

Anlage B: Technische und organisatorische Maßnahmen

1 Vertraulichkeit

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der ihm übertragenen Leistungen genutzten technischen Einrichtungen zu verwehren.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation der Vergabe von Schlüsseln, RFID-Chipkarten oder -Transpondern; Die Vergabe von Schlüsseln, RFID-Chipkarten oder -Transpondern erfolgt ausschließlich an Mitarbeiter. Die Vergabe erfolgt erst nach Unterzeichnung eines Übergabeprotokolls. Im Protokoll werden die beteiligten Personen, das Datum und die Uhrzeit der Vergabe, die Schlüssel-Nummer oder die ID der Chipkarte festgehalten. Das Protokoll wird an zentraler Stelle sicher verwahrt. Alle Inhaber werden zudem darüber informiert, dass Schlüssel, RFID-Chipkarten oder -Transponder sicher zu verwahren sind und deren Verlust umgehend zu melden ist.

Protokollierung von Besuchern und Dienstleistern;
Besucher und Dienstleister, erhalten nur nach vorheriger Anmeldung Zugang zum Bürogebäude. Zudem werden Besucher und Dienstleister namentlich erfasst und deren Besuchszeiten protokolliert.

Rückgabe von Schlüsseln, RFID-Chipkarten oder -Transpondern nach Austritt von Mitarbeitern;
Vor Beendigung des Anstellungsverhältnisses müssen Mitarbeiter zuvor ausgehändigte Schlüssel, RFID-Chipkarten oder -Transponder zurückgeben. Die Namen der beteiligten Personen, das Datum und die Uhrzeit der Rückgabe, die Schlüssel-Nummer oder die ID der Chipkarte oder des Transponders werden im Übergabeprotokoll festgehalten. Das Protokoll wird an zentraler Stelle sicher verwahrt.

Verwendung einer Zutrittskontrolle;
Der Zutritt zum Bürogebäude ist ausschließlich mit Hilfe eines entsprechenden Schlüssels, einer RFID-Chipkarte oder eines RFID-Transponders möglich. Diese werden ausschließlich an Mitarbeiter ausgeteilt und müssen vor Austritt aus dem Unternehmen wieder zurückgegeben werden. Eine Vervielfältigung der eingesetzten Schlüssel, RFID-Chipkarten oder -Transponder ist nicht möglich.

Verwendung sicherer Türen und Fenster;
Innerhalb des gesamten Bürogebäudes sind moderne und einbruchssichere Türen und Fenster verbaut.

1.2 Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der in der beschriebenen IT- Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Automatisches Sperren von PCs / Macs nach fünf Minuten;
Alle im Einsatz befindlichen Arbeitsplatzrechner (PCs, Macs) rufen nach fünfminütiger Inaktivität automatisch die Anmeldemaske des jeweiligen Betriebssystems auf. Ein Zugriff auf die Arbeitsplatzrechner ist dann nur nach vorheriger Eingabe des Nutzerpassworts möglich. So wird verhindert, dass Unbefugte beispielsweise während der Pausenzeiten Zugriff auf kritische Daten erlangen können.

Tägliches Aufräumen der Arbeitsplätze ("Clean desk");
Die Schreibtische im gesamten Bürogebäude werden stets vor dem Feierabend bzw. dem Wochenende aufgeräumt. In diesem Zuge werden vertrauenswürdige Dokumente mit personenbezogenen Daten sicher verwahrt (z. B. durch das Verschließen in einem Schrank). So kann verhindert werden, dass Dokumente mit personenbezogenen Daten versehentlich entsorgt werden (z. B. durch Reinigungskräfte) oder unberechtigte Personen Zugang zu diesen Dokumenten erlangen.

Verwendung einer Firewall;
Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und die angelegten Firewall-Richtlinien in diesem Zuge überprüft. Nicht mehr benötigte Richtlinien werden entfernt, um eine höchstmögliche Sicherheit zu gewährleisten.

Verwendung personalisierter Logins;
Sowohl für interne als auch externe Systeme werden grundsätzlich personalisierte Logins vergeben. So kann sichergestellt werden, dass durchgeführte Aktionen nachträglich dem jeweiligen Benutzer zugeordnet werden können. Zudem können einzelne Zugänge zielgerichtet gesperrt oder gelöscht werden, ohne dass dies Einfluss auf die Zugänge anderer Mitarbeiter hat.

Verwendung sicherer und individueller Passwörter;
Sowohl für interne als auch externe Zugänge werden ausschließlich sichere Passwörter mit einer Länge von mindestens zehn Zeichen verwendet. Die Passwörter beinhalten zudem mindestens einen Groß- und Kleinbuchstaben, eine Zahl sowie ein Sonderzeichen. Auch wird sichergestellt, dass ein Passwort nicht für mehrere Zugänge verwendet wird. Wird einer der genutzten Zugänge kompromittiert, bleibt die Sicherheit der übrigen Zugänge nachwievor gewahrt.

Verwendung und regelmäßige Aktualisierung eines Virenschanners;
Eingehende E-Mails sowie Arbeitsplatzrechner werden durch einen Virenschanner vor den Auswirkungen von schädlichen Dateien geschützt. Die zur Erkennung von aktuellen Bedrohungen notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Als gefährlich eingestufte Dateien oder E-Mails werden in einen separaten Quarantäne-Ordner verschoben. Die Wiederherstellung von Dateien aus dem Quarantäne-Ordner ist nur nach vorheriger Freigabe durch ausgewählte Mitarbeiter möglich. Um die korrekte Funktion des eingesetzten Virenschanners sicherzustellen, erfolgt der regelmäßige Scan einer speziellen Testdatei, die von allen aktuellen Virenschutzlösungen erkannt wird.

1.3. Zugriffskontrolle

Es ist sicherzustellen, 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 oder verändert werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation eingerichteter Zugänge für Mitarbeiter;
Alle Zugänge zu internen und externen Systemen werden vor deren Einrichtung dokumentiert. Dabei werden der Name des Mitarbeiters, das jeweilige System sowie der eingerichtete Benutzername protokolliert. Diese Informationen stellen die Basis dafür dar, dass bei einem späteren Austritt zielgerichtet die Zugänge des jeweiligen Mitarbeiters gesperrt bzw. gelöscht werden können.

Minimale Anzahl an Mitarbeitern mit administrativen Rechten;
Um zu gewährleisten, dass lediglich autorisierte Personen Zugriff auf kritische IT-Systeme sowie darauf gespeicherter Daten haben, verfügen nur ausgewählte Mitarbeiter über die notwendigen administrativen Rechte. Diese Mitarbeiter schalten projektbezogen die Zugriffsrechte der anderen Mitarbeiter frei, sofern diese für ihre Arbeit notwendig sind. Nach Abschluss der jeweiligen Arbeiten werden die entsprechenden Rechte wieder entzogen. So wird die Anzahl der Mitarbeiter, die theoretisch Zugriff auf alle im Unternehmen gespeicherten personenbezogenen Daten haben, auf ein absolutes Minimum reduziert.

Nutzung von Benutzer- und Rollenkonzepten für interne und externe Systeme;
Für interne und externe Systeme, die diese Funktionalität unterstützen, werden Benutzer- und Rollenkonzepte beim Anlegen von Zugängen verwendet. Anstatt jeden einzelnen Zugang mit entsprechenden Berechtigungen auszustatten, wird jedem Zugang eine Rolle zugewiesen. Diesen übergeordneten Rollen werden wiederum die notwendigen Berechtigungen zugewiesen. So können Änderungen an den Berechtigungen zentral über die Anpassung der jeweiligen Rolle erfolgen. So kann verhindert werden, dass einzelne Zugänge über Berechtigungen verfügen, die dies eigentlich nicht gestattet wären.

Sicheres Löschen von Daten auf Datenträgern;
Werden Daten mit personenbezogenem Inhalt auf lokalen Datenträgern gelöscht, erfolgt dies grundsätzlich durch Anwendung spezieller Löschroutinen. So werden auch vom Betriebssystem angelegte Schattenkopie sowie Daten auf SSD-Speichermedien zuverlässig gelöscht. Eine nachträgliche Wiederherstellung der gelöschten Daten ist so nicht mehr möglich.

Sperrung von Zugängen beim Austritt von Mitarbeitern;
Verlässt ein Mitarbeiter das Unternehmen, so erfolgt noch vor dessen Austritt die Sperrung bzw. Löschung aller ihm zugewiesenen Zugänge für interne und externe Systeme. Als Basis für diesen Vorgang wird die Dokumentation der zuvor angelegten Zugänge verwendet. In der Dokumentation wird abschließend ebenfalls die Sperrung bzw. Löschung der Zugänge vermerkt.

Verwendung sicherer und individueller Passwörter;
Sowohl für interne als auch externe Zugänge werden ausschließlich sichere Passwörter mit einer Länge von mindestens zehn Zeichen verwendet. Die Passwörter beinhalten zudem mindestens einen Groß- und Kleinbuchstaben, eine Zahl sowie ein Sonderzeichen. Auch wird sichergestellt, dass ein Passwort nicht für mehrere Zugänge verwendet wird. Wird einer der genutzten Zugänge kompromittiert, bleibt die Sicherheit der übrigen Zugänge nach wie vor gewahrt.

Zentrale Verwaltung von Benutzerzugängen und -rechten;
Zur Dokumentation aller Zugänge für interne und externe Systeme kommt eine Software zum Einsatz, in der alle Informationen zu Mitarbeitern sowie deren Zugängen erfasst werden. Die softwaregestützte Erfassung und Verwaltung aller Benutzerzugänge

stellt u.A. sicher, dass beim Austritt von Mitarbeitern alle für ihn angelegten Zugänge vollständig gesperrt bzw. gelöscht werden.

1.4 Weitergabekontrolle

Es muss dafür gesorgt werden, 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 welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Beim Auftragnehmer umgesetzte Maßnahmen:

Beauftragung zuverlässiger Transportunternehmen;

Beim Versand von Daten auf dem Postweg oder beim Transport von Servern wird darauf geachtet, dass nur zuverlässige und vertrauenswürdige Transportunternehmen eingesetzt werden.

Nutzung SSL-verschlüsselter Übertragungswege im Internet;

Für die Übermittlung von Daten mit personenbezogenem Inhalt über das Internet werden ausschließlich SSL/TLS-verschlüsselte Übertragungswege genutzt. Die gesicherte Verbindung zwischen Browser und Zielsystem stellt sicher, dass Daten zwischen diesen beiden Systemen nicht von Dritten eingesehen oder manipuliert werden können.

Persönliche Übergabe von personenbezogenen Daten mit Protokoll;

Eine persönliche Übergabe von personenbezogenen Daten an Dienstleister erfolgt ausschließlich, wenn dies er bereit ist, Ort, Zeit und Empfänger zu protokollieren und anschließend an uns zu übermitteln. So kann sichergestellt werden, dass die Zustellung der personenbezogenen Daten im gewünschten Zeitraum und an den zuvor benannten Empfänger erfolgt ist.

Sicheres Löschen von Daten auf Datenträgern;

Werden Daten mit personenbezogenem Inhalt auf lokalen Datenträgern gelöscht, erfolgt dies grundsätzlich durch Anwendung spezieller Löschroutinen. So werden auch vom Betriebssystem angelegte Schattenkopie sowie Daten auf SSD-Speichermedien zuverlässig gelöscht. Eine nachträgliche Wiederherstellung der gelöschten Daten ist so nicht mehr möglich.

Sicherung von Dokumenten beim Versand auf dem Postweg;

Beim Versand von Dokumenten mit personenbezogenem Inhalt auf dem Postweg (z. B. Verträge) kommen ausschließlich undurchsichtige Briefumschläge und Versandtaschen zum Einsatz.

Sorgfältige Auswahl von Transportunternehmen und -fahrzeugen;

Beim physischen Transport von personenbezogenen Daten (z. B. Übermittlung großer Datenmengen auf einer Blu-ray Disc durch einen Kurier) werden nur ausgesuchte und zuverlässige Transportunternehmen mit einwandfreier Reputation beauftragt, die zudem über die notwendige Erfahrung für einen Transport von sensiblen Daten verfügen. Auch die Verfügbarkeit geeigneter Transportfahrzeuge hat Einfluss auf die Auswahl. Nach erfolgreicher Übermittlung wird zudem die Rückmeldung des Empfängers eingeholt, welcher ebenfalls zu seiner Erfahrung mit dem Transportunternehmen befragt wird.

Verwendung von VPN-Systemen zum Login in das Firmennetzwerk;
Ein externer Zugriff auf das Firmennetzwerk ist nur mittels einer VPN-Verbindung möglich. Die hierfür verwendeten Komponenten werden regelmäßig aktualisiert. Zugriffe über VPN werden vollständig protokolliert, um durchgeführte Aktionen nachträglich nachvollziehen zu können. Außerdem sind Zugriffe von außerhalb Europas grundsätzlich gesperrt. Zur Nutzung von VPN wird jedem Mitarbeiter, der einen solchen Zugang für seine Arbeit benötigt, ein individueller Zugang erstellt.

Weitergabe von Daten in anonymisierter oder pseudonymisierter Form;
Wann immer möglich, erfolgt die Weitergabe von Daten in anonymisierter oder pseudonymisierter Form. Bei anonymisierten Daten ist eine Beziehung zu einer natürlichen Person unter keinen Umständen mehr möglich. Pseudonymisierte Daten können unter Zuhilfenahme einer weiteren, separat gespeicherten Datenquelle, wieder den jeweiligen Personen zugeordnet werden. Beim Versand von pseudonymisierten Daten bleibt diese zusätzliche Quelle ausschließlich im Besitz unseres Unternehmens.

1.5 Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Mandantenfähigkeit von bereitgestellten Anwendungen;
Durch uns entwickelte und bereitgestellte Anwendungen und Webanwendungen sind grundsätzlich mandantenfähig. Personenbezogene Daten eines Mandanten werden im System getrennt von den Daten anderer Mandanten gespeichert. Gelingt es einem Mandanten, beispielsweise durch einen bislang unbekanntem Bug oder durch eine gezielte Attacke, lesenden Zugriff auf seinen Bereich der Datenbank zu erlangen, so sind andere Mandanten von dieser Kompromittierung nicht betroffen.

Trennung von internem WLAN und Gäste-WLAN;
Gäste, denen ein Zugang zum Internet ermöglicht werden soll, erhalten einen individualisierten Zugang oder die Zugangsdaten zu einem eigenem WLAN. Von diesem separaten WLAN aus ist ein Zugriff auf das firmeninterne Netzwerk und alle dort hinterlegten Daten nicht möglich. So wird verhindert, dass Gäste unberechtigterweise auf personenbezogene Daten im Firmennetzwerk zugreifen können.

Trennung von Live- und Entwicklungssystemen;
Für die Entwicklung und Programmierung stehen den Entwicklern eigene Entwicklungsumgebungen mit anonymisierten oder pseudonymisierten Testdaten zur Verfügung, sodass eine Entwicklung am Produktivsystem mit den darin gespeicherten Echtdateien nicht notwendig ist. So kann verhindert werden, dass versehentlich eine ungewollte Veränderung oder Weitergabe von personenbezogenen Daten erfolgt. Ausschließlich die gemeinsam mit dem Endkunden durchgeführten Live-Tests vor Projektabschluss erfolgen unter Zuhilfenahme der jeweiligen Echtdateien.

Verbot der Nutzung von privaten Endgeräten im Firmennetzwerk;
Die Nutzung privater Laptops oder Speichermedien wie Festplatten oder USB- Sticks, die nicht durch die Firma ausgegeben wurden, ist den Mitarbeitern im Unternehmen nicht gestattet. Eine entsprechende Erklärung wurden durch jeden Mitarbeiter unterzeichnet. So werden mögliche Schäden an kritischen IT- Systemen durch bewusst oder unbewusst eingeschleuste Schadsoftware verhindert und bereits kompromittierte Systeme aus dem Firmennetzwerk ferngehalten. Einzig Geräte, über

die keine fremden Daten ins Firmennetzwerk übertragen werden können (z. B. Mäuse oder Tastaturen), dürfen nach ausdrücklicher Genehmigung im Unternehmen genutzt werden.

Verwendung von Zugriffsberechtigungen für interne Systeme;

Alle internen Systeme sind vor unbefugtem Zugriff gesichert. Es ist nicht möglich, diese ohne eine weitere Anmeldung zu verwenden, wenn man sich im Firmennetzwerk befindet. Die Berechtigungen zur Nutzung der verschiedenen Systeme werden individuell vergeben und können individuell und systembezogen widerrufen werden. Ein genereller Zugriff auf alle im Firmennetzwerk befindlichen Daten wird somit unterbunden.

1.6 Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

Beim Auftragnehmer umgesetzte Maßnahmen:

Verwendung verschlüsselter Übertragungswege für den Datenaustausch;
Werden Daten digital ausgetauscht, die unter Umständen personenbezogene Daten enthalten könnten, findet dies ausschließlich auf sicheren und verschlüsselten Übertragungswegen statt. Es werden insbesondere SSH- Verbindungen genutzt und keine unverschlüsselten Protokolle verwendet, wenn verschlüsselte Alternativen zur Verfügung stehen. So werden E-Mails zum Beispiel via IMAP nur mit SSL/TLS oder HTTPS-Verbindungen gesendet.

Verwendung von SSL-Zertifikaten für Hostingumgebungen;

Alle von uns betreuten Webseiten sowie die hierfür genutzten Hostingumgebungen, über die personenbezogene Daten über das Internet übermittelt werden, z. B. durch Kontaktformulare oder Eingabemasken, werden von uns mit SSL-Zertifikaten geschützt. Die Zertifikate werden in regelmäßigen Abständen neu ausgestellt, um einen Diebstahl des Zertifikats und somit das Abgreifen von Daten zu verhindern.

2 Integrität

2.1 Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Beim Auftragnehmer umgesetzte Maßnahmen:

Nutzung von Benutzer- und Rollenkonzepten für interne und externe Systeme;
Für interne und externe Systeme, die diese Funktionalität unterstützen, werden Benutzer- und Rollenkonzepte beim Anlegen von Zugängen verwendet. Anstatt jeden einzelnen Zugang mit entsprechenden Berechtigungen auszustatten, wird jedem Zugang eine Rolle zugewiesen. Diesen übergeordneten Rollen werden wiederum die notwendigen Berechtigungen zugewiesen. So können Änderungen an den Berechtigungen zentral über die Anpassung der jeweiligen Rolle erfolgen. So kann verhindert werden, dass einzelne Zugänge über Berechtigungen verfügen, die dies eigentlich nicht gestattet wären.

Verwendung personalisierter Logins;
Sowohl für interne als auch externe Systeme werden grundsätzlich personalisierte Logins vergeben. So kann sichergestellt werden, dass durchgeführte Aktionen nachträglich dem jeweiligen Benutzer zugeordnet werden können. Zudem können einzelne Zugänge zielgerichtet gesperrt oder gelöscht werden, ohne dass dies Einfluss auf die Zugänge anderer Mitarbeiter hat.

2.2 Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gem. 1.4 dienen auch der Sicherstellung der Integrität.

3 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Vom Auftragnehmer umgesetzte Maßnahmen:

Erstellung von Code-Dokumentationen in der Entwicklung;
Alle entwickelten Systeme und darin verwendete Code-Bestandteile werden durch die Entwickler hinreichend dokumentiert. Dies stellt u. A. eine schnelle Einarbeitung anderer Mitarbeiter in das jeweilige Projekt sicher. Darüber hinaus kann eine Weiterentwicklung der jeweiligen Code-Bestandteile zukünftig auch dann erfolgen, wenn der ursprüngliche Entwickler nicht mehr im Unternehmen tätig ist. Durch eine hinreichende Dokumentation wird zudem sichergestellt, dass Bugs oder Fehler schneller identifiziert und behoben werden können.

Nutzung einer Versionskontrolle in der Entwicklung;
Für die Entwicklung von Anwendungen werden gängige Versionierungssysteme (z.B. Git) eingesetzt. Diese stellen sicher, dass vorherige Softwarestände nicht versehentlich überschrieben werden und die parallele Entwicklung durch mehrere Mitarbeiter an einem System nicht zu Fehlern oder zum Überschreiben von bestehenden Daten führt. Zudem können durch eine Versionskontrolle Änderungen und Fehler nachträglich schneller und besser nachvollzogen und behoben werden. Unabsichtlich durchgeführte Änderungen können außerdem rückgängig gemacht werden.

Regelmäßige Durchführung von Updates;
Alle im Einsatz befindlichen Betriebssysteme sowie darauf installierte Anwendungen und Bibliotheken werden stets aktuell gehalten. Entsprechende Updates werden regelmäßig eingespielt. Zur Verfügung gestellte Security-Patches werden ebenfalls zeitnah eingespielt, um die entsprechenden Sicherheitslücken schnellstmöglich zu schließen. Werden für Anwendungen oder Bibliotheken keine Security-Updates mehr ausgeliefert oder wird die Anwendung vom Hersteller nicht mehr weiterentwickelt oder betreut, findet ein Upgrade auf eine aktuelle Version statt oder es findet ein Wechsel auf eine noch unterstützte alternative Anwendung statt.

Überprüfung erstellter Datensicherungen;
Erstellte Datensicherungen werden regelmäßig auf ihre Integrität und Wiederherstellbarkeit hin überprüft. Hierfür werden zufällig ausgewählte Daten von einem zufällig ausgewählten Zeitpunkt testweise aus einer Datensicherung wiederhergestellt und mit den Originaldateien verglichen. So können unbrauchbare

Datensicherungen oder Fehler im Backup- bzw. Wiederherstellungssystem frühzeitig erkannt und behoben werden.

Verwendung von Brandmeldern;

Zur Vermeidung von Schäden durch Feuer werden Brandmelder verwendet. Diese wurden in jedem Bereich des Bürogebäudes angebracht vernetzt. Im unwahrscheinlichen Fall eines Feuers kann so der betroffene mit Hilfe von öffentlich zugänglichen Feuerlöschern bei Bedarf gelöscht werden.

Verwendung einer Firewall;

Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt. Die Firewall-Firmware wird regelmäßig aktualisiert und die angelegten Firewall-Richtlinien in diesem Zuge überprüft.

Verwendung eines Überspannungsschutzes für interne Systeme;

Zum Schutz vor Schäden durch Blitzeinschlag oder eine fehlerhafte Netzeinspeisung, werden Einrichtungen verwendet, die eine zu hohe Netzspannung in allen sicherheitskritischen Bereichen des Bürogebäudes verhindern.

Verwendung und regelmäßige Aktualisierung eines Virenschanners;

Eingehende E-Mails sowie Arbeitsplatzrechner werden durch einen Virenschanner vor den Auswirkungen von schädlichen Dateien geschützt. Die zur Erkennung von aktuellen Bedrohungen notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Als gefährlich eingestufte Dateien oder E-Mails werden in einen separaten Quarantäne-Ordner verschoben. Die Wiederherstellung von Dateien aus dem Quarantäne-Ordner ist nur nach vorheriger Freigabe durch aus gewählte Mitarbeiter möglich. Um die korrekte Funktion des eingesetzten Virenschanners sicherzustellen, erfolgt der regelmäßige Scan einer speziellen Testdatei, die von allen aktuellen Virenschutzlösungen erkannt wird.

3.2 Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall wiederherzustellen.

Beim Auftragnehmer umgesetzte Maßnahmen:

Dokumentation von datenschutzrelevanten Zwischenfällen;

Datenschutzrelevante Zwischenfälle, bei denen nicht ausgeschlossen werden kann, dass personenbezogene Daten gelöscht oder an unberechtigte Dritte weitergeleitet wurden, werden umfassend dokumentiert. Die Unterlagen dienen zum einen einer lückenlosen Kommunikation an die Datenschutzbehörden sowie die betroffenen Kunden, zum anderen können auf Basis dieser Informationen Verbesserungen umgesetzt werden, die ähnliche Vorfälle zukünftig verhindern.

Nutzung einer Versionskontrolle in der Entwicklung;

Für die Entwicklung von Anwendungen werden gängige Versionierungssysteme (z.B. Git) eingesetzt. Diese stellen sicher, dass vorherige Softwarestände nicht versehentlich überschrieben werden und die parallele Entwicklung durch mehrere Mitarbeiter an einem System nicht zu Fehlern oder zum Überschreiben von bestehenden Daten führt. Zudem können durch eine Versionskontrolle Änderungen und Fehler nachträglich schneller und besser nachvollzogen und behoben werden. Unabsichtlich durchgeführte Änderungen können außerdem rückgängig gemacht werden.

Überprüfung erstellter Datensicherungen;
Erstellte Datensicherungen werden regelmäßig auf ihre Integrität und Wiederherstellbarkeit hin überprüft. Hierfür werden zufällig ausgewählte Daten von einem zufällig ausgewählten Zeitpunkt testweise aus einer Datensicherung wiederhergestellt und mit den Originaldateien verglichen. So können unbrauchbare Datensicherungen oder Fehler im Backup- bzw. Wiederherstellungssystem frühzeitig erkannt und behoben werden.

Verwendung und regelmäßige Aktualisierung eines Spamfilters;
Um Kunden deren Mitarbeiter, für die wir im Rahmen unserer Dienstleistungen auch das E-Mail-Hosting übernehmen, vor Spam-E-Mails und Phishing-E-Mails zu schützen, kommen spezielle Spamschutzlösungen auf den von uns genutzten Mailservern zum Einsatz. Die zur Erkennung von Spam- und Phishing-E-Mails notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Um die korrekte Funktion des eingesetzten Spam-Filters sicherzustellen, erfolgt der regelmäßige Scan einer speziellen Testdatei, die von allen aktuellen Spamschutzlösungen erkannt wird.

Verwendung und regelmäßige Aktualisierung eines Virencanners;
Eingehende E-Mails sowie Arbeitsplatzrechner werden durch einen Virencanner vor den Auswirkungen von schädlichen Dateien geschützt. Die zur Erkennung von aktuellen Bedrohungen notwendigen Definitionen und Regeln werden regelmäßig aktualisiert. Als gefährlich eingestufte Dateien oder E-Mails werden in einen separaten Quarantäne-Ordner verschoben. Die Wiederherstellung von Dateien aus dem Quarantäne-Ordner ist nur nach vorheriger Freigabe durch ausgewählte Mitarbeiter möglich. Um die korrekte Funktion des eingesetzten Virencanners sicherzustellen, erfolgt der regelmäßige Scan einer speziellen Testdatei, die von allen aktuellen Virenschutzlösungen erkannt wird.

4 Weitere Maßnahmen

4.1 Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

Beim Auftragnehmer umgesetzte Maßnahmen:

Bedarfsweise Durchführung der Datenschutz-Folgenabschätzung (DSFA);
Vor einer geplanten Datenverarbeitung wird laut Art. 35 DSGVO eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dies ist zum Beispiel dann der Fall, wenn neue Technologien zum Einsatz kommen, zu denen bis lang wenig Erfahrungswerte vorliegen oder wenn eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten erfolgt (z.B. Verarbeitung von Gesundheitsdaten). Die Datenschutz-Folgenabschätzung enthält mindestens folgende Informationen: eine systematische Beschreibung der geplanten Verarbeitungsvorgänge, Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge, eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen. Nach Art. 35 DSGVO wird die Datenschutz-Folgenabschätzung spätestens nach drei Jahren wiederholt.

Dokumentation von datenschutzrelevanten Zwischenfällen;
Datenschutzrelevante Zwischenfälle, bei denen nicht ausgeschlossen werden kann, dass personenbezogene Daten gelöscht oder an unberechtigte Dritte weitergeleitet

wurden, werden umfassend dokumentiert. Die Unterlagen dienen zum einen einer lückenlosen Kommunikation an die Datenschutzbehörden sowie die betroffenen Kunden, zum anderen können auf Basis dieser Informationen Verbesserungen umgesetzt werden, die ähnliche Vorfälle zukünftig verhindern.

Jährliche Überprüfung der Wirksamkeit der ergriffenen Schutzmaßnahmen;
Es erfolgt jährlich eine innerbetriebliche Überprüfung zur Wirksamkeit der ergriffenen technischen und organisatorischen Schutzmaßnahmen. Hierzu werden die aktuellen Schutzmaßnahmen gemeinsam mit Vertretern aller Verantwortungsbereiche beleuchtet und sofern sinnvoll entsprechende Optimierungen festgelegt.

Sichere Entsorgung von gedruckten Dokumenten;
Gedruckte Dokumente mit sensiblem Inhalt werden nicht über den normalen Papiermüll entsorgt. Stattdessen stehen für deren sichere Entsorgung spezielle Aktenvernichter bzw. abschließbare Papiersammelbehälter zur Verfügung, die von einem Spezialunternehmen (z. B. Reisswolf) nachweislich vernichtet und entsorgt werden.

Sicheres Löschen nicht mehr benötigter Daten;
Nicht mehr benötigte Daten, wie zum Beispiel veraltete Kunden- sowie Projektdaten oder Daten aus Test- bzw. Entwicklungsumgebungen, werden gelöscht, sobald diese nicht mehr für die jeweilige Vertragserfüllung benötigt werden. Die Löschung erfolgt unter Zuhilfenahme spezieller Löschmodulare, welche eine nachträgliche Wiederherstellung der Daten unmöglich machen.

Zuteilung von datenschutzrelevanten Verantwortungsbereichen;
Datenschutzrelevante Verantwortungsbereiche werden je nach Tätigkeitsbereich auf Mitarbeiter verteilt. Dabei wird die Eignung der Mitarbeiter für den jeweiligen Verantwortungsbereich stets sichergestellt. Ggf. notwendige Schulungen oder Fortbildungen erfolgen vor der Übertragung eines Verantwortungsbereichs an einen Mitarbeiter. Alle datenschutzrelevanten Verantwortungsbereiche werden schriftlich festgehalten und auch in AV-Verträgen mit Endkunden berücksichtigt. Bei Austritt eines Mitarbeiters wird unverzüglich ein geeigneter Nachfolger benannt.

4.2 Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Beim Auftragnehmer umgesetzte Maßnahmen:

Abschluss von AV-Verträgen mit Dienstleistern, Partnern und Kunden;
Mit allen Dienstleistern, Partnern und Kunden, mit denen ein Austausch sowie eine Verarbeitung von personenbezogenen Daten erfolgen, wird ein Vertrag zur Auftragsdatenverarbeitung (AV-Vertrag) gemäß Art. 28 DSGVO geschlossen. In dem AV-Vertrag werden u. a. die folgenden Aspekte zwischen den beiden Vertragspartnern geregelt: "Anwendungsbereich und Verantwortlichkeit", "Gegenstand und Dauer des Auftrages", "Beschreibung der Verarbeitung, Daten und betroffener Personen", "Technische und organisatorische Maßnahmen zum Datenschutz", "Berichtigung, Einschränkung und Löschung von Daten", "Pflichten des Auftragnehmers", "Rechte und Pflichten des Auftraggebers", "Wahrung von Rechten der betroffenen Person", "Kontrollbefugnisse", "Unterauftragsverhältnisse", "Datengeheimnis und Geheimhaltungspflichten", "Haftung" und "Informationspflichten, Schriftformklausel,

Rechtswahl". Der AV- Vertrag wird von beiden Vertragsparteien in schriftlicher oder alternativ in digitaler Form geschlossen. Beide Vertragsparteien verpflichten sich zudem, unverzüglich über relevante Änderungen zu informieren, so dass der AV-Vertrag entsprechend geändert und erneut abgeschlossen werden kann.

Aufklärung von Kunden zum Thema Datenschutz;

Nach Auftragserteilung klären wir Kunden über die von uns ergriffenen Maßnahmen zum Datenschutz auf und binden diese so gut wie möglich in die entsprechenden Prozesse mit ein. Falls notwendig, empfehlen und installieren wir beim Kunden entsprechende Anwendungen, um einen optimalen Schutz personenbezogener Daten auch auf Kundenseite zu ermöglichen. So soll ein gleichermaßen hohes Sicherheitsniveau bei beiden Vertragspartnern sichergestellt werden.

Auswahl geeigneter Dienstleister und Partner unter Datenschutzaspekten;

Bei der Beauftragung von Dienstleistern und Partnern erfolgt vorab ein Vergleich möglicher Anbieter unter Datenschutzaspekten. Hierzu holen wir je nach Art und Umfang des Auftrags Informationen zur Verarbeitung von personenbezogenen beim jeweiligen Anbieter ein. Bewertet werden Aspekte wie die Übermittlung von Daten, deren konkrete Verarbeitung sowie die getroffenen technischen und organisatorischen Schutzmaßnahmen. Eine Zusammenarbeit erfolgt ausschließlich mit Dienstleistern und Partnern, die das geforderte Datenschutzniveau glaubhaft sicherstellen können.

Beauftragung zertifizierter Dienstleister und Partner;

Eine Zusammenarbeit erfolgt vorzugsweise mit Dienstleistern und Partnern, die über eine nachgewiesene Zertifizierung verfügen. Dies gilt insbesondere dann, wenn die Zertifizierung auf ein hohes Datenschutzniveau schließen lässt, zum Beispiel bei Anbietern von Webhosting-Dienstleistungen. Die Fristen der jeweiligen Zertifizierungen werden kontrolliert und ggf. neue Zertifizierungen von Dienstleistern und Partnern angefordert, sobald diese neu ausgestellt wurden. Erfolgt keine erneute Zertifizierung, so werden zukünftig vorzugsweise andere Dienstleister und Partner beauftragt, die über das jeweilige Zertifikat verfügen.

Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter;

Bei Eintritt in das Unternehmen werden alle wesentlichen Verhaltensrichtlinien zum Thema Datenschutz in schriftlicher wie persönlicher Form an neue Mitarbeiter kommuniziert. Neben unserem grundsätzlichen Verständnis vom Umgang mit personenbezogenen Daten vermitteln wir auch das notwendige Wissen zur korrekten Anwendung aller technischen und organisatorischen Datenschutzmaßnahmen.

Regelmäßige Unterweisung und Fortbildung von Mitarbeitern zum Thema Datenschutz;

Unsere Mitarbeiter werden regelmäßig zu relevanten Datenschutzthemen geschult. Dabei werden sowohl Grundlagen aufgefrischt als auch aktuelle Themen sowie rechtliche Änderungen vermittelt. Neben den entsprechenden datenschutztechnischen Kompetenzen soll so eine hohe Sensibilität für den Schutz personenbezogener Daten bei allen Mitarbeitern gefördert werden.

Schriftliche Anweisungen an Dienstleister;

Sämtliche Anweisungen für die Verarbeitung von personenbezogenen Daten durch Dienstleister werden schriftlich übermittelt und im persönlichen Gespräch erläutert. Die schriftlichen Anweisungen enthalten Informationen zur Art der personenbezogenen Daten sowie zu deren datenschutzkonformer Verarbeitung. Ebenfalls schriftlich vereinbart wird, wie Daten zwischen den beiden Parteien ausgetauscht werden und was bei datenschutzrelevanten Ereignissen zu tun ist.

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags;
Auftragsbezogene Daten mit personenbezogenen Inhalten, die zur Verarbeitung an uns übermittelt werden, werden bei Beendigung des Auftrags gelöscht, sofern diese nicht aus wichtigem Grund behalten werden müssen. Dies kann zum Beispiel dann notwendig sein, wenn sich aus dem Auftrag weitere Folgeaufträge ergeben, für deren vertragliche Umsetzung die Daten noch einmal benötigt werden. Eine ordnungsgemäße Löschung erfolgt dann nach Abschluss des letzten Folgeauftrags.

Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter;
Alle Mitarbeiter unterzeichnen beim Eintritt in das Unternehmen eine gesonderte Verschwiegenheitserklärung. Darin verpflichten sich die Mitarbeiter, personenbezogene Daten vertraulich zu behandeln und diese ausschließlich auf Weisung ihrer Vorgesetzten zu verarbeiten. Darüber hinaus wird der Mitarbeiter über mögliche Folgen von Verstößen gegen die Vertraulichkeitsverpflichtung aufgeklärt. Alle in der Verschwiegenheitserklärung vereinbarten Punkte gelten auch über den Zeitraum der Anstellung hinaus.