Leitfaden technische und organisatorische Maßnahmen im Rahmen der **DSGVO**

WIR SCHAUEN AUF ÖSTERREICH
WKO WIRTSCHAFTSKAMMERN ÖSTERREICHS

Bundesministerium
Digitalisierung und
Wirtschaftsstandort

it-safe.at

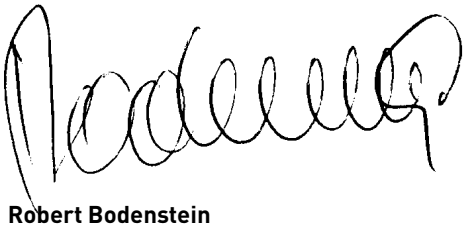
Vorwort

Seit dem 25. Mai 2018 – dem Stichtag für das Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) – hat sich einiges getan: Die österreichischen Betriebe haben sich informiert und weitergebildet, Veranstaltungen besucht und Beratungen in Anspruch genommen, um ihre Unternehmen fit für die neue Rechtslage zu machen: Datenschutz und Datensicherheit sind ins Zentrum der Aufmerksamkeit gerückt.

Speziell kleine und mittlere Betriebe konnte die Wirtschaftskammer Österreich (WKÖ) mit zahlreichen Anleitungen, Vorlagen und Musterdokumenten unterstützen. Ein Bereich ist aber immer noch von Unsicherheit betroffen: die technisch-organisatorischen Maßnahmen (TOMs), die die Unternehmen zum Schutz personenbezogener Maßnahmen umsetzen müssen. Denn der Gesetzestext bleibt hier – mit Absicht – recht vage: Da ist von „Datenschutz nach dem Stand der Technik" die Rede und von einem „dem Risiko angemessenen Schutzniveau" für personenbezogene Daten.

Mit dem vorliegenden Leitfaden wollen wir vor allem kleinen Betrieben eine Übersicht geben, welche technischen Sicherheitsvorkehrungen sinnvoll sind. Auch die Bedeutung der organisatorischen Maßnahmen und Regeln im Umgang mit Mitarbeiterinnen und Mitarbeiter und Kunden beleuchtet dieses Handbuch. Für drei exemplarische Kleinunternehmen stellen wir Ihnen außerdem die konkrete Umsetzung der TOMs vor. Anhand dieser Fallstudien können Sie die Umsetzung in der Praxis direkt nachvollziehen.

Wir wünschen Ihnen viel Erfolg mit dem Leitfaden.



Robert Bodenstein
Obmann der Bundessparte Information & Consulting
Wirtschaftskammer Österreich

WKO INFORMATION · CONSULTING

Die Broschüre erscheint im Rahmen von it-safe 2020, einem gemeinsamen Projekt der Wirtschaftskammer Österreich und des Bundesministeriums für Digitalisierung und Wirtschaftsstandort.

1. Auflage, Dezember 2018
Für den Inhalt verantwortlich: Prof. Mag. Dr. Manfred Wöhrl, Mag. Verena Becker, BSc

Impressum:
Medieninhaber/Verleger:
Wirtschaftskammer Österreich, Bundessparte Information und Consulting, 1045 Wien,
Wiedner Hauptstraße 63; ic@wko.at, https://wko.at/ic
Grafische Umsetzung: www.designag.at

Einleitung

Warum sollten Sie sich überhaupt Gedanken über IT-Sicherheit und Datenschutz in Ihrem Unternehmen machen? Das Datenschutzrecht schreibt vor, dass Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung personenbezogener Daten zu treffen sind. Dafür ist es notwendig, die entsprechenden Prozesse im Unternehmen zu **lokalisieren**, zu **dokumentieren** und zu **optimieren**.

Nutzen Sie die rechtlichen Vorgaben gleich zu Ihrem unternehmerischen Vorteil! Machen Sie sich jetzt Gedanken, wie es mit IT-Sicherheit und Datensicherheit in Ihrem Unternehmen aussieht. Sie schaffen dadurch eine sichere Grundlage für Ihre digitalisierten Geschäftsprozesse, beugen zeit- und kostenintensiven Vorfällen vor und verschaffen sich dadurch einen wesentlichen Wettbewerbsvorteil.

Datensicherheit und Datenschutz sind Chefsache. Die Geschäftsleitung muss entscheiden, welche Maßnahmen zu treffen sind und die entsprechenden finanziellen und personellen Ressourcen zur Verfügung stellen. Sie ist für die Umsetzung der EU-Datenschutzgrundverordnung (DSGVO) verantwortlich und haftet bei Verletzung der Datenschutzvorgaben.

Schieben Sie daher eventuell bisher vernachlässigte Schritte im Bereich der **Security-Maßnahmen** nicht mehr auf die lange Bank und handeln Sie jetzt.

Dieser Leitfaden legt in einfacher Form das Zusammenspiel technischer und organisatorischer Maßnahmen im Sinne des Datenschutzrechts (DSGVO und Datenschutz Anpassungsgesetz 2018) dar und zeigt Ihnen gleichzeitig **sinnvolle Schritte** für die Optimierung sicherheitsrelevanter Prozesse in Ihrem Unternehmen.

Zu Beginn des Leitfadens befassen wir uns mit den **technischen Grundlagen**. Dann erfahren Sie, welche **organisatorischen Grundlagen** es gibt und wie Sie auch in kleinen Unternehmen ein sinnvolles **Datenschutzmanagementsystem** (DSM) einführen oder ein bestehendes optimieren können. Das Kapitel **TOMs (=technische und organisatorische Maßnahmen)** geht auf die konkreten Umsetzungsschritte im Unternehmen ein.

Denken Sie auch an Ihre **Mitarbeiterinnen und Mitarbeiter**! Ein eigenes Kapitel beschäftigt sich mit deren wichtiger Rolle bei der Umsetzung der Maßnahmen im Unternehmen. Selbstverständlich dürfen auch die **rechtlichen Grundlagen** nicht fehlen.

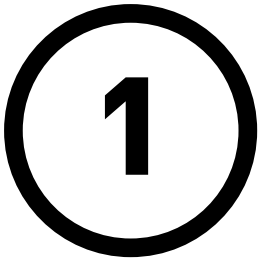
In den **Fallbeispielen** finden Sie konkrete Formulierungsbeispiele für technische und organisatorische Maßnahmen (TOMs) als Unterstützung für Ihre eigene Dokumentation.

Wir wünschen Ihnen viel Erfolg bei der Umsetzung.

Weiterführende Informationen:

- Datenschutzrecht
- IT-Sicherheit
- FAQs Datensicherheit nach der EU-Datenschutz-Grundverordnung

Inhalt



Technische Grundlagen

Die Technik entwickelt sich rasant weiter, bestehende Technologien werden rasch durch neue ersetzt. Dabei dürfen datenschutzrechtliche Vorgaben nicht vergessen werden. Die EU-Datenschutz-Grundverordnung (DSGVO) regelt den Umgang mit personenbezogenen Daten. Sie gibt vor, dass technische und organisatorische Maßnahmen (TOMs) zu treffen sind, die den Schutz personenbezogener Daten gewährleisten.

Diese TOMs sind zu dokumentieren (z.B. mittels Word-Dateien und/oder Tabellen) und in regelmäßigen Abständen auf ihre Wirksamkeit hin zu überprüfen. Außerdem müssen sie dem Stand der Technik entsprechen, d.h. sowohl die Maßnahmen als auch die verwendete Technik sind regelmäßig anzupassen.

1.1. Zusammenspiel Server-Client

Der Servicegedanke ist zum Kernthema der gesamten IT-Industrie geworden: Anwendungen (z.B. Office-Paket, Buchhaltungssoftware) laufen auf Servern und werden von Endgeräten (z.B. PC, Smartphone, Drucker) bzw. Benutzern als „Clients" verwendet.

Dadurch entstehen neue Herausforderungen an die Netzwerkorganisation und zugleich auch an die Informationssicherheit: Daten - und damit klarerweise auch personenbezogene Daten - sind oft bei Partnerfirmen (Rechenzentren) gespeichert, wodurch auch die Datenübertragung zu einem Sicherheitsthema wird.

1.2. Firewall

Eine Firewall kontrolliert die Netzwerkverbindungen zwischen Firmennetzwerk und Internet und blockiert alle Verbindungen, die nicht als „erlaubt" konfiguriert wurden. Der Einsatz von Firewalls gehört heute zum Standard jeder IT-Installation, das gilt im besonderen Fall auch für ein Home-Office.

TIPP

Jede Firewall muss richtig installiert und konfiguriert werden, um wirksamen Schutz zu bieten. Hinterfragen Sie, wie Ihre Firewall konfiguriert ist und notieren Sie das entsprechend.

In Firewall-Regelwerken kann genau angegeben werden, welche Datenpakete die Firewall passieren dürfen, welche ignoriert oder zurückgewiesen werden.

Firewalls von heute sind nicht nur mehr „Schutzmauern" eines lokalen Netzwerkes gegen Angriffe aus dem Internet, sie können auch weitere Sicherheitsaufgaben erfüllen:

- Ausführliche Protokollierung des Datenverkehrs
- Setzen von Aktionen bei Einbruchsversuchen (Intrusion-Protection-Systems IPS/Intrusion-Reaction-Systems IRS)
- Verwaltung sicherer Zugänge von Remote Geräten
- Malware-Detection für das zu sichernde LAN

TIPP

Sehr häufig sind die oben genannten Services in der IT-Fernwartung inkludiert und sind dementsprechend im Hinblick auf Datenschutz als spezieller Vertragspunkt in den Auftragsverarbeitungs-Vertrag aufzunehmen.

1.3. Remote Zugriff

Ein Fernzugriff auf Rechner in Ihrem Unternehmen kann aus unterschiedlichen Gründen sinnvoll und notwendig sein, z.B.:

- Mitarbeiterinnen oder Mitarbeiter benötigen Daten während eines mobilen Einsatzes
- die Administration der IT wurde extern vergeben

In beiden Fällen ist der externe Zugang entsprechend abzusichern. Dabei geht es auch darum, den unbefugten physischen Zugriff auf die Geräte zu verhindern, von denen auf firmeninterne Server zurückgegriffen wird.

TIPP

Beachten Sie, dass auch bei einem Home-Office betriebsfremde Personen (Familienmitglieder, Reinigungskraft, Gäste) Zugriff haben können und Schutzmaßnahmen vor unbefugtem Zugriff oder Diebstahl zu treffen sind (z.B. Bildschirmsperre beim Verlassen Arbeitsplatzes, Versperren von Dokumenten in einem Safe).

1.4. Cloud

Cloudlösungen (z.B. office365, icloud, viele E-Mail-Systeme, viele Webshop-Lösungen, File-Ablagen zum Datenaustausch) sind aus dem unternehmerischen Umfeld nicht mehr wegzudenken. Für die Verwendung von Cloudlösungen ist die Einhaltung einiger Regeln für den DSGVO-konformen Betrieb wichtig.

Cloud-Anbieter sind Auftragsverarbeiter im Sinne der DSGVO. Der Verantwortliche darf nur solche Auftragsverarbeiter beauftragen, die eine datenschutzkonforme Verarbeitung gewährleisten. Der Cloudanbieter muss ebenfalls geeignete technische und organisatorische Maßnahmen zur Sicherung personenbezogener Daten treffen und diese auch nachweisen.

TIPP

Mit dem Gütesiegel „Austrian Cloud" weisen österreichische Cloud-Anbieter darauf hin, dass die Daten in Österreich gespeichert werden und die Vorgaben des Datenschutzes und Sicherheitsaspekte eingehalten werden.

Austriancloud

1.5. Verschlüsselung

Verschlüsselung bedeutet, dass ein klar lesbarer Text mittels kryptologischer Verfahren in einen „Geheimtext" umgewandelt wird und nur mittels eines Schlüssels wieder lesbar gemacht werden kann. Artikel 32 DSGVO nennt die Verschlüsselung von Daten ausdrücklich als eine mögliche Maßnahme um Daten zu schützen.

Die Verschlüsselung von Daten kann das Risiko eines Vorfalls bei der Datenverarbeitung wesentlich minimieren. Außerdem bringt sie für Unternehmen einen großen Vorteil bei der Meldepflicht. Im Falle eines Datenverlustes (z.B. durch Verlust eines mobilen Gerätes) entfällt bei entsprechender Verschlüsselung der Daten die Pflicht, dies der Datenschutzbehörde zu melden bzw. auch die betroffenen Personen zu verständigen.

Die Qualität einer Verschlüsselung hängt in der IT dabei immer von drei Parametern ab:

VERSCHLÜSSELUNGSMETHODE

Derzeit werden nach dem Stand der Technik zwei Verfahren eingesetzt:

- **Symmetrisches Verfahren**

Für die Verschlüsselung und Entschlüsselung wird derselbe Schlüssel (Key) verwendet, das Verfahren ist schnell, benötigt weniger Rechnerressourcen, ist aber bei durchschnittlicher Key-Länge nicht sehr sicher. Für Realzeitanwendungen (Festplattenverschlüsselung, Verschlüsselung der Datenübertragung per VPN) ist dieses Verfahren bevorzugt im Einsatz. Derzeit ist die Verschlüsselungsvariante AES256 als Stand der Technik anzusehen.

Bei Einsatz von Internet-of-Things-Devices zur Erfassung personenbezogener Daten (z.B. Überwachungskameras, Zutrittskontrollsystem), die oft eine sehr geringe Rechenleistung besitzen, ist meistens nur ein symmetrisches Verfahren zu Verschlüsselung möglich. Achten Sie hier besonders auf die Einhaltung entsprechender zusätzlicher Sicherheitsvorkehrungen, wie z.B. einem Firewallschutz bei einem Zugriff über das Internet.

In der Praxis wird aus Sicherheitsgründen der symmetrische Key in regelmäßigen Abständen automatisch erneuert. (Bei VPNs zum Beispiel täglich). Der neu generierte Key muss dem Kommunikationspartner übermittelt werden. Damit steigt das Risiko, dass jemand diesen Schlüssel entwendet. Aus diesem Grund wird der neue Key mit dem sicheren asymmetrischen Verfahren übermittelt.

- **Asymmetrisches Verfahren**

Für die Verschlüsselung und Entschlüsselung kommen zwei unterschiedliche Keys zum Einsatz, die nach einem komplexen Algorithmus gemeinsam erzeugt werden. Nur beide Keys zusammen ermöglichen eine sichere Kommunikation:

Public-Key: Dieser Schlüssel kann – wie der Name schon sagt – öffentlich abgelegt werden bzw. jedem gewünschten Kommunikationspartner übermittelt werden. Er dient dazu, eine Datei für einen einzigen Adressaten zu verschlüsseln, der den dazu passenden Private-Key besitzt. Damit ist das Problem des Abhörens gelöst: Jeder kann die Datei betrachten, sie bleibt für alle – außer dem Empfänger als Besitzer des zugehörigen Private-Keys – ein unbekanntes Bitmuster.

Private-Key: Dieser Schlüssel ist sorgfältig zu verwahren, nur dieser ermöglicht das Entschlüsseln einer übertragenen Datei. Klarerweise ist dieser Schlüssel mit einem PIN geschützt. In weiterer Folge kann im Rahmen der Erstellung des Schlüsselpaars eine unabhängige Organisation (CA für „Certificate-Authority")bestätigen, dass dieser Private-Key einer ausgewiesenen Person gehört.

- **Länge eines Schlüssels (Keys)**

Die Länge eines Schlüssels wird in Bit angegeben und sollte ein möglichst zufälliges Bitmuster darstellen. Wie auch bei normalen Passwörtern wäre sonst ein Angriff durch Erraten und Probieren („Brute-Force-Attack") leicht möglich.

- **Umgang mit dem Schlüssel (Key Management)**

Gerade dieser Punkt ist mit einem hohen Risiko behaftet, hier spielt der Mensch die wesentliche Rolle. Es beginnt mit der Erstellung des Schlüssels bzw. eines Schlüsselpaares. In weiterer Folge muss der Schlüssel (de facto ein Bitmuster), irgendwo sicher gespeichert werden. Schlüssel sind in der Regel mit einem PIN oder Passwort geschützt, die gut auszuwählen und sorgsam zu verwahren sind.

1.6. Digitale Signatur

Eine digitale Signatur ist ein Bitmuster, das aus einem Dokument errechnet wird und die Echtheit dieses Dokuments bestätigt. Diese Bit-Folge wird als Zeichensequenz am Ende des Dokuments angefügt.

Folgende Informationen werden durch eine digitale Signatur garantiert:

- **Unverfälschtheit der Information**
- **Autor des Dokuments (Absender)**
- **Datum der Erstellung**
- **Organisation, die die Echtheit bestätigt**

Die Qualität einer digitalen Signatur hängt klarerweise mit der Vertrauenswürdigkeit der Organisation zusammen, die ein Public/Privat-Key-Paar erstellt.

TIPP

Mit der „Handy-Signatur" können Sie PDFs rechtsgültig mit einer elektronischen Unterschrift versehen und so z.B. Verträge schnell und unkompliziert unterzeichnen.

Handy-Signatur

1.7. Virtual Private Networks (VPN)

Verwenden Sie bei heiklen Geschäften (z.B. Onlinebanking, Online-Bestellungen) und im Unternehmensbereich immer sichere Datenverbindungen. Dazu wird eine Verschlüsselungstechnik benötigt, die eine „private" Verbindung von Ihrem Arbeitsplatz zum Zielrechner aufbaut.

Unter einem Virtual Private Network (kurz VPN) versteht man eine Verbindung von lokalen Netzwerken oder Zugängen zu diesen, die durch geeignete Verschlüsselungsmethoden vor fremdem Zugriff geschützt ist.

Prinzipiell werden zwei Varianten von VPNs unterschieden:

- **Sichere Anbindung einer Außenstelle** mit dem eigenen lokalen Netzwerk, z. B. in der Firmenzentrale. In diesem Fall wird eine sichere Verbindung über das Internet als VPN von der Firewall der Filiale zur Firewall der Firmenzentrale geschaltet.

- **Zugang zum Firmen-LAN mittels einzelner Devices,** z.B. einem Notebook oder einem Remote Arbeitsplatzrechner. Bei dieser Lösung erfolgt der Aufbau des VPN vom Client zu einem Zielsystem (in der Regel Server im Firmen LAN) oder einem sogenannten VPN-Konzentrator. Letzteres wird meistens bevorzugt, da ein „Terminieren" des VPN-Tunnels auf der Firmenfirewall diese in ihren sonstigen Aufgaben behindern könnte (Performance-Verlust). VPNs sind eine rechenintensive Anwendung.

TIPP

Ein VPN ist eine wichtige Schutzmaßnahme für den Weg der Datenübertragung, es schützt aber nicht die Endpunkte! Wurde der Server oder Client im Zuge eines Hackerangriffs übernommen, besteht trotz „sicherer" VPN-Verbindung ein Risiko für den jeweils anderen Endpunkt. Sichern Sie daher zusätzlich beide Endpunkte (Server und Client) ab.

1.8. Anonymisierung und Pseudonymisierung

Gemäß DSGVO ist das Pseudonymisieren von Daten eine der empfohlenen Maßnahmen für den Schutz personenbezogener Daten.

Pseudonymisierung von Daten bedeutet, dass nur durch Hinzuziehen weiterer Informationen ein Rückschluss auf personenbezogene Daten erfolgen kann. Das kann zum Beispiel eine Personal-ID sein, deren Personenzuordnung getrennt abgelegt ist. Damit kann man einen Datensatz nach Entfernen relevanter Informationen (z.B. Name oder Adresse) an einen Auftragsverarbeiter übermitteln und erreicht so, dass dieser keinen Rückschluss auf die tatsächlich betroffene Person ziehen kann.

Bei anonymisierten Daten werden die personenbezogenen Informationen nicht nur getrennt gespeichert, sondern vollständig entfernt. Die verbleibenden Informationen sind damit datenschutzrechtlich nicht mehr relevant.

TIPP

Wenn Datensätze pseudonymisiert gespeichert werden, muss im Falle eines Datenverlustes (Data-Breach) keine Meldung an die Datenschutzbehörde gemacht werden, da kein Risiko für Betroffene besteht.

Managementsysteme

In der Praxis bieten Managementsysteme aufeinander abgestimmte Regeln und Dokumente (Prozessdokumentationen, Arbeitsanweisungen, Checklisten usw.) als verbundenes System, um bestimmte Ziele einer Organisation zu erreichen.

Die Einführung und der Aufbau von Managementsystemen liegt in der Verantwortung der Unternehmensleitung. Um die inhaltliche Wirksamkeit von Managementsystemen beurteilen zu können, werden sogenannte Audits – intern oder von externen Spezialisten oder Organisationen – in regelmäßigen Abständen durchgeführt.

TIPP

Speziell bei Ein-Personen-Unternehmen werden Managementsysteme kaum verwendet – alle Daten, Fakten und Abläufe für die konkrete Betriebsführung sind dem Unternehmer ja selbst bekannt. Denken Sie aber auch hier rechtzeitig an Maßnahmen zur Aufrechterhaltung der Betriebskontinuität, z.B. wenn sich das Unternehmen zu einem Kleinunternehmen mit mehreren Mitarbeiterinnen und Mitarbeitern entwickelt oder eine Betriebsübergabe geplant ist.

2.1. Dokumentation und Verarbeitungsverzeichnis

Die DSGVO sieht vor, dass Verantwortliche und Auftragsverarbeiter ein „Verzeichnis von Verarbeitungstätigkeiten“ (Verarbeitungsverzeichnis) führen: Der Inhalt ist ähnlich den alten DVR-Meldungen und muss folgende Informationen enthalten: Den Zweck der Verarbeitung, die Kategorien der betroffenen Personen und die Kategorien der personenbezogenen Daten, die Kategorien von Empfängern, gegebenenfalls die Übermittlung von personenbezogenen Daten an ein Drittland und die vorgesehene Speicherdauer. Weiters sind die konkreten technischen und organisatorischen Datensicherheitsmaßnahmen (TOMs) ausführlich anzuführen.

Verarbeitungsverzeichnis für Verantwortliche

Verarbeitungsverzeichnis für Auftragsverarbeiter

TIPP

Nutzen Sie das verpflichtende Verarbeitungsverzeichnis mit der Aufstellung ihrer TOMs und erstellen Sie damit eine erweiterte Version des Verarbeitungsverzeichnisses für rein interne Zwecke, die konkret und detailliert auf die firmeninternen Maßnahmen eingeht.
Beispiel:
Verarbeitungsverzeichnis TOM: Systemadministration
interne Version TOM: Konfiguration der Server inkl. Beschreibung der Softwareversionen

Sie erhalten damit eine laufend aktuelle Dokumentation Ihrer Netzwerkumgebung. Dadurch können firmenkritische Ausfälle bei Vorfällen (z.B. Servertausch, technischer Defekt, Wechsel des Administrators) reduziert und oft zeit- und kostenintensive Schäden vermieden werden.

Auftragsverarbeitungs-Vertrag

Aus der DSGVO ergibt sich eine erhebliche Rechenschaftspflicht, im Rahmen derer Unternehmen nachweisen müssen, dass sie alle Anforderungen erfüllt haben.

Für diese Dokumentation der Abläufe im Unternehmen sind das Verarbeitungsverzeichnis und Auftragsverarbeitungs-Verträge verpflichtend vorgesehen.

Weitere Dokumente zur Dokumentation können z.B. sein:

- Richtlinien
- Checklisten
- Protokolle
- To-Do-Listen
- Aus- und Weiterbildungsunterlagen

2.2. Prozesse & Verfahren

In einem Unternehmen laufen eine Reihe verschiedener Prozesse (z.B. der Prozess zur Aufnahme eines neuen Mitarbeiters) gleichzeitig ab. Die Summe aller Prozesse eines Unternehmens stellen im Prinzip das Unternehmen selbst dar.

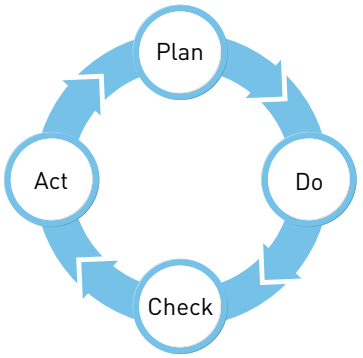
Im Verarbeitungsverzeichnis werden mehrere Prozesse sinnvoll zu Verfahren zusammengefasst. Zum Beispiel würde im Verarbeitungsverzeichnis bei kleinen Unternehmen das Verfahren „Personalmanagement" genannt werden, bei größeren Unternehmen würde dieses in einzelne Verfahren wie z.B. Anstellungsverfahren, Verfahren zum Abteilungswechsel, etc. aufgesplittet werden.

2.3. Zyklische Kontrolle der Wirksamkeit

Gemäß DSGVO sind personenbezogene Daten nach dem „Stand der Technik" zu schützen. Da sich dieser Stand der Technik genauso wie die Abläufe im Unternehmen ständig weiterentwickeln, sind auch die TOMs regelmäßig auf ihre Wirksamkeit hin zu überprüfen, damit das definierte Datenschutzniveau erhalten bleibt.

Diese zyklische Vorgangsweise nennt man PDCA-Zyklus:

- Plan (Planen)
- Check (Überprüfen)
- Do (Durchführen)
- Act (Anpassen)



Sinn dieses bewährten Verfahrens ist es, einen kontinuierlichen Verbesserungsprozess sicherzustellen. Dabei werden die technischen und organisatorischen Maßnahmen zuerst geplant („plan"), im „Kleinen Kreis" getestet („do"), danach die Wirksamkeit überprüft („check") und bei Bedarf angepasst und schließlich „im Großen" eingeführt („act"). Es handelt sich dabei um einen nie endenden Kreislauf, sodass sichergestellt ist, dass nach jeder Verbesserung eine erneute Überprüfung zu erfolgen hat.

2.4. Security Management

Wenn wir heute über Sicherheit sprechen, meinen wir nicht nur die technischen Aspekte der IT-Sicherheit, sondern in einem umfassenderen Begriff die Informationssicherheit, die in der DSGVO – bezogen auf personenbezogene Daten – gefordert wird. Die Basis dafür ist ein sogenanntes Informationssicherheits-Managementsystem (ISMS) oder konkret in Richtung Datenschutz ein Datenschutz-Managementsystem (DSM).

TIPP

Auch das Wissen in den Köpfen der Mitarbeiterinnen und Mitarbeitern betrifft in vielen Fällen personenbezogene Daten und kann – auch unbewusst – zu unberechtigter Weitergabe führen! Treffen Sie auch hier entsprechende Vorkehrungen und weisen Sie Ihre Mitarbeiterinnen und Mitarbeiter auf die Datenschutzvorgaben hin.

2.5. Risikomanagement

Der Umgang mit Risiken und die Einführung geeigneter Gegenmaßnahmen sowie deren Kontrolle auf Wirksamkeit wird als Risikomanagement bezeichnet.

In der Praxis sind Sicherheit und Kosten stets gegeneinander abzuwägen: Im Rahmen einer Risikoanalyse ist abzuschätzen, ob und welche Sicherheitsmaßnahmen im konkreten Fall sinnvoll sind. Dabei sind die Gesamtkosten (inklusive der Kosten einer allfälligen Betriebsunterbrechung) bei Sicherheitsvorfällen entsprechend zu berücksichtigen.

Ein Beispiel aus der Praxis: Der Ausfall eines Bauteils in einem Kühlsystem (z.B. in einer Klimaanlage) könnte im Schadensfall Kosten von weniger als 1000 € verursachen. Derselbe Bauteil in einem Kühlsystem eines Reaktors könnte einen Millionenschaden nach sich ziehen.

Ziel des Risikomanagements muss es sein, Schäden so gering wie möglich zu halten. Einen ähnlichen Ansatz – betrachtet von der positiven Seite – verfolgt das sogenannte Business-Continuity-Management, das dafür sorgen soll, dass alle geschäftskritischen Prozesse – je nach ihrer Klassifizierung – auch im Krisenfall (in einem kalkulierbaren Notbetrieb) weiterlaufen können.

Teil des Risikomanagements ist auch die Einbindung von Partnern. Wenn Anbieter (z.B. Cloud-Dienste, Newsletter-Management-Anbieter, IT-Dienstleister) personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten, sind diese Auftragsverarbeiter im Sinne der DSGVO. Auch diese müssen DSGVO-konform vorgehen und entsprechende technische und organisatorische Maßnahmen vorsehen. Zur Dokumentation ist ein Auftragsverarbeitungs-Vertrag anzuschließen.

2.6. Datenschutz-Management

Ein Datenschutzmanagementsystem (DSMS) ist die Sammlung aller Prozesse und deren Dokumentation, die beim Umgang mit personenbezogenen Daten notwendig sind.

Eine konkrete Vorschrift über die Form eines DSMS gibt es in der DSGVO nicht. Das kann in einfacher Form für Ein-Personen-Unternehmen als Sammlung von Office-Dokumenten bis zu eigenen Programmen für Kleinunternehmen reichen, die Datenbank-basierend in einer benutzerfreundlichen Oberfläche die Hauptaufgaben gemäß DSGVO abbilden.

Diese, meist kostenpflichtigen Lösungen, bieten die Möglichkeit, ausgehend von einem Verarbeitungsverzeichnis und einer Reihe von gespeicherten Dokumenten, in einfacher Form Auskunftsbegehren zu beantworten und auch Lösch-Verfahren durchzuführen.

Beim Aufbau eines DSM kann es hilfreich sein, sich an bereits bestehenden Normen (z.B. BS 10012:2017 „Data Protection - Specification for a personal information management system“, die in Abschnitt 8 die DSGVO-Anforderungen in das Managementsystem integriert hat) zu orientieren oder ein entsprechendes Zertifikat zu erwerben.

2.7. User Management

Die Verwaltung von Benutzern stellt einen kritischen Bereich dar. Durch die Erstellung von Benutzerprofilen sollte genau geregelt werden, wer auf welche Daten zugreifen darf und auch das Recht hat, diese zu verändern oder zu löschen.

Administratoren, die diese Aufgaben erfüllen, sind entsprechend zu schulen und müssen auch nachweislich den vorgegebenen organisatorischen Regeln folgen. Dazu gehört vor allem die revisionssichere Protokollierung bei der Einrichtung von Benutzern.

Kapitel 4.4. Mitarbeiterinnen und Mitarbeiter

3

DSGVO & TOMs

Die DSGVO fordert in Artikel 32 konkrete technische und organisatorische Sicherheitsmaßnahmen zum Schutz personenbezogener Daten. Welche Risiken tatsächlich zu beachten sind und welche Maßnahmen für das Einhalten entsprechender Datenschutzniveaus zu setzen sind, liegt in der Verpflichtung des Verantwortlichen, somit der Geschäftsleitung. Basis dieser Entscheidungen bildet eine Risikoanalyse.

3.1. Stand der Technik

Der Stand der Technik ist ein unbestimmter Rechtsbegriff, sowohl in der DSGVO als auch im Datenschutzgesetz, der in verschiedenen Bereichen Verwendung findet und auf die Entwicklung von Wissenschaft und Technik Bezug nimmt.

Im technischen Umfeld findet eine dynamische Weiterentwicklung statt. Je nach Kernkompetenz eines Unternehmens muss selbst oder durch Hinzuziehen von externen Experten dafür gesorgt werden, dass die gesamte für den Betrieb notwendige Technologie auf dem aktuellen Stand der Technik betrieben wird. Das gilt im IT-Security-Umfeld ganz speziell, da mögliche Angriffe von innen und außen sich ebenfalls neuester Techniken bedienen.

Als Stand der Technik im Sinne der DSGVO ist für Unternehmen jeder Größe z.B. der Einsatz einer entsprechend konfigurierten Firewall zum Schutz personenbezogener Daten zu sehen.

3.2. Maßnahmen und Auswirkungen allgemein

Nach der DSGVO muss jeder Verantwortliche dafür sorgen, dass er die vom Betroffenen übergebenen personenbezogene Daten nach dem Stand der Technik schützt. Das gilt bei der Weitergabe der personenbezogenen Daten auch für den Auftragsverarbeiter.

Data Breach Notification – Meldung an die Datenschutzbehörde

Data Breach Notification – Benachrichtigung der betroffenen Person

3.2.1. Datenverlust (Data Breach)

Unter einem „Data Breach" (Datenverlust) versteht man den Verlust personenbezogener Daten bzw. den Fall, dass Unberechtigte Zugriff auf personenbezogene Daten bekommen. Das reicht vom Verlust eines Datenträgers über den Diebstahl eines Notebooks bis hin zu einem Hackerangriff aus dem Internet. Es sind nach dem Stand der Technik geeignete technische und organisatorische Maßnahmen zum Schutz der Daten zu treffen.

3.3. Vertraulichkeit

Grundsätzlich dürfen nur berechtigte Personen Zugriffe auf personenbezogene Daten durchführen.

TIPP

Bei Einsatz eines Fileservers dürfen nur Mitarbeiterinnen und Mitarbeiter des jeweiligen Projektes auf einem Projektordner, der personenbezogene Daten enthält, Zugriff haben. Der Schutz kann sich bis auf Datei-Ebene erstrecken.

3.4. Integrität

Unter Integrität der Daten versteht man den Schutz personenbezogener Daten vor unberechtigter Veränderung. Ein Angriff auf die Integrität wäre z.B. die Verfälschung von Daten, wenn der Empfänger eine andere Nachricht erhält, als vom Sender abgeschickt wurde. Die Integrität kann aber z.B. auch durch fehlerhafte Soft- oder Hardware, die falsche Ergebnisse liefert, verletzt sein. Vorbeugend kann man Daten z.B. mit einer digitalen Signatur versehen (technische Maßnahme), damit wäre jede Veränderung sofort erkennbar.

Unter Einsatz entsprechender Protokollierung des Zugriffs auf personenbezogene Daten kann über die entsprechenden Logfiles ungewollte oder unberechtigte Veränderung erkannt und zeitnah reagiert werden (organisatorische Maßnahme).

3.5. Verfügbarkeit

Die Verfügbarkeit personenbezogener Daten ist nicht nur ein wichtiger Faktor für Geschäftsprozesse des Unternehmens, sondern auch seitens der DSGVO gefordert.

Im ersten Schritt ist zu analysieren, wo in meinem Unternehmen sich sogenannte SPOFs (Single-Point-of-Failure) befinden, die den Betrieb meiner wichtigsten Geschäftsprozesse unterbrechen könnten. Im Anschluss daran ist jeder SPOF zu klassifizieren und je nach seiner Wichtigkeit für das Unternehmen entsprechend technisch oder organisatorisch durch geeignete Maßnahmen abzusichern. Diese sollten ganz konkret in den internen TOMs abgebildet werden.

Ursachen für den Ausfall von Systemen oder Teilen davon können sein:

SCHWACHSTELLEN IN DER HARDWARE

Hier spielt die Qualität der ausgewählten Geräte und damit auch deren Lebensdauer eine wichtige Rolle. In der Praxis gibt es zwei Möglichkeiten zur Absicherung aus technischer Sicht:

- **„Cold Standby":** Sie haben ein Ersatzgerät ausgeschaltet im Lager, das im Bedarfsfall das ausgefallene Gerät ersetzen kann. Zu beachten ist dabei, wie lange es dauert, bis das Ersatzgerät die Funktion übernommen hat und dass alle notwendigen Konfigurationen richtig eingestellt sind.

- **„Hot Standby“:** Ein Ersatzgerät läuft einsatzbereit und eingeschaltet zum Originalgerät, bei Problemen kann das Zweitgerät die Aufgaben des ersten sofort übernehmen. Der Vorteil ist, dass ein Benutzer mitunter den Ausfall des Erstgerätes nicht einmal bemerkt. Der Nachteil darin liegt in den Kosten und leider auch darin, dass man bei vielen Installationen auf Dauer unbemerkt nur mehr mit dem Zweitgerät arbeitet.

TIPP

Sorgen Sie dafür, dass ein Ersatzgerät in seiner Konfiguration immer dem aktuellen Stand entspricht, damit der Betrieb im Ernstfall nach dem Tausch problemlos weiterlaufen kann.

Als rein organisatorische Maßnahme zur Absicherung der Hardware können Wartungsverträge abgeschlossen werden. Darin sollte aber nicht nur eine **Antwortzeit** im Falle eines Vorfalls genau definiert sein, sondern auch die **Lösungszeit**, da diese für das Weiterführen des Betriebes wesentlich ist!

TIPP

Bei hochqualitativen Systemen mit besonders langer Lebensdauer rechnet man mit keinem Ausfall mehr. Wenn dieser dann eintritt kann es möglicherweise keine Ersatzsysteme am Markt mehr geben.
Dieser Umstand ist unbedingt zu beachten und entsprechend organisatorisch vorzusorgen, z.B. mit geprüften Wartungsverträgen oder einem Ersatzgerät auf Lager!

MÄNGEL IN DER SOFTWARE

Durch Fehler in der Software kann es zu Programmabstürzen kommen. Dieser Schwachstellen in der Verfügbarkeit kann man vor allem durch entsprechende Qualitätsmanagementmaßnahmen entgegenwirken. Das betrifft vor allem den Update-Prozess einer Software.

TIPP

„Sand-Box-Technik“: Führen Sie heikle System- oder Software-Updates nicht im Echtsystem durch, sondern in einer gesicherten Testumgebung und führen Sie diese erst nach Freigabe in den Echtbetrieb über.

FEHLER IN DER ORGANISATION

Organisatorische Risiken für die Verfügbarkeit können durch entsprechende Schulung/Belehrung und entsprechende Richtlinien verringert werden.

Ursachen können sein:
- **Fehlbedienung** (z.B. irrtümliches Löschen)
- **Fehladministration** (z.B. falsche Berechtigungen in Benutzer-Profilen)

3.6. Belastbarkeit

Eine Überlastung laufender Systeme kann zum Ausfall einzelner Services bis zum Zusammenbruch des Gesamtsystems führen.

Die Belastbarkeit ist in engem Zusammenhang mit der Verfügbarkeit zu betrachten. Maßnahmen wie der Einsatz von Hot-Stand-by-Systemen zum Ausbalancieren von Serveranfragen reduzieren die Belastung einzelner Systeme.

Eine kontinuierliche Beobachtung der Auslastung einzelner Systeme (speziell der Serversysteme) führt zu einer rechtzeitigen Erkennung von möglichen Engpässen. Damit können in den meisten Fällen zeitgerecht vor Eintreten einer kritischen Situation geeignete Maßnahmen ergriffen werden.

3.7. Wiederherstellbarkeit

Die Strategie zur Wiederherstellung ausgefallener Systeme hängt direkt mit deren Bedeutung für die firmeninternen Prozesse zusammen. Auch hier ist eine rechtzeitige Vorbereitung für den Notfall wesentlich.

Folgende Fragen sind vorab zu klären:
- Wie lange darf ein (Teil-)System ausfallen?
- Wird für die Fehlerbehebung eine Ersatzhardware benötigt?
- Wie lange dauert die Beschaffung eines Ersatzsystems?
- Wieviel Zeit benötigt die Re-Installation und neuerliche Inbetriebnahme?

Speziell der letzte Punkt betrifft personelle Ressourcen und auch entsprechendes Know-how. Darauf ist besonders dann zu achten, wenn Systeme jahrelang fehlerfrei laufen.

TIPP

Gerade bei der Wiederherstellung von ausgefallenen Systemen ist eine richtige und vor allem aktuelle Dokumentation wesentlich. Sorgen Sie hier vor, dass z.B. Zugangscodes, Konfigurationstabellen oder Lizenzinformationen schnell verfügbar sind. Dies muss auch gewährleistet sein, wenn z.B. der zuständige Mitarbeiter krankheitsbedingt nicht erreichbar ist.

3.7.1. Backup-Strategien

Im Normalfall versteht man unter Backup die Sicherungskopien von Dateien. Eine entsprechende Strategie soll die Wiederherstellung im Krisenfall gewährleisten. Dabei ist besonders zu beachten:

Wie wird ein Backup gemacht?

In der Praxis findet man zwei Varianten:
- **vollständiges Backup:** ein gesamtes System (z.B. Server) wird vollständig gesichert
- **inkrementelles Backup:** nur die Änderung seit dem letzten Backup werden gesichert

Wie oft wird ein Backup gemacht?

Für Kleinunternehmen und Ein-Personen-Unternehmen empfiehlt sich ein dreistufiges Backup:
- Täglich
- Wöchentlich
- Monatlich

Sind die Backups vor fremdem Zugriff geschützt?

Dieser Schutz kann physisch oder logisch durch Verschlüsselung erfolgen. Eine Backup-Kopie sollte z.B. als Schutz im Brandfall räumlich getrennt vom Datenträger gelagert sein. Als organisatorische Maßnahme ist die lokale Ablage in einem feuerfesten Daten-Tresor sinnvoll.

Wird der Wiederherstellungs-Prozess regelmäßig geprüft?

Überprüfen Sie mindestens einmal jährlich die Wiederherstellung der Daten vom Backup.

TIPP

Machen Sie mit dem Online-Ratgeber Datensicherung eine Bestandsaufnahme über die Datensicherung in Ihrem Unternehmen und erhalten Sie nützliche Tipps, wie Sie die Sicherung Ihrer Daten optimieren können.

Online-Ratgeber Datensicherung

3.8. Datenschutz durch Technik und durch datenschutzfreundliche Voreinstellungen (Privacy by design/ Privacy by default)

Zum Schutz der personenbezogenen Daten haben die Verantwortlichen und die Auftragsverarbeiter auch die Grundsätze des Datenschutzes durch Technik (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) zu berücksichtigen und geeignete interne Strategien festzulegen sowie entsprechende Maßnahmen zu setzen.

3.8.1 Datenschutz durch Technik

Sowohl bei der Planung als auch bei der Datenverarbeitung selbst haben der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen zu berücksichtigen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten (z.B. durch Pseudonymisierung der Daten). Dabei sind der Stand der Technik, die Implementierungskosten, die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

3.8.2 Datenschutzfreundliche Voreinstellungen

Der Verantwortliche hat geeignete technische und organisatorische Maßnahmen zu treffen, die sicherstellen, dass durch entsprechende Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten nicht ohne Eingreifen einer Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Die Einhaltung eines genehmigten Zertifizierungsverfahrens kann als Faktor herangezogen werden, um die Erfüllung der genannten Maßnahmen nachzuweisen.

3.9. Regelmäßige Überarbeitung der TOMs

TIPP

Überprüfen Sie mindestens einmal jährlich die TOMs und aktualisieren Sie diese im Bedarfsfall.

3.9.1. Überprüfung

Eine Überprüfung ist regelmäßig aus technischer sowie aus organisatorischer Sicht durchzuführen:

- **Technische Überprüfung**
  Sämtliche technische Vorgaben sind auf deren technische Wirksamkeit hin zu überprüfen. Das reicht von der Klärung, ob Notebooks tatsächlich verschlüsselt sind bis zur korrekten Konfiguration von Standby-Systemen.

TIPP

Beim Einsatz von „Cold-Standby"-Systemen für Server, die selten oder kaum ausfallen, werden die Ersatzsysteme oft für andere Zwecke „missbraucht" und sind dann im Ernstfall nicht einsatzbereit! Überprüfen Sie, ob die Geräte auf dem aktuellen Stand sind und für den Notfall bereitstehen.

- **Organisatorische Überprüfung**

Hier ist zu klären, ob vorgesehene Maßnahmen, festgehalten in Richtlinien, von den betroffenen Personen auch tatsächlich eingehalten werden.

Beispiel: Ein Raum ist gemäß Sicherheits-Richtlinie versperrt zu halten. Bei häufiger Benutzung stellt dies für die Mitarbeiterinnen und Mitarbeiter einen lästigen Mehraufwand dar und kann dazu führen, dass sie den Raum erst am Ende des Arbeitstages abschließen.

3.9.2. Bewertung

Die Ergebnisse der Überprüfung der TOMs können in einer verbalen Bewertung erfolgen, aber auch unter Hinzuziehung von Kennzahlen. Damit kann im Rahmen einer Erfolgskontrolle die Nachhaltigkeit der Maßnahmen nachgewiesen bzw. Korrekturen der Maßnahmen durchgeführt werden.

3.9.3. Evaluierung der Wirksamkeit

Neben der Überprüfung der TOMs ist vor allem zu klären, ob sie noch dem Stand der Technik entsprechen und vor allem auch ihren Zweck zur Einhaltung eines definierten Datenschutzniveaus tatsächlich erfüllen.

TIPP

Führen Sie einmal jährlich eine – interne oder externe – allgemeine Überprüfung der DSGVO-Maßnahmen durch (DSGVO-Audit).

3.10. Dokumentation

Die Dokumentation spielt eine wesentliche Rolle im Rahmen der DSGVO und insbesondere bei den TOMs. Sie dient sowohl der Qualitätssicherung, als auch gegebenenfalls der Rechtfertigung gegenüber der Datenschutzbehörde.

Wie bei allen Managementsystemen sind die Dokumente entsprechend übersichtlich zu gestalten und sollten mindestens folgende Informationen beinhalten:

- **Autor**
  (eventuell wer das Dokument geprüft und freigegeben hat)
- **Art des Dokuments**
  Richtlinie, Checkliste, Protokoll...
- **Datum**
  (eventuell Uhrzeit)
- **Version**
  (eventuell auch letzte/vorhergehende Version des Dokuments)
- **Betroffene Personengruppen**

Mitarbeiterinnen und Mitarbeiter

IT-Sicherheit kann auch bei besten technischen Maßnahmen nur funktionieren, wenn die Mitarbeiterinnen und Mitarbeiter ausgeprägtes Sicherheitsbewusstsein besitzen und in der Lage sind, die Vorgaben in der täglichen Praxis umzusetzen. Schulung und Sensibilisierung für Fragen der IT-Sicherheit sind daher unbedingt notwendig.

4.1. Regelungen für Mitarbeiterinnen und Mitarbeiter

Bereits im Rahmen des Bewerbungsverfahrens werden dem Unternehmen personenbezogene Daten bekannt. Schon ab diesem Zeitpunkt sind entsprechende Vorkehrungen betreffend die interne Personalverwaltung in den TOMs zu treffen.

Bei der Einstellung von Mitarbeiterinnen und Mitarbeitern sind diese zur Einhaltung einschlägiger Gesetze, Vorschriften und interner Regelungen zu verpflichten.

Es empfiehlt sich, insbesondere Richtlinien zu folgenden Bereichen zu treffen, die in Form einer Verpflichtungserklärung zu unterzeichnen sind.

- Einhaltung der PC-Benutzungsregeln
- Einhaltung der Regeln für die Benutzung von Internet und E-Mail
- Einhaltung der Verpflichtungserklärung auf das Datengeheimnis (Artikel 32 Abs. 4 DSGVO und § 6 DSG).

Neue Mitarbeiterinnen und Mitarbeiter müssen unbedingt auf interne Regelungen, Gepflogenheiten und Verfahrensweisen im IT-Einsatz hingewiesen werden. Ohne entsprechende Einweisung kennen sie ihre Ansprechpersonen in Sicherheitsfragen nicht und wissen nicht, welche IT-Sicherheitsmaßnahmen einzuhalten sind.

In die Stellenbeschreibungen müssen alle sicherheitsrelevanten Aufgaben und Verantwortlichkeiten explizit aufgenommen werden. Dies gilt besonders für Mitarbeiterinnen und Mitarbeiter mit speziellen Sicherheitsaufgaben (Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Applikations- und Projektverantwortliche...).

Bei der Einstellung von IT-Administratorinnen und Administratoren ist besondere Sorgfalt nötig: Sie haben weitgehende und umfassende Befugnisse, insbesondere sind sie in der Lage, auf alle Daten zuzugreifen, sie zu verändern und Berechtigungen so zu vergeben, dass erheblicher Missbrauch möglich ist. Das hierfür eingesetzte Personal muss sorgfältig ausgewählt werden und absolut vertrauenswürdig sein.

Für Mitarbeiter-Richtlinien gilt im Besonderen:

- sie müssen einfach, klar und verständlich formuliert sein
- nicht in zu großem Umfang, maximal 1-2 A4 Seiten
- die Formulierung muss an die Zielgruppe angepasst sein, vom Hilfspersonal bis zum IT-Techniker
- für die Einhaltung der Richtlinien sollten Prüfmethoden existieren
- im Rahmen von Schulungen und Weiterbildungen muss das Verständnis der Regeln überprüft werden

TIPP

Stellen Sie sicher, dass alle (auch neue!) Mitarbeiterinnen und Mitarbeiter die Richtlinien kennen (z.B. durch Schulungen und Überprüfungen) und dokumentieren Sie dies mittels Unterschrift. Bei neu eintretenden Mitarbeiterinnen und Mitarbeitern kann dies auch Bestandteil des Dienstvertrags sein.

Die Richtlinien sollten für alle Mitarbeiterinnen und Mitarbeiter in der aktuellen Version jederzeit zur Verfügung stehen (z.B. online auf einem Fileserver).

4.2. Verfahren bei personellen Veränderungen

Bei personellen Veränderungen, insbesondere beim Ausscheiden von Mitarbeiterinnen und Mitarbeitern aus dem Unternehmen, sollten folgende grundlegende Punkte beachtet werden:

- Sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (z.B. Mobilgeräte, Speichermedien, Dokumentationen) sind zurückzufordern.
- Sämtliche Zugangsberechtigungen und Zugriffsrechte müssen angepasst, entzogen oder gelöscht werden. Dies betrifft unter anderem auch Berechtigungen für eventuelle Telearbeitszugänge sowie Daten auf privaten Smartphones oder Notebooks.
- Wenn eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt wurde (z.B. mittels eines gemeinsamen Passwortes), muss nach Ausscheiden einer der Personen die Zugangsberechtigung sofort geändert werden. Wenn Administratoren oder andere Schlüsselpersonen ausscheiden, müssen auch alle anderen Passwörter geändert werden, die ihnen bekannt waren.
- Die Neuvergabe eines bestehenden Benutzerkontos an neue Mitarbeiterinnen oder Mitarbeiter sollte möglichst vermieden werden.

Es empfiehlt sich eine Checkliste für personelle Veränderungen bereitzuhalten.

4.3. Regelungen für den Einsatz von Fremdpersonal

Betriebsfremde Personen wie z.B. Personal von Reinigungsfirmen oder IT-Dienstleister können leicht Zugang zu vertraulichen Unternehmensdaten erhalten und stellen unter Umständen eine erhebliche Bedrohung dar.

Einige einfache Regeln sollten beachtet werden, um vertrauliche Informationen zu schützen:

- Externe Mitarbeiterinnen und Mitarbeiter, die über einen längeren Zeitraum in einem Unternehmen tätig sind und Zugang zu vertraulichen Unterlagen und Daten erhalten könnten, müssen schriftlich (im Rahmen von Geheimhaltungsverpflichtungen) auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen verpflichtet werden.
- Für Fremdpersonal, das nur kurzfristig oder einmalig zum Einsatz kommt, gelten die gleichen Regeln wie für Besucherinnen und Besucher, d.h. dass etwa der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von unternehmenseigenem Personal erlaubt ist.
- Ist es nicht möglich, betriebsfremde Personen ständig zu begleiten oder zu beaufsichtigen, sollten zumindest die persönlichen Arbeitsbereiche abgeschlossen werden (Schreibtisch, Schrank; Abmeldung/Sperre am PC).

4.4. Sicherheitssensiblisierung und -schulung

Um die IT-Sicherheit zu verbessern, sollten alle Mitarbeiterinnen und Mitarbeiter über angemessene Kenntnisse im Umgang mit IT-Systemen und den Gefahren und Gegenmaßnahmen in ihrem eigenen Arbeitsgebiet verfügen. Es liegt in der Verantwortung der Geschäftsführung durch geeignete

Schulungsmaßnahmen die nötigen Voraussetzungen zu schaffen. Darüber hinaus sollte alle Benutzer dazu motiviert werden, sich auch in Eigeninitiative Kenntnisse anzueignen.

Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit oder Bequemlichkeit. Das Aufzeigen der Abhängigkeit des Unternehmens von Informationen und vom reibungslosen Funktionieren der IT-Systeme ist ein geeigneter Einstieg in die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter für Sicherheitsanliegen.

Weitere mögliche Inhalte einer Benutzerschulung sind:

- Der richtige Umgang mit Passwörtern
- Richtiges Verhalten beim Auftreten von Sicherheitsproblemen
- Der Umgang mit personenbezogenen Daten
- Wirkungsweise und Arten von Schadprogrammen
- Erkennen eines Befalls mit Schadprogrammen
- Sofortmaßnahmen im Verdachtsfall und Maßnahmen zur Entfernung von Schadprogrammen
- Das richtige Verhalten im Internet
- Das richtige Verhalten bei unzulässigen Anfragen
- Risiken bei der Verwendung mobiler IT-Geräte und Datenträger
- Die Bedeutung der Datensicherung und ihrer Durchführung

IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter

Als Behelf für Benutzerschulungen und zum Selbststudium empfehlen wir das „IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter“ aus der it-safe-Reihe.

4.4.1. Abwehr von Social-Engineering-Angriffen

Als Social Engineering bezeichnet man das Manipulieren von Personen, um unbefugt Zugang zu vertraulichen Informationen oder IT-Systemen zu erhalten.

Social Engineering-Angriffe werden meistens über das Telefon, gelegentlich aber auch über soziale Netzwerke oder durch persönliches Auftreten des „Social Engineers“ geführt: Angreifer geben sich als Mitarbeiter, Kunden oder IT-Fachkräfte aus und überzeugen ihre Gesprächspartner durch geschickte Täuschung von ihrer vorgetäuschten Identität. Bei geeigneter Gelegenheit – oft erst nach mehrmaligen Telefonaten – gelangen sie so an Informationen, die die Opfer üblicherweise nie herausgeben würden. Gute Social Engineers können unvorbereitete Mitarbeiterinnen und Mitarbeiter zu verschiedensten unerlaubten Handlungen, insbesondere zu Verstößen gegen Sicherheitsauflagen und -richtlinien bewegen.

Social Engineering-Angriffe sind häufig erfolgreich, weil sie menschliche Eigenschaften und Schwächen gezielt ausnützen: Hilfsbereitschaft und Höflichkeit, Kundenfreundlichkeit, aber auch Autoritätshörigkeit und Angst. Einige Maßnahmen können aber helfen, das Risiko zu verringern:

- Schulungen über Social Engineering-Strategien und -Methoden helfen den Mitarbeiterinnen und Mitarbeitern, sich auf Angriffe dieser Art vorzubereiten.
- Alle Mitarbeiterinnen und Mitarbeiter müssen sich regelmäßig den Wert der von ihnen bearbeiteten Daten bewusstmachen, insbesondere hinsichtlich des Schadens, der entstehen kann, wenn sie in falsche Hände geraten.
- Schriftliche Festlegungen, welche Informationen vertraulich behandelt werden müssen und welche auch an Unbekannte weitergegeben werden dürfen, können Benutzern zur Orientierung dienen und dem Unternehmen außerdem als Argumentationshilfe nach Sicherheitsvorfällen nützlich werden.

- Festlegungen zur Anfragenform sind empfehlenswert: Das Anfordern einer Rückrufnummer oder einer schriftlichen Anfrage kann den Social Engineer unter Umständen bereits zurückschrecken und gibt den betroffenen Mitarbeiterinnen und Mitarbeitern Gelegenheit zur Nachfrage. Auskünfte zu sensiblen Daten sollten generell nur bei persönlichem Erscheinen erteilt werden.
- Besonders neuen Mitarbeiterinnen und Mitarbeitern sollte empfohlen werden, Anfragen, bei denen sie unsicher sind, ob deren Beantwortung zulässig ist, an Vorgesetzte oder andere erfahrene Personen weiterzuleiten.
- Mitarbeiterkommunikation ist wichtig: Bei „verdächtigen" Anfragen sollten auch die anderen Mitarbeiterinnen und Mitarbeiter informiert werden, um zu verhindern, dass ein abgewiesener Angreifer sein Glück bei anderen, zugänglicheren Kolleginnen und Kollegen versucht.

4.5. Clear Desk/Clear Screen Policy

In ungesicherten Arbeitsumgebungen hilft eine Clear Desk-Policy beim Schutz vertraulicher Dokumente und Daten vor unbefugten Zugriffen.

Alle Mitarbeiterinnen und Mitarbeiter sollten bei Abwesenheit vertrauliche Unterlagen verschließen. Dies gilt insbesondere für Großraumbüros, aber auch in anderen Fällen ist dafür Sorge zu tragen, dass keine unberechtigten Personen (Kunden, Besucher, Reinigungspersonal, unbefugte Mitarbeiter etc.) Zugriff auf Schriftstücke oder Datenträger mit heiklen Inhalten haben. Ähnliches gilt auch für die Computer: Beim Verlassen des Arbeitsplatzes muss sich jeder Benutzer vom PC abmelden. Wenn nur eine kurze Unterbrechung der Arbeit erforderlich ist, kann der Computer stattdessen gesperrt werden. Zusätzlich sollte auch eine automatische Sperre bei Nicht-Nutzung, z.B. durch einen passwortgeschützten Bildschirmschoner, vorgesehen werden.

Es sollte darauf geachtet werden, dass den Mitarbeiterinnen und Mitarbeitern ausreichende Möglichkeiten zum Versperren der sensiblen Arbeitsunterlagen zur Verfügung stehen. Alle Benutzer sollten außerdem über die Tastenkombinationen (z.B. „Windows-Taste + L") zum schnellen Sperren des PCs informiert werden. Falls möglich, sollten besonders in der ersten Zeit auch Kontrollen und wiederholte Aufforderungen erfolgen, um die Durchsetzung dieser Anweisungen zu sichern.

4.6. Entsorgung von Datenträgern und Papierdokumenten

Datenträger und Dokumente mit vertraulichen Inhalten müssen auf sichere Art entsorgt werden, z.B. durch ein dafür zertifiziertes Unternehmen.
In vielen Unternehmen stellt der Umgang mit Dokumenten ein Sicherheitsrisiko dar. Dokumente mit vertraulichen oder personenbezogenen Inhalten werden mit dem Altpapier entsorgt, ohne vorher unlesbar gemacht zu werden. Ähnliches gilt für nicht mehr gebrauchte Datenträger wie z.B. defekte Festplatten, Sicherungsbänder oder USB-Sticks.

Unbefugte Personen können auf einfache Art an kritische Daten gelangen, indem sie Altpapiercontainer durchsuchen und entsorgte Datenträger wieder lesbar machen. Daher müssen entsprechende Sicherheitsmaßnahmen befolgt werden:

- Die Mitarbeiterinnen und Mitarbeiter müssen über das Entsorgungskonzept informiert und insbesondere darüber in Kenntnis gesetzt werden, welche Dokumente nicht über das Altpapier entsorgt werden dürfen.
- Papierdokumente müssen mit einem cross-cut-Shredder oder über ein Entsorgungsunternehmen vernichtet werden.

- Eine ausreichende Anzahl von Entsorgungsmöglichkeiten in erreichbarer Nähe der Mitarbeiterinnen und Mitarbeiter sowie Ansprechpartner für Rückfragen im Zweifelsfall sollten vorgesehen werden.
- Datenträger müssen auf sichere Art vernichtet werden: Sicherungsbänder werden geshreddert, Festplatten müssen physisch zerstört werden (durch Aufschrauben und Zertrümmern der einzelnen Plattenscheiben).
- Bei Festplatten und Wechseldatenträgern ist zudem der Einsatz von Löschprogrammen ratsam, die ein sicheres Löschen der Daten gewährleisten.
- Die Vernichtung der Datenträger kann auch durch ein entsprechendes Entsorgungsunternehmen erfolgen, wobei jedenfalls eine Bestätigung der Vernichtung zu verlangen ist.

4.7. Telearbeit

Unter Telearbeit versteht man Tätigkeiten, die räumlich entfernt vom Standort des Arbeitgebers durchgeführt werden und deren Erledigung durch eine kommunikationstechnische Anbindung an die IT-Infrastruktur des Arbeitgebers unterstützt wird.

Bestimmte Anforderungen sollten möglichst noch vor der Einrichtung und Vergabe von Telearbeitszugängen überlegt und definiert werden. Z.B. sollte ein Telearbeitsplatz möglichst in einem eigenen, von der übrigen Wohnung getrennten Zimmer eingerichtet werden und Versperrmöglichkeiten für Datenträger und Dokumente vorsehen.

Für die verwendeten Computer müssen ebenfalls bestimmte Auflagen erteilt werden: Aktuelle Virenschutzsoftware ist unbedingt nötig, ebenso der Einsatz eines Zugriffsschutzes durch Benutzeranmeldung und Passworteingabe. Soweit das umsetzbar ist, sollte eine Liste von Software erstellt werden, die auf dem Telearbeit-PC aus Sicherheitsgründen nicht betrieben werden darf. Werden diese Auflagen nicht eingehalten, darf der Telearbeitszugang nicht vergeben oder muss wieder entzogen werden.

Aus diesen Gründen ist es oft sinnvoll, den für die Telearbeit verwendeten PC vom Unternehmen bereitzustellen. In diesem Fall sollte schriftlich festgelegt werden, dass der Rechner ausschließlich für die berufliche Nutzung verwendet werden darf und dass andere Personen keinen Zugang erhalten dürfen. Auch die Festlegung der Softwareausstattung des Telearbeit-PCs und die Vereinbarung zusätzlicher Kontrollrechte des Arbeitgebers sind in solchen Fällen einfacher möglich.

Weitere Regelungen, z.B. zur Durchführung regelmäßiger Datensicherungen, zu Sicherheitsmaßnahmen bei sensiblen Daten oder zum Vorgehen bei Problemen, sollten zu einer schriftlichen Richtlinie zusammengefasst werden, die allen Telearbeiterinnen und Telearbeitern übergeben wird.

4.8. Technik der Mitarbeiterinnen und Mitarbeiter

4.8.1. Mobiltelefon

Besonders bei der Benutzung des Mobiltelefons sind die Mitarbeiterinnen und Mitarbeiter durch entsprechende technische und organisatorische Maßnahmen zu unterstützen.

Derzeit bieten eine Reihe von Herstellern proprietäre Lösungen zum Schutz ihrer Mobiltelefone an. Als ein Beispiel für eine getrennte Benutzerumgebung (unternehmerische und private Nutzung) stellen wir nachstehend das System „KNOX“ von SAMSUNG vor.

Damit kann man auf Mobiltelefonen – ähnlich wie bei Linux Systemen (SE-LINUX: Secure- Enhanced LINUX) – einen Schutz auf Kernel-Ebene anbieten.

Mit KNOX kann man auf Systemebene des Mobiltelefons einen getrennten Benutzerbereich einrichten – ähnlich wie bei virtuellen Betriebssystemen - diesen nennt man Knox-Container. Dieser stellt eine völlig getrennte Benutzerumgebung innerhalb des Android-Profils dar.

Damit bietet KNOX zwei interessante Ansätze:

- Ein dienstliches mobiles Endgerät darf privat genutzt werden, wobei private und unternehmerische App-Daten voneinander getrennt werden. Außerhalb des Knox-Containers dürfen Apps frei aus dem Play Store installiert werden. Der Knox-Container selbst enthält aber nur vom Unternehmen freigegebene Apps.
- Im Falle eines BYOD-Ansatzes (siehe Kapitel 4.8.7.) stellt ein Benutzer sein privates Gerät dem Unternehmen zur Verfügung. Durch den Knox-Container kann das Unternehmen Daten getrennt ablegen und es können auch firmeninterne Android-Apps installiert werden.

Falls der Benutzer die Organisation verlässt, können durch ein einfaches Löschen des Containers die Daten des Unternehmens wieder vollständig entfernt werden.

In der einfachsten Form kann ein Knox-Container durch Installation und Einrichtung der App My Knox erstellt werden. Hiermit wird ein (aber nicht zentral verwaltbarer) Knox-Container lokal am Mobiltelefon installiert.

Zusätzlich zum individuellen Schutz des Mobiltelefons sollte in einem Unternehmen ein Mobile Device Management (MDM)-System eingerichtet werden. Die wichtigste Grundfunktion dabei ist dabei das Fernlöschen aller am Mobiltelefon gespeicherten Daten.

In weiterer Folge unterstützt ein MDM die sichere Benutzung des Mobiltelefons – und auch eines Notebooks – auf mehreren Ebenen:

- Erweiterung des Fernlöschens für Notebooks
- Definition von Sicherheitsrichtlinien für Mobile Devices
- Ausrollen von Apps
- Dokumentation verwendeter mobiler Geräte im Unternehmen

4.8.2. E-Mail

TIPP

Für einen übersichtlichen Umgang mit personenbezogenen Daten sollten E-Mails und deren Attachments mit personenbezogenen Daten in den entsprechenden Projektordnern im Filesystem oder einer Datenbank abgelegt und anschließend im E-Mail System vollständig gelöscht werden. Ziel ist es, einem Auskunftsbegehren oder Löschbegehren einer betroffenen Person korrekt und ohne zu großem Aufwand nachkommen zu können.

Eine wichtige organisatorische Maßnahme ist das Erstellen einer Richtlinie für den Umgang mit E-Mails, die folgende Punkte beinhalten sollte:

- **Wo sollen Attachments gespeichert werden?** Bedenken Sie, dass es gerade bei undokumentiertem lokalen Ablegen dazu kommen kann, dass personenbezogene Daten später nicht mehr lokalisierbar sind und dadurch z.B. das vollständige Löschen von diesen Daten sehr erschwert oder sogar unmöglich wird.
- **E-Mails mit personenbezogenen Daten dürfen in keinem Fall an Freemailer-Systeme (z.B. gmx, gmail) weitergeleitet werden.** Das ist besonders zu beachten, wenn private E-Mail-Adressen von Mitarbeiterinnen und Mitarbeiter in Unternehmen zum Einsatz kommen.

Bei Verwendung von Ordnern im E-Mail System fehlt oft eine entsprechende Struktur der gespeicherten Daten wie in gut organisierten Datenbanksystemen, wo Daten de facto nur einmal abgespeichert werden und dann darauf referenziert wird. Beachten Sie auch, dass viele Mitarbeiterinnen und Mitarbeiter ihre E-Mails am Mobiltelefon bearbeiten. Bei Verlust des Mobiltelefons könnte das zu einem Data-Breach führen. Die Absicherung könnte hier z.B. durch die Möglichkeit der Fernlöschung erfolgen.

4.8.3. Umgang mit verdächtigen E-Mails

Es ist extrem einfach, den Absender einer E-Mail allein im Mail-Client, den man verwendet, einzustellen, also sich für eine andere Person auszugeben.

Daher ist unbedingt notwendig, bei „verdächtigen" E-Mails, die eventuell gefälscht sein könnten, nochmals beim Absender nachzufragen.

4.8.4. E-Mail Verschlüsselung

Grundsätzlich schreibt die DSGVO nicht vor, dass E-Mails mit personenbezogenen Daten verschlüsselt werden müssen. Dennoch stellt dies eine sehr sinnvolle Schutzmaßnahme dar.

Verschlüsselung der E-Mail im Rahmen der Übertragung
Eine E-Mail kann auf dem Übertragungsweg einfach mittels TLS verschlüsselt werden. Um eine End-to-End Sicherheit zu erreichen, d.h. dass nur der Empfänger die E-Mail öffnen kann, benötigt man eine Identifikation des Empfängers. Dafür wird bei vielen kommerziellen Anwendungen im Hintergrund auf schon seit vielen Jahren bekannte weit verbreitete Lösungen zurückgegriffen, die beide auf dem Public/Private-Key-Verfahren basieren (siehe Kapitel 1.5. über Verschlüsselung): PGP („Pretty-Good-Privacy") und S/MIME (Secure/Multipurpose Internet Mail Extensions)

Sollte der Empfänger nicht imstande sein, mit verschlüsselten E-Mails dieser Technologie umgehen zu können, erfolgt bei manchen Lösungen eine automatische Umlenkung auf einen webbasierenden Ansatz. Die E-Mail wird dann per Passwort zum Download auf einem Webserver bereitgestellt.

Um ihren E-Mail Client „S/MIME-tauglich" zu machen, damit Sie sowohl ihre E-Mails als auch ihre Attachments verschlüsselt mit einem Geschäftspartner austauschen können, sind folgende zwei Schritte notwendig:

Anfordern eines Schlüssels/Zertifikat von einer Zertifizierungsstelle.

Einrichten dieses Zertifikats im E-Mail Client
am Beispiel Outlook

Das Zertifikat wird über das „Trust-Center" importiert:

Abfolge der Menüpunkte in MS Outlook:
Datei → Optionen → Trust Center → Einstellungen für das Trust Center → E-Mail-Sicherheit → importieren/exportieren → Durchsuchen (Speicherplatz des Zertifikates auswählen, Aktivierungspasswort eingeben und lokalen Namen für das Zertifikat wählen) → OK

Damit ist das Zertifikat in Outlook installiert und Sie können E-Mails verschlüsselt versenden und empfangen.

In ähnlicher Form erfolgt die Installation des Zertifikates bei anderen E-Mail Clients.

Speziell für S/MIME gibt es im Internet eine Reihe von einfachen Schritt für Schritt Anweisungen, wie Sie Ihren E-Mail Client – auch auf ihrem Mobiltelefon – S/MIME-tauglich machen können.

E-Zustellung

Anstelle der Übertragung per E-Mail könnten personenbezogene Daten z.B. über einen sicheren Webserver, über den kritische Daten benutzerspezifisch und passwortgeschützt per Upload und Download ausgetauscht bzw. übertragen werden.

TIPP

Mittels E-Zustellung können Sie vertrauliche Nachrichten und Dokumente elektronisch, genauso einfach und schnell wie per E-Mail, aber viel sicherer, versenden und empfangen.

4.8.5. Remote Arbeitsplatz und Teleworking

Selbstverständlich erfordert auch ein Remote-Arbeitsplatz entsprechende Sicherheitsmaßnahmen. Dieser ist vor Angriffen aus dem Internet durch eine Firewallbox („Appliance") zu schützen, die auch der Endpunkt für den sicheren Zugang in das Unternehmen per VPN sein sollte.

TIPP

Ähnlich wie bei mobilen Arbeitsplätzen mit einem Notebook ist auch ein fester Remote-Arbeitsplatz mittels Festplatten-Verschlüsselung vor unbefugtem Zugriff auf die Daten zu schützen.

Beim Teleworking werden einige zusätzliche technische und organisatorische Maßnahmen notwendig, da im Privatbereich zusätzliche Risiken durch Unbefugte (z.B. Familienmitglieder, Besucher, aber auch Einbrecher) auftreten können.

Dabei sind folgende Fragen zu klären:

- Wem gehört das Equipment, das vor Ort zum Einsatz kommt?
- Wer betreut die Systeme des Mitarbeiters in seinem Home-Office (PC, Drucker, WLAN, Firewall)?
- Wie erfolgt der Zugang zu firmeninternen Ressourcen (VPN, Remote-Desktop)?

4.8.6. Mobiles Arbeiten unterwegs

Durch eine Netzverbindung zum Internet entstehen Gefahren. Werden bei mobilem Internetzugang keine zusätzlichen Schutzmaßnahmen eingerichtet, ist die Verbindung in beide Richtungen offen, d.h. es kann von einem beliebigen Rechner auf das ganze Netzwerk zugegriffen werden. Eine richtig konfigurierte Firewall gestattet nur die unbedingt notwendigen und tatsächlich gebrauchten Verbindungen und blockiert alle anderen.

Für mobiles Arbeiten am Notebook werden in der Regel folgende Zugänge zum Internet verwendet:

- **GSM**

Die Anbindung des Notebooks im Internet kann über eine integrierte SIM-Karte erfolgen oder auch über das mobile Telefon als eigener WLAN-Hotspot. In beiden Fällen ist zu beachten, dass ein Firewallschutz am Notebook installiert sein muss.

- **WLAN in einem bekannten LAN**

Viele Firmen bieten ein WLAN-Gästenetz für Besucher an. Auch in diesem Fall sind entsprechende Schutzmaßnahmen (insbesondere Firewall) auf dem Notebook unerlässlich.

- **WLAN in einem öffentlichen Netz (Public Hotspot)**

Beachten Sie, dass es für kriminelle Hacker sehr einfach ist, öffentliche Netzzugänge dafür zu nutzen Ihre Daten auszuspähen. Verschlüsseln Sie Ihren Datenverkehr hier unbedingt mittels eines sicheren VPN.

Deaktivieren Sie Funktionen wie WLAN oder Bluetooth, wenn Sie sie gerade nicht brauchen.

4.8.7. BYOD (Bring Your Own Device)

Bring Your Own Device bedeutet, dass Geräte (vor allem private Smartphones oder Notebooks) betrieblich zum Einsatz kommen, die den Mitarbeiterinnen und Mitarbeitern gehören.

Dabei sind folgende wichtige Fragen zu klären:
- Wer administriert die privatenGeräte?
- Welche Applikationen dürfen auf dem Gerät laufen?
- Wie wird der Remote Zugang zu Firmendaten abgesichert?
- Wie geht man mit Daten auf den privaten Geräten um, wenn die Mitarbeiterin bzw. der Mitarbeiter das Unternehmen verlässt? (z.B. im Rahmen eines Mobile Device Management Systems Fernlöschen der betrieblichen Daten entsprechend DSGVO)

4.8.8. Richtiger Umgang mit mobilen Geräten

Aufgrund des hohen Verlustrisikos stellen mobile Geräte ein besonderes Risiko beim Umgang mit personenbezogenen Daten dar. Daher ist bei der Gestaltung der TOMs auf den Umgang mit mobilen Geräten besonderes Gewicht zu legen.

Betroffen sind Mobiltelefone, Notebooks, aber auch mobile Datenträger wie zum Beispiel USB-Sticks, digitale Kameras oder Diktiergeräte. Weisen Sie die Mitarbeiterinnen und Mitarbeiter (idealerweise in einer entsprechenden Richtlinie) darauf hin, mobile Geräte nie ungeschützt unbeaufsichtigt zu lassen. Insbesondere gilt dies aufgrund der hohen Diebstahlsgefahr für das Zurücklassen in PKWs (keinesfalls sichtbar!).

TIPP

Beachten Sie bei mobilen Geräten besonders:
- Verschlüsselung personenbezogener Daten
- Unverzügliche Meldung eines Verlustes an die zuständige Stelle
- Möglichkeit der Fernlöschung bzw. Fernadministration

4.8.9. Meldung eines Vorfalls

Bei vielen Vorfällen ist nicht sofort klar erkennbar, ob es sich um ein Fehlverhalten eines Benutzers, einen technischen Defekt oder vielleicht sogar um einen Hacker-Angriff handelt. Aus diesem Grund zögern Benutzer manchmal mit der Meldung eines Vorfalls.

Jede Mitarbeiterin und jeder Mitarbeiter muss wissen, an wen er sich im Falle des Auftretens oder Erkennens eines Vorfalls zu wenden hat. Diese Meldung hat **unverzüglich** zu erfolgen, da bei einem Datenverlust unter Umständen eine verpflichtende Meldung an die Datenschutzbehörde durch den Verantwortlichen innerhalb von 72 Stunden gemacht werden muss und betroffene Personen verständigt werden müssen (siehe dazu auch Kapitel 3.2.1 Databreach).

TIPP

Sorgen Sie für ein Betriebsklima, in dem das Erkennen und die Meldung von Schwachstellen gefördert wird.

4.8.10. Erfolgskontrolle

Die DSGVO fordert eine regelmäßige Kontrolle und Bewertung der Maßnahmen, die zum Schutz personenbezogener Daten ergriffen wurden.

Dazu zählt auch die Erfolgskontrolle bezüglich der Weiterbildung der Mitarbeiter. In der einfachsten Form kann dies mittels regelmäßig durchgeführter Tests durchgeführt werden.

Beispiel: Bezüglich Awareness kann als Test für die Wirksamkeit der Maßnahmen sein, wie viele Mitarbeiterinnen und Mitarbeiter einem gezielten „falschen" E-Mail nachkommen (gegebenenfalls in Absprache mit dem Betriebsrat). Text E-Mail: „Setzen Sie bitte sofort ihr Passwort auf A3141, wir müssen einen Systemcheck durchführen! Ihr Systemadministrator (bzw. die Geschäftsleitung)." Im Sinne vorhergegangener Schulungen sollten die Mitarbeiterinnen und Mitarbeiter dieses E-Mail entweder ignorieren oder den Systemadministrator kontaktieren.

5

Rechtliche Grundlagen, Standards, Normen und Zertifikate

5.1. DSGVO und das österreichisches Datenschutzgesetz

Grundlagen des österreichischen Datenschutzrechts sind seit 25. Mai 2018 die DSGVO und das Datenschutzgesetz (DSG) in der Fassung des Datenschutz-Anpassungsgesetzes 2018 und des Datenschutz-Deregulierungs-Gesetzes 2018. Alle Datenverarbeitungen müssen dieser Rechtslage entsprechen.

Die Sicherheit der Verarbeitung personenbezogener Daten ist in Art. 32 DSGVO geregelt: Unternehmen müssen daher unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

5.2. Strafen

Die Missachtung der Verpflichtung zu Datensicherheitsmaßnahmen ist mit bis zu EUR 10 Mio. oder 2% des letztjährigen weltweiten Jahresumsatzes sanktioniert.

5.3. Institutionen

Eine Reihe von Organisationen beschäftigt sich auf internationaler und nationaler Ebene mit dem Thema der Informationssicherheit und speziell mit dem Schutz personenbezogener Daten. Unterschiedlichste Standards werden dabei von (Normungs-) Gremien definiert, diesbezügliche Ausbildungen und Zertifikate angeboten.

Für kleine Unternehmen ist oft der Weg zur Zertifizierung aufgrund der Kosten nicht sinnvoll. Auf der anderen Seite können entsprechende Zertifikate aber bei Auftragsverarbeitern als Nachweis für deren Befähigung dienen.

Beispiele:

- *Sie haben eine Cisco-Firewall in ihrem Unternehmen zum Schutz ihrer lokalen Ressourcen im Einsatz. Ihr IT-Dienstleister kann mit einem Cisco-Zertifikat seine Fähigkeit die Firewall korrekt fehlerfrei konfigurieren zu können, nachweisen.*
- *Sie haben Ihre Webseite inklusive Webshop bei einem großen deutschen Rechenzentrum laufen. Als Nachweis der technischen Kompetenz in Richtung Sicherheitsmanagement kann eine ISO/IEC-27001 Zertifizierung dienen.*

Normen und Standards im IT-Security Umfeld sind für Klein- oder gar Ein-Personen-Unternehmen meistens kein Thema – allerdings beinhalten sie das Wissen und die Erfahrungen aus jahrzehntelanger Praxis von Experten. Die zugrundeliegenden Prinzipien und Methoden können durchaus auch bei kleineren Unternehmen sinnvoll sein.

So spielt z.B. die Dokumentation in allen Normen und Standards eine wichtige Rolle und wird von der DSGVO auch im Rahmen der Rechenschaftspflicht von jedem Unternehmen gefordert.

International Organization for Standardization (ISO)
Die internationale Norm ISO/IEC 27001 spezifiziert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines Informationssicherheits-Managementsystems.

ISO/IEC 27001

Deutsches Bundesamt für Sicherheit in der Informationstechnik (BSI)
Der vom BSI entwickelte IT-Grundschutz ermöglicht es, durch ein systematisches Vorgehen notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen.

BSI Grundschutz

Österreichisches Informationssicherheitshandbuch
Das Handbuch ist ein Standardwerk für Österreich, ähnlich dem deutschen BSI-Grundschutzhandbuch, und wird von A-SIT, dem österreichischen Zentrum für sichere Informationstechnologien, herausgegeben.

Österreichisches Informationssicherheitshandbuch

Österreichische Datenschutzbehörde
Aufgabe der Datenschutzbehörde ist es für die Einhaltung des Datenschutzes in Österreich zu sorgen.

Datenschutzbehörde

Zu Fragen der Standardisierung und Normung bzw. Zertifizierung sind in Österreich u.a. folgende Institutionen zu nennen:

- TÜV-Austria
- Austrian Standards International (A.S.I.)
- CIS-CERT
- Incite

5.4. Zertifikate in der DSGVO

Ein Zertifikat ist ein Zeugnis über eine abgelegte Prüfung oder eine Überprüfung von vorgegebenen Parametern. Diese Prüfung wird in der Regel von einer unabhängigen Instanz („Prüfstelle“) durchgeführt. Diese Instanz muss für diese Aufgabe autorisiert sein („Akkreditierung“), etwa durch eine staatliche Stelle, zum Beispiel ein Ministerium, von der Zentrale eines Unternehmens, wenn es sich um Firmenzertifikate handelt oder – im Bereich der DSGVO – durch die Datenschutzbehörde.

Der Begriff Zertifikat per se ist nicht geschützt. Daher findet man derzeit eine Reihe von Ausbildungsinstitutionen, die Zertifikate zum Thema DSGVO ausstellen.

Organisationen wie TÜV, A.S.I., CIS-Cert, Incite usw. haben nach einer internationalen Norm (Personen-Zertifizierung) jeweils einen Anforderungskatalog definiert, nach dem Personen geprüft werden und damit eine Zertifizierung zum Datenschutzexperten oder Datenschutzbeauftragten erlangen können.

Seitens der Datenschutzbehörde fehlt derzeit noch die Akkreditierung von Prüfstellen inklusive Vorgaben von Inhalten und Anforderungen, damit eine einheitliche Regelung zumindest in Österreich gegeben wäre.

TIPP

Für Unternehmen sind Zertifikate interessant, da damit die eigene Pflicht von Qualitäts-Überprüfungen – speziell im Bereich der TOMs – zumindest teilweise an kompetente Institutionen delegiert werden kann.

6

Fallstudien

6.1. Ein-Personen-Unternehmen (Unternehmensberater)

Die Unternehmensberatung „Alfred Berger Consulting e.U." wurde vor 3 Jahren als Einzelunternehmen gegründet.

Als Bürostandort wurde ein Coworking Center im 15. Bezirk in Wien ausgewählt, das Arbeitsplätze und Infrastruktur (Besprechungsräume, Küche etc.) zur gemeinsamen Nutzung anbietet. Dieses stellt für ihre Mieter ein WLAN zur Verfügung und bietet darüber hinaus keine zusätzliche IT-Leistungen an.

Alfred Berger nutzt einen Exchange-Anbieter in Österreich für die Abwicklung seiner E-Mails, ein Auftragsdatenverarbeitungs-Vertrag liegt vor.

Für seine Beratungstätigkeiten verwendet Alfred Berger ein Apple-Notebook und ein Windows-Notebook (im Büro angeschlossen an eine Dockingstation mit Drucker).

In einem deutschen Rechenzentrum betreibt er einen eigenen Cloud-Server (Private-Cloud: „NextCloud") für den gesicherten Datenaustausch mit seinen Kunden über https.
Ein ISO/IEC-27001-Zertifikat dieses Rechenzentrums liegt vor.

Technische und organisatorische Maßnahmen (DSGVO Art. 30 Abs. 1 lit. g)	Alfred Berger Consulting e.U.
Datum der Erstellung	24.5.2018
Datum der letzten Änderung	5.12.2018
Pseudonymisierung und Verschlüsselung Art. 32 Abs. 1 lit. a	• Verschlüsselung aller mobilen Datenträger und mobilen Geräte mittels VeraCrypt. • verschlüsselte Datenübertragung (SSL/TSL, SSL mit 2048-bit-Key) an Cloud-Anbieter und verschlüsselte Speicherung (AES mit 256-bit-Schlüssel) bei Cloud-Anbieter • verschlüsselte Datenübertragung (SSL) zum Hosted-Exchange-Anbieter

Sicherstellung von Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste Art. 32 Abs. 1 lit. b	• Passwortschutz aller Geräte • Virenschutz & Firewall aktiv auf den Notebooks • 2-Faktor-Authentifizierung bei Online-Diensten, sofern verfügbar • Firewall-Box bei stationärem Einsatz (vor der Dockingstation) • Fernlöschbarkeit: Einsatz von „KNOX“ auf SAMSUNG-Phone • redundante Datenspeicherung auf mehreren Datenträgern an physisch getrennten Orten • Synchronisierung mit Hosted-Exchange-Anbieter • wöchentliches Komplett-Backup auf externe Festplatte (Nr. 1) • quartalsweises Komplett-Backup auf externe Festplatte (Nr. 2) • jährliches Komplett-Backup auf externe Festplatte (Nr. 3.) • Offline-Verfügbarkeit aller Online-Daten im Falle eines Internetausfalls (SYNC aus der eigenen Private Cloud) • redundante Arbeitsplatzumgebung (Weiterarbeiten bei Ausfall eines Notebooks durch das zweite Gerät jederzeit möglich)
Datenwiederherstellungs-möglichkeiten Art. 32 Abs. 1 lit. c	• Restore aus Cloud-Backup • von Backups auf externen HDD (Nr. 1, 2, 3)
Evaluierungsmaßnahmen Art. 32 Abs. 1 lit. d	• jährliche Überprüfung der Maßnahmen auf DSGVO-Konformität

6.2. Unternehmen mit 5 Mitarbeiterinnen und Mitarbeitern (Handel)

Das Handelsunternehmen „Audio4You" wird als GmbH mit Standort in Wien geführt, hat 5 Mitarbeiterinnen und Mitarbeiter und zusätzlich für den Vertrieb seiner Produkte einen Webshop. Dieser wird im Outsourcing in der Cloud von einem deutschen Anbieter betrieben. Die Webshop-Software wurde von einem kleinen österreichischen Softwarehaus erstellt, das ausgehend von einem Open Source-Produkt eine adaptierte Version entwickelt hat. Weitere Anpassungen und Weiterentwicklungen erfolgen nach individuellem Auftrag.

Das Kundenportfolio erstreckt sich vor allem auf den B2B-Markt (das Produktportfolio der Audioanlagen bewegt sich im technischen/preislichen Highend-Bereich), nur 10 % des Geschäftes werden im Laden im Bereich B2C abgewickelt. Dieser Laden, der je nach Bedarf von ein bis zwei Mitarbeiterinnen betreut wird, befindet sich im Erdgeschoss, im ersten Stock ist ein kleines Büro mit einem Serverraum eingerichtet.

Die interne IT-Betreuung und auch alle Aufgaben bezüglich DSGVO hat die Geschäftsführerin persönlich übernommen, da sie eine entsprechende technische Schulausbildung besitzt. Bei kritischen Fragen wird ein externer Berater zugezogen, der auch Remote auf die Systeme per VPN zugreifen kann.

Technische und organisatorische Maßnahmen

der Audio4You GmbH (DSGVO Art. 30 Abs. 1 lit. g)

I. ÜBERTRAGUNGSKONTROLLE

Sämtliche personenbezogenen Daten werden ausschließlich mit verschlüsselten USB-Platten an Kunden und Geschäftspartner übergeben bzw. per VPN übertragen (Webshop).

technische Maßnahmen:

- Verwendung des Verschlüsselung Programmes 7-zip.
- VPN (https:)

organisatorische Maßnahmen:

- Protokollierung der Datenübermittlungen (Logs)
- Festlegung von Übermittlungswegen (wie wird an welche Empfängerkategorie übermittelt)

II. BENUTZERKONTROLLE

Der IT-Administrator vergibt die Benutzerrechte nach dem Minimalprinzip. Benutzer bekommen nur Rechte auf die Daten, die sie für die Ausübung ihrer Tätigkeit benötigen.

technische Maßnahmen:

- Firewall, Intrusion Detection/Prevention
- Benutzeridentifikation
- Passwortvorgabe
- Absicherung der Geräte/des Netzwerks vor unbefugtem Zutritt

organisatorische Maßnahmen:

- Protokollierung der Benutzeraktivitäten
- Festlegung der Zutrittsberechtigungen der Benutzer
- Passwortrichtlinie
- Clean-Desk-Policy

III. DATENINTEGRITÄT

Die Betriebssystem-Updates am Server und auf den Notebooks werden automatisch durchgeführt, sonstige Programme werden manuell auf den neuesten Stand gebracht;

technische Maßnahmen:

- Datensicherungen in 3 Hierarchien: täglich-wöchentlich-monatlich
- Einsatz Virenscanner Kaspersky
- PC-Firewall (Windows-Defender)
- LAN-Firewall (Fortinet)
- Spam-Filter
- USP am Server (Stromversorgung bei Ausfall)

organisatorische Maßnahmen:

- Datensicherungs- und Wiederherstellungskonzept
- Systemüberwachung der Hard- und Software
- Serveradministratoren können 24x7x365 in den Serverraum

IV. DATENTRÄGERKONTROLLE

Die Daten liegen ausschließlich auf dem S-Laufwerk des Servers oder einer verschlüsselten Partition auf den Arbeitsplatzrechner bzw. Laptops.

technische Maßnahmen:

- Speichermedien werden versperrt in einem Stahlschrank verwahrt
- datenschutzkonforme Löschung bei Wiederverwendung von Speichermedien

organisatorische Maßnahmen:

- protokollierte Entsorgung von Speichermedien
- protokollierte Entsorgung von Geräten mit integrierten Datenträgern
- Dokumentation der Ausgabe von mobilen Speichermedien
- Kontrolle/Protokollierung Weitergabe personenbezogener Daten

V. EINGABEKONTROLLE

Es wird per Logfiles mitprotokolliert, welcher Benutzer zu welchem Zeitpunkt auf welchem Arbeitsplatz eingeloggt ist; diese Protokolle stehen der IT-Administration zur Verfügung.

technische Maßnahmen:

- Benutzeridentifikation

organisatorische Maßnahmen:

- Festlegung von projektbezogenen Benutzerberechtigungen
- sichere Ablage von Protokollen
- Löschen der Protokolle am Ende des Folgejahres der Speicherung (Art. 6 Abs 1 lit. f DSGVO – berechtigtes Interesse)

VI. SPEICHERKONTROLLE

Es wird sichergestellt, dass nur befugte (zuständige) Personen die Möglichkeit haben, auf personenbezogene Daten zuzugreifen und diese zu bearbeiten.

technische Maßnahmen:

- Benutzeridentifikation
- Automatische Sperre des Arbeitsplatzcomputers und der Notebooks nach 10 Minuten Inaktivität
- Trennung von Administrations- und Produktionsbereich
- Speicherung der personenbezogenen Daten auf einer verschlüsselten Partition

organisatorische Maßnahmen:

- Einsatz einer fein granulierten Zugriffsberechtigung

VII. TRANSPORTKONTROLLE

Es besteht die dienstliche Weisung, dass personenbezogene Daten keinesfalls auf unverschlüsselten mobilen Datenträgern (USB-Sticks, Smartphones) gespeichert werden dürfen. Der Laptop/PC darf nur von befugten Personen verwendet werden.

technische Maßnahmen:

- Verschlüsselte Speicherung auf Datenträger
- Remote Server-Zugriff ausschließlich per VPN

organisatorische Maßnahmen:

- Dienstanweisung für den Umgang mit Datenträgern
- Bei Weitergabe: Datenträger-Eingangs- und Ausgangsprotokoll

VIII. WIEDERHERSTELLUNG

Backup-Strategie siehe Sicherungskonzept. Die IT-Administration kann kurzfristig die Sicherungskopien einspielen, der Restore-Prozess wird zweimal pro Jahr getestet.

technische Maßnahmen:

- Backup Erstellung täglich-wöchentlich-monatlich auf USB-Platte
- Master Backup (Backup des gesamten Datenbestandes) alle sechs Monate auf USB-Platte oder z.B. vor Serverwechsel
- Server Backups: 1:1 Cold Standby

organisatorische Maßnahmen:

- Serveradmin-Fernzugriff zu den Servern per VPN
- Worst-Case: Serveradministratoren können jederzeit lokal in den Serverraum in die Firma (z.B. Standby-Aktivierung)

IX. ZUGANGSKONTROLLE

Der Serverraum ist versperrt; der Laptop/PC ist nur mit einem Passwort verwendbar; der Zutritt zum Serverraum wird protokolliert ist nur für berechtigte Personen gestattet.

technische Maßnahmen:

- Gebäudesicherung, Zugriffskontrolle durch Einsatz eines Sicherheitsschlüssel-Systems mit Hochsicherheitszylinder der Firma EVVA mit individueller Zugangsfreigabe und Protokollierung des Zutritts im Bürobereich im 1. Stock.
- Alarmanlage mit Polizeimeldung im Laden und im Büro.
- Videoüberwachung des Ladens

organisatorische Maßnahmen:

- Mitarbeiterinnen und Mitarbeiter dürfen Besuchern die Eingangstür zum Büro nur nach Identifikation öffnen, zur Unterstützung existiert am Eingang eine Life-Video-Kamera.
- Besucher dürfen die Büro-Räumlichkeiten immer nur in Begleitung betreten.
- Jeder Büro-Besucher wird mit Name, Firma, Datum, Uhrzeit und besuchter Person protokolliert
- Personenbezogene Daten in gedruckter Form werden ausschließlich in versperrten Stahlschränken aufbewahrt.

X. ZUGRIFFSKONTROLLE

Es besteht eine firmenweit gültige Passwort-Richtlinie, diese ist den Mitarbeiterinnen und Mitarbeiter auch nachweislich zur Kenntnis gebracht.

technische Maßnahmen:

- Berechtigungskonzept
- Benutzeridentifikation
- Schnittstellensicherung
- Verschlüsselung
- kein Fremdgerät im Netz gestattet

organisatorische Maßnahmen:

- Verwaltung und Kontrolle der Zugriffsberechtigungen
- Kontrolle der Zugriffe (Protokollierung)
- Dokumentation der Maßnahmen zur Datenvernichtung

6.3. Unternehmen, 20 Mitarbeiterinnen und Mitarbeiter (Gastronomie)

„Steakhouse – Eat & Drink" ist ein Steak-Restaurant mit einer Zentrale in Wien und einem zweiten Lokalstandort in St. Pölten. Am Hauptstandort sind 14 Mitarbeiterinnen und Mitarbeiter tätig, 6 in Niederösterreich. Sämtliche administrative Tätigkeiten werden von Wien aus erledigt.

Die Kernkompetenz der Mitarbeiterinnen und Mitarbeiter und auch der Geschäftsleitung liegt im Bereich der Gastronomie. Daher hat sich der Geschäftsführer entschieden, möglichst viele Tätigkeiten der IT auszulagern. Damit konzentriert sich die Verpflichtung des Geschäftsführers im Bereich der TOMs auf das Führen eines korrekten Verarbeitungsverzeichnisses und einem entsprechenden Auftragsdatenverarbeitungs-Vertrags mit dem IT-Dienstleister „LAN-Competence-Support GmbH". Dieser hat für eine entsprechende Dokumentation der technischen und organisatorischen Maßnahmen im Rahmen des Vertrages zu sorgen.

Vor Beauftragung eines IT-Dienstleisters ist bezüglich TOMs zu beachten:

- Ist der Dienstleister befugt und befähigt die Betreuung durchzuführen?
- Führt der Dienstleister selbst ein Verarbeitungsverzeichnis?
- Welche TOMs sind in seinem eigenen Unternehmen umgesetzt?

Als fachlich kompetenter Geschäftspartner hat er als Teil seiner Auftrags-Leistung auch die entsprechenden technischen und organisatorischen Maßnahmen, die er für das Steakhouse einführt und betreut, klar und verständlich gemäß DSGVO zu dokumentieren.

Unabhängig davon muss auch der Betreiber der beiden Steak-Lokale seine TOMs dokumentieren, die sich verstärkt mit dem organisatorischen Umfeld befassen werden. Details bezüglich weiterer Informationen zu den TOMs sind dem Anhang des Auftragsdatenverabeitungsvertrags zu entnehmen.

Technische und organisatorische Maßnahmen

der Steakhouse – Eat & Drink GmbH (DSGVO Art. 30 Abs. 1 lit. g)

ZUTRITTSKONTROLLE

technische Maßnahmen:

- Alarmanlage
- Manuelles Schließsystem
- Sicherheitsschlösser
- Videoüberwachung der Eingänge

organisatorische Maßnahmen:

- Schlüsselregelung
- Schlüsselausgabe/Rückgabeliste

ZUGANGSKONTROLLE

technische Maßnahmen:

- Login mit Benutzername und Passwort
- Antivirensoftware am Server
- Antivirensoftware auf den Clients
- Antivirensoftware auf Notebooks
- Firewall: Cisco (LANs)
- VPN zwischen den Restaurants
- Fernlöschung von Mobiltelefonen
- Desktop/Notebooksperre nach 10 Minuten Inaktivität
- Verschlüsselung von Notebooks/Datenträger

organisatorische Maßnahmen:

- Einrichten von Benutzern mit entsprechenden Profilen
- Zentrale Verwaltung von Berechtigungen und Passwörtern
- Zentrale Passwortvergabe
- Richtlinie zum Löschen personenbezogener Daten
- Mobile Device Richtlinie
- Clean Desktop Policy
- Richtlinie für die Benutzung des Mobiltelefons (PIN, Apps...)

ZUGRIFFSKONTROLLE

technische Maßnahmen:

- Aktenvernichter mit Kreuzschnitt

organisatorische Maßnahmen:

- Externe Aktenvernichter (Vertrag)
- Externe Datenträgerlöschung (Vertrag)

WEITERGABE KONTROLLE

technische Maßnahmen:

- Einsatz von VPN/https
- Verschlüsselung von E-Mail Attachments mit 7-zip, z.B. bei Übermittlung der Buchhaltungs-unterlagen an den Steuerberater
- Verschlüsselung von Datenträgern, die zur Übermittlung verwendet werden

organisatorische Maßnahmen:

- Dokumentation der Übergabe und Entgegennahme von Datenträgern
- Verlässlichkeits-Überprüfung bei Übergabe von personenbezogenen Daten an Transport-Firmen
- Protokollierung bei persönlicher Übergabe von personenbezogenen Daten

VERFÜGBARKEITSKONTROLLE

technische Maßnahmen:

- Feuer-und Rauchmeldeanlagen
- Serverraum klimatisiert
- Unterbrechungsfreie Stromversorgung der Server
- Datenschutztresor für Backups lokal

organisatorische Maßnahmen:

- Backup und Wiederherstellungs-Konzept
- Backup extern gelagert
- Regelmäßige Tests des Restorevorgangs auf Funktion

ÜBERPRÜFUNG, BEWERTUNG, EVALUIERUNG DER MASSNAHMEN

technische Maßnahmen:

- Aktualisierung der Firewall und der Virenscanner überprüfen
- Überprüfung des Minimalprinzips – es werden nur die für den Zweck notwendigen personenbezogenen Daten gespeichert.

organisatorische Maßnahmen:

- Mitarbeiter – Vertraulichkeitserklärung
- Prozessdefinition für Auskunftsbegehren
- Prozessdefinition für die Meldung von Datenschutz-Vorfällen (incidents)
- Überprüfung der Gültigkeit von Zertifikaten und TOMs von Auftragsverarbeitern, auch bezüglich eventueller neuer Subunternehmer
- Regelmäßige Kontrollen bezüglich Einhaltung der Richtlinien durch die Mitarbeiterinnen und Mitarbeiter

Anhang

ANHANG 1

Artikel 32 DSGVO: Sicherheit personenbezogener Daten

Sicherheit der Verarbeitung

1. Unter Berücksichtigung des **Stands der Technik**, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der **Verantwortliche** und der **Auftragsverarbeiter** geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

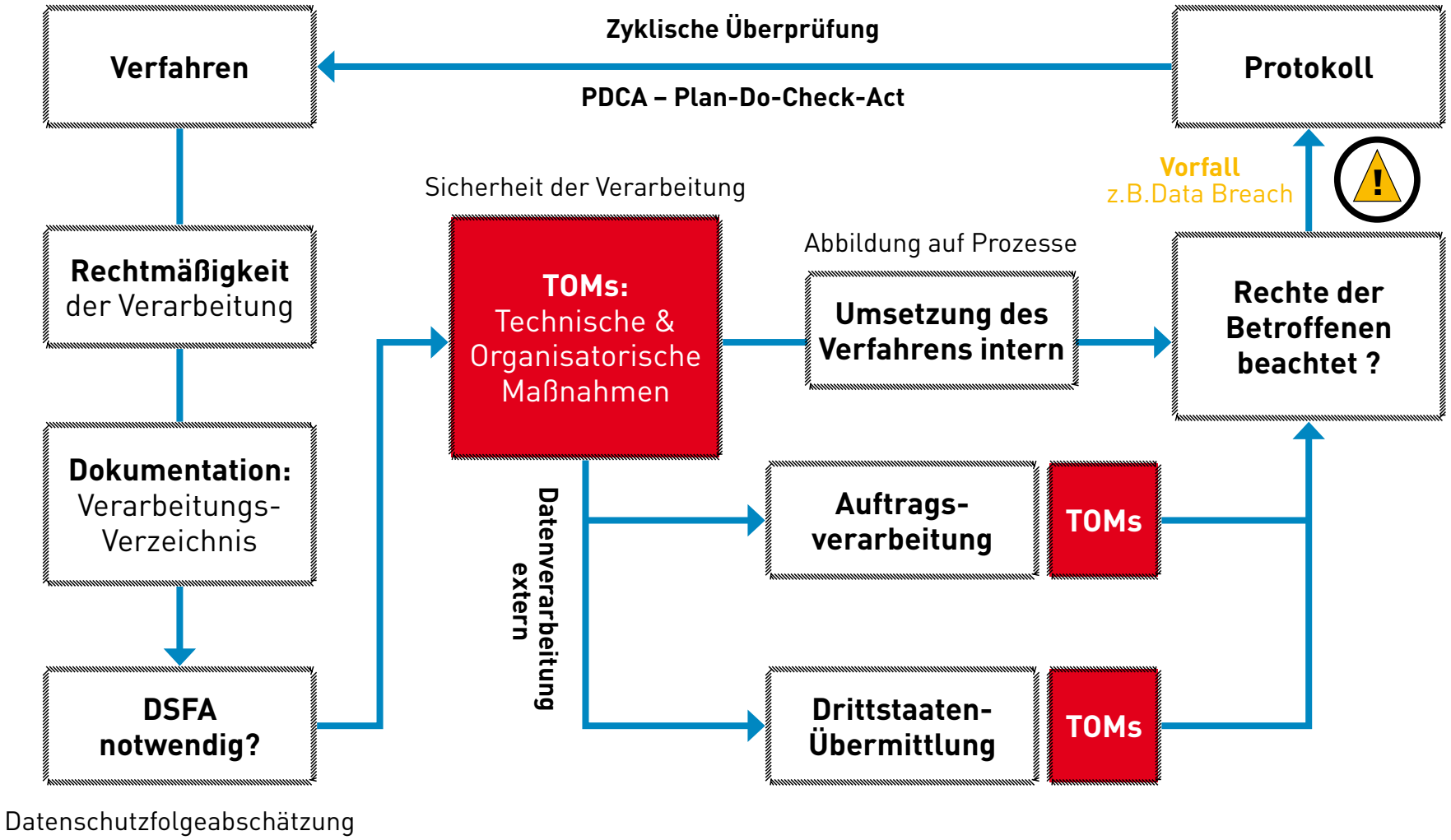
a) **die Pseudonymisierung und Verschlüsselung personenbezogener Daten;**
b) die Fähigkeit, **die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch **wiederherzustellen**
d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der **Sicherheit der Verarbeitung**.

2. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – **Vernichtung, Verlust, Veränderung** oder **unbefugte Offenlegung** von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

3. Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten **Anforderungen nachzuweisen**.

4. Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die **Zugang zu personenbezogenen Daten haben**, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

ANHANG 2 Die Rolle der TOMs im DSGVO Lebenszyklus



Die Rolle der TOMs im DSGVO Lebenszyklus

Für die Einführung eines neuen Verfahrens zur Bearbeitung personenbezogener Daten ist im ersten Schritt die **Rechtmäßigkeit** dieser Verarbeitung zu überprüfen. Ist diese erfüllt wird das Verfahren im **Verarbeitungsverzeichnis** aufgenommen und regelkonform dokumentiert.

In weiterer Folge muss sich der Verantwortliche überlegen, wo Risiken für die Rechte von Betroffenen bei der Durchführung dieses Verfahrens entstehen könnten. Bei entsprechend hohem Risiko ist eine genaue **Datenschutzfolgen-Abschätzung** (DSFA) durchzuführen. Aus diesen Überlegungen heraus kommt es zur Definition eines Datenschutzniveaus.

Datenschutzfolgen-Abschätzung

Um die Einhaltung dieser Datenschutzniveaus zu garantieren, müssen im nächsten Schritt alle **technischen und organisatorischen Maßnahmen (TOMs)** getroffen werden, um die Einhaltung dieser Datenschutzniveaus zu gewährleisten.

Diese TOMs sind auch bei der Weitergabe personenbezogener Daten an **Auftragsverarbeiter** (z.B. IT-Dienstleister; externer Buchhalter) einzufordern und zu überprüfen – klarerweise auch wenn diese Auftragsbearbeitung in **Drittstaaten** (nicht EU-Staaten) erfolgt (z.B. Cloud-Anbieter in den USA). Um der Rechenschaftspflicht (z.B. bei einer möglichen Überprüfung durch die Datenschutzbehörde) gemäß DSGVO nachkommen zu können, sind möglichst ausführliche Protokolle im Rahmen der Verarbeitung von personenbezogenen Daten zu erstellen.

Sollte im Rahmen eines **Vorfalls** (z.B. Verlust des Notebooks) festgestellt werden, dass für das entsprechende Verfahren ausreichende Sicherheitsmaßnahmen (z.B. durch Verschlüsselung der Daten) im Rahmen der TOMs erfolgt sind, ist nach einem entsprechenden Protokolleintrag keine Meldung an die Datenschutzbehörde durchzuführen, wenn keine Risiken für die **Rechte und Freiheiten der Betroffenen** bestehen.

Gemäß DSGVO sind die TOMs regelmäßig auf ihre Wirksamkeit hin zu überprüfen und gegebenenfalls (z.B. durch Änderung des Standes der Technik oder Einführung eines neuen Verfahrens) anzupassen. Führen Sie die zyklische Überprüfung im Anlassfall (z.B. bei Einführung neuer Methode zur Datenverarbeitung) bzw. zumindest einmal pro Jahr durch.

ANHANG 3 Vorlage einfacher TOMs für Ein-Personen-Unternehmen

Technische und organisatorische Maßnahmen gem. Art. 32 Abs. 1 DSGVO f. Verantwortliche (Art. 30 Abs. 1 lit. g)

TOM	Ich habe folgende Maßnahme gesetzt:
Pseudonymisierung	Kommt bei mir nicht zum Einsatz.
Verschlüsselung	Ich verwende ausschließlich Windows am Server, PC und Notebook, die alle mit Bitlocker verschlüsselt sind. Externe Datenträger sind mit Veracrypt verschlüsselt.
Gewährleistung der Vertraulichkeit	Alle Systeme sind passwortgeschützt.
Gewährleistung der Integrität	Sicherungskopien sind in einem Tresor versperrt (lokal und extern).
Gewährleistung der Verfügbarkeit	Einsatz von RAID-Platten im Server und Verfügbarkeit eines LTE-Modems, falls der normale Internetzugang ausfällt.
Gewährleistung der Belastbarkeit	Austausch des Servers alle fünf Jahre durch eine neue Hardware.
Maßnahmen zur Wiederherstellung der Verfügbarkeit nach einem Vorfall	Dokumentierte Backup Strategie, überprüft einmal pro Jahr
Verfahren zur regelm. Überprüfung, Bewertung, Evaluierung der Wirksamkeit der TOMs	DSGVO-Audit einmal pro Jahr durch einen externen Berater.
Ergänzende Dokumente	• Datensicherheitsbeschreibung • Netzplan/Netzwerkbeschreibung • Konfigurations-Doku der Systeme • Wiederanlaufkonzept • Auftragsverarbeiter Verträge + ext.TOMs • Sonstige Dokumentation: – Notfallkontakt-Liste – Passwort-Kuvert im Bank-Tresor

_____ Datum

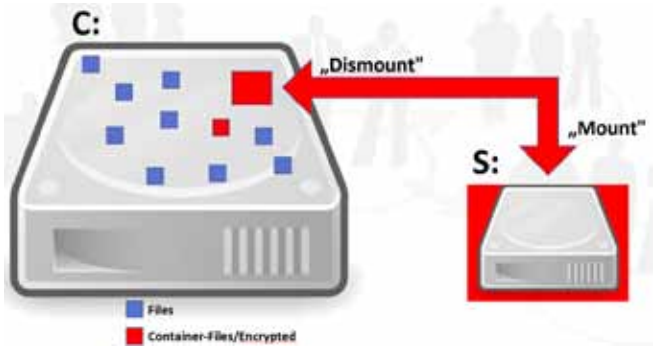
_____ Unterschrift

ANHANG 4

Verschlüsselungs-Tool „ VeraCrypt“

Diese Beschreibung zeigt die einfachste Verwendung des Verschlüsselungswerkzeugs VeraCrypt für die Praxis.

VeraCrypt ist als Freeware eines der beliebtesten Verschlüsselungsprogramme für die Sicherheit von Festplatten, SSD, USB-Sticks und SD-Karten. Damit kann man ganze Festplatten oder Partitionen verschlüsseln, aber auch nur „Containerfiles“ erzeugen, die quasi als Tresor dienen und nach dem Öffnen ein neues „virtuelles“ Laufwerk am PC bilden. Solange dieses Laufwerk geöffnet ist („mounted“), kann man damit wie mit einem physischen Laufwerk arbeiten. Werden die kritischen Daten nicht mehr benötigt, kann man das virtuelle Laufwerk wieder entfernen („dismount“), der Container wird geschlossen und liegt nur mehr als verschlüsselte Datei am System.

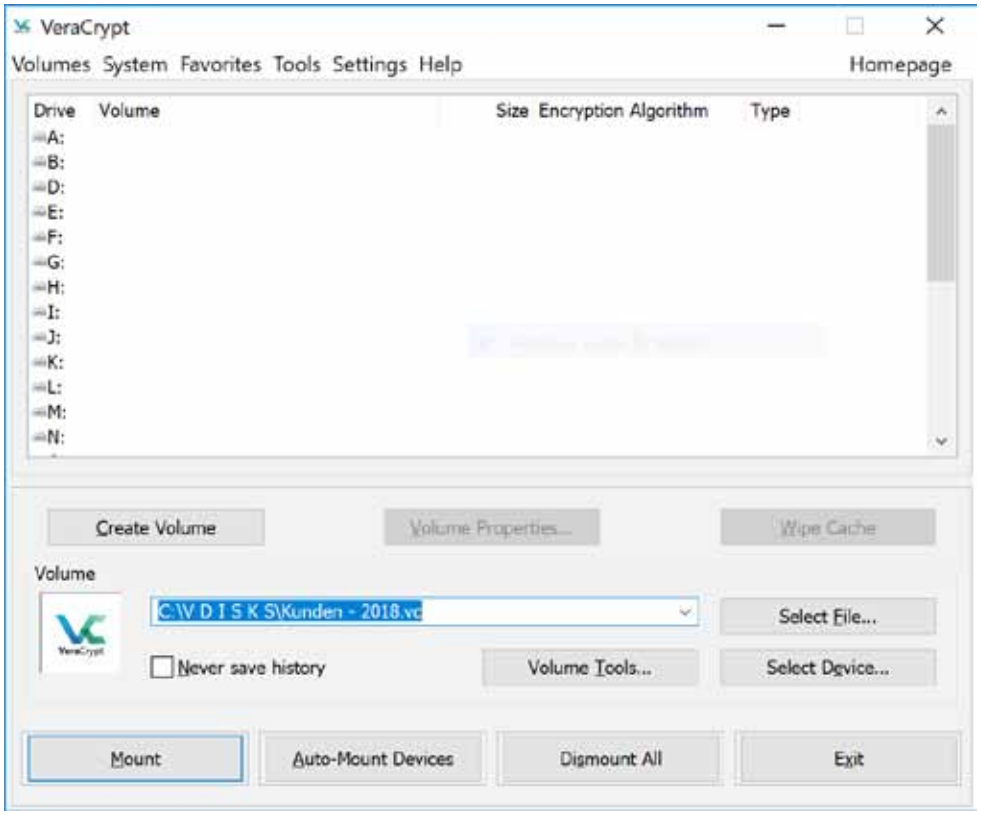


VeraCrypt

Einer der Links, über die man VeraCrypt kostenlos herunterladen kann ist: Download VeraCrypt über heise.de

Nach der Installation finden Sie am Desktop das entsprechende Icon ➔

Erzeugen eines File-Containers („Virtuelle-Disk“):
Nach Aufruf des Programms erscheint das Einstiegsfenster, das die freien Laufwerksbuchstaben anzeigt. Für das Erstellen eines neuen File-Containers geben Sie den Ablageort des Containers an und wählen den Button „Create Volume“:

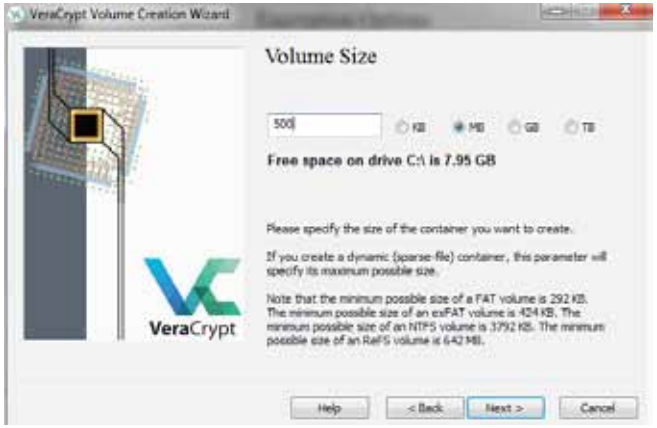


Im nächsten Fenster wählen Sie aus, ob Sie nur einen kryptischen File- Container erzeugen oder ein Laufwerk/Partition verschlüsseln wollen.

VeraCrypt bietet die Möglichkeit, den File-Container – der im Filesystem als Datei mit der Änderung „vc" standardmäßig abgelegt wird – zusätzlich zu verbergen. Darauf wird hier der Einfachheit halber nicht eingegangen, daher wählen wir einen Standard-Container.

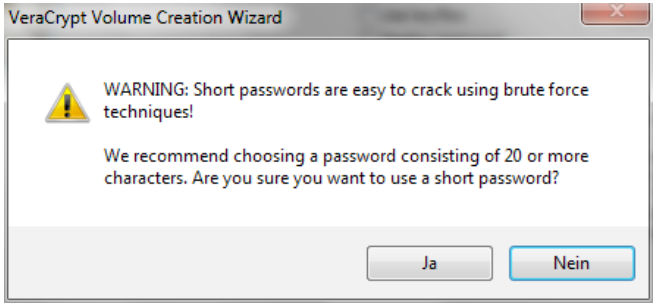
Auch bei der Auswahl des Verschlüsselungs-Algorithmus sind die Standardeinstellungen ein guter Vorschlag.

Über den „Next"-Button wählen Sie jetzt die Größe des Containerfiles aus, in das Sie Ihre verschlüsselten Daten hineinspielen wollen.

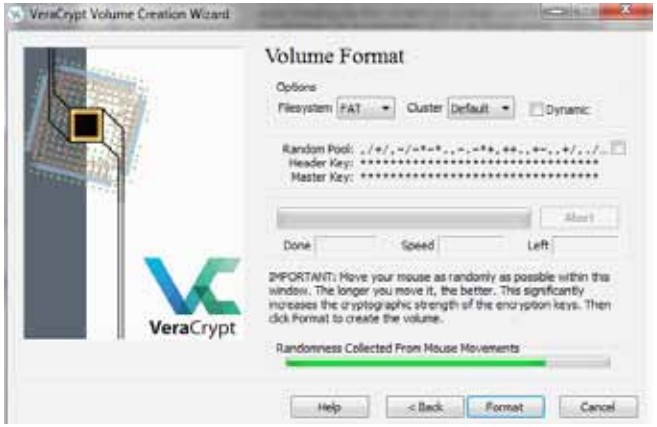


Um den verschlüsselten Container-Inhalt lesbar zu machen setzen Sie ein Passwort ein (Varianten für höheren Sicherheitslevel möglich).

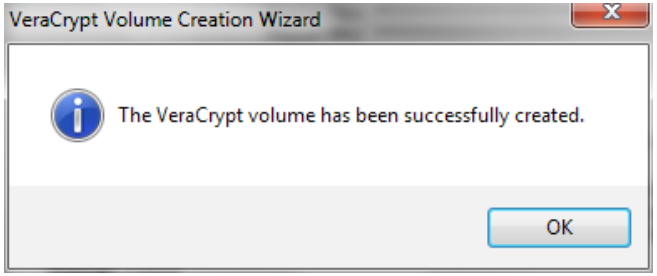
Für den normalen Betrieb ist ein Passwort mit mindestens zwölf Zeichen und Ziffern bzw. Sonderzeichen ausreichend, für einen höheren Sicherheitslevel sollte man noch längere Passwörter verwenden.



Wie bereits erwähnt, entsteht in dem Container-File ein virtuelles Laufwerk, das auch zu formatieren ist. Wie bei jedem Sicherheitsalgorithmus ist eine Basis für den Sicherheitslevel ein Startwert, der möglichst zufällig sein soll. VeraCrypt verwendet dafür die zufällige Mausbewegung, diese ist solange zu bewegen, bis der Balken im unteren Bereich grün wird.



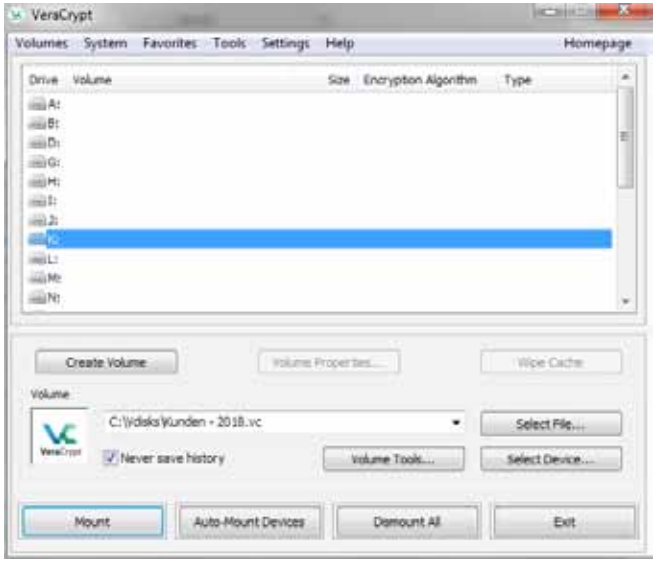
Nach Betätigen des Buttons „Format“ wird der kryptische Filecontainer erzeugt, dies kann bei größeren virtuellen Disks im Gigabyte Bereich auch einige Minuten dauern. Nach Fertigstellung erhalten Sie eine Erfolgsmeldung.



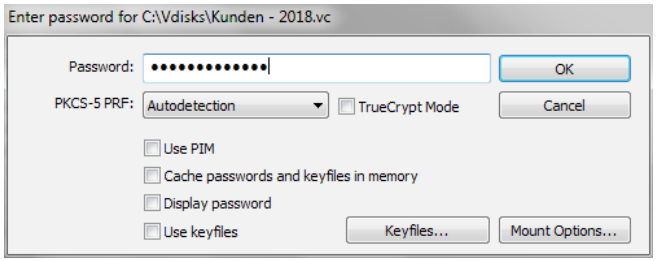
Jetzt ist der File-Container erzeugt, liegt unter dem entsprechenden Namen im Filesystem und kann verwendet werden.

Verwenden eines File-Containers („Virtuelle-Disk“)

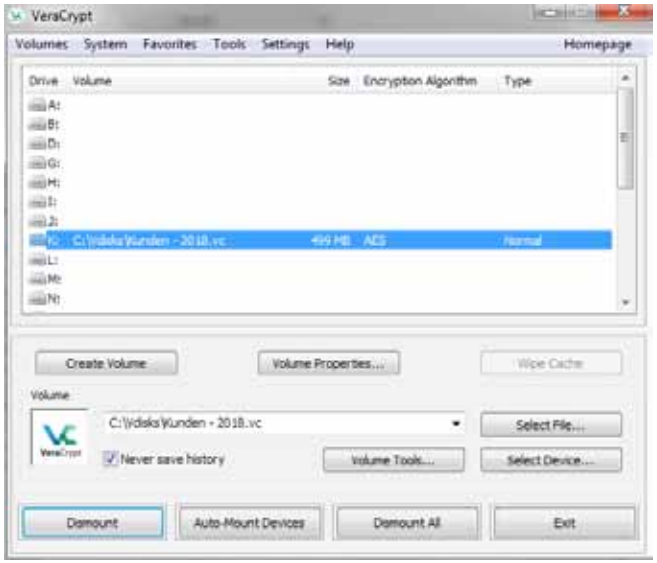
Nach dem Aufruf von VeraCrypt (kann automatisch beim Hochfahren des Systems erfolgen – dann wird nur mehr das Passwort verlangt) wählen Sie einen der freien Laufwerksbuchstaben und natürlich auch den Containernamen selbst. Der Öffnungsvorgang wird gestartet mit dem Button mount“.



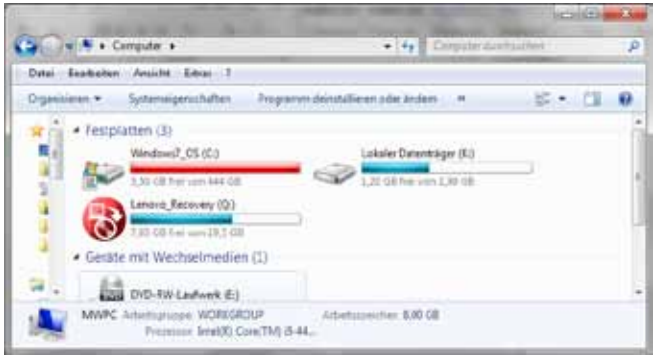
Im nächsten Schritt wird das bei der Erzeugung des Containers festgelegte Passwort verlangt. Sollte man einen kryptischen Container aus dem Vorläuferprodukt („truecrypt“) verwenden wollen, müsste man den „TrueCryptMode“ auswählen.

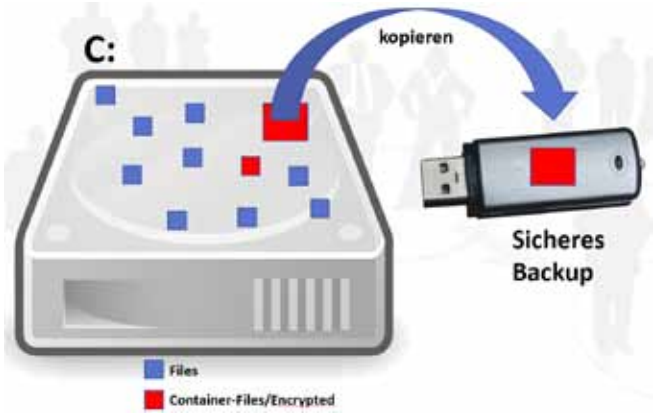


Jetzt sind alle Ihre verschlüsselten Daten des Containers unter dem Laufwerksbuchstaben „K:“ verfügbar, bis Sie den Container wieder mittels des Buttons „Dismount“ schließen. Der Container wird automatisch beim Herunterfahren des Systems geschlossen.



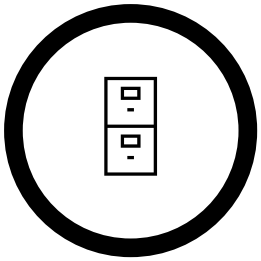
Der Container ist als virtuelles Laufwerk im System wie jedes andere Laufwerk zu verwenden:





Nach dem „Dismount" – bzw. im ungeöffneten Zustand – ist das Laufwerk nicht mehr vorhanden, die Containerdatei ist für einen Hacker nur mehr eine nicht entschlüsselbare Bit-Folge. Daher kann man diese Datei auch bei einem externen Dienste-Anbieter lagern, zum Beispiel auch in der Cloud. Klarerweise kann man die Container Datei – wie jedes andere File – auf einen anderen Datenträger kopieren und somit als sicheres Backup gemäß DSGVO – auch extern – lagern.

Sollten auf dem Backup–USB-Stick personenbezogene Daten gespeichert sein, muss man auch im Falle eines Verlustes des PCs/Notebooks oder auch einer Sicherungskopie keine Meldung an die Datenschutzbehörde machen, eine einfache interne Protokollierung des Verlustes reicht aus.



Glossar

AES

„Advanced Encryption Standard“ ist ein symmetrisches Verschlüsselungsverfahren, derzeit im Einsatz mit einer Schlüssellänge bis zu 256 Bit. Der Algorithmus ist frei verfügbar und darf ohne Lizenzgebühren in Soft- und Hardware-Lösungen eingesetzt werden. Bedingt durch seinen relativ geringen Rechenaufwand im Vergleich zu hochsicheren Verschlüsselungstechniken wird AES bevorzugt bei Realzeitanwendungen, wie zum Beispiel VPNs eingesetzt.

Auftragsverarbeiter

Ein „Auftragsverarbeiter“ ist gemäß DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

BYOD

BYOD (Bring Your Own Device, d.h. „Bring dein eigenes Gerät“) ist eine Strategie, Kosten einzusparen und die Mitarbeitermotivation anzuheben, indem die Verwendung privater IT-Geräte wie Smartphones oder Notebooks für berufliche Zwecke zugelassen wird. Dabei entstehen allerdings verschiedene Probleme in rechtlicher und sicherheitstechnischer Hinsicht, die vor dem Einsatz unbedingt geklärt werden müssen.

Dateisystem

Ein „Dateisystem“ ist gemäß DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

Digitale Signatur

Zum Unterschied einer E-Mail Signatur, die nur eine reine Zeichenfolge zur Angabe des Absenders ist und keinen Zusammenhang zum Inhalt der E-Mail darstellt, bildet die digitale Signatur über einen kryptischen Algorithmus aus dem Text der E-Mail-Nachricht eine Zeichenfolge, die eindeutig zeigt, von wem dieser Text stammt und dass er während der Übertragung nicht verändert wurde. Sollte auch nur ein Zeichen ausgetauscht oder gelöscht worden sein, passt die digitale Prüfsumme nicht mehr mit dem darüber liegenden Text zusammen.

Personenbezogene Daten

„personenbezogene Daten“ sind gemäß DSGVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Profiling

„Profiling“ ist gemäß DSGVO jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

Pseudonymisierung

„Pseudonymisierung“ ist gemäß DSGVO die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

SPOF

“Single-Point-of-Failure” – einzelne Devices oder organisatorische Einheiten, deren Ausfall systemkritische Folgen nach sich zieht. Diese sollten im Rahmen von TOMs besonders beachtet, werden wie zum Beispiel eine Firewall, deren Ausfall keinen Internetzugang mehr ermöglicht.

SSL/https

HTTPS ist die Abkürzung für HyperText Transfer Protocol Secure, das durch die Verwendung des Verschlüsselungsverfahrens SSL ausreichende Sicherheit für die Übertragung sensibler Daten bietet. Mit Hilfe dieses Verfahrens werden einerseits die übertragenen Daten verschlüsselt und abhörsicher gemacht, andererseits wird durch die Verwendung von digitalen Zertifikaten die Identität des Webservers gesichert. Einem Angreifer sollte es – richtige Handhabung vorausgesetzt – nicht möglich sein, sich z.B. als E-Banking-Server auszugeben, um Benutzerinnen und Benutzern ihre Passwörter, PINs oder TANs zu entlocken. Dabei ist zu beachten, dass nur der Datenweg und nicht die Front-End-Systeme (Client, Server) damit geschützt werden!

Verantwortlicher

Ein „Verantwortlicher“ ist gemäß DSGVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.