sind nicht mit einfachen Mitteln erreichbar. Dennoch sollen die Fenster beim Verlassen der Büros verschlossen werden.

10. Innerhalb des Objekts werden keine Kundensysteme betrieben. Diese befinden sich auf Servern in Rechenzentren außerhalb der Betriebs- und Geschäftsräume.
11. Aus obigem Grund wurden auf die Etablierung von Sicherheitsbereichen verzichtet. Ebenfalls gibt es keine weitergehenden Zugangsregelungen.
12. Besprechungen mit Betriebsfremden finden in einem separaten Besprechungsraum statt.

Zugangskontrolle

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

Um Unbefugten den Zugang zu IT-Systemen zu verwehren, wurden seitens der constancy GmbH folgende Maßnahmen getroffen:

1. Die Beschäftigten der constancy GmbH verfügen über Notebooks zur Erfüllung der dienstlichen Aufgaben.
2. Jeder Person ist dabei ein Gerät zugeordnet. Es ist nicht vorgesehen, dass Geräte untereinander geteilt werden. Neben dem administrativen Zugang verfügen die Geräte nur über ein Konto für die jeweiligen Benutzer.
3. Mitarbeiterinnen und Mitarbeiter arbeiten mit Nutzerrechten an den zugewiesenen Geräten. Das Passwort zur Administration ist nur zur Administration befugten Personen bekannt.
4. Der Zugang zu IT-Systemen erfolgt mittels eines Benutzernamens und dazugehörigem Passwort. Der Benutzername wird in der Regel bei Betriebseintritt vergeben. Dazu wird mittels der Software 1Password ein zufälliges Passwort erzeugt, welches durch den Benutzer zu ändern ist. Die Mitarbeiter sind angehalten 1Password für die Verwaltung ihrer Zugänge zu nutzen. Dort werden auch Standardzugänge für verschiedene Systeme verwaltet.
5. Standardmäßig verlangt das System eine Passwortlänge von 16 Zeichen. Dieses muss aus Buchstaben, Zahlen und Sonderzeichen bestehen. Allerdings kann ein Benutzer auch ein Passwort mit einer geringeren Komplexität wählen. Ein regelmäßiger Wechsel der Passwörter ist nicht vorgesehen. Passwörter werden in einer nicht rückführbaren Form (Hashwerte) gespeichert.
6. Es ist erlaubt und gewünscht, dass die verwendeten Passwörter in einem Passwort-Manager verwaltet werden. Dieser Passwort-Manager ist mit einem Generalpasswort zu versehen, welches eine Mindestlänge von 15 Stellen hat. Die Geschäftsführung hat Empfehlungen für derartige Software gegeben.
7. Die Zugangsberechtigungen zu Fremdsystemen werden dokumentiert.
8. Ein Einsatz mobiler Datenträger erfolgt nicht. Daher sind keine Maßnahmen zur Verschlüsselung dieser Geräte im Einsatz.
9. Bei weiteren IT-Systemen (Router, Officegeräte, Handys etc.) wird geprüft, ob herstellerseitig Passwörter oder andere Standardzugänge vergeben wurden. Sofern dies der Fall ist, werden die Passwörter durch sichere Varianten ersetzt. Die Passwörter werden geschützt abgelegt und sind nur der Geschäftsleitung sowie dazu befugtem Personal zugänglich.

Zugriffskontrolle

Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten personenbezogenen Daten Zugang haben.

1. Die Firma constancy setzt keine mobilen Datenträger ein. Daher beschränken sich die unten stehenden Betrachtungen auf Datenträger, die in den Geräten verbaut sind.
2. Die Laptops und andere Arbeitssysteme werden mit Festplatten beschafft.
3. Für den Fall, dass ein Datenträger defekt ist, wird Ersatz beschafft.
4. Der defekte Datenträger wird entweder durch mehrfaches Überschreiben vernichtet oder physisch zerstört.
5. Die Mitarbeiterinnen und Mitarbeiter arbeiten lokal auf deren Geräten. Innerhalb der Firma existiert ein Netzlaufwerk dessen Zugriff mittels Passwort geschützt ist.
6. Die Geschäftsführung bzw. ein von ihr benannter Mitarbeiter legt Zugriffsberechtigungen für fremde Systeme fest. Diese werden bei der Einrichtung eines Zugangs so eingestellt.
7. Die Zugriffsberechtigungen werden regelmäßig, mindestens jedoch einmal jährlich geprüft und ggf. angepasst.

Trennung

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

1. Die IT-Systeme, auf denen Daten im Auftrag verarbeitet werden, sind mandantenfähig. Es ist sichergestellt, dass Daten getrennt voneinander verarbeitet werden. Dies ist auch dann der Fall, wenn Daten für gleiche Zwecke verarbeitet werden.

Auftragskontrolle

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

1. Der Schutz personenbezogener Daten und auch der Schutz von Betriebs- und Geschäftsgeheimnissen hat bei der constancy GmbH eine hohe Priorität. Alle Mitarbeiter:innen sind auf das Datengeheimnis verpflichtet.
2. Alle Mitarbeiter:innen erhalten eine Schulung zum Datenschutz. Diese wird regelmäßig aufgefrischt.
3. Die Datenschutzvorkehrungen der constancy GmbH beinhalten auch eine regelmäßige Überprüfung und Bewertung der getroffenen technischen und organisatorischen Maßnahmen zur Datensicherheit. Die Belegschaft kann sich mit Verbesserungsvorschlägen beteiligen. Die constancy gewährleistet so eine kontinuierliche Verbesserung der Prozesse im Umgang mit personenbezogenen Daten.

Pseudonymisierung und Verschlüsselung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

1. Eine Pseudonymisierung personenbezogener Daten ist derzeit nicht geplant.

Integrität

Eingabekontrolle

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.

1. Änderungen an personenbezogenen Daten können von der Belegschaft durchgeführt werden.
2. Sofern Daten durch Mitarbeiterinnen oder Mitarbeiter geändert werden, werden alle Aktionen innerhalb der Software aufgezeichnet. Es ist nachvollziehbar, welche Änderungen vorgenommen wurden.
3. Die Notebook-Rechner setzen Mac OS als Betriebssystem ein.
4. Die Rechner der Firma besitzen einen Schutz von Schadsoftware. Eine regelmäßige Aktualisierung der Antiviren-Software wie auch der Virensignaturen ist konfiguriert. Eine Prüfung auf Updates erfolgt einmal täglich. Updates werden automatisiert eingespielt.
5. Bei anderer Software werden ebenfalls automatische Update-Prozesse, sofern vorhanden, verwendet. Sollte Software dies nicht anbieten, ist die Belegschaft angewiesen, regelmäßige Prüfungen (mindestens aber einmal pro Woche) auf Updates durchzuführen.
6. Die Daten und Programme auf den Arbeitsplatzrechnern sind in unterschiedlichen Bereichen, getrennt voneinander, gespeichert.

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können. Dabei ist weiterhin zu klären, welche Daten protokolliert werden, wer Zugriff auf Protokolle hat, durch wen und bei welchem Anlass/Zeitpunkt diese kontrolliert werden, wie lange eine Aufbewahrung erforderlich ist und wann eine Löschung der Protokolle stattfindet.

1. Seitens der constancy werden keine externen Datenträger verwendet. Daher existieren keine Prozesse zum Versand oder zur Weitergabe von Datenträgern.
2. Aus obigen Gründen ist eine Aufbewahrung externer Datenträger nicht geregelt.
3. Sollten sich diesbezüglich Änderungen ergeben, ist geplant, Regelungen zur Weitergabe, Aufbewahrung, Vernichtung und ggf. weiterer Sachverhalte zu treffen.

4. Zur Weitergabe von Daten wird das Internet genutzt.
5. Die Übertragung personenbezogener Daten erfolgt über HTTP. Alle Verbindungen sind mittels TLS verschlüsselt. Dabei kommt mindestens Version 1.1. In der Regel Version 1.2 zum Einsatz. Für TLS kommen nur Algorithmen in Frage, die laut der Technischen Richtlinie 02102 des Bundesamtes für Sicherheit in der Informationstechnik (BSI TR-02102) der Stand der Technik sind.
6. Die constancy prüft die Übertragungswege in regelmäßigen Abständen und passt die Mittel an den jeweiligen Stand der Technik an.
7. Wenn Mitarbeiterinnen und Mitarbeiter andere Arbeitsbereiche erhalten oder nicht mit den entsprechenden personenbezogenen Daten betraut sind, werden diesen Zugänge entzogen.
8. Sofern Personen das Unternehmen verlassen, werden alle Zugänge zu den IT-Systemen gesperrt.
9. Sofern es gemeinsam genutzte Ressourcen gibt, werden die Passwörter nach dem Ausscheiden geändert.

Verfügbarkeit und Belastbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. Hier geht es um Themen wie eine unterbrechungsfreie Stromversorgung, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.

1. Die Speicherung personenbezogener Daten erfolgt nicht auf den Geräten der Belegschaft. Dort ist maximal eine Zwischenspeicherung vorgesehen.
2. Die Belegschaft ist angewiesen, personenbezogene Daten dauerhaft auf externen Systemen zu speichern.
3. Die Laptops sind mit Standardsoftware installiert und können bei Ausfall schnell durch ein Zweitgerät ersetzt werden.
4. Bei externen Dienstleistern wird ein regelmäßiges Backup vertraglich zugesichert.

Datenschutzfreundliche Voreinstellungen

1. Vor dem Start der Verarbeitung findet eine Prüfung des Zwecks der Verarbeitung statt und es wird festgelegt, welche personenbezogenen Daten erforderlich sind. Damit wird insbesondere dem Grundsatz der Datenminimierung Rechnung getragen.
2. Betroffene können ihr Widerrufsrecht über einfache Kommunikationswege ausüben.