MÄUSCHEN
Mein Tag in der Kita

Technische und Organisatorische Maßnahmen

1. Zutrittskontrolle

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

Das Unternehmen hat kein eigenes Betriebsgelände. Der Zutritt zu den Büroräumen ist durch Türen mit Schlössern gesichert. Außerhalb der Arbeitszeiten ist der Haupteingang des Bürogebäudes Video-überwacht. Mitarbeiter gelangen mit einem Schlüssel in die Büroräume und zu den Arbeitsplätzen. Die Reinigungsfirma kommt mit Hilfe eines Schlüssels in die Büroräume. Die Ausgabe und der Einzug von Schlüsseln werden dokumentiert.

Besucher werden aus dem öffentlichen Bereich des Bürogebäudes von einem Mitarbeiter abgeholt und in den jeweiligen Konferenzraum begleitet. Das Betreten von weiteren Räumlichkeiten erfolgt ausschließlich in Begleitung eines Mitarbeiters.

Ungenutzte Papierakten werden in verschließbaren Räumen und Schränken verstaut.

Ungenutzte Hardware wird abgeschlossen. Zugriff hierauf hat nur die Geschäftsführung.

Das Unternehmen hat keine eigenen Server.

Als ausgelagerter Server wird OVHcloud in einem deutschen Rechenzentrum (Frankfurt/Main) genutzt, mit einer Datenreplikation in zwei französischen Rechenzentren (Gravelines und Straßburg) für geografisch getrennte Backups (siehe auch Abschnitt *Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)*). OVHcloud ist u.a. nach ISO/IEC 27001, 27017, 27018 und 27701, nach PCI DSS sowie nach SOC 1 TYPE II und SOC 2 TYPE II zertifiziert. Mit OVHcloud wurde ein Auftragsverarbeitungsvertrag geschlossen, der die Erfüllung von gleichwertigen Verpflichtungen sicherstellt, wie sie von uns (als Datenverarbeiter) verlangt und in unserem Auftragsverarbeitungsvertrag zugesichert werden. Die von OVHcloud ergriffenen technischen und organisatorischen Maßnahmen wurden geprüft und dokumentiert (siehe auch https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml).

2. Zugangs- und Zugriffskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können sowie, dass die berechtigten Personen ausschließlich innerhalb ihrer Berechtigung am Datenverarbeitungssystem arbeiten.

Zugang zur Mäuschen App durch Kunden

Für die Web App erhalten jeder Kunde sowie die von ihm eingesetzten Benutzter einen individuellen Benutzeraccount mit einem individuellen zu generierenden Benutzerpasswort. Die Passwörter müssen mindestens 12 Zeichen lang sein und einen Groß-, Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten.

Der Zugriff auf Daten des Kunden mit der Mobile App ist ausschließlich nach der Koppelung eines Geräts über einen dazu berechtigten Web App Account möglich. Nach der Koppelung ist der Zugriff

auf die Mobile App auf dem gekoppelten Gerät zusätzlich durch eine vom Kunden festgelegte PIN geschützt.

Sowohl für die Web App als auch für die Mobile App wird der Zugriff nach dreimaliger Falscheingabe des Passworts bzw. der PIN gesperrt. Eine erfolgreiche Authentifikation wird in der Web App nach fünfminütiger und in der Mobile App nach einminütiger Inaktivität aufgehoben.

Der Kunde kann entscheiden, auf den PIN-Schutz einer Mobile App Instanz zu verzichten, sofern das gekoppelte Gerät seinerseits durch eine PIN und ausreichende Sicherheitseinstellungen geschützt ist (mindestens Zahlen-PIN, Sperre bei mehrmaliger Falscheingabe, automatische Sperre nach Inaktivität).

Zugang zur Mäuschen App durch Mitarbeiter

Eine Zugriffsberechtigung für Auftraggeber-bezogene Daten besitzt ausschließlich die Geschäftsführung. Weitere Zugriffsberechtigungen darauf werden nur in Einzelfällen restriktiv nach der Regel der geringsten Berechtigung erteilt, dokumentiert und wieder entzogen.

Mitarbeiter-Zugänge zu internen Systemen und vom Unternehmen verwendeten Services

Die Ausgabe und Rücknahme an Mitarbeiter ausgehändigter unternehmenseigener Hardware wird dokumentiert.

Im Unternehmen sind verschiedene Zugangsebenen geregelt, so dass jeder Mitarbeiter nur die Berechtigungen im IT-System erhält, die er für seine Tätigkeit auch benötigt. Alle Berechtigungen jedes einzelnen Mitarbeiters sind dokumentiert.

Jedem Mitarbeiter wird beim Einstieg in das Unternehmen ein individueller Benutzeraccount zugeteilt, für den er bei der Aktivierung ein persönliches Passwort wählen und einen zweiten Authentifizierungsfaktor festlegen muss (Hardware-Token oder App). Bei der Festlegung wird das Passwort systemseitig mit einer Liste häufiger Passwörter sowie einem globalen Verzeichnis gehackter Passwörter abgeglichen. Passwörter müssen außerdem mindestens 12 Zeichen lang sein und einen Groß-, Kleinbuchstaben, eine Zahl und ein Sonderzeichen enthalten. Der Name darf nicht enthalten sein. Das Passwort muss exklusiv sein und darf für keinen anderen beruflichen oder privaten Account des Mitarbeiters verwendet werden. Nach dreimaliger Falscheingabe des Passwortes wird der Benutzerzugang automatisch gesperrt.

Auch alle weiteren webbasierten Programme und Anwendungen sind jeweils mit einem Mitarbeiter-spezifischen Passwort geschützt. Die Vorgaben zur Verwendung und Sicherheit von Passwörtern sind in einer Passwortrichtlinie festgehalten. Jedes Passwort ist exklusiv zu vergeben und über einen vom Unternehmen bereitgestellten und gewarteten Passwortgenerator zu erstellen, der die Einhaltung der Passwortrichtlinie systematisch sicherstellt. Passwörter dürfen ausschließlich verschlüsselt im unternehmenseigenen oder einem vom Unternehmen freigegebenen Passwortmanager gespeichert werden, demgegenüber keinesfalls im Klartext bzw. auf Papier.

Jeder von Mitarbeitern verwendete PC ist mit einem Passwort geschützt. Nach einer Inaktivität von 15 Minuten wird der PC-Bildschirm automatisch gesperrt. Alle Mitarbeiter sind angewiesen, den Bildschirm zu sperren, sobald sie ihren Arbeitsplatz – auch nur für kurze Zeit – verlassen.

Hardware-Zugänge

Personenbezogene Daten sowie sämtliche weiteren Mitarbeiter- und Kundendaten werden ausschließlich auf verschlüsselten Datenträgern gesichert und/oder ihrerseits hochsicher verschlüsselt gespeichert (einschließlich Backups). Die Schlüssel sind bei von Mitarbeitern genutzter Hardware nur dem jeweiligen Mitarbeiter, bei auf externer Hardware gespeicherten Daten der Geschäftsführung bekannt. Weitere Zugriffsberechtigungen darauf werden restriktiv nach der Regel der geringsten Berechtigung erteilt und dokumentiert.

Die externen Server von OVHcloud werden durch Virenschutz, Firewalls, Monitoring und regelmäßige Sicherheitsupdates der Systeme geschützt.

Das WLAN ist WPA2 verschlüsselt.

Alle Mitarbeiter-PCs sind mit einem Enterprise Level Antivirus Programm sowie einer Firewall gesichert – jeweils mit regelmäßigen Updates.

Im Unternehmen gibt es eine Clean Desk Policy.

3. 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.

Durch die Festlegung von Berechtigungen wird sichergestellt, dass nur berechtigte Personen in der Mäuschen App Zugriff auf personenbezogene Daten erhalten und Downloads durchführen dürfen. Benutzeraktivitäten wie das Eingeben, Verändern und Löschen sowie auch der Download personenbezogener Daten werden in einem Log erfasst.

4. Auftragskontrolle

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

Mit Auftragsverarbeitern werden Auftragsverarbeitungsverträge abgeschlossen, die die zwingenden Punkte des Art. 28 DSGVO enthalten. Durch schriftliche Weisungen sowie eine Dokumentation der Weisungen wird sichergestellt, dass die Auftragsverarbeiter die personenbezogenen Daten gemäß den Weisungen des Unternehmens verarbeiten. Vor der Beauftragung eines Auftragsverarbeiters werden dessen technische und organisatorische Maßnahmen geprüft.

Alle abgeschlossenen Auftragsverarbeitungsverträge werden zentral dokumentiert und abgelegt. Die Rückgabe bzw. Löschung der personenbezogenen Daten, die im Auftrag verarbeitet werden, wird durch interne Prozesse sichergestellt. Der zuständige Projektmanager sowie die Finance Abteilung stellen ebenfalls sicher, dass nach Beendigung eines Auftrages, bei dem der Auftragsverarbeiter Auftraggeber ist, die personenbezogenen Daten zurückgegeben oder datenschutzkonform vernichtet werden.

5. Datentrennungskontrolle

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

Die Mäuschen App ist mandantenfähig, inklusive einer mandantenspezifischen Verschlüsselung besonders sensibler personenbezogener Daten (insb. sämtlicher vom Kunden verwalteter Aufnahmen). Den Export und die Löschung der Daten des Kunden kann dieser in der Mäuschen App selbständig vornehmen oder uns damit beauftragen.

Die Trennung der außerhalb der Mäuschen App verwalteten Daten verschiedener Kunden wird durch eine getrennte Ordnerstruktur sowie die Struktur im CRM gewährleistet. Damit wird auch eine Trennung nach dem Zweck der Datenverarbeitung erreicht. Durch diese getrennte Struktur sowohl auf dem Server als auch im CRM kann die Einhaltung getrennter Löschfristen gewährleistet werden.

6. 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.

Als Auftragsverarbeiter in der in der Mäuschen App verwaltete Daten unserer Kunden werden jeweils pseudonymisiert oder – im Falle sensibler Daten mandantenspezifisch verschlüsselt – von ihrem persistenten Speicher zu unserem API-Service übertragen und nur zur Laufzeit erst unmittelbar vor der Auslieferung an den Browser oder das Mobilgerät zusammengesetzt und entschlüsselt. Dieser Prozess ist wiederum jeweils nur mit einem nutzerspezifischen Identifikations-Token möglich, der nur durch einen authentifizierten Nutzer der Web App oder Mobile App generiert werden kann.

Die Übertragung der auf diese Weise zusammengesetzten und mandantenspezifisch entschlüsselten Daten vom API-Service zum Browser oder Mobilgerät erfolgt wiederum, wie auch die Übertragung aller anderen Informationen zu oder von unseren Servern, mit einem SSL-Zertifikat verschlüsselt. So ist die Kommunikation zwischen dem Mobilgerät oder Browser des Nutzers und dem jeweiligen Server geschützt und sicher. Es wird die neueste TLS Version verwendet, die für den Browser bzw. das Mobilgerät des jeweiligen Nutzers verfügbar ist.

Unser Support erfolgt ausschließlich durch eigene Mitarbeiter. Die Email-Kommunikation mit uns ist transportverschlüsselt und kann auf Wunsch eines Kunden und nach dem Austausch von Zertifikaten auch Ende-zu-Ende-verschlüsselt erfolgen.

Nicht mehr benötigte Papierakten werden mit Hilfe eines Aktenvernichters der Sicherheitsstufe 4 datenschutzkonform vernichtet.

7. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Privacy by Design bedeutet übersetzt „Datenschutz durch Technikgestaltung". Ziel soll es sein, dass bereits bei der Entwicklung von Verarbeitungsvorgängen geeignete technische Maßnahmen implementiert werden, um die geplanten Verarbeitungsvorgänge datenschutzkonform zu gestalten.

Bei der Entwicklung der Mäuschen App wurde und wird stets darauf geachtet, sowohl die Lösung als auch die damit beim Kunden beeinflussten internen Prozesse so datenschutzfreundlich wie möglich zu gestalten. Dies ist sogar eine der beworbenen Kernfunktionen der App. Nutzer werden durch die reine Verwendung der App für den gewissenhaften Umgang mit den von ihnen verwalteten Daten sensibilisiert und verwalten diese Daten schon durch die von der Software vorgegebenen Funktionen und Abläufe datenschutzfreundlich.

Auch in unserem Unternehmen wird bei der Einführung von neuen internen Verarbeitungsvorgängen bereits bei der Planung darauf geachtet, diese datenschutzkonform auszugestalten.

Privacy by Default bedeutet übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen". Das heißt, bereits die Werkeinstellungen eines Programms/ einer Software sollen datenschutzfreundlich ausgestaltet sein. Hierdurch sollen vor allem die Daten der Nutzer geschützt werden.

Wann immer die Mäuschen App datenschutzrelevante Nutzereinstellungen ermöglicht, wird per Default die sicherste Voreinstellung gesetzt. Möchte ein Nutzer zu einer weniger sicheren Einstellung wechseln, wird er zunächst über die Konsequenzen aufgeklärt und muss mindestens das Lesen bestätigen, je nach Einstellung auch das Vorhandensein alternativer Sicherheitsmechanismen (z.B. bei Deaktivierung des PIN-Schutzes für die Mobile App eine eingerichtete Bildschirmsperre des gesamten Geräts mit ausreichenden Sicherheitseinstellungen).

8. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

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

Die Daten der Mäuschen App werden ausschließlich bei OVHcloud gespeichert (siehe Abschnitt *Zutrittskontrolle*), in einem deutschen Rechenzentrum (Frankfurt/Main), mit kontinuierlichen Backups in ein französisches Rechenzentrum (Gravelines bzw. Straßburg).

Sämtliche Daten werden dabei nach der 3-2-1 Backup-Strategie vor Zerstörung oder Verlust gesichert: Mindestens 3 Kopien mit mindestens 2 verschiedenen Speichertechnologien, davon 1 Backup an einem geografisch getrennten Speicherort.

OVHcloud ist u.a. nach ISO/IEC 27001, 27017, 27018 und 27701, nach PCI DSS sowie nach SOC 1 TYPE II und SOC 2 TYPE II zertifiziert. Bei den Serverstandorten handelt es sich um professionelle Rechenzentren, die über Brandmeldesystem, Einbruchschutz, Stromersatz USV sowie weitere Maßnahmen im Bereich Business IT verfügen (Details siehe https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml).

9. Organisationskontrolle

Hierbei handelt es sich um Maßnahmen, die sicherstellen, dass die Mitarbeiter über die Anforderungen des Datenschutzes informiert sowie sensibilisiert sind und dass sie auf die Einhaltung des Datenschutzes verpflichtet werden. Außerdem fallen unter den Punkt der Organisation übergreifende Konzepte, in denen die Unternehmensleitung festlegt, wie es den Datenschutz im Unternehmen handhaben will.

Alle Mitarbeiter des Unternehmens sind zur Vertraulichkeit verpflichtet und haben an einer Schulung zum Datenschutz teilgenommen. Mit jedem neuen Mitarbeiter wird eine Zusatzvereinbarung zum Arbeitsvertrag zur Arbeit im Homeoffice / Mobile Office abgeschlossen, um die Sicherheit der Daten auch dort zu gewährleisten.

10. Wirksamkeitskontrolle

Alle Handlungen, die zu einem Nachweis führen, dass die eingesetzten Maßnahmen regelmäßig überprüft werden und tatsächlich funktionieren.

Die Wirksamkeit der eingesetzten technischen und organisatorischen Maßnahmen wird regelmäßig (jährlich) überprüft.