Technische & organisatorische Maßnahmen

gemäß Art. 32 DS-GVO

Zusätzlich zu den im Datenschutzkonzept beschriebenen Maßnahmen wird eine Vielzahl von konkreten Schutzmaßnahmen getroffen. Somit werden die Forderungen der DS-GVO nach geeigneten technische und organisatorische Maßnahmen und die Gewährleistung eines dem Risiko angemessenes Schutzniveau erfüllt werden.

leadprint
web-to-print solutions

Stand Mai 2018
Version: 1.1

Die vorliegenden technischen und organisatorischen Maßnahmen wurden durch die Geschäftsführung (André Hausmann) genehmigt.

Datenschutzbeauftragter: Sven Rahn Datenschutz

Be.Beyond GmbH & Co KG

SITZ DER GESELLSCHAFT	hanns-martin-schleyer-straße 35 47877 willich T +49 (0) 2154 / 48 09-60 F +49 (0) 2154 / 48 09-19 info@bebeyond.de www.bebeyond.de	GESCHÄFTSFÜHRER	andré hausmann falk löffler
HANDELSREGISTER	amtsgericht krefeld hra 4635 Steuernummer: 5102/5751/0464	KOMPLEMENTÄR-GESELLSCHAFT	Be.Beyond GmbH amtsgericht krefeld hrb 8907

BE.BEYOND
WERKSTATT FÜR DIGITALE GESTALTUNG

1. Gewährleistung der Vertraulichkeit

1.1. Zutrittskontrolle

Die Maßnahmen zur Zutrittskontrolle sollen unbefugte Zutritte bspw. durch Magnet- und Chipkarten, Schlüssel, elektronische Türöffner, Werkschutz bzw. Pförtner oder Alarm- und Videoanlagen zu Datenverarbeitungsanlagen bestmöglich verhindern.

Das Gelände/Gebäude ist außen gut beleuchtet. Ein Sicherheitsdienst patrouilliert auch in der Nacht und schreckt somit Täter ab. Auf den Sicherheitsdienst wird offen erkennbar hingewiesen, um Gelegenheitstäter abzuschrecken. Es findet kaum Publikumsverkehr statt. Alle Fenster sind doppelglasig. Alle Tür- und Fensterrahmen sind aus Metall. Doppelflügelige Gebäudetüren lassen sich nicht durch das Anheben eines zentralen Bolzens öffnen. Mitarbeiter sind angewiesen die möglichen Schlupfwinkel (WC, Schränke, etc.) vor Feierabend zu kontrollieren. Es sind Attrappen einer Einbruchmeldeanlage zur Abschreckung vorhanden und von außen erkennbar.

Gäste werden von Mitarbeitern abgeholt und begleitet. Die elektronische Schließanlage ermöglicht den Zutritt meist nur zu den üblichen Geschäftszeiten. Ein abends gestohlener Schlüssel kann also nicht missbraucht werden. Die mechanischen Schlüssel der Schließanlage lassen sich nicht unbefugt duplizieren, weil dafür eine spezielle Schlüsselkarte notwendig ist. Die Ausgabe von Schlüsseln oder (Alarmanlagen-) Codes werden schriftlich protokolliert. Überzählige Schlüssel werden in Tresoren sicher verwahrt. Es wird überwacht, ob alle notwendigen Schlüssel (z.B. Tresorschlüssel) vollzählig vorhanden sind. Sobald Schlüssel vermisst werden, wird darauf angemessen reagiert. Eine schriftliche Dienstvereinbarung bestimmt über den Umgang mit den Schlüsseln und Codes. Hier wird auch bestimmt, wie im Falle eines Verlusts zu reagieren ist.

Die Schließanlage verfügt über verschiedene Schließkreise. Die Mitarbeiter erhalten nur die Schlüssel, die für die eigene Tätigkeit wirklich notwendig sind. Die Büroschränke des Unternehmens sind nicht gleichschließend, sondern in jedem Büro individuell. Dadurch können die Kollegen sich nicht gegenseitig die Schränke aufschließen. Die elektronische Schließanlage speichert die Schließvorgänge. Bei Ausscheiden eines Mitarbeiters werden alle relevanten Mitarbeiter sofort informiert. Somit können die jeweiligen Abteilungen ihre Maßnahmen einleiten (E-Mail Account löschen, Codes und Passwörter ändern, Kunden informieren, etc.). Ggf. vorhandene Codes werden umgehend geändert. Ggf. vorhandene RFID-Tags werden deaktiviert, falls sie nicht zurückgegeben wurden. Schlösser, deren Schlüssel nicht zurückgegeben wurden, werden ausgetauscht. Die internen Server sind in speziellen Serverschränken verschlossen. Alle anderen – insbesondere in Bezug auf bereitgestellte Software und zu erbringende Dienstleistungen – relevanten Server sind in ein Rechenzentrum ausgelagert.

1.2. Zugangskontrolle

Die Maßnahmen zur Zugangskontrolle sollen die unbefugte Systembenutzung bspw. durch (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung oder die Verschlüsselung von Datenträgern verhindert werden.

Bei ausnahmslos allen Computern ist die Auswahl eines Benutzerkontos und die Angabe eines Passwortes notwendig, um das Betriebssystem zu starten. Jeder Benutzer muss sich individuell mit seinem Benutzernamen anmelden. Es gibt keine Sammelkonten (bspw. für Auszubildende oder ganze Abteilungen). In sensiblen Abteilungen sind die Mitarbeiter schriftlich angewiesen, dass sie täglich den

PC hinsichtlich Hardware-Keyloggern untersuchen müssen. Somit ist ausgeschlossen, dass Unbefugte an Kennwörter gelangen, die über die Tastatur eingegeben werden.

Die Mindestlänge der Passwörter beträgt 8 Zeichen und es müssen Groß- und Kleinbuchstaben enthalten sein. Darüber hinaus müssen Sonderzeichen und Ziffern enthalten sein. Diese Richtlinien werden serverseitig technisch erzwungen. Die Mitarbeiter sind angewiesen, dass alle Passwörter vertraulich zu halten sind und den KollegInnen nicht ohne wichtigen Grund mitgeteilt werden dürfen. Die Mitarbeiter sind angewiesen das Passwort zu erneuern, sobald der Verdacht besteht, dass unbefugte Personen das Passwort kennen könnten.

Es ist den Mitarbeitern explizit untersagt, dass Passwörter im Web-Browser gespeichert werden. Die Software "1Password" wird als zentraler Tresor vorgeschrieben. Es ist bei allen Mitarbeitern ein automatischer Bildschirmschoner installiert, der sich automatisch nach 5 Minuten aktiviert und nur mittels Passwort abgeschaltet werden kann. Die Mitarbeiter sind angewiesen, den Computer (ggf. trotz Bildschirmschoner) aktiv zu sperren, wenn sie den Computer verlassen. Die obigen Regelungen wurden schriftlich getroffen und sind von den Mitarbeitern unterschrieben worden.

Es wird sichergestellt, dass externe Techniker wirklich angefordert wurden und dass sie wirklich von der beauftragten Firma stammen (z.B. per Telefonanruf). Die Arbeiten werden durch interne Kräfte beaufsichtigt. Sofern notwendig: Werden Datenträger anschließend auf Viren etc. überprüft. Sofern notwendig: Werden frühere Sicherheitsmaßnahmen (z.B. Firewall-Einstellungen) auf die früheren Einstellungen zurückgestellt.

1.3. Zugriffskontrolle

Die Maßnahmen zur Zugriffskontrolle sollen ein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems bspw. durch Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte sowie die Protokollierung von Zugriffen verhindern und Zugriffe nachvollziehbar machen.

Papierunterlagen werden prinzipiell sicher verschlossen. Die Putzkräfte sind im Datenschutz unterwiesen. Die Putzkräfte haben keinen Zugriff auf zu vernichtende Papiere. Die lokale Speicherung auf Arbeitsplatzcomputern ist verboten. Abteilungen mit sensiblen Daten drucken auf lokalen Druckern und nicht auf den Netzwerkdruckern.

Bei Office-Dokumenten wird die Möglichkeit von Schreib- und Lesekennwörtern aktiv genutzt. Im Zweifelsfall werden Dokumente im PDF-Format verteilt, die in der Regel nicht von Jedermann editierbar sind. Die Mitarbeiter wissen, dass z.B. in MS-Office Dokumenten durch die „Änderungs-Nachverfolgung“ sensible Informationen preisgegeben werden könnten. Es werden Maßnahmen getroffen, dass diese Informationen vor der Weitergabe gelöscht werden.

Die Daten werden verschlüsselt, bevor sie auf die Medien der Datensicherung gespeichert werden. Die Datenträger werden sicher verschlossen aufbewahrt. Es ist sichergestellt, dass der Transport der Datenträger vom Server bis zum Ort der Aufbewahrung wirklich sicher ist. Jeder Mitarbeiter erhält im Netzwerk nur die für das eigene Tätigkeitsfeld relevanten Daten. Daten werden (teilweise) im Unternehmen verschlüsselt, sodass u.a. die EDV-Administratoren keinen Zugriff auf die Inhalte erlangen können.

Die Zugriffsrechte auf Dateien und E-Mails werden sofort nach dem Ausscheiden eines Mitarbeiters gelöscht. Die Vergabe von Berechtigungen erfolgt auf einem standardisierten, schriftlichen Weg (und somit nicht auf „Zuruf“). Nur bestimmte Vorgesetzte dürfen Berechtigungen erteilen. Die erteilten

Berechtigungen werden regelmäßig (zumindest stichprobenartig) überprüft, um festzustellen, ob die Berechtigungen noch immer korrekt sind. Firewalls trennen den Datenverkehr. Switches trennen Netzwerksegmente.

Es sind keine PCs im Einsatz mit MS-Windows XP (oder älter). Es sind keine Server im Einsatz mit MS-Server 2003 (oder älter). Zur Authentifizierung in Windows-Netzwerken wird nicht mehr das Protokoll „NTLM“ eingesetzt, sondern der sichere Nachfolger „NTLMv2“. Bei der Fernwartung wird auf dem Zielsystem die Bildschirmdarstellung abgeschaltet, damit unbefugte Personen die Daten nicht einsehen können. Der Zugriff erfolgt nur mittels betrieblich zugelassener Computer.

Private Computer werden nicht genutzt. Anmeldungen zu Ferneinwahl / Fernwartung werden protokolliert und zeitnah ausgewertet, um unbefugte Zugriffe feststellen zu können. Die Mitarbeiter sind angewiesen Notebooks nicht unbeaufsichtigt zu lassen (z.B. im Auto oder bei Kunden).

Die Vernichtung von Datenträgern wird von einem externen Dienstleister vorgenommen. Die EDV ist dahingehend sensibilisiert, dass Zugangs- und personenbezogene Daten auch auf diversen Geräten (WLAN-Router, VPN-Router etc.) gespeichert sein könnten und die Geräte deswegen ebenfalls sorgfältig vernichtet werden müssen. Akten werden von einem externen Unternehmen geschreddert, welches eine Entsorgungsbescheinigung erstellt. Datensicherungen (z.B. verschiedener Kunden) werden separiert durchgeführt und individuell verschlüsselt.

Spezielle pDaten werden nicht auf den unternehmensweiten Backups erfasst. Spezielle pDaten werden separat z.B. auf USB-Sticks gesichert, um sie zeitnah sicher löschen zu können.

Die Server werden durch einen Antivirus etc. geschützt. Die Clients werden lokal durch einen Antivirus etc. geschützt. Die Aktualisierung der Antivirus-Daten wird mindestens täglich aktualisiert. Sensible Daten werden zentral verschlüsselt und können nur von befugten Mitarbeitern entschlüsselt werden. EDV-Administratoren können die Daten in der Regel nicht unverschlüsselt einsehen. In allen notwendigen Computerprogrammen und auf allen (Datei-) Servern können Daten gelöscht werden, wenn die Betroffenen dies wünschen. Alternativ ist eine Sperrung möglich. Die Mitarbeiter sind über die diesbezüglichen Rechte der Betroffenen informiert und sind in der Lage zeitnah zu reagieren.

1.4. Trennungskontrolle

Die Maßnahmen zur Trennungskontrolle sollen eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden bspw. durch mandantenfähige Systeme oder Sandboxing gewährleisten.

Die Daten verschiedener Mandanten/Kunden werden in eigenen Verzeichnissen gespeichert. Die Zugriffsrechte werden entsprechend vergeben. Die Datensicherungen (Backups) verschiedener Mandanten/Kunden werden separat erstellt, damit den späteren Löschfristen individuell entsprochen werden kann. Produktionsdaten werden anonymisiert, bevor sie zu Testzwecken eingesetzt werden.

2. Gewährleistung der Integrität

2.1. Eingabekontrolle

Die Maßnahmen zur Eingabekontrolle sollen die Feststellung von Anlagen, Veränderungen oder Löschungen personenbezogener Daten innerhalb eines Datenverarbeitungssystems bspw. durch die Protokollierung oder ein geeignetes Dokumentenmanagement ermöglichen.

Änderungen und Eingaben an der Software werden innerhalb der Versionierung, aber auch in einigen Programmen nachgehalten. Diese Eingabekontrolle umfasst nicht nur die letzte Änderung, sondern alle getätigten Änderungen an der Software. Eingaben und Änderungen von personenbezogenen Daten werden innerhalb der Software mit dem Benutzer verknüpft.

2.2. Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle sollen ein unbefugtes Lesen, Kopieren, Verändern und Entfernen bei elektronischer Übertragung oder Transport bspw. durch Verschlüsselung, Virtual Private Networks (VPN) oder elektronische Signaturen gewährleisten.

Die E-Mail Server unterstützen die TLS-Transportverschlüsselung. Sensible Dateianhänge werden gezippt und verschlüsselt. Die Empfänger erhalten das Passwort auf separatem Wege. Sensible Dateianhänge werden auf einem separaten Server gespeichert und sind per Hyperlink in der E-Mail erreichbar. Der Empfänger benötigt zum Abruf der Anhänge ein individuelles Passwort, welches ihm separat mitgeteilt wird.

Bei Bedarf können E-Mails mit einer elektronischen Signatur versehen werden, sodass der Empfänger sicher beurteilen kann, ob die E-Mail vom angegebenen Absender stammt, und ob der Inhalt manipuliert wurde. Es werden keine E-Mail Server eingesetzt, die unverschlüsselt über das Internet erreichbar sind. Andernfalls könnten die Passworte für IMAP und/oder POP3 abgehört werden – ein unbefugter Lese- und Schreibzugriff wäre das Resultat.

Der Fernzugriff ist per Zugang über ein Terminal-Programm (via VPN-verschlüsselter Verbindung) bzw. einen Zugang über Fernwartung des lokalen PCs (RemoteDesktop, RealVNC, …) abgesichert. Einzelne Partitionen/Verzeichnisse der Notebooks sind verschlüsselt. Heimarbeiter / Telearbeiter werden speziell instruiert. WLAN-Netzwerke werden per WPA2 abgesichert.

Die Anmeldung per RADIUS-Server sorgt dafür, dass nur befugte Personen Zugriff auf das Netzwerk erhalten. Der Dateitransfer per FTP wird in Hinsicht auf pDaten nicht verwendet, weil das Passwort im Klartext übertragen wird. Gegebenenfalls wird sFTP genutzt. Der Dateitransfer per HTTP wird in Hinsicht auf pDaten nicht verwendet, weil die Daten unverschlüsselt übertragen werden. Gegebenenfalls wird HTTPs genutzt.

Der VoIP-Datenverkehr ist verschlüsselt.

Die Firewall der mobilen Computer wird auf „öffentliches Netzwerk“ umgestellt, damit beispielsweise Netzwerkfreigaben von außen nicht mehr erreichbar sind. Die Mitarbeiter verbinden sich zuerst per VPN mit einem Unternehmensserver und benutzen das Internet über diese Verbindung.

Insbesondere in Großraumbüros gibt es separate Telefon-Arbeitsplätze, wo die Mitarbeiter vertraulich telefonieren können. Insbesondere in Großraumbüros muss es Rückzugsgebiete geben, wo die Mitarbeiter sich treffen können, und vertrauliche Gespräche führen können.

3. Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme

Die Maßnahmen zur Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme sollen bestmöglichen Schutz gegen zufällige und mutwillige Zerstörung bspw. durch geeignete Backup-Strategien (online / offline, on- / off-site), unterbrechungsfreie Stromversorgung relevanter Systeme (USV), Virenschutz und Firewall, Meldewege und Notfallpläne bieten.

Alle relevanten Computer werden regelmäßig gesichert. Die Backups werden solange aufgehoben, wie die gesetzlichen/vertraglichen Pflichten dies erfordern. Die Datensicherungsbänder werden in einem anderen Brandschutzbereich gelagert, als die betroffenen Computer. Backups werden (auch) außerhalb der Geschäftsräume gelagert. Die Backups werden verschlüsselt. Die Backups werden z.B. auf NAS gespiegelt (ggf. standortübergreifend). Es ist sichergestellt, dass auch beim Ausfall von Backup-Lesegeräten die Daten bei Bedarf schnell wiederhergestellt werden können (z.B. Ersatzgerät, wenn das Originallaufwerk defekt ist).

Die durchgeführten Backups werden grundsätzlich auf Fehlermeldung bzw. Plausibilität (z.B. Datenmange) geprüft. Die Wiederherstellung von Daten wird regelmäßig praktiziert oder getestet. Server sind durch unterbrechungsfreie Stromversorgungen (USV) für einen ausreichenden Zeitraum vor Stromausfall geschützt. Die USV werden regelmäßig gewartet. Die USV werden regelmäßig getestet. Im Falle eines Stromausfalls werden sensible Server automatisiert heruntergefahren. Die USV können bei Stromausfällen alarmieren (z.B. per E-Mail, SMS, Telefon).

Die Telefonanlage ist durch eine USV geschützt. Zentrale Netzwerk-Komponenten (Router etc.) sind durch USV geschützt. Die USV haben einen integrierten Überspannungsschutz. Alternativ sind Blitzschutzstecker an den Steckdosen montiert.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Die Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung sollen gewährleisten, dass keine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers bspw. durch eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl von Dienstleistern oder Nachkontrollen stattfindet.

4.1. Datenschutz-Management (DSM)

Es wurden standardisierte Routinen zur frühzeitigen (Risiko-)Bewertung von neuen Verfahren, regelmäßige Überprüfungen sowie zur Verbesserung der eingeführten Verfahren und der damit verbundenen technischen und organisatorischen Maßnahmen im Unternehmen implementiert, die sich an den Empfehlungen der GDD orientieren.

Damit diese Prozesse bestmöglich eingehalten und verbessert werden können, steht neben einem Datenschutzbeauftragten auch ein interner Datenschutzkoordinator als Ansprechpartner zur Verfügung.

4.2. Incident-Response-Management (IRM)

Im Falle eines erkannten oder vermuteten sicherheitsrelevanten Vorfall bzw. einer Störung der IT-Systeme werden zunächst nach internen Vorgaben definierte Prozesse ausgelöst (u. a. zur Priorisierung), die die Prüfung des Vorfalls und ggf. die Behebung der Ursache sicherstellen. Sofern personenbezogene Daten oder den Kunden betreffende Vorfälle festgestellt werden, werden die betroffenen Kunden im Rahmen der gesetzlichen Vorschriften über den Vorfall informiert.

4.3. Datenschutzfreundliche Voreinstellungen

Die angebotene Software wird in den Standardeinstellungen so ausgeliefert, dass nur die minimal erforderlichen Daten erfasst werden. Diese Einstellungen können kundenseitig oder über Erweiterungen verändert werden.

4.4. Auftragskontrolle

Maßnahmen durch den Auftraggeber

Die Auftragnehmer werden sorgfältig ausgewählt, vorab geprüft und unterzeichnen eine gesetzeskonforme Datenschutzvereinbarung. Der Auftraggeber legt fest, welche Personen überhaupt weisungsberechtigt sind. Fernwartungen werden durch aktive Einsichtnahme auf einem Monitor beobachtet. Sollten verdächtige Aktionen stattfinden, so könnte die Fernwartung abgebrochen werden.

Maßnahmen durch den Auftragnehmer

Die Mitarbeiter werden über die Weisungen informiert. Das ist essentiell. Wie sonst sollten sie in der Lage sein, die Weisungen einzuhalten? Wenn sich im betrieblichen Alltag herausstellt, dass die bestehenden Weisungen nicht ausreichen, so wird sofort der Auftraggeber kontaktiert, damit neue Weisungen erteilt werden können. Fallen im Rahmen der Arbeiten auch Logfiles an, so könnte möglicherweise darauf zurückgegriffen werden, um den korrekten Umgang mit den Daten nachzuweisen.

Ein DSB mit der notwendigen Fachkunde ist bestellt. Ihm sind die Weisungen der Datenschutzvereinbarung bekannt. Das Unternehmen achtet darauf, dass der DSB über Änderungen im Umgang mit den pDaten rechtzeitig informiert wird.

Die Fernwartungssoftware wird so konfiguriert, dass eine aktive Einsichtnahme durch den Auftraggeber möglich ist. Die Fernwartungssoftware wird so konfiguriert, dass lokale Drucker des Auftragnehmers nicht ansprechbar sind. Die Fernwartungssoftware wird so konfiguriert, dass lokale Laufwerke des Auftragnehmers nicht ansprechbar sind. Die Fernwartungssoftware wird so konfiguriert, dass die Zwischenablage in Richtung des Auftragnehmers abgeschaltet ist.