FORBA FORSCHUNGS- UND BERATUNGSSTELLE ARBEITSWELT

Datenmonster (Home-)Office Arbeitsplatz?

Im Spannungsfeld von IT- und Datensicherheit und versteckter Kontrolle

Ein Leitfaden zur Mitbestimmung für die betriebliche Interessenvertretung (Betriebsrat und Personalvertretung)

Jänner 2023

GEFÖRDERT DURCH Digifonds AK WIEN

Thomas Riesenecker-Caba

FORBA

FORSCHUNGS- UND BERATUNGSSTELLE
ARBEITSWELT

KONTAKT:
ASPERNBRÜCKENGASSE 4/5
1020 WIEN
TEL. +43 1 21 24 700-0
OFFICE@FORBA.AT

WWW.FORBA.AT

INHALT

1 EINLEITUNG

In den Medien war in den letzten Jahren viel über Cyberangriffe auf Unternehmen, Behörden und Betreiber kritischer Infrastruktur zu lesen. Expert:innen sind sich einig, dass einerseits die Bedrohung durch Cyberangriffe immer weiter zunehmen wird und dass andererseits durch die umfassende und stetig steigende technologische Vernetzung der eintretende Schaden deutlich höher sein wird.

Die COVID-19-Pandemie, verbunden mit dem Umstand, dass viele Mitarbeiter:innen zum Teil mit eigenen Geräten aus dem Home-Office arbeiten und auch in Zukunft arbeiten werden, steigert die Anforderungen an eine sichere (über)betriebliche Informationsverarbeitung und führt zu neuen Aufgaben in der IT- und Datensicherheit.

Mobiles Arbeiten, die Nutzung von Cloud-Anwendungen oder auch die umfassende Vernetzung betrieblicher Maschinen und Geräte(komponenten) – gemeinhin als Internet der Dinge („Internet of Things“) bezeichnet – führen zu vielfältigeren betrieblichen IT-Landschaften und somit zu mehr möglichen Angriffsflächen, die von Cyberkriminellen attackiert werden können.

Durch diese geänderte Gefahrenlage sehen sich die Unternehmen vor der Herausforderung, IT- und Datensicherheit neu zu bewerten und angepasste technische und organisatorische Maßnahmen zu entwickeln.

Sicherheitsmaßnahmen wie die Regelung der Verwendung von Passwörtern, der Einsatz von Firewalls oder das regelmäßige Updaten der eingesetzten Software genügen dabei schon lange nicht mehr, um die betriebliche Infrastruktur und die darin befindlichen Daten und Informationen sicher zu halten. Zu professionell und umfassend sind die Angriffe und Bedrohungen der Cyberkriminalität geworden.

Parallel dazu wachsen die Angebote die Hersteller von Softwarelösungen zu IT- und Datensicherheit anbieten und neue technische Begriffe wie SIEM[1], SOAR oder XDR beherrschen dieses Thema.

Schlussendlich finden sich Anforderungen an IT- und Datensicherheit auch in den unterschiedlichsten rechtlichen Materien zum Datenschutz oder in Regelungen zur Netz- und Informationssystemsicherheit. In der Europäischen Union wird seit Jahren an neuen Normen gearbeitet. Die bekannteste EU-Verordnung ist dabei die Datenschutz-Grundverordnung.

In diesem Gewirr an rechtlichen Anforderungen, technischen Lösungen und geänderten Bedrohungslagen einen Über- beziehungsweise Durchblick zu erhalten, ist nicht einfach. Erschwert wird dies auch durch die Tatsache, dass die Sicherstellung der IT- und Datensicherheit zu keiner Zeit als abgeschlossen betrachtet werden kann. Es ist ein laufender Prozess mit sich ständig ändernden Herausforderungen!

[1] Alle wichtigen Abkürzungen werden im Glossar erklärt.

Da das Thema IT- und Datensicherheit auch Mitarbeiter:innen unmittelbar an ihren Arbeitsplätzen betrifft und die eingesetzten technischen Sicherheitslösungen auch personenbezogene Daten der Mitarbeiter:innen verarbeiten (müssen), ist eine aktive Einbindung der betrieblichen Interessenvertretung zur datenschutzrechtlichen und arbeitsrechtlichen Regelung notwendig, um Betriebsrat oder Personalvertretung die Möglichkeit zur Mitgestaltung zu geben.

Aufgrund von bestehenden gesetzlichen Mitwirkungsrechten sind betriebliche Interessenvertretungen (Betriebsrat oder Personalvertretung) seitens ihrer Dienst- bzw. Arbeitgeber:innen über gesetzte oder geplante Maßnahmen zu IT- und Datensicherheit zu informieren. Die Auswirkungen auf die betroffenen Mitarbeiter:innen sind gemeinsam zu bewerten und Vereinbarungen zum Umgang mit den Daten der Mitarbeiter:innen festzuschreiben.

Um Mitgliedern aus Betriebsrat oder Personalvertretung das dazu notwendige Hintergrundwissen zu vermitteln, werden in diesem Leitfaden die wesentlichen Aspekte von IT- und Datensicherheit bei der elektronischen Datenverarbeitung (am betrieblichen Arbeitsplatz, beim mobilen Arbeiten oder im Home-Office) beschrieben und Ansätze zur aktiven Mitgestaltung aufgezeigt.

Eine erste Begriffsklärung zu IT- und Datensicherheit

Wird über IT- und Datensicherheit gesprochen, verschwimmen oft die Begrifflichkeiten und es ist häufig unklar, was in einem Unternehmen konkret darunter verstanden wird.

Vielen Betriebsrät:innen und Personalvertreter:innen werden in diesem Zusammenhang sofort das geltende Datenschutzrecht, die Datenschutz-Grundverordnung (DSGVO) und das nationale Datenschutzrecht (DSG) einfallen. Die DSGVO behandelt in ihrem Artikel 32 die ***Sicherheit personenbezogener Daten*** (siehe dazu ausführlich Kap 4) und führt den Begriff der „***technischen und organisatorischen Maßnahmen“*** (abgekürzt TOM) zur Etablierung eines *„angemessenen Schutzniveaus“* ein.

Der Begriff IT- und Datensicherheit bezieht sich auf zwei Bereiche: Es sind nicht nur die Daten beziehungsweise Informationen zu schützen (Datensicherheit), sondern auch die dazugehörige technische Infrastruktur, in denen diese Daten/Informationen verarbeitet werden (IT-Sicherheit).

Um auf die Bedeutung der vermehrten Nutzung von Cloud-Lösungen beziehungsweise die Verarbeitung von Daten im globalen Verbund (Nutzung des Internets) stärker hinzuweisen, wird in diesem Leitfaden auch vermehrt der Begriff Cybersicherheit verwendet.

Folgende Begriffe werden verwendet:

- **IT-Sicherheit** (im Englischen IT-Security) beschreibt Maßnahmen zur Gewährleistung einer sicheren technischen Infrastruktur, darunter fallen alle eingesetzten Informationstechniken oder Informationstechnologien (IT).
- **Daten- und Informationssicherheit** (im Englischen Data Security, Data Privacy, Data Safety) bezieht sich auf die sichere Verarbeitung von (personenbezogenen und nicht personenbezogenen) Daten und Informationen. Diese Daten und Informationen müssen sowohl vor unberechtigter Verwendung oder Manipulation, unberechtigtem Zugang als vor Verlust bei technischen Problemen der eingesetzten Systeme geschützt werden.
- **Cybersicherheit** erweitert diese beiden Ansätze, indem in die Bewertung der zu treffenden Maßnahmen der gesamte „Cyber-Raum" mit einbezogen wird. Cybersicherheit umfasst nach der Definition der NIS-Richtlinie der EU *„alle Tätigkeiten, die notwendig sind um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen"*.

Bei der Erstellung dieses Leitfadens wurden das Wissen und die wertvolle Unterstützung von Dr. Wolfgang Goricnik von der Arbeiterkammer Salzburg sowie Betriebsrät:innen aus ausgewählten Unternehmen und Institutionen zur Verfügung gestellt. Herzlichen Dank dafür!

2 INHALTE UND STRUKTUR DIESES LEITFADENS

Im Fokus dieses Leitfadens steht IT- und Datensicherheit, somit die **Sicherheit der Verarbeitung von personenbezogenen und nicht-personenbezogenen Daten sowie von Betriebs- und Geschäftsgeheimnissen in IT-Systemen**. Andere datenschutzrechtliche Fragen und Anforderungen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten von Mitarbeiter:innen (beispielsweise Fragen zur Dauer der Speicherung solcher Daten oder die Übermittlung von Daten in das EU-Ausland) werden hier nur am Rande oder vor allem in Verbindung mit sicherheitstechnischen Fragen angeführt.

Informationen zu allgemeinen Themen des Datenschutzes und der Mitbestimmung durch Betriebsrat oder Personalvertretung finden sich in gesonderten Publikationen von Gewerkschaften und Arbeiterkammern oder im einschlägigen Fachhandel.

Auf drei Veröffentlichungen wird hier exemplarisch verwiesen:

- Martina Chlestil, Thomas Riesenecker-Caba: Verarbeitung von personenbezogenen MitarbeiterInnen-Daten. Mitbestimmung und Datenschutz, Praktische Gewerkschaftsarbeit, Band 5, ÖGB-Verlag, 2022. Freier Download unter: https://tinyurl.com/k2v69mdf
- Wolfgang Goricnik, Josef Grünanger: Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle, Manz-Verlag, Wien 2018
- Susanne Haslinger, Andreas Krisch und Thomas Riesenecker-Caba (Hrsg): Beschäftigtendatenschutz - Handbuch für die betriebliche Praxis, 2. Auflage. ÖGB Verlag, Wien 2020.

2.1 Aufbau der einzelnen Kapitel

Jedes der folgenden Kapitel besteht aus einem kurzen Aufriss des Themas (Das Wichtigste in Kürze) gefolgt von einer umfassenden Darstellung der wesentlichen Aspekte des Themas mit besonderer Berücksichtigung der Zielgruppe Betriebsrat/Personalvertretung (Zum Thema). Je Kapitel werden abschließend Fragen zur betrieblichen Klärung angeführt (Fragen an Arbeitgeber:in/Dienstgeber:in), die für Betriebsräte und Personalvertretungen bei der Behandlung des Themas im Betrieb hilfreich sein können. Ergänzt wird jedes Kapitel mit Links zu weiteren relevanten Informationen (Weiterführende Informationen).

Da es in Gesprächen mit Expert:innen häufig üblich ist, das englische Fachvokabular zu verwenden, werden bei Schlüsselwörtern sowohl die englischen Fachbegriffe als auch die deutsche

Übersetzung angeführt. Am Ende des Leitfadens findet sich ein Glossar, in dem die wichtigsten Begriffe erklärt werden.

Abbildung 1: Aufbau des Leitfadens

<table>
<tr><td>  </td><td colspan="3">Die betriebliche IT-Landschaft</td></tr>
<tr><td>  </td><td>Sicherheit der Verarbeitung – IT- und Datensicherheit im Datenschutzrecht</td><td>Weitere rechtliche Bestimmungen zu IT- und Datensicherheit</td><td>Internationale Standards und „anerkannte Leitfäden“ zu IT- und Datensicherheit</td></tr>
<tr><td>  </td><td>Cyberkriminalität und Bedrohungslagen</td><td>IT- und Datensicherheit durch ein Informationssicherheits-managementsystem</td><td>Sicherheitslösungen zur Unterstützung von IT- und Datensicherheit</td></tr>
<tr><td>  </td><td colspan="3">Überwachung und IT- und Datensicherheit im Home-Office</td></tr>
<tr><td>  </td><td colspan="2">IT- und Datensicherheit und Mitbestimmung</td><td>Muster einer Betriebsvereinbarung zu IT- und Datensicherheit</td></tr>
<tr><td>  </td><td colspan="3">Glossar
Abkürzungsverzeichnis</td></tr>
</table>

Quelle: FORBA, eigene Darstellung

Alle in diesem Leitfaden angeführten Links wurden im Jänner 2023 geprüft.

Eine online-Version dieses Leitfadens und des Musters einer Betriebsvereinbarung zu IT- und Datensicherheit ist auch unter https://www.forba.at/beratung/it-sicherheit-und-mitbestimmung/ verfügbar.

3 DIE BETRIEBLICHE IT-LANDSCHAFT

3.1 Das Wichtigste in Kürze

Heutzutage kommen in der betrieblichen Informationsverarbeitung unterschiedlichste technische Komponenten zum Einsatz. Diese werden in globalen Unternehmensnetzwerken, in überbetrieblichen Lieferketten oder auch unter Nutzung von Cloud-Technologien verwendet. Ein wichtiger Schritt zu IT- und Datensicherheit ist daher, einen Überblick über die eigene IT-Landschaft und die daraus abgeleiteten möglichen Schwachstellen und Angriffsflächen zu erhalten.

Um zu diesem Gesamtbild zu gelangen, wird bei der Darstellung und Dokumentation der IT-Landschaft empfohlen, eine Unterscheidung in Identitäten (Identities), Endpunkte (Endpoints), Anwendungen (Applications), Netzwerk (Network), Infrastruktur (Infrastructure) und verarbeitete Daten (Data) vorzunehmen.

3.2 Zum Thema

In einer vernetzten Welt nutzen immer mehr Unternehmen Cloud-Technologien (als Beispiel Microsoft 365) und es erfolgen die Kommunikation (E-Mail, Chat) sowie die Zusammenarbeit (collaboration) über Unternehmensgrenzen hinweg. Diese Datenverarbeitung sicher zu gestalten ist eine wesentliche Herausforderung für alle Unternehmen. Immer wieder wird in Medien von Angriffen auf Betriebe und deren IT-Netzwerke berichtet. Cyberkriminalität ist ein weltweites Phänomen geworden und durch die Nutzung des Internets ist kein Unternehmen mehr vor Attacken oder Angriffen sicher.

Um das Thema IT- und Datensicherheit umfassend planen und gestalten zu können, sind unterschiedlichste technische und organisatorische Maßnahmen (TOM) notwendig, wie es auch die Datenschutz-Grundverordnung fordert.

Welche unterschiedlichen Komponenten einer IT-Landschaft dabei zu berücksichtigen sind und was die jeweiligen Herausforderungen zur Verwaltung dieser Komponenten sind, wird in Folge kurz dargestellt:

3.2.1 Identitäten (Identities)

Ein erster Ansatzpunkt zur Verbesserung von IT- und Datensicherheit ist, einen Überblick über die berechtigten Personen und Geräte (Devices) zu erhalten. Alle Personen, die auf IT-Systeme zugreifen können, müssen in jedem dieser IT-Systeme über ihre Nutzerkennung (User-ID) eindeutig identifizierbar sein. Kann eine User-ID nicht eindeutig einer Person zugeordnet werden, so wäre das bei der Definition von Zugriffsberechtigungen auf Daten, Geräte oder Systeme ein zu hohes Risiko. Durchgeführte Verarbeitungsschritte könnten dann nicht durch Sicherheitssysteme auf ihre Rechtmäßigkeit überprüft werden.

Gleiches gilt für die Vielzahl an verwendeten Geräten, unabhängig davon, ob es sich um einen PC, einen Laptop, ein Tablet oder ein Smartphone handelt. Jedes Gerät muss einer oder mehreren Nutzer:innen eindeutig zuordenbar sein, um dieses Gerät für die notwendigen Zugriffe auf die Unternehmens-IT, die einzelne Systeme und Daten berechtigen zu können.

3.2.2 Endpunkte (Endpoints)

Durch die stetig anwachsende Vernetzung von Geräten ist der Ansatz einer transparenten Verwaltung von Berechtigungen nicht nur auf Nutzer:innen und die von ihnen verwendeten Geräte anzuwenden, sondern auch auf alle anderen vernetzten Geräte wie Produktionsmaschinen, Videokameras, Stockwerksdrucker und dergleichen. All diese im Unternehmen genutzten Geräte sind zu dokumentieren, um deren Verhalten überwachen zu können, da auch diese ein potenzieller Angriffspunkt für Cyberangriffe sein können.

3.2.3 Netzwerk (Network)

Die im Unternehmen verarbeiteten Daten fließen inner- und überbetrieblich über (eigene oder fremde) Netzwerkinfrastrukturen von einer versendenden zu einer empfangenden Stelle. Über Netzwerke werden beispielsweise E-Mails versendet, Systemzustände von Produktionsmaschinen an den Leitstand gemeldet, Videobilder einer Kamera eines überwachten Firmenbereichs der Sicherheitszentrale zur Verfügung gestellt oder ein Kund:innenanruf an die zuständige Stelle im Call-Center übermittelt. Stetig fließen Daten über Netzwerke, wobei diese Übermittlung ohne Beeinträchtigung erfolgen und vor unberechtigtem Zugriff oder vor Verfälschung geschützt werden muss.

3.2.4 Anwendungen (Apps, Applications)

Im Unternehmen kommen verschiedene Computerprogramme zum Einsatz. Der früher verwendete Begriff „Software“ rückt dabei immer mehr in den Hintergrund. Durch die Nutzung von mobilen Geräten (Smartphones) hat sich in der Zwischenzeit der Begriff App, als Abkürzung für Application Software (Anwendungsprogramm), durchgesetzt. Eine der großen Herausforderungen in den Unternehmen besteht darin, einen umfassenden Überblick über alle eingesetzten Anwendungen zu erhalten. Denn um mit einzelnen Anwendungen sicher arbeiten zu können, sind diese auf aktuellem (Versions-)Stand zu halten, die berechtigten Nutzer:innen festzulegen und Regeln für den Umgang mit den in diesen Anwendungen verarbeiteten Daten festzuschreiben.

3.2.5 Daten (Data)

Neben den eingesetzten IT-Systemen und Geräten bilden die verarbeiteten Daten eine weitere zentrale Grundlage der betrieblichen Informationsverarbeitung.

Daten werden als *„jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material“*[2] beschrieben.

Im Datenschutzrecht[3] liegt der Fokus auf der Verarbeitung von personenbezogenen Daten. Personenbezogene Daten sind *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen“*. Die Bestimmungen des (europäischen) Datenschutzrechts betreffen dabei auch nicht digital verarbeitete Daten (Papierablagen, Ordnersysteme in Papierform), aber nur, sofern eine strukturierte Sammlung vorliegt, die zumindest nach einem Suchkriterium zugänglich ist (eine lose Ablage von Aufzeichnungen fällt sohin nicht darunter, geordnete Personalakte schon).

Der Schutz aller verarbeiteten Daten (nicht nur der personenbezogenen) stellt eine weitere zentrale Aufgabe für Unternehmen dar. Dabei gilt es einerseits, personenbezogene Daten im Sinne der Anforderungen der Datenschutz-Grundverordnung zu schützen, andererseits für die Vertraulichkeit von Betriebs- und Geschäftsgeheimnissen zu sorgen. Aber auch für alle über diese zwei Bereiche hinausgehenden Datenkategorien, das können beispielsweise Systemzustände von Maschinen oder technische Protokolldaten sein, sind betriebliche Regelungen für den sorgsamen Umgang mit diesen zu definieren.

3.2.6 Infrastruktur (Infrastructure)

Die betriebliche IT-Infrastruktur erfuhr in den letzten Jahrzehnten durch den technologischen Wandel und die vermehrte Digitalisierung vielfältige Veränderungen. Durch umfassende Angebote an verschiedenen Cloud-Diensten (im Internet = in der Cloud), durch die Virtualisierung von Arbeitsplätzen (die eigentliche Datenverarbeitung findet nicht mehr unmittelbar am verwendeten Gerät statt, sondern in betrieblichen Systemen im Hintergrund[4]) sowie durch die Mobilität der Belegschaft (mobiles Arbeiten, Home-Office) werden physische Systeme im Unternehmen reduziert und durch virtuelle Systeme (unter der Nutzung des Internets – in der Cloud) ersetzt.

3.2.7 Bedarfsorientierte Bereitstellung von IT-Ressourcen (Everything as a service)

Die betriebliche Infrastruktur ist, wie die Überschrift dieses Kapitels („IT-Landschaft“) vermuten lässt, schon lange nicht mehr auf physische, das heißt dem Betrieb zuordenbare Standorte beschränkt. Viele Unternehmen übertragen Aufgaben und Dienste an Auftragsverarbeiter und Anbieter von Cloud-Lösungen.

---

2 Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt)

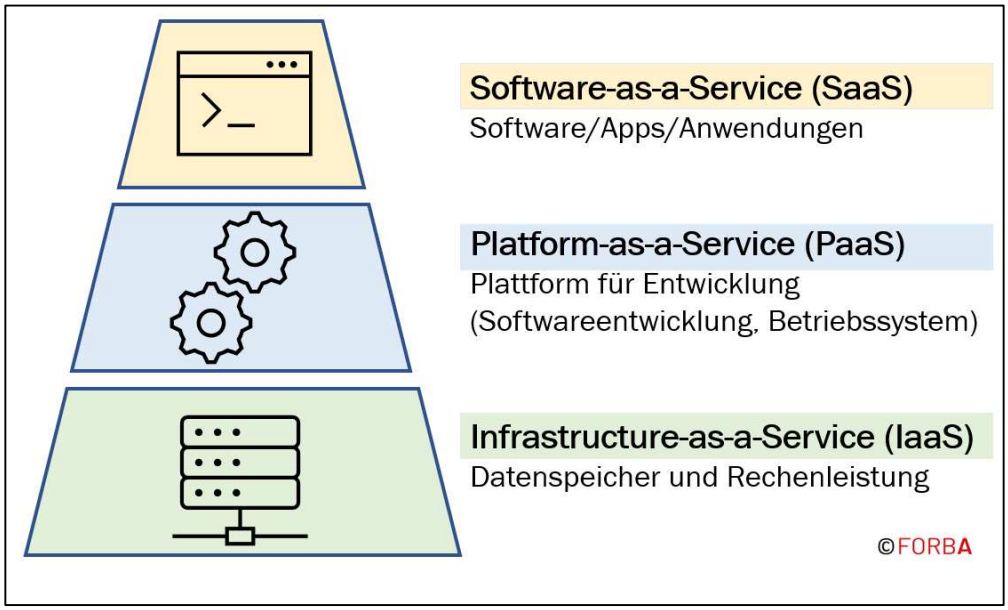
3 Begriffsbestimmungen sind in Art 4 der DSGVO zu finden.

4 Ein einfaches Anwendungsbeispiel für die Virtualisierung von Aufgaben ist Telebanking: Das dabei verwendete Gerät (PC, Laptop oder Smartphone) zeigt die Daten aus dem externen Banksystem an und ermöglicht Nutzer:innen die Verarbeitung von Daten (Überweisungen) in diesem externen System anzustoßen.

In diesem Zusammenhang fallen oft die Begriffe SaaS, PaaS, IaaS, die im Folgenden kurz erklärt werden:

- SaaS = Software as a service: Nutzer:innen verwenden Apps (Software), die über eine Cloud-Plattform zur Verfügung gestellt werden.
- PaaS = Platform as a service: Anbietern stellen neben der Infrastruktur auch das Betriebssystem oder eine Entwicklungsumgebung für Anwendungen zur Verfügung gestellt.
- IaaS = Infrastructure as a Service: Teile der betrieblichen IT-Infrastruktur (beispielsweise die Datenspeicherung) werden über die Cloud zur Verfügung gestellt und genutzt. Ein Vorteil dieses Service ist, dass nicht mehr das Unternehmen für eine sichere Datenhaltung sorgen muss, sondern diese an einen Auftragsverarbeiter (Dienstleister) auslagert wird. Die bekanntesten Anbieter sind Amazon (Amazon Web Services), Microsoft (Microsoft Azure) oder Google Cloud Platform (GCP).

Abbildung 2: Cloud-Services



Quelle: FORBA, eigene Darstellung

Um einen ganzheitlichen Überblick über die eigene IT-Landschaft zu erhalten, die auch die Nutzung externer Dienste/Services beinhalten kann, sind eine Analyse und Dokumentation aller oben beschrieben Komponenten notwendig. Diese Dokumentation und deren Darstellung sind die Basis für die Definition von Maßnahmen zu IT- und Datensicherheit.

3.3 Fragen an Arbeitgeber:in/Dienstgeber:in

- In welcher Form ist die betriebliche IT-Landschaft dokumentiert?
- Wird zur Dokumentation der betrieblichen IT-Landschaft ein technisches System eingesetzt?
- Welche IT-Sicherheitssysteme werden für welchen Zweck verwendet?
- Wie sind diese IT-Sicherheitssysteme nach den Anforderungen der Datenschutz-Grundverordnung in einem Verzeichnis von Verarbeitungstätigkeiten (nach Art 30 DSGVO) dokumentiert und wo liegt diese Dokumentation auf?
- Welche Auftragsverarbeiter (inkl. Cloud-Dienstanbieter) werden genutzt? Unter Auftragsverarbeitung können auch Datenverarbeitungen fallen, die von anderen Konzerntöchtern oder der Konzernmutter konzernweit angeboten werden. Wo liegen die dabei notwendigen Auftragsverarbeiterverträge auf?
- Welche dieser durch Dritte zur Verfügung gestellten Dienste/Services verarbeiten personenbezogene Daten von Mitarbeiter:innen?

3.4 Weiterführende Informationen

Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt):
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R0868&from=EN

Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG ("Datenschutz-Grundverordnung", DSGVO).
https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE

4 SICHERHEIT DER VERARBEITUNG – IT- UND DATENSICHERHEIT IM DATENSCHUTZRECHT

4.1 Das Wichtigste in Kürze

Die Datenschutz-Grundverordnung (DSGVO) verpflichtet Unternehmen (als datenschutzrechtliche Verantwortliche) zur Entwicklung von technischen und organisatorischen Maßnahmen (TOM) zur Sicherheit der Verarbeitung. Auch wenn die DSGVO nur von personenbezogenen Daten spricht, können in Unternehmen viele dieser Maßnahmen auch zum Schutz von Betriebs- und Geschäftsgeheimnissen sowie generell zur sicheren Informationsverarbeitung in technischen Systemen herangezogen werden.

4.2 Zum Thema

Die (europäische) Datenschutz-Grundverordnung, die seit 2018 Regelungen zum Umgang mit personenbezogenen Daten vorgibt, weist auf die Bedeutung einer angemessenen Sicherheit und Vertraulichkeit dieser Daten hin: „*Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können*.“ (Erwägungsgrund 39)

Um die Sicherheit der Verarbeitung von personenbezogenen Daten sowie Betriebs- und Geschäftsgeheimnissen gewährleisten zu können, sind im Rahmen einer wirtschaftlichen und sicherheitstechnischen Bewertung mehrere Aspekte zu berücksichtigen. Artikel 32 DSGVO definiert diese für personenbezogene Daten, gleiche Ansätze gelten jedoch auch für Betriebs- und Geschäftsgeheimnisse.

Art 32 Abs 1 DSGVO führt zur Sicherheit der Verarbeitung Folgendes aus:

„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.“

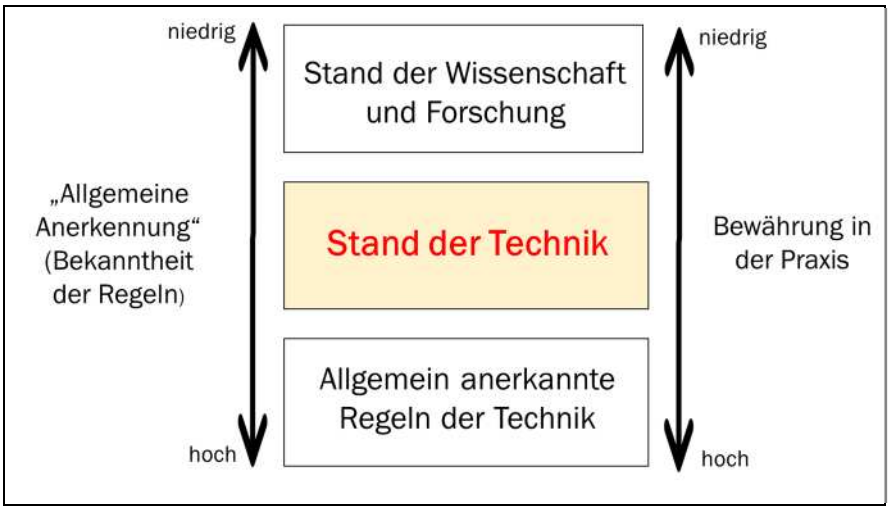
Das bedeutet, dass bei der Sicherheit der Verarbeitung insbesondere folgende Aspekte zu prüfen sind:

1. **Stand der Technik**[5]

   Die Einordnung, was unter der Bedingung „Stand der Technik“ zu verstehen ist, beruht auf der Verfügbarkeit von technischen Lösungen zur Erreichung eines Ziels. Diese Lösungen (Maßnahmen) müssen auf einschlägigen (wissenschaftlichen) Erkenntnissen beruhen und fortschrittliche (technische) Verfahren verwenden, die in der Praxis geeignet erscheinen, IT- und Datensicherheit am **Stand der Technik** zu gewährleisten. Betriebliche Maßnahmen wie beispielsweise „Wir benötigen einen Virenschutz“ oder „Ein Passwort muss aus 8 Zeichen bestehen“, sind zwar allgemein bekannt und akzeptiert, aber im Hinblick auf den Stand der Technik nicht (mehr) ausreichend (siehe folgende Abbildung 3).

   Alle im Unternehmen festgeschriebenen technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung haben daher einerseits über bereits „allgemein anerkannte Regeln der Techniken“ hinauszugehen, müssen aber andererseits (noch) nicht dem aktuellen „Stand der Wissenschaft und Forschung“ entsprechen. Die getroffenen Maßnahmen sind jedoch regelmäßig zu evaluieren und gegebenenfalls anzupassen, da sich technische Lösungen und somit der Stand der Technik stetig weiterentwickeln und daher die Einordnung neu zu erfolgen hat.

Abbildung 3: Stand der Technik



Quelle: FORBA, eigene Darstellung auf Basis Drei-Stufen-Theorie

2. **Implementierungskosten**

   Die geplanten Maßnahmen zur Sicherheit der Verarbeitung müssen von den jeweiligen Unternehmen auch finanziert werden können. Kleinbetriebe oder Einzelunternehmer:innen haben in diesem Bereich weniger Möglichkeiten als ein internationaler Konzern. Beide müssen jedoch auf Grundlage ihrer Möglichkeiten,

[5] https://www.teletrust.de/fileadmin/user_upload/2021-09_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

angemessene Maßnahmen setzen, die im Falle eines möglichen Datenverlustes auch von den Datenschutzbehörden beurteilt werden könnten.

3. **Art, Umfang, Umstände und Zwecke der Verarbeitung**
   Bei den zu treffenden Maßnahmen zur Sicherheit der Verarbeitung ist weiters zu prüfen, wie sensibel die verarbeiteten Daten sind. Bei personenbezogenen Daten, insbesondere bei aus Sicht der Betroffenen schutzwürdigen Daten (wie beispielsweise Gehalt, Gesundheitsdaten oder betriebliche Beurteilungen), oder vertraulichen Geschäftsinformationen (Verträge, Produktpläne) sind strengere Maßstäbe anzusetzen als bei allgemein verfügbaren Daten (Adresse eines Unternehmens).

4. **Eintrittswahrscheinlichkeit** und **Schwere** eines möglichen Sicherheitsvorfalls
   Unternehmen müssen beurteilen können, welche Daten und Informationen bei einem Datenschutzproblem in die Hände Unbefugter geraten könnten und wie schutzwürdig beziehungsweise wie sensibel diese Informationen sind.

In Artikel 32 der DSGVO werden zu diesen Aspekten konkrete technische und organisatorische Maßnahmen angeführt. Nachdem im Unternehmen das mögliche Risiko einer Datenschutzverletzung oder eines Datenverlustes nach obigen Kriterien bewertet wurde, sollen die schlussendlich getroffenen Maßnahmen ein angemessenes Schutzniveau gewährleisten.

Die Umsetzung von technischen Maßnahmen erfolgt durch die Nutzung von speziellen IT-Sicherheitssystemen (siehe dazu Kapitel 9) und durch konkrete Maßnahmen, die in diesen IT-Systemen gesetzt werden, wie beispielsweise die automatische Verschlüsselung von E-Mails mit vertraulichem Inhalt. Organisatorische Maßnahmen umfassen hingegen betriebliche Regelungen zum Umgang mit technischen Systemen und den dabei verarbeiteten Daten und Informationen (Papierdokumente/Ausdrucke unterliegen ebenfalls den Anforderungen des Datenschutzes) wie beispielsweise eine Clean-Desk Regelung.

Die in Artikel 32 DSGVO angeführten technischen und organisatorischen Maßnahmen umfassen:

- **Pseudonymisierung** personenbezogener Daten:
  Die Verarbeitung oder Darstellung von personenbezogenen Daten erfolgt in einer Form, in der kein direkter Bezug auf eine konkrete natürliche Person möglich ist, da es zur Bestimmung dieser Person zusätzlicher Information bedürfte, die im zugrunde liegenden IT-System nicht angeboten wird. So könnten beispielsweise Personen in einem IT-System oder einer Auswertung nur durch einen Zahlencode beschrieben werden und die Tabelle mit der Zuordnung konkreter Personen zu dem verwendeten Code ist nicht im selben System verfügbar und nur ausgewählte Personen besitzen Zugriff auf diese Tabelle.

- **Verschlüsselung** von Daten:
  Durch von technischen Maßnahmen vorgenommene Schritte wird verhindert, dass unberechtigte Personen, welche zufällig oder in rechtswidriger Absicht an Daten gelangen, diese lesen können.

- **Vertraulichkeit** der Systeme und Dienste:
  Im Zusammenhang mit der Verarbeitung von Daten und Informationen wird auf Dauer sichergestellt, dass diese nur von (vorher) berechtigten Personen **eingesehen** oder im Rahmen von (vorher) definierten Abläufen/Prozessen **offengelegt** werden können.

- **Integrität** der Systeme und Dienste:
  Im Zusammenhang mit der Verarbeitung von Daten und Informationen wird auf Dauer sichergestellt, dass diese nur von (vorher) berechtigten Personen **bearbeitet** oder im Rahmen von (vorher) definierten Abläufen/Prozessen **verändert** werden können.

- **Verfügbarkeit** der Systeme und Dienste:
  Im Zusammenhang mit der Verarbeitung von Daten und Informationen wird auf Dauer sichergestellt, dass diese nur dann berechtigten Personen oder in Abläufen/Prozesse **bereitgestellt** werden, wenn diese auch benötigt werden.

- **Belastbarkeit** der Systeme und Dienste:
  Im Zusammenhang mit der Verarbeitung von Daten und Informationen wird auf Dauer sichergestellt, dass die Verfügbarkeit und der Zugang zu diesen bei einem physischen oder technischen Zwischenfall rasch **wiederhergestellt** werden können. Sollte aus systemtechnischen Gründen oder auf Grund eines technischen Gebrechens ein Zugriff nicht möglich sein, so können Daten und Informationen in kurzer Zeit wieder zur Verfügung gestellt werden (durch ein Backup).

- **Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung** der Systeme und Dienste:
  Die Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind regelmäßig zu überprüfen und bewerten.

Ein Aspekt, der in Artikel 32 DSGVO nicht direkt angesprochen wird, jedoch in anderen Rechtsnormen wie beispielsweise dem Netz- und Informationssystemsicherheitsgesetz (NISG) enthalten ist, ist die **Authentizität** von Daten und Informationen zu erkennen, das bedeutet die Fähigkeit diese Daten als richtig (im Unterschied zu Fake Daten) einordnen zu können.

4.3 Fragen an Arbeitgeber:in/Dienstgeber:in

- In welcher Form fand für die verschiedenen IT-Systeme eine Risikoabschätzung in Bezug auf die Verarbeitung von personenbezogenen Daten statt?
- In welcher Form fand für die verschiedenen IT-Systeme eine Risikoabschätzung in Bezug auf die Verarbeitung von Betriebs- und Geschäftsgeheimnissen statt?
- Welche konkreten technischen und organisatorischen Maßnahmen wurden ergriffen?
- Welche Softwareprodukte werden dazu eingesetzt und welche personenbezogenen Daten von Mitarbeiter:innen werden dabei verarbeitet?
- In welcher Form und durch wen werden diese technischen und organisatorischen Maßnahmen in regelmäßigen Abständen überprüft (Evaluierung)?

4.4 Weiterführende Informationen

Bundesverband IT-Sicherheit e.V. (TeleTrusT) (2021): IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum „Stand der Technik“. Technische und organisatorische Maßnahmen.
https://www.teletrust.de/fileadmin/user_upload/2021-09_TeleTrusT-Handreichung_Stand_der_Technik_in_der_IT-Sicherheit_DE.pdf

5 WEITERE RECHTLICHE BESTIMMUNGEN ZU IT- UND DATENSICHERHEIT

5.1 Das Wichtigste in Kürze

Die Europäische Union hat durch die Verabschiedung der Datenschutz-Grundverordnung (DSGVO) auf die Bedeutung eines sorgsamen Umgangs mit personenbezogenen Daten, mit digitaler Technik und den damit verbundenen Veränderungen im beruflichen und privaten Alltag hingewiesen. Dies war ein erster Schritt in ihrer digitalen Agenda. Weitere EU-Verordnungen, die unmittelbar in Österreich Gültigkeit erlangen, sowie EU-Richtlinien, die in nationale Gesetze umgesetzt werden müssen, sind bereits gefolgt oder werden noch folgen. In diesem Kapitel wird auf die, aus Sicht von IT- und Datensicherheit, wesentlichen Bestimmungen seitens der Europäischen Union sowie die schon bestehenden nationalen Regelungen eingegangen. Diese Bestimmungen können für Betriebsrat oder Personalvertretung bereits jetzt, jedenfalls aber in absehbarer Zukunft wichtige Informationen zu IT- und Datensicherheit liefern.

5.2 Zum Thema

Die Datenschutz-Grundverordnung (DSGVO) verpflichtet Unternehmen (wie in Kapitel 4 beschrieben) unter anderem zur Sicherheit der Verarbeitung personenbezogener Daten. Aber auch andere rechtliche Bestimmungen, die in Österreich Gültigkeit besitzen, behandeln Aspekte zu IT- und Datensicherheit.

5.2.1 Geschäfts- oder Betriebsgeheimnisse

Der Umgang mit Geschäfts- oder Betriebsgeheimnissen (unabhängig ob in digitaler oder analoger Form) wurde in Österreich 2018 durch eine Überarbeitung des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) geregelt. Dies ist die nationale Umsetzung der EU-Richtlinie über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung.

Nach § 26b UWG ist ein Geschäftsgeheimnis eine Information, die

1. *geheim ist, weil sie weder in ihrer Gesamtheit noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen zu tun haben, allgemein bekannt noch ohne weiteres zugänglich ist,*
2. *von kommerziellem Wert ist, weil sie geheim ist, und*

3. *Gegenstand von den Umständen entsprechenden angemessenen Geheimhaltungsmaßnahmen[6] durch die Person ist, welche die rechtmäßige Verfügungsgewalt über diese Informationen ausübt.*

Das heißt, dass zum Schutz von Geschäftsgeheimnissen (wie auch von personenbezogenen Daten) sowohl technische als auch organisatorische und juristische Maßnahmen in den Betrieben ergriffen werden (müssen) und deren Einhaltung in der Folge überprüft wird.

5.2.2 Kritische Infrastruktur

Bedrohungen durch Cyberkriminalität und Sicherheitsvorfälle durch technische oder menschliche Fehler können bei Betreibern und Nutzer:innen kritischer Infrastruktur weitreichende Folgen haben. Um diesen Bedrohungen entgegenzuwirken, legt das *Netz- und Informationssystemsicherheitsgesetz (NISG[7])* eine Reihe an Maßnahmen fest, welche ein hohes Sicherheitsniveau von Netz- und Informationssystemen gewährleisten sollen.

Das NISG verpflichtet Betreiber wesentlicher Dienste (derzeit[8] in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur) sowie Anbieter digitaler Dienste und Einrichtungen der öffentlichen Verwaltung, geeignete und verhältnismäßige technisch/organisatorische Sicherheitsvorkehrungen zu treffen.

Damit sollen diese Unternehmen und Einrichtungen die Fähigkeit erlangen, Sicherheitsvorfälle

- vorzubeugen,
- diese (frühzeitig) zu erkennen,
- diese abzuwehren und
- (sollten die ersten drei Schritte nicht umfassend erfolgreich gewesen sein) zu beseitigen

Diese Aufzählung zeigt bereits, dass herkömmliche Ansätze der IT- und Datensicherheit (wie Betreiben einer Firewall oder der Einsatz von Virenschutzsoftware) nur noch einen geringen Anteil einer umfassenden betrieblichen Sicherheitsstrategie darstellen (mehr dazu in Kapitel 8 und 9).

Konkrete Sicherheitsmaßnahmen sind in der Netz- und Informationssystemsicherheitsverordnung – NISV) und im Besonderen in deren Anlage 1 beschrieben (siehe folgende Tabelle 1).

Diese Maßnahmen bieten auch für Betriebe, die nicht unter den Geltungsbereich des NISG fallen, wertvolle Hinweise zur Etablierung eines umfassenden Sicherheitssystems.

---

6 Das bedeutet, dass die Person, welche die rechtmäßige Verfügungsgewalt über ein Geschäftsgeheimnis besitzt, Maßnahmen zum Schutz dieser Informationen ergriffen hat, damit sie unberechtigten Dritten nicht zugänglich sind.

7 Das NISG ist die österreichische Umsetzung der EU Netz- und Informationssicherheitsrichtline (NIS-RL). Die NIS-Richtlinie wurde Ende 2022 seitens der EU in einer erweiterten Fassung (NIS-2-Richtline) verabschiedet. In Österreich müssen daher die derzeitigen Gesetze und Verordnungen zur Netz- und Informationssystemsicherheit bis Herbst 2024 aktualisiert werden.

8 Die NIS-2 Richtlinie erweitert die derzeitigen Sektoren.

Tabelle 1: Sicherheitsmaßnahmen (verkürzte Darstellung) nach NISV

Sicherheitsmaßnahme	Regelungsbereiche
1. Governance und Risikomanagement	– Durchführung einer Risikoanalyse – Erstellung einer Sicherheitsrichtlinie und periodische Aktualisierung dieser – Prüfplan zur regelmäßigen Evaluierung – Planung der dafür notwendigen Ressourcen – Periodische Überprüfung des Informationssicherheits-managementsystems ISMS (siehe Kapitel 8) – Umsetzung sicherheitsrelevanter Aspekte in Prozessen des Personalwesens
2. Umgang mit Dienstleistern, Lieferanten und Dritten	– Definition und Überprüfung/Überwachung der getroffenen Anforderungen an Dienstleister, Lieferanten und Dritte
3. Sicherheitsarchitektur	– Dokumentation der Systemkonfiguration – Dokumentation der Vermögenswerte – Netzwerksegmentierung – Netzwerksicherheit – Einsatz kryptographischer[9] Verfahren und Technologien
4. Systemadministration	– Zugangsrechte nach Minimalrechtsprinzip
5. Identitäts- und Zugriffsmanagement	– Identifikation und Authentifikation von Nutzer:innen und Diensten – Unterbindung unautorisierte Zugriffe
6. Systemwartung und Betrieb	– Gewährleistung eines sicheren Systembetriebs – Einschränkung des Fernzugriffs
7. Physische Sicherheit	– Schutz vor unbefugtem Zutritt und Zugang
8. Erkennung von Vorfällen	– Dokumentation erkannter Vorfälle (beispielsweise Warnmeldungen von technischen Systemen)
9. Bewältigung von Vorfällen	– Menschliche oder technische Reaktion bei erkannten Vorfällen und Analyse der Wirksamkeit der getroffenen Reaktion
10. Betriebskontinuität	– Wiederherstellung nach Sicherheitsvorfall ist zu gewährleisten – Erstellung von Notfallplänen
11. Krisenmanagement	– Klare Regelung und Festschreibung von Zuständigkeiten und Kommunikationsabläufen

Quelle: FORBA, eigene Darstellung nach NISV

[9] Kryptographie bezeichnet die Ver- und Entschlüsselung von Daten/Informationen mit Hilfe mathematischer Verfahren.

5.3 Fragen an Arbeitgeber:in/Dienstgeber:in

- Ist das eigene Unternehmen durch das NISG bzw. von der EU NIS 2 Richtlinie unmittelbar betroffen?
- Welche technischen und organisatorischen Maßnahmen zum Schutz von personenbezogenen Daten wurden ergriffen?
- Welche technischen und organisatorischen Maßnahmen zum Schutz von Betriebs- und Geschäftsgeheimnissen wurden ergriffen?
- Welche Maßnahmen, angelehnt an die in der NISV angeführten Sicherheitsmaßnahmen (siehe Tabelle 1), wurden im Betrieb bereits getroffen oder sind geplant?
- In welcher Form liegt eine Dokumentation der getroffenen Sicherheitsmaßnahmen vor?

5.4 Weiterführende Informationen

Bundesgesetz gegen den unlauteren Wettbewerb 1984 – UWG
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002665

Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen (Netz- und Informationssystemsicherheitsgesetz – NISG)
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010536

Verordnung des Bundesministers für EU, Kunst, Kultur und Medien zur Festlegung von Sicherheitsvorkehrungen und näheren Regelungen zu den Sektoren sowie zu Sicherheitsvorfällen nach dem Netz- und Informationssystemsicherheitsgesetz (Netz- und Informationssystemsicherheitsverordnung – NISV)
https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010722

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555&from=EN

6 INTERNATIONALE STANDARDS UND „ANERKANNTE LEITFÄDEN“ ZU IT- UND DATENSICHERHEIT

6.1 Das Wichtigste in Kürze

Unterschiedliche staatliche Organe, Organisationen und Beratungseinrichtungen geben eine Vielzahl an Hinweisen, auf welche Weise rechtliche Anforderungen zu IT- und Datensicherheit umgesetzt werden können und welche wesentlichen Aspekte dabei zu berücksichtigen sind. Für österreichische Unternehmen liefern dabei insbesondere die ISO/IEC-Norm 27001 sowie das *Österreichische Informationssicherheitshandbuch* wertvolle Ansätze zur Verbesserung von IT- und Datensicherheit, verbunden mit Vorschlägen zur Einführung und Etablierung eines Informationssicherheitsmanagementsystems. Aber auch Branchenstandards oder Ansprüche von Kund:innen (im Rahmen vertraglicher Verpflichtungen) können zusätzliche Anforderungen an IT- und Datensicherheit stellen.

6.2 Zum Thema

6.2.1 IT- und Datensicherheit in der Standardisierung

Der Bereich der Normierung liefert seit über 100 Jahren Vorgaben für die unterschiedlichsten Bereiche unseres Lebens. So gibt es beispielsweise Standards für Papierformate (DIN A4: die durch das Deutsche Instituts für Normung [DIN] definierte Größe für ein Blatt Papier) oder für das Qualitätsmanagement von Produkten und Dienstleistungen (die internationale Normenreihe ISO 9000 und folgende). Standards zur Informationssicherheit definiert die sogenannte ISO 27000-Reihe, die von der International Organization for Standardization (ISO) gemeinsam mit der International Electrotechnical Commission (IEC) herausgegeben wird.

Für die Umsetzung von Maßnahmen zu IT- und Datensicherheit und für die betriebliche Gestaltung eines Informationssicherheitsmanagementsystems (ISMS, siehe Kapitel 8) liefert insbesondere die ISO/IEC Norm 27002[10] *„Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen“* eine gute Darstellung wesentlicher technischer und organisatorischer Maßnahmen (TOM). Derartige Maßnahmen werden auch in der DSGVO gefordert und stellen somit Handlungsanleitungen für die Verantwortlichen in Betrieben dar. In einzelnen Fällen, vor allem bei der vertraglichen Ausgestaltung von Kund:innenbeziehungen, kommt es vor, dass Vertragspartner:innen eine betriebliche Zertifizierung nach der ISO 27000-Reihe verlangen. Aber auch Branchenstandards können weitere Auflagen für IT- und Datensicherheit fordern. In der Automobilindustrie sind beispielsweise die Anforderungen des TISAX (Trusted Information Security Assessment Exchange/vertrauenswürdiger Austausch von Informations-Sicherheits-Gutachten und den damit verbundenen Informationen) zu erfüllen.

[10] https://www.iso.org/standard/75652.html

Informationssicherheit kann laut ISO/IEC 27002 durch die Implementierung eines (für das jeweilige Unternehmen geeigneten) Maßnahmensets von Richtlinien, Regeln, Prozessen, Verfahren und organisatorischen Strukturen sowie darauf abgestimmter Anforderungen/Funktionen an Hard- und Software erreicht werden.

Die ISO/IEC Norm 27002 wurde 2022 in überarbeiteter Form veröffentlicht und beschreibt Maßnahmen in folgenden Bereichen:

Organisatorische Maßnahmen (organizational controls)

- betriebliche Regelungen zu IT-Sicherheit: Das sind in der Regel Ordnungsvorschriften oder Maßnahmen zur zweckentsprechenden Benutzung von Betriebseinrichtungen und Betriebsmitteln, die im Sinne des § 97 Abs 1 ArbVG durch Betriebsvereinbarung geregelt werden können.
- Verteilung von Verantwortlichkeiten: Ähnlich der Bestellung eines Datenschutzbeauftragen werden Verantwortlichkeiten für IT-Sicherheit festgelegt.
- Definition von unterschiedlichen Vertraulichkeitsstufen von Daten oder Dokumenten: Vergabe von Kennzeichnungen („labels“) wie öffentlich/intern/vertraulich/geheim.

Da zur Gewährleistung einer umfassenden IT- und Datensicherheit aus Sicherheitsgründen Aktivitäten von Nutzer:innen in technischen Systemen protokolliert werden müssen, widmet sich eine der beschriebenen Maßnahmen auch dem Schutz der davon Betroffenen mit dem Verweis auf „Privacy and Protection of PII[11]“ (personally identifiable information/personenbezogene Information). Somit ist immer auf die Verhältnismäßigkeit zwischen Schutz der IT und der durch die Schutzmaßnahmen betroffenen Nutzer:innen zu achten.

Personenbezogene Maßnahmen

- Schulungen und Trainings
- Verpflichtung zur Geheimhaltung auch nach dem Ausscheiden aus dem Unternehmen
- Regelungen bei „remote work“: Unter remote work werden unterschiedlichste Formen der Arbeit außerhalb gesicherter Unternehmensbereiche verstanden, wie Telework, Telearbeit (tele commuting), flexible Arbeitsplätze, virtuelle Arbeitsumgebungen, Fernwartung und auch die Arbeit im Home-Office.

Physische Maßnahmen

- Zutrittskontrollen und Sicherung besonders sensibler Firmenbereiche (Rechenzentrum)
- Schutz vor schädlichen Umwelteinflüssen
- Clear-Desk-Politik: Entfernen aller schutzwürdigen Geschäftsinformationen vom Schreibtisch
- Technische Maßnahmen

[11] ISO/IEC 27002:2022, Kapitel 5.34, Seite 54

- Schutz der Infrastruktur vor Schadsoftware
- Schutz vor Datenverlust durch Nutzung technischer Systeme zur „Data Loss Prevention“
- Protokollierung von Nutzer:innen- oder Geräteaktivitäten

In Summe weist die ISO/IEC 27002:2022 Version fast 100 Maßnahmen auf und bildet somit einen guten Gradmesser für betriebliche IT- und Datensicherheitsmaßnahmen sowie eine umfassende Beschreibung des Stands der Technik.

Im US-amerikanischen Raum, und somit auch in Betrieben, die einen starken Bezug zu Nordamerika besitzen, wird oft auf das US National Institute of Standards and Technology (NIST)[12] verwiesen, dessen Rahmenwerk aus Standards, Richtlinien und Best-practice-Beispielen besteht.

6.2.2 Das Österreichische Informationssicherheitshandbuch

Das „Österreichische Informationssicherheitshandbuch“, das seit Februar 2022 in einer neuen Version vorliegt, beschreibt auf über 700 Seiten Maßnahmen zur Etablierung eines umfassenden Informationssicherheitsmanagementsystems (ISMS). Es zeigt zum einen Risiken auf, die durch eine vermehrte Informationsverarbeitung auftreten können, zum anderen werden Maßnahmen angeführt, wie diesen Bedrohungen begegnet werden kann. Im Aufbau orientiert es sich an der oben angeführten ISO/IEC 27000 Normenreihe und entstand in Kooperation mit Behörden anderer Länder, wie etwa dem deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI[13]).

Ergänzt wird das Handbuch, das sowohl online als auch als PDF-Download angeboten wird, um Checklisten zu ausgewählten Themen. Eine der Checklisten behandelt die Sicherheit im Home-Office[14].

6.2.3 Die Wissensdatenbank MITRE Att&ck

Für betriebliche Sicherheitsverantwortliche ist es nicht einfach einen Überblick über die technischen Entwicklungen und aktuellen Bedrohungen zu erhalten. Hierbei können Wissensdatenbanken wie etwa „MITRE Att&ck[15]“ unterstützen. Die US-amerikanischen NPO-Einrichtung MITRE ist eine Abspaltung des MIT (Massachusetts Institute of Technology). Deren im Internet frei verfügbare Wissensdatenbank zeigt auf, wie Cyberkriminelle agieren. Es werden tatsächliche Berichte über Angriffe und deren Analyse dargestellt, die konkret gewählten Techniken und Taktiken beschrieben und es wird erklärt, wie diese erkannt und im besten Fall abgewehrt beziehungsweise beseitigt werden können.

12 https://www.nist.gov/cybersecurity
13 https://www.bsi.bund.de
14 https://www.sicherheitshandbuch.gv.at/downloads/Home-Office-Checkliste.pdf
15 https://attack.mitre.org/

6.3 Fragen an Arbeitgeber:in/Dienstgeber:in

- Welche Informationsquellen wurden zur Festlegung der betrieblichen Maßnahmen zu IT- und Datensicherheit herangezogen?
- Gibt es in den Kundenbeziehungen die vertragliche Verpflichtung, relevante Normen oder Branchenstandards einzuhalten und wie ist diese Verpflichtung nachzuweisen?

6.4 Weiterführende Informationen

ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection — Information security controls
https://www.iso.org/standard/75652.html

Österreichischen Informationssicherheitshandbuch
https://www.sicherheitshandbuch.gv.at/

7 CYBERKRIMINALITÄT UND BEDROHUNGSLAGEN

7.1 Das Wichtigste in Kürze

Regelmäßig ist in den Medien von erfolgreichen Cyberangriffen auf Unternehmen zu lesen. Der vom Bundeskanzleramt jährlich veröffentlichte Bericht zur Cybersicherheit[16] zeigt die Bedrohungen durch Cyberkriminelle auf, die in Österreich zu beobachten sind. Vor diesem Hintergrund offerieren Anbieter von Sicherheitslösungen eine Vielzahl an technischen Produkten.

Welche unterschiedlichen Arten von Bedrohungen es für Unternehmen (aber auch Privatnutzer:innen) geben kann, beschreibt ein Bericht der ENISA (Agentur der Europäischen Union für Cybersicherheit), der die verschiedenen Angriffsmuster anhand einer Bedrohungslandkarte (Threat Landscape) darstellt.

7.2 Zum Thema

Wenn in Medien von erfolgreichen Cyberangriffen zu lesen ist, wird häufig von der Verschlüsselung von Daten mit anschließender Lösegelderpressung berichtet und von Attacken auf die Infrastruktur von Unternehmen, um deren Services zu beeinträchtigen oder lahmzulegen.

Wie vielfältig die Angriffe auf die Infrastruktur oder die Datenbestände von Unternehmen sein können, zeigt die Agentur der Europäischen Union für Cybersicherheit (ENISA) regelmäßig in ihren Berichten auf. In einem im Herbst 2022[17] veröffentlichten Bericht werden, bezugnehmend auf den Berichtszeitraum von Juli 2021 bis Juli 2022, acht vorrangige Kategorien an Bedrohungen klassifiziert (siehe Abbildung 4). Die Angreifer können laut ENISA dabei sowohl staatlich unterstützt und gefördert sein (während des Ukrainekrieges haben beispielsweise russische Hacker die technische Infrastruktur der Ukraine angegriffen), kriminellen Organisationen angehören, im Darknet[18] Dienstleistung oder Zugangsdaten von gehackten Unternehmen beziehungsweise Personen[19] anbieten oder beziehen (AaaS = Access as a Service als Teil von CaaS = Cybercrime as a Service) oder politisch motivierten Protestaktivitäten verfolgen (Hacktivist:innen).

Um die Vielfältigkeit der Bedrohungslagen aufzuzeigen, werden in der Folge die acht verschiedenen Bedrohungsszenarien kurz skizziert:

[16] https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/bericht-cybersicherheit.html
[17] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport
[18] Beim Darknet handelt es sich um einen versteckten Teil des Internets, der nur durch spezielle Software (zB Tor Browser) erreichbar ist. Eine Identifizierung von Nutzer:innen ist nur schwer möglich, Nutzer:innen genießen ein hohes Maß an Anonymität.
[19] Ob Zugangsdaten einer Privatperson im Darknet zum Verkauf angeboten werden, kann über die Seite https://haveibeenpwned.com/ geprüft werden.

Abbildung 4: Bedrohungsszenarien nach ENISA

Quelle: ENISA Bedrohungslandkarte (Threat Landscape) 2022

7.2.1 Erpressungssoftware oder Verschlüsselungssoftware (Ransomware)

Ransomware ist eine spezielle Art von Schadsoftware, bei der Cyberkriminelle nach erfolgtem Zugriff auf die betriebliche Infrastruktur Daten des betroffenen Unternehmens verschlüsseln und den Zugriff auf diese Daten erst nach Zahlung eines Geldbetrages (in digitaler Währung auf ein anonymes Konto) in Aussicht stellen.

7.2.2 Schadprogramme (Malware)

Ein Schadprogramm ist eine Software oder eine Firmware (Betriebssoftware), die das Ziel verfolgt, sich unberechtigt Zugang zu einer betrieblichen Infrastruktur zu schaffen, um dort, wie der Name schon andeutet, Schaden anzurichten. Der Begriff Malware ist abgeleitet aus „Malicious software“ und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meist schädliche Funktionen auszuführen. Malware wird auch häufig als (Computer)Virus, Trojanisches Pferd oder Spyware bezeichnet.

7.2.3 Bedrohung durch soziale Manipulation (Social Engineering Threats)

Bei dieser Bedrohungsart wird versucht, Nutzer:innen durch manipulative Informationen zu Fehlern zu verleiten oder unaufmerksam werden zu lassen. Derartige Angriffe mittels E-Mails kennen die meisten Nutzer:innen, weil sie diesen, je nach Sicherheitsstandard im eigenen Unternehmen oder

auch im privaten Bereich[20] regelmäßig ausgesetzt sind. Die Angriffe setzen auf das Unwissen oder die Neugier der Nutzer:innen, indem diesen vermeintlich wichtige Information angeboten wird („Ihr Paket konnte nicht zugestellt werden“) oder mit persönlichen Nachteilen gedroht wird („Ihr Konto wird gesperrt, wenn Sie nicht…“). Nutzer:innen werden aufgefordert, einen E-Mailanhang (mit Schadsoftware) zu öffnen oder auf einen (mit Schadsoftware unterlegten) Link im Internet zu klicken.

Ein in diesem Zusammenhang immer wieder verwendeter Begriff ist Phishing (password fishing = „Passwort angeln“). Gelangen auf diese Weise die eigenen Zugangsdaten in fremde Hände, können sich Cyberkriminelle Zugang zu betrieblichen IT-Systemen verschaffen.

7.2.4 Bedrohung für Daten (Threats against data)

Diese Bedrohungskategorie beschreibt die Verletzung des Datenschutzes oder den Verlust von personenbezogenen und nicht personenbezogenen Daten an unberechtigte Personen. Die Verletzung von Persönlichkeitsrechten/Betriebsgeheimnissen, der Verlust von Daten oder die Kenntnisnahme von Informationen durch nicht berechtigte Personen können das Resultat eines Cyberangriffes sein, eines internen Datenlecks oder aus einer unabsichtlichen Handlung resultieren.

7.2.5 Bedrohung für Verfügbarkeit und Integrität (Threats against availability: Denial of Service and Internet threats)

Viele Informationen und Dienstleistungen werden heute über das Internet angeboten. Ein weiteres Bedrohungsszenario ist daher, die Verfügbarkeit der angebotenen Informationen oder Dienstleistungen (beispielsweise eine online-Bestellmöglichkeit von Waren) durch die Überlastung dieser Systeme zu beeinträchtigen. Das zeitgleiche und massenhafte Zugreifen auf bestimmte Internetressourcen - dies kann der Aufruf einer Informationsseite einer Behörde oder eines Unternehmens im Internet sein - wird als DoS oder DDoS-Attacken (Distributed Denial of Service) bezeichnet. Die Infrastruktur des angegriffenen Unternehmens wird dadurch so stark überlastet oder sogar komplett lahmgelegt, sodass es seinen Geschäften, für die diese Infrastruktur benötigt wird, nicht mehr nachgehen kann.

7.2.6 Fehl-/Falschinformation (Desinformation)

Eine von ENISA neu bewertete und deutlich anwachsende Bedrohung liegt in der Desinformation und Fehlinformation von Betroffenen (verstärkt aufgetreten in der COVID-19-Pandemie). Ziel ist es, Nutzer:innen durch falsche Information (umgangssprachlich „Fake-News“) zu verunsichern oder zu unüberlegten Handlungen zu motivieren (Öffnen von E-Mailanhängen oder Surfen auf Webseiten

[20] Siehe beispielsweise https://www.watchlist-internet.at/. Die Watchlist Internet ist eine unabhängige Informationsplattform zum Thema Internetbetrug und informiert Privatpersonen und Unternehmen zu aktuellen Betrugsfällen im Internet. Darüber hinaus werden Tipps gegeben, um sich vor Internetbetrug zu schützen.

mit Schadsoftware). Aber auch das bewusste Verbreiten von Falschinformationen über Unternehmen kann diesen massiven Schaden zufügen.

7.2.7 Angriffe auf Lieferketten (Supply-chain attacks)

In einer vernetzten Wirtschaft mit vielfältigen Geschäftsbeziehungen, die primär technikunterstützt erfolgen, muss jedes Teil einer Lieferkette, somit jede:r Partner:in einer Geschäftsbeziehung, IT- und datensicher operieren können. Erfolgreiche und nicht erkannte Angriffe auf ein Unternehmen einer Lieferkette (oft das am wenigsten geschützte und somit schwächste Teil) können Angreifer in die Lage versetzen, unentdeckt auch andere Unternehmen dieser Geschäftsbeziehung und somit den gesamten Geschäftsprozess zu gefährden.

Angreifer nutzen oft eine Kombination der oben beschriebenen Bedrohungsszenarien. In diesem Zusammenhang wird dann von „Angriffsvektoren“ (attack vector) gesprochen. Ein Angriffsvektor beschreibt den Angriffsweg (über die technische Infrastruktur oder Nutzer:innen) in Verbindung mit der dabei verwendeten Angriffstechnik.

Mitunter betreiben Angreifer einen hohen Aufwand, um zielgerichtet die Infrastruktur eines Unternehmens oder einer Behörde zu schädigen. Mit hohem personellem Aufwand und umfangreichem Fachwissen wird versucht, in die Systeme einzudringen und Angreifer halten sich dann mitunter über Wochen und Monate versteckt in diesen Systemen auf, um betriebliche Abläufe und Zuständigkeiten für konkrete Erpressungsversuche besser kennen zu lernen. In diesem Zusammenhang spricht man von fortgeschrittenen andauernden Bedrohungen oder Advanced Persistent Threats (APT).

Neben den bewussten Angriffen auf Daten und Infrastruktur von Unternehmen, gibt es eine Vielzahl an weiteren Bedrohungen, die durch fahrlässiges Verhalten von Nutzer:innen (menschliches Versagen), fehlerhaftete Systemkonfigurationen (der Zugriff auf vertrauliche Informationen wird nicht eingeschränkt), Softwaremängel oder physische Katastrophen (Feuer, Zerstörung von Netzwerkkabeln) und schädliche Umwelteinflüsse entstehen.

7.3 Fragen an Arbeitgeber:in/Dienstgeber:in

- Mit welchen Bedrohungen war das Unternehmen im letzten Jahr konfrontiert?
- Wie werden die festgestellten Angriffe analysiert?
- Wer ist für die Analyse der festgestellten Angriffen zuständig?
- Welche Konsequenzen wurden daraus abgeleitet?

7.4 Weiterführende Informationen

Bericht Cybersicherheit für das Jahr 2021, Bundeskanzleramt
https://www.bundeskanzleramt.gv.at/dam/jcr:925d0221-a59a-4ca8-99c2-c805f8985fb7/bericht_cybersicherheit_2021.pdf

ENISA Threat Landscape (Bedrohungslandkarte) 2022
https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

8 IT- UND DATENSICHERHEIT DURCH EIN INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM

8.1 Das Wichtigste in Kürze

Um den betrieblichen Schutz von Daten und Informationen und den sicheren Betrieb der technischen Systeme zu gewährleisten, werden in der Praxis unterschiedliche Begriffe verwendet: Informationssicherheit, Datensicherheit oder auch Cyber-Security. Allen Maßnahmen gemein sind die technischen und organisatorischen Bestrebungen der Unternehmen

- IT-Systeme sicher zu betreiben und zu nutzen,
- Informationen nur berechtigten Personen und Stellen zur Verfügung zu stellen,
- die technische Infrastruktur vor Angriffen zu schützen beziehungsweise Angriffe zu vermeiden, sowie
- erfolgreiche Angriffe oder Systemfehler möglichst frühzeitig zu erkennen und unmittelbar darauf reagieren zu können.

Oft münden diese betrieblichen Anstrengungen in der Definition einer Reihe von Maßnahmen, welche in der Folge durch ein Informationssicherheitsmanagementsystem (ISMS) umgesetzt werden. Diese Maßnahmen sind regelmäßig zu prüfen, da die Gewährleistung von IT- und Datensicherheit eine fortlaufende Aufgabe darstellt.

8.2 Zum Thema

Die Digitalisierung hat zu einer vermehrten Nutzung technischer Systeme in den Unternehmen und über Unternehmensgrenzen hinweg geführt. Um Informationssysteme sicher zu betreiben, die Informationsverarbeitungen im Einklang mit rechtlichen Erfordernissen und betrieblichen Notwendigkeiten zu gestalten sowie um die Infrastruktur vor Angriffen zu schützen, sind umfangreiche Aktivitäten erforderlich. Diese Aktivitäten beschränken sich schon lange nicht mehr auf rein technische Schutzmechanismen wie eine Firewall (siehe auch Kapitel 9), es benötigt heute vielmehr eines umfassenden organisatorischen Ansatzes, welcher die an der Informationsverarbeitung beteiligten Personen, Geräte (devices), technischen Systeme und Komponenten gemeinsam berücksichtigt.

Einen derartigen umfassenden Ansatz fordert unter anderem auch die Datenschutz-Grundverordnung im Artikel 32 *Sicherheit der Verarbeitung* (siehe Kapitel 4). Um in diesem Zusammenhang alle Aufgaben planen, steuern und anpassen zu können, sind unterschiedlichste Überlegungen und die Klärung von Zuständigkeiten notwendig. Betriebliche Überlegungen, Strategien und Zuständigkeiten sowie die daraus abgeleiteten Regeln und Verfahren finden sich in der Folge in einem sogenannten Informationssicherheitsmanagementsystem (ISMS). Wie dieses

gestaltet werden kann, was dabei zu berücksichtigen ist und weitere wertvolle Tipps zur Umsetzung liefert das *Österreichische Informationssicherheitshandbuch*[21] (siehe auch Kap 6).

8.2.1 Informationssicherheitsmanagementsystem (ISMS)

Informationssicherheitsmanagement ist ein fortlaufender Prozess, dessen Strategien und Konzepte – so führt es das *Österreichische Informationssicherheitshandbuch* aus – ständig auf ihre Leistungsfähigkeit und Wirksamkeit zu überprüfen und bei Bedarf anzupassen sind.

Zentrale Aktivitäten im Rahmen des ISMS sind:

- die Entwicklung einer organisationsweiten Informationssicherheitspolitik
- die Durchführung einer Risikoanalyse (dies fordert auch die DSGVO bei der Verarbeitung personenbezogener Daten)
- die Erstellung eines Sicherheitskonzeptes
- die Umsetzung der Sicherheitsmaßnahmen
- die Gewährleistung der Informationssicherheit im laufenden Betrieb sowie
- die kontinuierliche Überwachung und Verbesserung des ISMS

In Normen, in behördlichen Vorgaben oder in der Literatur zum Thema IT-Sicherheit wird immer wieder auf die Bedeutung eines betrieblichen Informationssicherheitsmanagementsystems (ISMS) verwiesen. Dabei handelt es sich jedoch nicht um ein einmalig zu erstellendes Konzept, sondern um die Gestaltung von technischen und organisatorischen Maßnahmen, die in einem kontinuierlichen operativen Prozess regelmäßig auf sich ändernde Rahmenbedingungen und Bedrohungslagen (siehe Kapitel 7) überprüft werden. In der Literatur wird dieser fortlaufende Prozess mit dem PDCA-Zyklus (Plan-Do-Check-Act = Planen-Durchführen-Prüfen-Handeln) beschrieben, der nicht nur im Bereich der IT- und Datensicherheit Anwendung findet.

Im *Österreichischen Informationssicherheitshandbuch* wird dieser PDCA-Zyklus wie folgt dargestellt:

- Planen (Plan): Festlegen des ISMS durch die Ermittlung von relevanten Sicherheitszielen und -strategien, Erstellung einer organisationsspezifischen Informationssicherheitspolitik sowie Auswahl spezifisch geeigneter Sicherheitsmaßnahmen.
- Durchführen (Do): Umsetzen der in Schritt 1 geplanten Aktivitäten und Betreiben des ISMS. Dies beinhaltet die geplanten Sicherheitsmaßnahmen durchzuführen, für ihre

[21] https://www.sicherheitshandbuch.gv.at/

Einhaltung zu sorgen sowie Informationssicherheit im laufenden Betrieb und bei Notfällen zu gewährleisten.

- Prüfen (Check): Überwachung und Überprüfung des ISMS auf seine Wirksamkeit. Es werden das Vorhandensein, die Sinnhaftigkeit und die Einhaltung der getroffenen Sicherheitsmaßnahmen überprüft. Ziel ist aber auch, eingetretene Vorfälle und Bedrohungen zu erkennen sowie Know-how über Good-Practice-Beispiele zu erlangen.
- Handeln (Act): Instandhaltung und Verbesserung des ISMS. Auf erkannte Fehler, Schwachstellen und veränderte Umfeldbedingungen reagieren und die Ursachen erkannter Gefährdungen beseitigen.
  Dies führt zu einem erneuten Planen, womit sich der Kreislauf schließt.

Da durch die getroffenen Maßnahmen auch immer wieder Beschäftigte in ihrer täglichen Arbeit betroffen sind (beispielsweise durch die betriebliche Verpflichtung, Regeln für den Umgang mit Daten oder Systemen einzuhalten) und aus Sicherheitsgründen Aktivitäten von Nutzer:innen protokolliert werden müssen, stellt sich die Frage, inwieweit die betriebliche Interessenvertretung in diese Prozesse einzubeziehen ist.

Einen klaren Hinweis auf die Notwendigkeit, Betriebsrat oder Personalvertretung einzubinden, liefert wiederum das *Österreichische Informationssicherheitshandbuch*, das bei der Zusammensetzung eines Informationssicherheits-Management-Teams[22] die Teilnahme folgender betrieblicher Bereiche – je nach Größe und Art der Organisation – vorschlägt:

- Informationssicherheit
- Fachabteilungen
- Haustechnik
- Revision
- IT, Datenschutz
- Personal
- **Betriebsrat**
- Finanz/Controlling
- Recht

[22] Österreichische Informationssicherheitshandbuch, Version 4.3.1 vom 02.02.2022 , Kapitel 3.2 Ressourcenmanagement, Seite 94

8.2.2 Rollen in der IT- und Datensicherheit

Im *Österreichischen Informationssicherheitshandbuch* wird auf die unterschiedlichen betrieblichen Fachbereiche hingewiesen, die bei der Ausgestaltung betrieblicher Regelungen zur IT- und Datensicherheit mitwirken sollen.

Da die Herausforderungen in der IT- und Datensicherheit in den letzten Jahren massiv gestiegen sind, haben sich auch spezialisierte Funktionen und Rollen herausgebildet, die vor allem in Großbetrieben eingerichtet werden.

Die wohl bekannteste Funktion ist die des sogenannten Chief Information Security Officer (CISO), der/die die Gesamtverantwortung für die IT- und Datensicherheit innehat. Diese:r wird durch ein aus Fachkräften zusammengesetztes Security Operations Center (SOC) unterstützt.

Um der dabei notwendigen Aufgabenteilung und Rollentrennung zu entsprechen und Unternehmen bei der Entwicklung der benötigten Sicherheitskenntnisse zu unterstützen, hat die ENISA, die Agentur der Europäischen Union für Cybersicherheit, 2022 ein Rahmendokument zur näheren Darstellung der verschiedenen Anforderungen erstellt. Dieses „European Cybersecurity Skills Framework“[23] beschreibt die in der folgenden Abbildung dargestellten Rollen.

Abbildung 5: Rollen des European Cybersecurity Skills Framework

Quelle: European Cybersecurity Skills Framework

[23] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

Jede dieser Rollen mit einer eigenen Person zu besetzen wird zwar auf Grund fehlender finanzieller und fachlicher Ressourcen für den Großteil der österreichischen Unternehmen nicht umsetzbar sein, die Unterteilung liefert aber wertvolle Hinweise, welche Rollen und daraus abgeleitete Zuständigkeiten und Aufgaben bei IT- und Datensicherheit berücksichtigt werden müssen.

8.3 Fragen an Arbeitgeber:in/Dienstgeber:in

- Welche organisatorischen Überlegungen und Strategien zu IT- und Datensicherheit sind im Betrieb vorhanden?
- Welche innerbetrieblichen Regeln und Verfahren zu IT- und Datensicherheit gibt es?
- Welche Zuständigkeiten zu IT- und Datensicherheit wurden vergeben?
- Das Österreichische Informationssicherheitshandbuch schlägt vor, den Betriebsrat/die Personalvertretung an der Gestaltung der technischen und organisatorischen Maßnahmen im Rahmen eines Informationssicherheitsmanagementsystem (ISMS) zu beteiligen. Welche Rolle wird dem Betriebsrat/der Personalvertretung im Betrieb zugedacht?
- In welcher Form werden die betrieblich getroffenen Maßnahmen evaluiert und wer ist dafür zuständig?

8.4 Weiterführende Informationen

European Cybersecurity Skills Framework Role Profiles, ENISA, 2022
https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles

9 SICHERHEITSLÖSUNGEN ZUR UNTERSTÜTZUNG DER IT- UND DATENSICHERHEIT

9.1 Das Wichtigste in Kürze

Im Bereich IT- und Datensicherheit werden technische (oft englischsprachige) Begriffe verwendet, die zum einen unterschiedliche Arten von Sicherheitssoftware beschreiben (beispielsweise Firewall), zum anderen Strategien, wie IT- und Datensicherheit verbessert werden kann (derzeit vor allem Zero Trust). Auch wenn diese – sich regelmäßig ändernden – Bezeichnungen auf den ersten Blick für Nicht-Expert:innen abschreckend wirken können, so beschreiben sie doch in der Regel nachvollziehbare Ansätze zur Sicherung der betrieblichen IT-Landschaft. In diesem Kapitel werden die wesentlichen technischen und organisatorischen Maßnahmen, die dabei zugrunde liegenden Strategien sowie die in diesem Zusammenhang verwendeten wichtigsten Begriffe angeführt.

9.2 Zum Thema

Der Bereich der technischen Sicherheitslösungen hat durch die Digitalisierung, die (über)betriebliche Vernetzung der IT-Systeme und Geräte (Maschinen, Kameras), die Nutzung mobiler Geräte (Tablet, Laptop, Smartphone) aber auch durch die Nutzung von Cloud-Dienstleistungen ein vielfältiges Aufgabengebiet erhalten.

Klassische Sicherheitslösungen, wie beispielsweise eine Firewall, bilden heute nur mehr einen kleinen Teil eines gesamtheitlichen Sicherheitskonzeptes. Anbieter von Softwarelösungen übertreffen sich mit technischen Schlagworten wie SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response) oder XDR (Extended Detection and Response), die auf den ersten Blick komplex erscheinen, bei näherer Analyse jedoch einem klaren technischen und organisatorischen Konzept folgen.

9.2.1 Aufgaben der IT- und Datensicherheit

Um IT- und Datensicherheit umfassend und ganzheitlich umsetzen zu können, ist zum einen ein organisatorisches Konzept im Sinne eines Informationssicherheitsmanagementsystems (ISMS) (siehe Kapitel 8) zu entwickeln, zum anderen auf eine geeignete Softwareunterstützung zurückzugreifen. Dabei werden vorerst unterschiedliche Phasen der Prüfung der eigenen betrieblichen Herausforderungen durchlaufen. Diese Phasen werden beispielsweise in dem Leitfaden zur Erfüllung von Anforderungen an die Cybersecurity des US-amerikanischen Normeninstituts NIST (National Institute of Standards and Technology)[24] beschrieben. Der Leitfaden war ursprünglich lediglich für Betreiber kritischer Infrastruktur vorgesehen, wurde aber in den letzten Jahren zu einer Standardempfehlung im Umgang mit Cyberrisiken.

[24] https://www.nist.gov/cyberframework

Entsprechend dem NIST-Leitfaden sind folgende Phasen zu durchlaufen und durch entsprechende technische Sicherheitslösungen zu unterstützen:

- Identifizieren: Kenntnis, Dokumentation und Verwaltung der eigenen IT-Landschaft (siehe dazu Kapitel 3). Dokumentation der für das eigene Unternehmen festgestellten Risiken und der daraus abgeleiteten Prozesse/Strategien, Definition von Rollen/Funktionen für die IT- und Datensicherheit
- Schützen: Setzen von technischen und organisatorischen Maßnahmen zum Schutz der betrieblichen Infrastruktur. Hierunter fallen beispielsweise das Management der Zugriffsberechtigungen, das regelmäßige Training der Nutzer:innen, der Einsatz technischer Sicherheitssoftware sowie die Klassifizierung von Informationen nach unterschiedlichen Schutzstufen und die daraus abgeleiteten Maßnahmen.
- Erkennen: die laufende Überwachung der betrieblichen IT-Infrastruktur, um auffälliges Verhalten (Anomalien) oder konkrete Sicherheitsvorfälle (oft als Event bezeichnet) rasch erkennen zu können
- Reagieren: Werden Sicherheitslücken, konkrete Angriffe oder eine bereits eingetretene Verletzung erkannt, ist unmittelbares Handeln notwendig, um weiteren Schaden abzuwenden. Neben diesen unmittelbaren Aktivitäten bedarf es einer nachträglichen Analyse der Sicherheitsvorfälle und daraus abgeleiteter Maßnahmen, um diese Vorfälle in Zukunft bestmöglich verhindern zu können.
- Wiederherstellen: Da keine technische Sicherheitslösung 100-prozentigen Schutz liefern kann und auch technische und menschliche Fehler nie ausgeschlossen werden können, ist es für Unternehmen notwendig, Sicherheitsmechanismen (beispielsweise ein regelmäßiges Backup) einzurichten, um den ursprünglichen Systemzustand und Datenbestand, der durch einen Fehler oder Angriff beeinträchtigt worden ist, wiederherzustellen oder um die korrekte Nutzung der betroffenen IT-Systeme wieder zu ermöglichen.

Im Zusammenhang mit der Fähigkeit eines Unternehmens auf Cyberrisiken zu reagieren, wird seit einigen Jahren auch der Begriff Resilienz verwendet. Dieser besagt in Bezug auf IT- und Datensicherheit, dass ein Unternehmen auf Grundlage erkannter oder aufgetretener Veränderungen oder Probleme in der Lage ist, darauf angemessen zu reagieren.

9.2.2 Wesentliche Begriffe kurz erklärt

In den beiden folgenden Tabellen werden wesentliche Begriffe aus dem Bereich IT- und Datensicherheit, die gegenwärtig in den Fachmedien oder in der betrieblichen Diskussion von den Sicherheitsverantwortlichen verwendet werden, kurz beschrieben. Diese Begriffe mögen auf den ersten Blick komplex wirken, folgen aber bei näherer Analyse den schon angeführten technischen

und organisatorischen Maßnahmen (TOM) zu IT- und Datensicherheit. In der Regel werden diese Ansätze parallel verfolgt und es kommen in einem Unternehmen verschiedene organisatorische und technische Sicherheitssysteme zu Einsatz.

Weitere Begrifflichkeiten finden sich im Glossar in Kapitel 13.

Tabelle 2: Darstellung wesentlicher Begriffe zu IT- und Datensicherheit

Begriff	Erklärung
DLP - Data Leakage/Loss Prevention (Verhindern von Datenlecks /Datenverlust)	DLP-Systeme verfolgen das Ziel, unerlaubten Datenabfluss zu verhindern. In einem ersten Schritt werden Daten/Informationen aufgrund ihrer Sensibilität nach unterschiedlichen Sicherheitsstufen klassifiziert (eine Möglichkeit der Klassifizierung wäre: öffentlich-intern-vertraulich-streng vertraulich/geheim). In einem nächsten Schritt werden Regeln und Richtlinien („Policies“) für den Umgang mit diesen festgelegt (siehe Abbildung 6). Durch den Einsatz von Sicherheitssoftware wird dann der Datentransfer (Übermittlung von Daten und Dokumenten) überprüft und Abweichungen vom betrieblich gewünschten Standard aufgezeigt (beispielsweise eine versuchte unverschlüsselte Versendung eines Dokuments oder ein versuchter Upload vertraulicher Daten). Dabei kann mittels einer Meldung an eine:n Nutzer:in diese:r darauf hingewiesen werden („Sind Sie sicher, dass Sie diese E-Mail versenden wollen?“) oder es wird der Transfer blockiert (beispielsweise kann ein als geheim klassifiziertes Dokument nicht per E-Mail versendet oder in einer Videositzung präsentiert werden). Parallel dazu werden diese Aktivitäten und die Reaktion der Nutzer:innen protokolliert.
EDR - Endpoint Detection and Response (Endpunkterkennung und -reaktion)	EDR-Systeme überwachen das jeweilige Geräteverhalten und damit auch das Verhalten der Nutzer:innen, die das Gerät verwenden. Algorithmen ermitteln daraus ein „normales Verhalten“ (Muster) und warnen Administrator:innen, sollte ein Gerät oder eine Gruppe von Geräten vom normalen Grundverhalten abweichen.
XDR - Extended Detection and Response (erweitere Erkennung und Reaktion)	XDR-Systeme erfassen und analysieren automatisiert Daten mehrerer Bereiche der betrieblichen IT-Landschaft (E-Mail, Endpunkte, Netzwerk) um Bedrohungen erkennen, untersuchen und angemessen darauf regieren zu können.
IAM - Identity- und Access Management (Identitäts- und Zugriffsverwaltung)	IAM-Systeme dienen zur Verwaltung von digitalen Identitäten (Nutzer:innen, Maschinen, Geräte) und den diesen Identitäten zugewiesenen (Zugriffs)Rechten. In vielen Betrieben (die Microsoft nutzen) erfolgt die Nutzer:innenverwaltung mittels dem sogenannten Active Directory (AD), einer zentralen Zuordnungsliste (vergleichbar mit einem Telefonbuch), in der die Zugriffsberechtigungen von Nutzer:innen auf verschiedene Programme oder Informationen verwaltet werden.

Quelle: FORBA, eigene Darstellung

Abbildung 6: Aufgaben der Data Loss Prevention

Quelle: FORBA, eigene Darstellung

Tabelle 3: Darstellung wesentlicher Begriffe zu IT- und Datensicherheit

Begriff	Erklärung
SIEM - Security Information and Event Management (Sicherheitsinformation und Ereignisverwaltung)	SIEM-Systeme sammeln und analysieren Protokolldaten unterschiedlichster IT-Systeme (Quellen) in einer gesonderten Datenbank- und Systemumgebung. Durch die Zusammenführung von Protokolldaten aus unterschiedlichen (Quell)Systemen ergibt sich ein umfassendes Bild, wie diese IT-Systeme im Unternehmen genutzt werden. Aus der Analyse der dabei gesammelten Informationen können Auffälligkeiten („Events“) erkannt werden, die auf eine Bedrohung schließen lassen.
SOAR - Security Orchestration, Automation and Response (Sicherheits-Orchestrierung[25], Automatisierung und Reaktion)	SOAR-Systeme erweitern den Ansatz der Analyse und des Aufzeigens von aktuellen Bedrohungen. In diesen Systemen werden - abhängig von den erkannten Bedrohungen - automatische Systemreaktionen ohne menschlichen Eingriff (der IT-Fachabteilung) definiert und durchgeführt. Dadurch kann die Reaktionszeit eines Unternehmens auf aktuell erkannte Bedrohungen verkürzt werden.
Zero Trust (Null Vertrauen)	Das Prinzip „Zero Trust“ beruht auf dem organisatorischen Konzept keiner Person, keinem Gerät (PC, Laptop, Tablet, Smartphone) und keiner Anwendung (App, Software) uneingeschränkt zu vertrauen, unabhängig davon, ob es sich um interne oder externe Nutzer:innen, Geräte oder Anwendungen handelt. Das Vertrauen muss jeweils (mit technischer Unterstützung) neu überprüft werden.

Quelle: FORBA, eigene Darstellung

9.2.3 Überblick von Softwarelösungen zu IT- und Datensicherheit

Aufgrund der steigenden Bedrohungslage und immer komplexerer IT-Landschaften ist der Markt an Sicherheitslösungen seit einigen Jahren in stetigem Wandel. Es werden laufend neue Lösungen vorgestellt, innovative junge oder auch bereits etablierte (Nischen)Unternehmen im IT- und Datensicherheitsbereich wurden von größeren Firmen übernommen und Kooperationen zwischen verschiedenen Providern umgesetzt. Viele Produkte zu IT- und Datensicherheit werden heute als Cloud-Lösung (SaaS) angeboten. Cloud-Lösungen haben dabei den Vorteil, dass diese Produkte oder Plattformen laufend von den Betreiber:innen aufgrund veränderter Problemlagen oder neuer Angriffsmuster aktualisiert werden können, ohne dass dazu ein betriebliches Handeln notwendig wäre.

In diesem Feld von organisatorischen und technischen Lösungen den Überblick zu bewahren, fällt nicht nur Personen aus dem Betriebsrat oder der Personalvertretung schwer.

Zwei US-amerikanische Anbieter haben sich daher dieser Aufgabe angenommen und zeigen auf ihren jeweiligen Webseiten zum einen die Vielfältigkeit der angebotenen Sicherheitsprodukte und liefern zum anderen eine anschauliche Darstellung und Unterteilung, für welche Zwecke diese Produkte zur Anwendung kommen. Auf beiden Webseiten kann nach Software- und/oder Herstellername gesucht werden, um erste Ansatzpunkte des geplanten Einsatzgebietes zu erhalten.

Hier finden Interessierte weitere Hinweise und Literatur zur Gestaltung der IT- und Datensicherheit. Die folgenden Tabelle 4 fasst die wichtigsten Unterteilungsmerkmale, nach denen die verschiedenen Softwareanbieter in den Abbildungen 7 und 8 thematisch unterschieden werden, zusammen.

[25] Unter Orchestrierung versteht man bei technischen Systemen die automatisierte Verwaltung und Steuerung von einzelnen Aktivitäten (Diensten). Der Begriff leitet sich aus der Musik (Orchester) ab. Wie in einem Orchester können einzelne Programme/Algorithmen (wie ein/e Musiker:in) gesteuert (dirigiert) werden.

Tabelle 4: Unterteilung der Anbieter nach Art der Produkte und Dienstleistungen

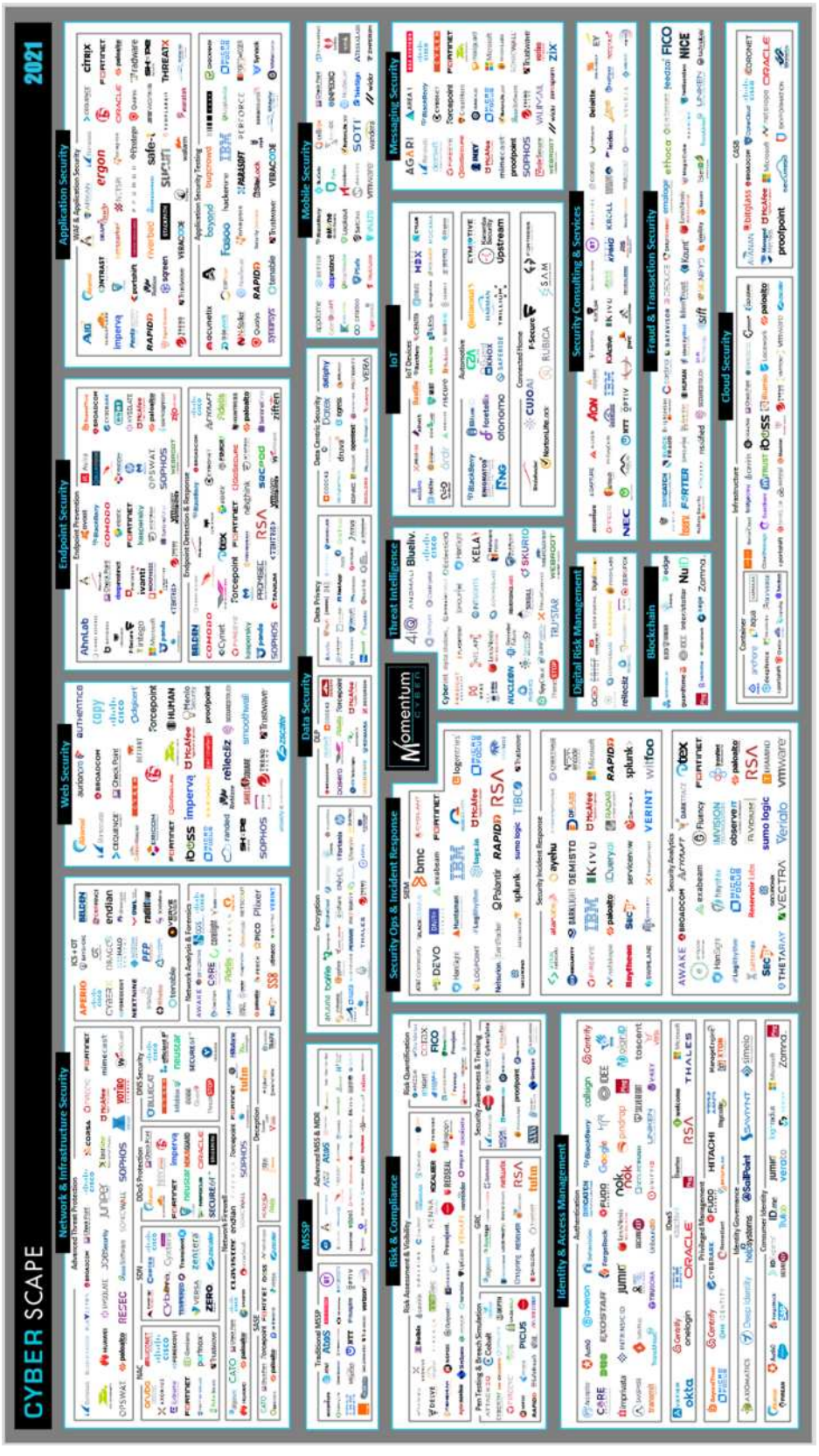
Momentum Cyberscape	Optiv Cybersecurity Technology Map
Application Security	Application Security
Blockchain	
Cloud Security	Cloud (Application) Security
Data Security	Data Protection
Digital Risk Management	
Endpoint Security	Identity Management
Fraud & Transaction Security	
Identity & Access Management	
IoT (Internet of Things)	IoT (Internet of Things)
Messaging Security	
Mobile Security	
MSSP (Managed security service provider)	
Network & Infrastructure Security	Foundational Security
Risk & Compliance	Risk and Compliance
Security Consulting & Services	
Security Ops & Incident Response	Security Operations
Threat Intelligence	
Web Security	

Quelle: FORBA, eigene Darstellung

Abbildung 7: Optiv Cybersecurity Technology Map

Quelle: https://www.optiv.com/sites/default/files/images/Cybersecurity-Technology-Map-Web-min.png

Abbildung 8: CyberScape Übersicht Momentum



Quelle: https://momentumcyber.com/docs/CYBERscape.pdf

Da in der Umsetzung von Maßnahmen zu IT- und Datensicherheit auch personenbezogene Daten der Beschäftigten verarbeitet werden, ist neben der datenschutzrechtlichen Prüfung und Dokumentation auch eine arbeitsrechtliche Regelung, wie etwa durch Betriebsvereinbarung (siehe Kapitel 11 und 12), notwendig.
Das Arbeitsverfassungsgesetz fordert nach § 91 ArbVG vom Dienstgeber, den Betriebsrat über den geplanten Einsatz von IT-Systemen, die Daten von Mitarbeiter:innen verarbeiten, deren Anwendungsgebiet und die geplante Datenverarbeitung zu informieren. Betriebsräte haben darüber hinaus das Recht, weitere Informationen (technische Handbücher, Systemdokumentationen) anzufordern.

9.3 Fragen an Arbeitgeber:in/Dienstgeber:in

- Welche technischen Sicherheitssysteme sind in Anwendung und für welche Zwecke werden diese eingesetzt?
- In welcher Form sind die Sicherheitssysteme nach den Anforderungen des Datenschutzrechts (insbesondere Art 30 DSGVO Verzeichnis der Verarbeitungstätigkeiten) dokumentiert?
- In welchen Sicherheitssystemen werden welche personenbezogenen Daten von Mitarbeiter:innen verarbeitet und wie lange (nicht anonymisiert) aufbewahrt?

9.4 Weiterführende Informationen

Cybersecurity Framework, NIST (US National Institute of Standards and Technology)
https://www.nist.gov/cyberframework

10 ÜBERWACHUNG UND IT- UND DATENSICHERHEIT IM HOME-OFFICE

10.1 Das Wichtigste in Kürze

Bedingt durch die COVID-19-Pandemie wurden viele Mitarbeiter:innen, soweit es deren Tätigkeit zuließ, verpflichtet, im Home-Office zu arbeiten. Überwiegend musste dieser Schritt ohne große Vorbereitungszeit durchgeführt werden und entsprechende gesetzliche Bestimmungen zum Home-Office wurden erst Monate danach beschlossen. Das Thema Datenschutz und Datensicherheit fand in den geänderten gesetzlichen Bestimmungen zum Home-Office keine Berücksichtigung beziehungsweise wurde auf bereits bestehende Regelungen aus dem Datenschutzrecht verwiesen. Unternehmen versuchten darüber hinaus, über interne Richtlinien Verhaltensregeln für das Arbeiten im Home-Office zu definieren. Diese blieben jedoch in der Regel sehr vage. Beschäftigte im Home-Office wurden lediglich sehr allgemein zu IT- und Datensicherheit verpflichtet, wie auch entsprechende Formulierungen einzelner Muster-Betriebsvereinbarungen unterstreichen. In dieser unsicheren Lage stieg – neben der Suche nach geeigneten Videokonferenzsystemen – die Nachfrage nach Systemen zu IT- und Datensicherheit (siehe Kapitel 9) und vereinzelt auch nach Kontrollsoftware für die im Home-Office Beschäftigten.

10.2 Zum Thema

Die Nutzung von betrieblichen IT-Systemen, aber auch die Nutzung privater Infrastruktur im Home-Office ("Bring your own Device") stellten während der COVID-19-Pandemie Unternehmen im Bereich der IT- und Datensicherheit vor neue Herausforderungen. Es zeigte sich, dass Beschäftigte im Home-Office zu einem neuen Angriffsziel für Cyberkriminelle wurden und dass betriebliche Sicherheitslösungen – insbesondere bei Nutzung privater Geräte – nur teilweise eingesetzt werden konnten. Aber auch der Kontakt zu Mitarbeiter:innen und Kolleg:innen oder in die IT-Abteilung wurde durch den Verlust der betrieblichen Anwesenheit erschwert. Aufgrund dieser unsicheren Lage investierten viele Unternehmen in neue IT-Sicherheitslösungen. Parallel dazu nutzten die Anbieter von Sicherheitslösungen diese Situation, um auf die wachsenden Gefahren aufgrund mobiler Arbeit und Home-Office und ihre dabei unterstützenden Produkte hinzuweisen.

Neben der Klärung von sicherheitstechnischen Fragen wurde auch der Wunsch von Arbeitgeber:innen größer, Beschäftigte aufgrund vermuteter nachlassender Produktivität im Home-Office zu kontrollieren und in hohem Umfang zu überwachen

Den gesteigerten Wunsch nach Kontrollsoftware zeigt eine von Top10VPN.com im Juni 2020 erstmals veröffentlichte (und im August 2022 aktualisierte) Studie[26], in der Suchanfragen im Internet analysiert und Nachfragen nach spezifischer Kontrollsoftware dokumentiert wurden. Die Nachfrage nach Mitarbeiterüberwachungssoftware nahm demnach deutlich zu. Für Österreich

[26] https://www.top10vpn.com/research/covid-employee-surveillance/

liegen zwar keine gesondert ausgewiesenen Daten vor, aber der Trend, Mitarbeiter:innen im Home-Office einer zusätzlichen Kontrolle zu unterziehen, dürfte sich auch in österreichischen Unternehmen widerspiegeln.

Zusätzlich zur datenschutzrechtlichen Frage, welche technisch-organisatorischen Maßnahmen im Home-Office sinnvoll und rechtskonform erscheinen, sind auch die arbeitsrechtlichen Fragen zu klären, inwieweit eine Kontrolle der im Home-Office Beschäftigten durch den/die Arbeitgeber:in gerechtfertigt ist und ob Beschäftigte im Home-Office anderen Regeln unterliegen als Beschäftigte am betrieblichen Arbeitsplatz[27]. Ein weiteres Thema ist, wie diese Kontrollansätze in Betrieben mit Betriebsrat vereinbart werden (zum Einsatz von Systemen zu IT- und Datensicherheit findet sich ein Betriebsvereinbarungsmuster in Kapitel 12).

10.2.1 Software zur Überwachung von Mitarbeiter:innen im Home-Office

Die oben und in Fußnote 26 erwähnte Studie von Top10VPN stellte - neben der Analyse der gestiegenen Nachfrage nach Softwareprodukten zur Kontrolle von Mitarbeiter:innen im Home-Office - auch Produkte („Top10“) vor, die besonders häufig nachgefragt werden und beschreibt, welche Funktionalitäten („Employee Surveillance Software Features“) diese anbieten. Bei einer ersten Analyse dieser Produkte zeigt sich, dass diese neben Ansätzen zur Verbesserung der IT- und Datensicherheit auch Funktionen enthalten, die rein zur Überwachung von Mitarbeiter:innen dienen und in der Regel weder datenschutzrechtlich noch arbeitsrechtlich angemessen erscheinen.

Betont werden muss in diesem Zusammenhang jedoch, dass eine genaue Einschätzung nur jeweils nach einer eingehenden Analyse der technischen Dokumentation und der im betroffenen Unternehmen definierten Bestimmungen gegeben werden kann. Betriebsräten steht eine Einsicht in die technische Dokumentation nach § 91 Abs 2 ArbVG zu.

In folgender Tabelle werden einige Funktionalitäten der „Top10“ Produkte angeführt und eine erste grobe Einschätzung aus datenschutzrechtlicher und arbeitsrechtlicher Sicht gegeben: „ok“ steht dabei für Funktionalitäten, die unter Einhaltung der rechtlichen Bestimmungen vertretbar sein können und „!!“ für Maßnahmen, die offensichtlich datenschutzrechtlichen und/oder arbeitsrechtlichen Bestimmungen entgegenstehen. Eine genauere betriebliche Analyse der eingesetzten Softwareprodukte, deren datenschutzkonforme Umsetzung und arbeitsrechtliche Regelung durch Betriebsvereinbarung ist daher unumgänglich.

[27] Siehe dazu Goricnik: Wider das „Trojanische Pferd“ Home-Office im Dauerrecht (https://www.drda.at/a/393_INFAS_41/Wider-das-Trojanische-Pferd-Home-Office-im-Dauerrecht)

Tabelle 5: Funktionalitäten von Software zur Überwachung von Mitarbeiter:innen

Funktionalität (nach Top10VPN.com)	Datenschutz-rechtliche Einschätzung[a)]	Arbeits-rechtliche Einschätzung[b)]
Software Monitoring (Überwachung des Verhaltens der verwendeten Software)	ok	ok[d)]
Remote Control Takeover (Übernahme durch Fernsteuerung)	ok[c)]	ok[c)]
Keystroke Logging (Protokollierung der Tastenanschläge)	!!	!!
Screen Monitoring (Bildschirmüberwachung)	!!	!!
Internet Monitoring/Filtering (Überwachung Internetnutzung, Filtern/Blockieren unerwünschter Seiten)	ok	ok[d)]
Call Tapping (Abhören von Telefonaten)	!!	!!
Location Tracking (Verfolgung des Standortes)	ok[d)]	ok[d)]
Webcam Surveillance (Überwachung durch Webcam)	!!	!!
Audio Recording (Audioaufnahme)	!!	!!
Email Monitoring (E-Mail-Überwachung)	ok[d)]	ok[b)]
IM Monitoring (Instant Messaging Überwachung)	!!	!!
Mobile Device Access (Kontrolle des Zugriff auf mobile Geräte)	ok	ok[d)]
User Action Alerts (Alarmmeldungen bei systemkritischen Aktivitäten von Nutzer:innen)	ok[d)]	ok[d)]
Time-Tracking (Zeitaufzeichnung)	ok[d)]	ok[b)]

a) Unter der Voraussetzung, dass die datenschutzrechtlichen Anforderungen (Rechenschaftspflicht nach Art 5 DSGVO, Transparenz, Technisch-organisatorische Maßnahmen und hinreichende Vorab-Information) bereits erfüllt sind.
b) Sofern diese IT-Systeme unter Berücksichtigung von §§ 96 und 96a ArbVG geprüft und soweit zutreffend, durch Betriebsvereinbarung geregelt sind und die Verarbeitung personenbezogener Daten klar definiert ist.
c) Nach Aufforderung und Wissen des/der Nutzer:in zu Zwecken der Fehlerbehebung, Zugriff nur durch autorisierte Mitarbeiter:innen der Fachabteilung
d) Ausschließlich zum Zweck der IT- und Datensicherheit für vorab definierte Zwecke durch die Fachabteilungen ohne Weitergabe dieser Information

Quelle: https://www.top10vpn.com/research/covid-employee-surveillance/ ergänzt um eine datenschutz- und arbeitsrechtliche Einschätzung

10.2.2 Technisch-organisatorische Maßnahmen im Home-Office

Unbestritten ist, dass für das vermehrte Arbeiten von Beschäftigten im Home-Office zusätzliche zu den bereits im Betrieb bestehenden Richtlinien weitere datensicherheitsrelevante Maßnahmen zu setzen sind. Eine Vielzahl an Einrichtungen wie etwa die Österreichische Datenschutzbehörde oder das Bundeskanzleramt haben dazu Leitfäden und Checklisten veröffentlicht. Eine Auswahl wird unter 10.4. (Weiterführende Informationen) beschrieben.

Eine Analyse und Zusammenführung der vorgestellten technischen und organisatorischen Maßnahmen dieser verschiedenen Leitfäden zeigen die folgenden Tabellen 6 und 7. Sie fassen die wesentlichen Maßnahmen, getrennt nach technischen und organisatorischen Maßnahmen zusammen, die in den Unternehmen zu **prüfen** und gegebenenfalls zu **adaptieren** sind, sowie in Folge jedenfalls **geschult** (!) und **veröffentlicht** (in Ordnungsvorschriften) beziehungsweise (in Betriebsvereinbarungen) **geregelt** werden sollten. Es empfiehlt sich auch bereits im Betrieb bestehende Richtlinien und Maßnahmen mittels der untenstehenden Tabellen zu prüfen.

Tabelle 6: Technische Maßnahmen im Home-Office (Zusammenfassung)

Technische Maßnahmen im Home-Office	
Software	– Verschlüsselung von Daten/Inhalten am Endgerät und auf Datenträger
	– regelmäßiges Update der eingesetzten Software/Apps
	– ausschließlicher Einsatz von geprüfter Software
	– keine Verwendung privater Software auf dienstlichen Geräten
	– verschlüsselte/VPN/sichere Verbindung zur Datenübertragung
Daten-übertragung	– Verschlüsselter Transport von Daten
	– Sicherstellung einer stabilen Verbindung mit ausreichender Bandbreite
	– Absicherung der privaten Infrastruktur (WLAN)
Sicherheit	– Verwaltung der eingesetzten Geräte (mobile Device Management) auch im Home-Office
	– Multi-Faktor-Authentifizierung (MFA)
	– Verwendung von starken Passwörtern
	– kein ungesichertes Speichern, Dokumentieren, Aufbewahren von Passwörtern (beispielsweise Verwendung von Passwortsafes)
	– Regelmäßiges Prüfen der Sicherheitsinfrastruktur
	– Verschlüsselung der E-Mail-Kommunikation
	– Kontrolle des Verhaltens von Nutzer:innen ausschließlich auf Basis von IT- und Datensicherheit und nicht zur Überwachung des Verhaltens oder der Leistung!

Quelle: FORBA, eigene Darstellung

Tabelle 7: Organisatorische Maßnahmen im Home-Office (Zusammenfassung)

Organisatorische Maßnahmen im Home-Office	
Hardware	– geschützter Transport der Arbeitsmittel zwischen Office und Home-Office
	– Verbot von USB-Sticks oder nur Verwendung verschlüsselter USB-Sticks
Arbeitsplatz	– geschützte Aufbewahrung der Arbeitsmittel (Laptop, Datenträger, Smartphone, Dokumente)
	– keine Einsicht in und kein Zugriff auf Geräte oder Daten/Informationen durch Dritte (Bildschirmsperre)
	– kein Mithören durch Dritte (Achtung bei Verwendung von digitalen Assistenten wie Alexa)
	– Clear-Desk-Policy: sichere Verwahrung der Arbeitsmittel außerhalb der Arbeitszeit
Umgang mit Daten und Information	– nur unbedingt notwendige Papierausdrucke im Home-Office verwenden
	– Sichere Vernichtung von Papierdokumenten im Home-Office
	– Trennung von beruflichen und privaten Daten
	– Klassifikation von Information und Daten nach Sicherheitsstufen (eine Möglichkeit der Klassifizierung wäre: öffentlich-intern-vertraulich-streng vertraulich/geheim)
	– regelmäßiges Sichern der Daten
	– Definition von Löschregeln
interne Richtlinien/ Policy	– Erstellung und regelmäßige Überprüfung der internen Richtlinien oder Policy zur Abbildung der technischen und organisatorischen Maßnahmen (TOM)
	– Entwicklung eines ISMS (Informationssicherheitsmanagementsystem)
	– Regelungen zum Umgang mit Messengern in Videokonferenzen
	– Verhaltensregeln für Videokonferenzen (beispielsweise welche Informationen dürfen mit Externen geteilt werden)
	– kritische Prüfung bei E-Mails mit Anhängen und Links
	– Schulung der Mitarbeiter:innen, Sensibilisierung zu IT- und Datensicherheit
	– Abschluss von Betriebsvereinbarungen zur Verarbeitung personenbezogener Daten von Mitarbeiter:innen im Bereich IT- und Datensicherheit
Zuständige Stellen	– Definition und Veröffentlichung von Ansprechpersonen in der IT-Abteilung für Fragen von Nutzer:innen
	– Definition und Veröffentlichung von Notfallkontakten (Telefon) und -adressen (E-Mail)
	– Definition klarer Abläufe bei auftretenden Problemen

Quelle: FORBA, eigene Darstellung

10.3 Fragen an Arbeitgeber:in/Dienstgeber:in

- Welche Regelungen zu Fragen der IT- und Datensicherheit im Home-Office bestehen?
- Wer erarbeitet diese Regelungen und auf Basis welcher Hintergrundinformationen?
- In welchem Rahmen werden die gesetzten Maßnahmen evaluiert?
- Welches Verhalten von Mitarbeiter:innen soll im Home-Office (im Gegensatz zum betrieblichen Arbeitsplatz) zusätzlich kontrolliert und/oder dokumentiert werden?
- Werden die Mitarbeiter:innen ausreichend und vorab über die Maßnahmen darüber informiert ?
- Welche Schulungen oder Informationen werden für Mitarbeiter:innen angeboten?

10.4 Weiterführende Informationen

Informationsblatt der Österreichischen Datenschutzbehörde, Datensicherheit und Home-Office https://www.dsb.gv.at/dam/jcr:d19d7890-4ba1-46f1-8ab3-767ee1514825/Informationsblatt_der_Datenschutzbehoerde_Datensicherheit_und_Home-Office.pdf

Cyber-Sicherheit im Home Office. Grundlegende Handlungsempfehlungen für Mitarbeiterinnen und Mitarbeiter mit Telearbeitsplätzen, Bundesministerium für Inneres https://dsn.gv.at/501/files/Cyber_Ratgeber/Schriftenreihe_Cybersicherheit_Cyber-Sicherheit_im_Home_Office_Februar_2022_20220216.pdf

Österreichisches Sicherheitshandbuch: Checkliste – Sicherheit im Home-Office. Die wichtigsten Aspekte zur IT-Sicherheit am Remote-Arbeitsplatz https://sicherheitshandbuch.gv.at/downloads/Home-Office-Checkliste.pdf

IT-Sicherheit im Home-Office, deutsches Bundesamt für Sicherheit in der Informationstechnik (BSI) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Umfrage-Home-Office/umfrage_home-office-2020.pdf?__blob=publicationFile&v=3

Top Tips for Cybersecurity when Working Remotely, ENISA (European Union Agency for Cybersecurity) https://www.enisa.europa.eu/news/executive-news/top-tips-for-cybersecurity-when-working-remotely

Tips for cybersecurity when working from home, ENISA (European Union Agency for Cybersecurity) https://www.enisa.europa.eu/tips-for-cybersecurity-when-working-from-home

Telearbeit und Mobiles Arbeiten. Ein Datenschutz-Wegweiser, Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Flyer/Telearbeit.pdf;jsessionid=A13CF0E5E10ED536DDDE2473D2BF2DE7.intranet241?__blob=publicationFile&v=7

Plötzlich im Homeoffice – und nun? Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
https://www.datenschutzzentrum.de/uploads/it/uld-ploetzlich-homeoffice.pdf

Landesbeauftragter für Datenschutz Sachsen-Anhalt, Checkliste Homeoffice
https://datenschutz.sachsen-anhalt.de/fileadmin/Bibliothek/Landesaemter/LfD/PDF/binary/Informationen/Hinweise/Checkliste_Homeoffice.pdf

Bayerisches Landesamt für Datenschutzaufsicht. Datenschutzrechtliche Regelungen bei Homeoffice. Checkliste mit Prüfkriterien nach DS-GVO
https://www.lda.bayern.de/media/checkliste/baylda_checkliste_homeoffice.pdf

Berliner Beauftragte für Datenschutz und Informationsfreiheit: Home-Office
www.datenschutz-berlin.de/themen/arbeit/home-office

Landesbeauftragte für den Datenschutz Niedersachsen: Hilfestellung zum Datenschutz im Homeoffice
https://lfd.niedersachsen.de/download/157542/Datenschutz_im_Homeoffice.pdf

11 IT- UND DATENSICHERHEIT UND MITBESTIMMUNG

11.1 Das Wichtigste in Kürze

Arbeitgeber:innen müssen in ihrer datenschutzrechtlichen Verantwortung technische und organisatorische Maßnahmen zur IT- und Datensicherheit ergreifen. Da dabei jedoch in der Regel auch personenbezogene Daten der Mitarbeiter:innen verarbeitet werden, sind auch die weiteren Anforderungen des Datenschutzrechts zum Schutz von personenbezogene Daten der Mitarbeiter:innen einzuhalten.

Darüber hinaus sind die Bestimmungen der Arbeitsverfassung, insbesondere die Betriebsvereinbarungstatbestände der §§ 96, 96a und 97 ArbVG zu prüfen und umzusetzen.

Zu diesem Zwecke ist der Betriebsrat nach den Bestimmungen des § 91 ArbVG verpflichtend vom/von der Arbeitgeber:in bzw. Dienstgeber:in über die geplante (auch nur beiläufige) Verarbeitung von Daten von Mitarbeiter:innen zu informieren.

11.2 Zum Thema

Die Sicherstellung von IT- und Datensicherheit ist eine wichtige betriebliche Herausforderung in der betrieblichen Informationsverarbeitung. Dies fordert auch die Datenschutz-Grundverordnung in Artikel 5 DSGVO, in dem die Grundsätze für die Verarbeitung von der personenbezogenen Daten angeführt werden. Personenbezogene Daten müssen nach Art 5 Abs 1 lit f DSGVO "*in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ('Integrität und Vertraulichkeit')*". Konkreter werden die Anforderung an die Sicherheit der Verarbeitung noch in Art 32 DSGVO (siehe Kap 4) ausgeführt.

In diesem Zusammenhang darf jedoch nicht außer Acht gelassen werden, dass bei der Verarbeitung von personenbezogenen Daten neben deren sicherer Verarbeitung noch weitere datenschutzrechtliche Aufgaben von Arbeitgeber:innen, in ihrer Rolle als Verantwortliche, zu erfüllen sind.

Zu diesen Aufgaben zählen vor allem

- Die Einhaltung der **Grundsätze der Datenverarbeitung nach Art 5 DSGVO**. So sind unter anderem die Rechtmäßigkeit der Verarbeitung oder die Zweckbindung zu prüfen. Zweckbindung bedeutet, dass die Verarbeitung für genau festgelegte, eindeutige und legitime Zwecke erfolgen muss. Darüber hinaus müssen die Verarbeitung auf das notwendige Maß beschränkt werden und die (je nach Zweck) erforderliche

Speicherdauer festgeschrieben werden. Die Einhaltung dieser Grundsätze muss begründet werden und nachweisbar sein („Rechenschaftspflicht“).

- Die **Betroffenen sind umfassend über die Datenverarbeitung zu informieren** und auf ihre **Rechte** hinzuweisen.
- Die geplanten Verarbeitungen sind in einem Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren. Der Umfang der Dokumentationspflicht ist in Art 30 DSGVO nachzulesen.
- Bei Verarbeitungen mit einem hohen Risiko für die Betroffenen ist vor der eigentlichen Verarbeitung eine **Datenschutz-Folgenabschätzung** durchzuführen und der Betriebsrat ist als Vertreter der Mitarbeiter:innen (mit einer Möglichkeit der Stellungnahme) einzubinden. Konkrete Anforderungen zu einer Datenschutz-Folgenabschätzung finden sich in Art 35 DSGVO[28].

Wie auch in Kapitel 3.2.5 beschrieben, ist die Definition, was unter personenbezogenen Daten zu verstehen ist, sehr weit zu interpretieren.

Personenbezogene Daten sind nach Art 4 Z 1 DSGVO *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „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.“*

Diese umfassende rechtliche Begriffsdefinition bedeutet, dass nicht unbedingt ein direkter Personenbezug über Personalnummer oder Name vorliegen muss, sondern der Personenbezug auch aus der Verknüpfung mehrerer Daten abgeleitet werden könnte.

Eine mögliche Unterteilung von personenbezogenen und -beziehbaren Daten könnte wie in Tabelle 8 dargestellt, aussehen.

[28] Zusätzlich zu den Bestimmungen in der Datenschutz-Grundverordnung sind die beiden österreichischen Verordnungen, die *Datenschutz-Folgenabschätzung-Ausnahmenverordnung* (DSFA-AV) und die *Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist* (DSFA-V), zu beachten. Siehe dazu https://www.dsb.gv.at/recht-entscheidungen/verordnungen-in-oesterreich.html

Tabelle 8: Unterteilung personenbezogene Datenklassen

Datenklasse	Erklärung und Beispiele
Funktionsdaten	Diese Daten sind zur Berechtigungssteuerung in den IT-Systemen notwendig Beispiele: Name, ID, Berechtigungsrolle
Stammdaten	Diese Daten umfassen die Stamm- und Kommunikationsdaten und die organisatorische Zuordnung somit allgemeine Angaben zur Person. Beispiele: Name, Organisationseinheit, Firmenanschrift, Büroraum, Telefonnummer, E-Mail-Adresse.
Abwicklungsdaten	Diese Daten müssen zur Erfüllung einer rechtlichen Verpflichtung aus dem Gesetz, Normen der kollektiven Rechtsgestaltung oder dem Arbeitsvertrag für einen eindeutigen und berechtigten Zweck verarbeitet werden. Beispiele: Gehalt, Zeitbuchungen
Geschäftsdaten	Diese Daten werden durch die Arbeit mit IT-Systemen erfasst und dokumentieren Tätigkeiten der ArbeitnehmerInnen. Beispiele: Bearbeitungsdauer (Beginn – Ende) eines Auftrages oder eines Telefonats, Anzahl der täglichen Kontierungen
besonders schutzwürdige (sensible) und strafrechtlich relevante Daten	Diese Daten werden nach Art 9 und 10 DSGVO als besonders schutzwürdig eingestuft und dürfen nur für einen eindeutigen und berechtigten Zweck verarbeitet werden. Beispiele: Gewerkschaftszugehörigkeit, biometrische Daten, Gesundheitsdaten
Geo-/Lokationsdaten	Diese Daten erlauben Rückschlüsse auf den Standort einer Person bzw. eines dieser Person überantwortetes Arbeitsmittel (Laptop, Fahrzeug) Beispiele: GPS-Daten eines Fahrzeugs
Audio- und Videodaten	Audio- oder Bilddaten, die eindeutig einer Person zugewiesen werden können. Beispiele: Aufzeichnung eines Videomeetings, Bilder einer Überwachungskamera
Protokolldaten	Diagnostische Daten, Verkehrs- und Telemetriedaten, die im Hintergrund der IT-Systeme anfallen Beispiele: Abschicken eines Druckauftrages, Speicherdatum eines Dokuments
Inhaltsdaten	Daten/Informationen/Dokumente, die durch das individuelle Arbeiten der Arbeitnehmer:innen in den unterschiedlichen Services/Komponenten entstehen und personenbezogene Informationen enthalten können. Beispiele: Inhalt einer E-Mail, eines Chats oder eines Dokuments

Quelle: FORBA, eigene Darstellung

Insbesondere im Bereich der IT- und Datensicherheit, in der das Verhalten der betrieblichen Infrastruktur protokolliert und analysiert wird, ist im Großteil der Anwendungsfälle ein Personenbezug oder eine Personenbeziehbarkeit gegeben. Da nur explizit berechtigte Nutzer:innen die betriebliche Infrastruktur, die verwendeten Applikation und die darin verarbeitete Information verwenden dürfen, ist der Bezug zu einer konkreten Person in der Regel gegeben.

Genauere Informationen zu den datenschutzrechtlichen Bestimmungen finden sich auch in den in Kapitel 2 angeführten Literaturhinweisen.

Neben der Prüfung und Erfüllung der datenschutzrechtlichen Verpflichtungen haben Arbeitgeber:innen auch die im Arbeitsverfassungsgesetz (ArbVG) festgeschriebenen Bestimmungen zu prüfen und einzuhalten. In Betrieben mit Betriebsrat ist dieser nach § 91 ArbVG umfassend über die geplanten Datenverarbeitungen zu informieren, sofern durch diese personenbezogene oder personenbeziehbare Daten der Mitarbeiter:innen verarbeitet werden können. Und dem Betriebsrat ist auf seinen Wunsch die entsprechende technische Dokumentation zur Verfügung zu stellen. In Folge sind die jeweiligen Systeme, die möglichen personenbezogenen Datenverarbeitungen und allfällige Maßnahmen für den sicheren Umgang mit Daten und Dokumenten im Sinne der §§ 96, 96a und 97 ArbVG durch Betriebsvereinbarungen zu regeln[29].

Im nächsten Kapitel 12 findet sich eine Mustervereinbarung, in welcher der generelle Umgang mit Systemen zur Sicherstellung der IT- und Datensicherheit und der Verarbeitung von personenbezogenen Daten von Mitarbeiter:innen beschrieben ist.

11.3 Fragen an Arbeitgeber:in/Dienstgeber:in

- Welche Systeme zur Sicherstellung der IT- und Datensicherheit sollen zum Einsatz kommen?

Je eingesetztem System sind folgende Fragen zu beantworten:

- Wer leitet das konkrete Projekt oder ist für das System zuständig?
- Was ist der jeweilige datenschutzrechtliche Zweck nach Art 5 DSGVO?
- Welche Prüf-, Kontroll- und Analysefunktion hat das jeweilige System?
- Wie lauten die konkrete Bezeichnung und der Anbieter des Systems?
- In welcher Form liegt eine Systemdokumentation vor?
- Wo kommt das System zum Einsatz?
- Sind mobile Geräte (von Mitarbeiter:innen im mobilen Außendienst) und/oder Geräte außerhalb des Unternehmens (von Mitarbeiter:innen im Home-Office) betroffen?

[29] Die Mitwirkungsbefugnisse des Betriebsrates nach dem ArbVG werden beispielsweise im Skriptum „Verarbeitung von personenbezogenen MitarbeiterInnen-Daten“ ab Seite 21 erklärt. Ein freie Download ist unter https://tinyurl.com/k2v69mdf möglich.

- Welche (personenbezogenen oder auch nur personenbeziehbaren) Daten werden im System erfasst?
- Welche Auswertungen sind vorgesehen?
- Wer hat Zugriff auf diese Daten und Auswertungen?
- Welche Daten werden zwischen dem System und anderen Systemen ausgetauscht (Schnittstellen)?
- Welche Daten werden an andere Unternehmensstandorte übermittelt (bzw. wird in einem globalen System gearbeitet)?
- Gibt es externe Auftragsverarbeiter und in welcher Form wurde die Zusammenarbeit mit diesen vertraglich vereinbart?
- Liegt bereits eine datenschutzrechtliche Dokumentation (Verzeichnis von Verarbeitungstätigkeiten nach Art 30 DSGVO) vor?
- Ist die Durchführung einer Datenschutz-Folgeabschätzung (DSFA) geplant (oder ist eine solche gar schon durchgeführt oder aus welchem Grund nicht durchgeführt worden) ?

11.4 Weiterführende Informationen

Datenschutz-Folgenabschätzung-Ausnahmenverordnung (DSFA-AV)
https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_108/BGBLA_2018_II_108.html

Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (DSFA-V)
https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_II_278/BGBLA_2018_II_278.html

12 MUSTER EINER BETRIEBSVEREINBARUNG ZU IT- UND DATENSICHERHEIT

Dieses Betriebsvereinbarungsmuster gibt die allgemeinen (arbeitsverfassungs- und datenschutz-) rechtlichen Bestimmungen und Regelungsbereiche bei der Verarbeitung von personenbezogenen Daten wieder und kann eine rechtliche Beratung im Einzelfall nicht ersetzen.

Unter https://www.forba.at/beratung/it-sicherheit-und-mitbestimmung/ ist das folgende Muster einer Betriebsvereinbarung über den Einsatz von Systemen zur IT- und Datensicherheit und die damit verbundene Verarbeitung personenbezogener Arbeitnehmer:innendaten verfügbar.

Betriebsvereinbarung

über den Einsatz von Systemen zur IT- und Datensicherheit und die damit verbundene Verarbeitung personenbezogener Arbeitnehmer:innendaten

1. Anwendungsbereich

(1) Die Betriebsvereinbarung regelt gemäß §§ 96, 96a und 97 ArbVG die Einführung und Nutzung von Systemen zur IT- und Datensicherheit und die in diesem Zusammenhang stattfindende Verarbeitung personenbezogener Arbeitnehmer:innendaten.

(2) Diese Betriebsvereinbarung gilt für alle Arbeitnehmer:innen iSd § 36 ArbVG der <NAME>.

(3) Alle in dieser Betriebsvereinbarung angeführten Anhänge (Datenblätter, Zusatz-BV) bilden einen integrativen Bestandteil dieser Vereinbarung und werden im Zuge der Erweiterung der Systeme sukzessive ergänzt.

(4) [sofern zutreffend: Bestehende Betriebsvereinbarungen zu verschiedenen bereits im Einsatz befindlichen Systemen zur IT- und Datensicherheit, werden nach beiderseitiger Prüfung der Aktualität durch die Vertragsparteien in die Anlage aufgenommen bzw überarbeitet.]

(5) [sofern zutreffend: Die Regelungen der Rahmen-Betriebsvereinbarung zur personenbezogenen Datenverarbeitung gelten sinngemäß, sofern in dieser Vereinbarung nicht Abweichendes vereinbart wurde.]

2. Zielsetzung

(1) Der/die Arbeitgeber:in ist als datenschutzrechtliche/r Verantwortliche:r verpflichtet, die IT-Infrastruktur gegen Cyber-Angriffe zu schützen. Darüber hinaus sind aufgrund der rechtlichen Bestimmungen der Datenschutz-Grundverordnung (DSGVO) technische und organisatorischen Maßnahmen (TOMs) zur Sicherheit der Verarbeitung zu treffen und betriebliche Daten sowie Betriebs- und Geschäftsgeheimnisse nur vorab definierten Berechtigten zur Verfügung zu stellen.

(2) Die Vertragsparteien sind sich daher einig, dass zum Schutz der lokal oder über Cloudplattformen vom/von der Arbeitgeber:in[30] verarbeiteten (personenbezogenen und nicht-personenbezogenen) Daten und Dokumente des/der Arbeitgeber:in Maßnahmen ergriffen werden müssen. Daher werden zu diesem Zweck technische Systeme zur Gewährleistung der IT- und Datensicherheit sowie zur Netzwerkanalyse eingesetzt, sowie Regelungen für den sorgsamen Umgang mit entsprechenden Daten und Betriebs- und Geschäftsgeheimnissen erlassen. Zugleich besteht Einigkeit, dass die Persönlichkeitsrechte der Arbeitnehmer:innen gewahrt bleiben müssen und die Verarbeitung personenbezogener Daten der Arbeitnehmer:innen nach den Regelungen des Datenschutzrechts und dieser Betriebsvereinbarung zu erfolgen hat.

(3) Die Systeme zur Gewährleistung der IT- und Datensicherheit dienen der IT-Abteilung/Systemadministration zur Prüfung datensicherheitsrelevanter Aspekte und unterstützen die Etablierung eines Informationssicherheitsmanagementsystem (ISMS).

(4) Darüber hinaus sollen Arbeitnehmer:innen in ihrer täglichen Arbeit unterstützt werden, indem mögliche Probleme an betrieblichen Endgeräten (Notebook, PC, Tablet, Smartphones, …) und im betrieblichen Netzwerk frühzeitig erkannt und behoben werden.

3. Definitionen

Die folgenden Definitionen finden in dieser Betriebsvereinbarung Anwendung:

a) Daten werden nach der Daten-Governance Verordnung der EU als *„jede digitale Darstellung von Handlungen, Tatsachen oder Informationen sowie jede Zusammenstellung solcher Handlungen, Tatsachen oder Informationen auch in Form von Ton-, Bild- oder audiovisuellem Material“* beschrieben.

b) Personenbezogene Daten sind nach Art 4 Z 1 DSGVO *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine*

[30] In Unternehmen mit mehreren Standorten werden Maßnahmen zur IT- und Datensicherheit durch die Unternehmensleitung gesetzt. Die Vereinbarung sollte daher sinnvollerweise vom Zentralbetriebsrat abgeschlossen werden.

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."

c) IT-Sicherheit beschreibt Maßnahmen zur Gewährleistung einer sicheren technischen Infrastruktur, darunter fallen alle eingesetzten Informationstechniken oder Informationstechnologien.

d) Datensicherheit (und Informationssicherheit) bezieht sich auf die sichere Verarbeitung von (personenbezogenen und nicht-personenbezogenen) Daten und Informationen. Diese Daten und Informationen müssen zum einen vor unberechtigtem Zugang und unberechtigter Verwendung (= Vertraulichkeit), zum anderen vor Verlust (insbesondere) bei technischen Problemen der eingesetzten Systeme geschützt werden (= Verfügbarkeit), wie auch die Sicherstellung der Korrektheit (= Integrität) von Daten und der korrekten Funktionsweise von Systemen sicherzustellen ist.

e) Cybersicherheit umfasst nach der Definition der NIS-Richtlinie der EU *„alle Tätigkeiten, die notwendig sind um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen*".

f) Ein „System der künstlichen Intelligenz" (KI-System) ist eine Software, die mit einer oder mehreren der im Folgenden aufgeführten Techniken und Konzepte entwickelt worden ist und im Hinblick auf eine Reihe von Zielen, die vom Menschen festgelegt werden, Ergebnisse wie Inhalte, Vorhersagen, Empfehlungen oder Entscheidungen hervorbringen kann, die das Umfeld beeinflussen, mit dem sie interagieren:

   – Konzepte des maschinellen Lernens, mit beaufsichtigtem, unbeaufsichtigtem und bestärkendem Lernen unter Verwendung einer breiten Palette von Methoden, einschließlich des tiefen Lernens (Deep Learning)

   – Logik- und wissensgestützte Konzepte, einschließlich Wissensrepräsentation, induktiver (logischer) Programmierung, Wissensgrundlagen, Inferenz- und Deduktionsmaschinen, (symbolischer) Schlussfolgerungs- und Expertensysteme

   – Statistische Ansätze, Bayessche Schätz-, Such- und Optimierungsmethoden.

g) E-Discovery bedeutet, dass für einen bestimmten Sachverhalt (zB eine datenforensische Suche aus einem bestimmten sicherheitsrelevanten Anlass) relevante Daten (meist aus den Inhalten von E-Mails und Dokumenten gewonnen) identifiziert, aufbereitet und bereitgestellt bzw an Dritte (zB Behörden) übergeben werden.

4. Datenverarbeitung

(1) Die eingesetzten Systeme zur Gewährleistung der IT- und Datensicherheit werden, soweit sie personenbezogene (oder personenbeziehbare) Daten der Arbeitnehmer:innen verarbeiten, in ***Anhang 1*** angeführt und werden zumindest unter Beschreibung folgender Punkte mittels Datenblatt oder Zusatz-Betriebsvereinbarung dokumentiert:

- Bezeichnung System/Maßnahme und Anbieter
- Prüfziele/Zwecke der Datenverarbeitung
- Zuständige Abteilung (Stellen, Funktionen)
- Fokus der Datenverarbeitung: Person (Arbeitnehmer:in, Nutzer:in), Gerät/Endpoint (PC, Laptop, Smartphone, ...), Netzwerk, Anwendung (Applikation), Infrastruktur
- Ort der Datenhaltung: in eigener Infrastruktur lokal (on-prem), in eigen genutzter Cloudlösung, bei einem anderen Konzern-Unternehmen, bei einem Auftragsverarbeiter (insbesondere bei einem Cloud-Anbieter)
- verarbeitete Datenkategorien
- mittels Datenblatt oder (Zusatz-)Betriebsvereinbarung vereinbarte personenbezogene Auswertungen und Analysen
- berechtigte Empfängerkreise

(2) Zur Unterstützung der IT- und Datensicherheit werden auf den betrieblichen Endgeräten (Notebook, PC, Tablet, Smartphone) und Applikationen sowie bei der Nutzung dieser Endgeräte Systemparameter und technische Daten (diagnostische Daten, Protokoll-, Verkehrs- und Telemetriedaten, die im Hintergrund der Services/Komponenten anfallen) gesammelt und in Verbindung mit der/dem jeweiligen User:in/Endgerät ausgewertet. Die dabei gesammelten Informationen sind je System im jeweiligen Datenblatt in Anhang 1 beschrieben.

(3) Eine Analyse personenbezogener Informationen im Hinblick auf die Arbeitsleistung oder das (gegenwärtige oder zukünftige [„predictive analytics“]) Verhalten von Beschäftigten ist untersagt. Untersagt wird auch der Einsatz von KI-Systemen, deren Einsatz ist nur nach Abschluss einer speziellen Zusatz-Betriebsvereinbarung zulässig. Auch der Einsatz von E-Discovery-Tools und -Features bedarf zu seiner Zulässigkeit des vorangehenden Abschlusses einer speziellen Zusatz-Betriebsvereinbarung. Zur Aufrechterhaltung der betrieblichen System-Sicherheit dürfen personenbezogene Daten ausschließlich in den in dieser Vereinbarung angeführten Fällen und unter Einhaltung der in dieser Vereinbarung definierten Prozesse (Prinzip der [nur] „stufenweise Kontrollverdichtung“) ausgewertet werden.

(4) Inhaltsdaten, wie zB der Text einer E-Mail oder eines Dokuments dürfen, sofern nicht in der Anlage ausdrücklich vereinbart, nicht ausgewertet werden, ebenso darf kein Keylogging (Erfassung aller Anschläge der Tastatur) stattfinden.

(5) Die erfassten Informationen dürfen auf verschiedene Bedrohungsszenarien und Verbesserungspotentiale hin zur Gewährleistung der IT- und Datensicherheit ausgewertet werden. Dazu stehen unterschiedliche Funktionalitäten (Alarmmeldungen, Standardauswertungen, Cockpitlösungen, Key Indikatoren, Dashboard) zur Verfügung. Die Darstellung der Auswertungsergebnisse darf in einem ersten Schritt nur in aggregierter Form ohne Bezug zu einzelnen Arbeitsplätzen/Beschäftigten (beispielsweise in Form von Dashboards) erfolgen. Die weiteren Auswertungsstufen und ihre Voraussetzungen finden sich im folgenden Absatz.

(6) Bei konkret erkannten Gefährdungen oder Alarmmeldungen ist bei der Auswertung von Daten und der Darstellung der Datenverarbeitung einzelner Endgeräte und damit der Herstellung des Bezuges zu einzelnen Nutzer:innen von der IT-Abteilung/Systemadministration im Sinne des folgenden Prozesses wie folgt vorzugehen. Ausgenommen von den ersten beiden Stufen 1 und 2 sind nur die Fälle einer konkreten unmittelbaren Gefährdung für die IT-Infrastruktur oder für ihre korrekte Funktionsfähigkeit, welche von der IT-Abteilung/Systemadministration schriftlich zu dokumentieren bzw systemseitig zu protokollieren sind. Darüber hinaus für all diejenigen Fälle, in denen ein begründeter Verdacht eines schwerwiegenden Verstoßes gegen dienstrechtliche Bestimmungen vorliegt.

a) Stufe 1: Die Auswertung des Endgeräte- und Applikationsverhaltens erfolgt durch technische Systeme ohne Darstellung personenbezogener Einzeldaten (beispielsweise in Form von Dashboards).

b) Stufe 2: Bei konkret erkannten Störungen oder Alarmmeldungen findet die Auswertung des Endgeräte- und Applikationsverhaltens und die entsprechende Problembehebung durch die verantwortlichen Stellen in der IT-Abteilung/Systemadministration statt. Die von der Auswertung betroffene Person wird im 4-Augengespräch durch eine zuständige Person in der IT-Abteilung (unter möglicher Rückfrage bei der IT-Leitung) über den Sachverhalt informiert und gegebenenfalls zur Stellungnahme aufgefordert. Eine Meldung an die vorgesetzte Stelle der betroffenen Person darf nicht erfolgen.

c) Stufe 3: Im Fall des Weiterbestehens des regelwidrigen Verhaltens zu Lasten der betrieblichen IT-Infrastruktur oder einer hohen Wahrscheinlichkeit, dass ein tatsächlicher Schaden für das Unternehmen entstehen könnte (zB Datenverlust), ist die betroffene Person durch eine zuständige Person aus der IT-Abteilung auf den regelwidrigen Umgang und die erforderliche Verhaltensänderung hinzuweisen. Die Geschäftsführung und der Betriebsrat dürfen über den Vorfall, aber ohne Personenbezug, informiert werden. Eine

allgemeine (nicht personenbeziehbare) Information an andere Arbeitnehmer:innenkreise kann erfolgen, um das regelkonforme IT-Verhalten zu veranschaulichen.

d) Stufe 4: Bei fortgesetzter pflichtwidriger und das IT-System gefährdender Nutzung darf eine personenbezogene Offenlegung des Vorfalls gegenüber der vorgesetzten Stelle der betroffenen Person unter Information an den Betriebsrat und sofern vorhanden an den Datenschutzbeauftragten und den Chief Information Security Officer (CISO) erfolgen.

e) Alle durchgeführten Verfahrensschritte, inklusive der dazu stattgefundenen datenforensischen Erhebungen und Auswertungen sind schriftlich zu dokumentieren und allen Betroffenen zur Verfügung zu stellen.

f) Nach Bereinigung der Gefährdungslage bzw Aufklärung des Vorfalles sind die zugrundeliegenden personenbezogenen Daten zu löschen bzw zu anonymisieren. Ausgenommen davon ist die allfällige Einleitung dienstrechtlicher Maßnahmen.

(7) In allfällig zu übermittelnden Auswertungsergebnissen an Dritte ist jedenfalls der Username zu pseudonymisieren, sodass ein Rückschluss auf einzelne Personen – mit Ausnahme der in dieser Betriebsvereinbarung getroffenen Regelung - ausgeschlossen ist.

(8) Auf Anfrage sind dem Betriebsrat je System die Berechtigungsrollen vorzulegen. Zugriffe durch die IT-Abteilung/Systemadministration sind zu protokollieren, damit tatsächlich durchgeführte Verarbeitungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Diese Protokolldaten sind in eine eigene Protokolldatenbank (mit einer jeweiligen Löschfrist von 2 Jahren) einzustellen, in die dem Betriebsrat Einsicht (vom BR-Account aus) einzuräumen ist. Mit allen zugriffsberechtigten Personen sind Vereinbarungen zur Wahrung des Datengeheimnisses gemäß DSGVO bzw § 6 DSG abzuschließen und diese Personen sind – zusätzlich zu regelmäßigen Datenschutz-Schulungen – nachweislich von den Regelungen dieser Vereinbarung zu informieren.

(9) Werden die Berechtigungen durch externe (unternehmensfremde) Personen ausgefüllt, ist dies in den dazu notwendigen Verträgen mit Auftragsverarbeitern unter Einhaltung des jeweils geltenden Datenschutzrechts festzuhalten. Diese Auftragsverarbeiter sind nachweislich zur Einhaltung der Bestimmungen dieser Vereinbarung zu verpflichten. Diese rechtliche Überbindung und die arbeitnehmerrelevanten Inhalte der Verträge über eine Auftrags(daten)verarbeitung sind dem Betriebsrat auf Anforderung vorzulegen.

5. Informationssicherheitsmanagementsystem (ISMS)

(1) Die <NAME> evaluiert zur Sicherstellung der IT- und Datensicherheit regelmäßig die getroffenen Strategien, Konzepte sowie technischen und organisatorischen Maßnahmen

(TOMs). In einem kontinuierlichen operativen Prozess werden die getroffenen Maßnahmen regelmäßig auf sich ändernde Rahmenbedingungen und aktuelle Bedrohungslagen überprüft.

(2) Dazu wird ein Informationssicherheitsmanagementsystem (ISMS) mit einem Informationssicherheits-Management-Team eingeführt.

(3) Zu den Mitgliedern des Informationssicherheits-Management-Teams gehört neben Personen aus den technischen und rechtlichen Fachabteilungen auch zumindest ein Mitglied des Betriebsrates.

(4) Die Entscheidungskompetenzen der Arbeitgeberin/des Arbeitgebers als Organ des Unternehmens und die des Betriebsrates als Organ der Belegschaft bleiben davon jedoch unberührt.

6. Beweismittel und -verwertungsverbot

(1) Eine Verarbeitung von personenbezogenen Daten der Arbeitnehmer:innen, die unter Zuhilfenahme der durch diese Betriebsvereinbarung erfassten Systeme und/oder gemäß der gegenständlichen Betriebsvereinbarung inklusive deren Anhänge in erlaubter oder unerlaubter Weise verarbeitet (erhoben/erfasst/ausgelesen/abgefragt) wurden, zur Leistungs- und Verhaltenskontrolle oder zur wie auch immer gearteten Beurteilung von Arbeitnehmer:innen ist untersagt und damit rechtwidrig.

(2) Es wird hiermit zur diesbezüglichen Bewehrung aus Gründen rechtlicher Vorsicht gemäß Art 88 Abs 1 DSGVO beschäftigtendatenschutzrechtlich ein entsprechendes außergerichtliches, gerichtliches und behördliches Beweismittel- und -verwertungsverbot, das sich an Jedermann (das sind insbesondere Arbeitgeber:in, Behörden und Gerichte) richtet, vereinbart, soferne von einem solchen Beweismittel- und -verwertungsverbot nicht sowieso schon eo ipso (europa-)rechtlich auszugehen ist.

(3) Erlangt der/die Arbeitgeber:in von derartigen Analysen Dritter Kenntnis (beispielsweise über eine entsprechende Verarbeitung im Konzern seitens eines anderen Konzernunternehmens oder seitens eines [Sub-]Auftragsverarbeiters eines Konzernunternehmens), sind der Betriebsrat und die davon betroffenen Arbeitnehmer:innen zu informieren. Darüber hinaus sind die Solches ausführenden Stellen von den Regelungen dieser Betriebsvereinbarung und ihren Anhängen zu informieren und sind diese Stellen sowie die entsprechenden Unternehmen nachweislich zur Unterlassung aufzufordern, welche Vorgehensweise dem Betriebsrat proaktiv zur Kenntnis zu bringen ist.

7. Auftragsverarbeitung

(1) Bei allen zum Einsatz kommenden Auftragsverarbeitern gemäß Artikel 28 DSGVO hat der/die Arbeitgeber:in sicherzustellen, dass diese Auftragsverarbeiter neben den Bestimmungen des Datenschutzrechts auch die Regelungen dieser Betriebsvereinbarung einhalten. Die Auftragsverarbeiter sind deshalb nachweislich zur Einhaltung der Bestimmungen dieser Betriebsvereinbarung zu verpflichten. Diese rechtliche Überbindung und die arbeitnehmerrelevanten Inhalte der Verträge über die jeweilige Auftrags(daten)verarbeitung sind dem Betriebsrat auf Anforderung vorzulegen.

8. Mitwirkungsrechte des Betriebsrates

(1) Dem Betriebsrat sind alle geltenden Ordnungsvorschriften zur IT- und Datensicherheit nachweislich zur Kenntnis zu bringen und diese sind im Hinblick auf die Bestimmungen dieser Betriebsvereinbarung auf Konformität mit dieser hin zu prüfen.

(2) Der Betriebsrat hat zur Überprüfung dieser Betriebsvereinbarung das Recht in sämtliche technischen Protokolle und Funktionalitäten (Alarmmeldungen, Standardauswertungen, Cockpitlösungen, Key Indikatoren, Dashboard) nach Maßgabe des § 89 und § 91 Abs 2 ArbVG Einsicht zu nehmen. Zugang zu Hardware und Software ist ihm zu gewähren.

(3) Es ist dem Betriebsrat gestattet, externe Expert:innen zur Unterstützung und zur technischen Prüfung der Einhaltung dieser Betriebsvereinbarung hinzuzuziehen. Diese Expert:innen sind nachweislich zur Verschwiegenheit zu verpflichten. Sie sind bei ihrer Tätigkeit von den Fachabteilungen zu unterstützen. Die entsprechenden Kosten sind bis zur maximalen Höhe von € x.xxx pro Jahr vom Unternehmen zu tragen. Wird ein Verstoß gegen Bestimmungen dieser Betriebsvereinbarung festgestellt, sind die entsprechenden Kosten dieser Hinzuziehung vom Unternehmen ohne Anrechnung auf den Jahresmaximalbetrag zu tragen.

9. Sanktionen bei Verstößen

(1) Verstöße des/der Arbeitgeber:in gegen die gegenständliche Betriebsvereinbarung, gegen das DSG oder gegen die DSGVO berechtigen den Betriebsrat, schriftlich auf diese Missstände hinzuweisen und deren Beseitigung binnen vierzehn Tage nach der Beanstandung zu fordern.

(2) Im Falle der Nichtbeseitigung des Missstandes innerhalb dieser Frist trotz schriftlicher Aufforderung hat der Betriebsrat das Recht, die gegenständliche Betriebsvereinbarung, den betroffenen Anhang bzw die Zusatz-Betriebsvereinbarung mittels eingeschriebenen Briefes an den/die Arbeitgeber:in einseitig mit sofortiger Wirkung aufzulösen, wobei eine Nachwirkung ausgeschlossen ist, sodass die von der gegenständlichen

Betriebsvereinbarung erfassten Datenverarbeitungen bzw die im Anhang geregelte betroffene Datenverarbeitung sofort zur Gänze einzustellen wären.

10. Rechte der ArbeitnehmerInnen

(1) Alle Arbeitnehmer:innen sind über ihre datenschutzrechtlichen Rechte und Pflichten, insbesondere geltende IT-Ordnungsvorschriften, nachweislich zu informieren.

(2) Alle Arbeitnehmer:innen sind in transparenter Form über die Verarbeitungen ihrer Daten zur Gewährleistung der IT- und Datensicherheit zu informieren.

(3) Technische und organisatorische Maßnahmen zur IT- und Datensicherheit sind so zu erlassen und zur Verfügung zu halten, dass sich die Arbeitnehmer:innen über die für sie geltenden Regelungen jederzeit informieren können.

(4) Alle diese Informationen sind (auch) in deutscher Sprache bereit zu stellen.

11. Geltungsdauer der Betriebsvereinbarung

(1) Diese Betriebsvereinbarung tritt mit TT. MM. JJJJ in Kraft und gilt vorerst befristet für achtzehn Monate.

(2) Während dieser Zeit besteht eine Phase der beiderseitigen Prüfung ihrer praktikablen Anwendbarkeit, binnen derer – über Wunsch einer Vertragsseite – auch ergänzende Gespräche mit dem Ziel einer einvernehmlichen Abänderung geführt werden können.

(3) Sollte bis 3 Monate vor Ablauf der achtzehnmonatigen Befristung keine Vertragsseite gegenüber der anderen Partei ausdrücklich und schriftlich (maßgeblich für die Rechtzeitigkeit ist, wie für alle der Schriftform bedürftigen Veranlassungen gemäß dieser Betriebsvereinbarung, das Einlangen bei der anderen Partei, wobei auch Übermittlung per E-Mail akzeptiert wird) auf einem Auslaufen der Betriebsvereinbarung mit Fristende bestehen, so verlängert sich diese Betriebsvereinbarung befristet um jeweils 24 Monate unter Beibehaltung des vorbeschriebenen Procederes für eine allfällige Nichtverlängerungserklärung.

13 GLOSSAR

Die wichtigsten in diesem Leitfaden verwendeten Fachbegriffe werden in Folge in alphabetischer Form nochmals zusammengefasst und erklärt.

AaaS	englische Bezeichnung	Access as a Service
	deutsche Bezeichnung	Zugang als eine Dienstleistung
Beschreibung	Cyberkriminelle bieten widerrechtlich erlangte oder gehackte Zugangsdaten zum Verkauf an. Dies erfolgt im sogenannten Darknet. Beim Darknet handelt es sich um einen versteckten Teil des Internets, der nur durch spezielle Software (zB Tor Browser) erreichbar ist. Eine Identifizierung von Nutzer:innen ist nur schwer möglich, Nutzer:innen genießen beim Surfen im Internet ein hohes Maß an Anonymität. Bezahlt wird in der Regel über digitale Währung (Kryptowährung wie beispielsweise Bitcoin).		

APT	englische Bezeichnung	Advanced Persistent Threats
	deutsche Bezeichnung	fortgeschrittene andauernde Bedrohungen
Beschreibung	Angreifer betreiben bei APT einen hohen Aufwand, um zielgerichtet die Infrastruktur eines Unternehmens oder einer Behörde zu schädigen. Umfangreiche personelle Ressourcen und Fachwissen sind notwendig, um unerkannt in die Systeme einzudringen. Angreifer halten sich dann mitunter über Wochen und Monate versteckt in diesen Systemen auf, um betriebliche Abläufe und Zuständigkeiten für konkrete Erpressungsversuche besser kennen zu lernen.		

CaaS	englische Bezeichnung	Cybercrime as a Service
	deutsche Bezeichnung	Cyberkriminalität als Dienstleistung
Beschreibung	Bei diesem kriminellen Geschäftsmodell bieten Hacker ihre Dienstleistungen oder Produkte im Darknet (einem versteckten Teil des Internets, der nur über spezielle Software wie den Tor Broser erreichbar ist und Nutzer:innen ein hohes Maß an Anonymität garantiert) an, um Unternehmen, Privatpersonen oder Behörden anzugreifen und Zugriff auf deren IT-Systeme oder Daten zu erhalten.		

CISO	englische Bezeichnung	Chief Information Security Officer
	deutsche Bezeichnung	Gesamtverantwortlichen für IT-Sicherheit
Beschreibung	Die betriebliche Funktion des CISO „hat dafür Sorge zu tragen, dass die einzelnen Sicherheitsrichtlinien mit der organisationsweiten Informationssicherheitspolitik kompatibel sind und auch untereinander ein einheitliches, vergleichbares Niveau aufweisen.“ (siehe Österreichisches Informationssicherheitshandbuch, Version 4.3.2, Seite 83)		

DDoS	englische Bezeichnung	Distributed Denial of Service
	deutsche Bezeichnung	Verteilte Verweigerung des Dienstes
Beschreibung	DDoS ist eine erweitere Form von DoS (Erklärung siehe unten). Bei dieser Form einer Attacke auf den Internetdienst eines Unternehmens oder einer Behörde findet gleichzeitig eine Vielzahl an Zugriffen und somit eine bewusst herbeigeführte Überlastung mit einer großen Zahl an unterschiedlichen Rechnern statt. Da die Quellen des Angriffs (= die einsetzten, zum Großteil im Vorfeld gehackten Rechner) sehr unterschiedlich sind, ist ein Blockieren dieser Zugriffe (ohne einer Beeinträchtigung von berechtigten Zugriffen) nicht möglich.		

DLP	englische Bezeichnung	Data Leakage/Loss Prevention
	deutsche Bezeichnung	Verhindern von Datenlecks /Datenverlust
Beschreibung	DLP-Systeme verfolgen das Ziel, unerlaubten Datenabfluss zu verhindern. Durch den Einsatz von DLP-Software wird der Datentransfer (Übermittlung von Daten und Dokumenten) überprüft und Abweichungen vom betrieblich gewünschten Standard aufgezeigt (beispielsweise eine versuchte unverschlüsselte Versendung eines Dokuments oder ein versuchter Upload vertraulicher Daten). Dabei kann mittels einer Meldung ein:e Nutzer:in darauf hingewiesen werden oder der Transfer gänzlich blockiert werden		

DoS	englische Bezeichnung	Denial of Service
	deutsche Bezeichnung	Verweigerung des Dienstes
Beschreibung	DoS bezeichnet die Nichtverfügbarkeit eines Internetdienstes (zB eine Seite im Internet kann nicht aufgerufen werden). In vielen Fällen liegt der Grund darin, dass der Dienst durch eine Vielzahl an gleichzeitig stattfindenden Zugriffen in bewusster Absicht und mutwillig überlastet wird und daher nicht mehr zur Verfügung steht.		

EDR	englische Bezeichnung	Endpoint Detection and Response
	deutsche Bezeichnung	Endpunkterkennung und -reaktion
Beschreibung	EDR-Systeme überwachen das Verhalten der betrieblichen IT-Infrastruktur (und damit auch das Verhalten der Nutzer:innen, die einzelne Geräte verwenden). Algorithmen ermitteln daraus ein „normales Verhalten“ (Muster) und warnen Administrator:innen, sollte ein Gerät oder eine Gruppe von Geräten vom normale/erwartbaren Verhalten abweichen.		

IaaS	englische Bezeichnung	Infrastructure as a Service
	deutsche Bezeichnung	Infrastruktur als Dienstleistung
Beschreibung	Bei IaaS werden grundlegende Infrastrukturleistungen über das Internet zur Verfügung gestellt (zB Rechenleistung, Speicherplatz), auf deren Basis Nutzer:innen individuelle Software wie Betriebssysteme oder Anwendungsprogramme betreiben können. Ein Vorteil dieses Service ist, dass nicht mehr das Unternehmen für eine sichere Datenhaltung sorgen muss, sondern diese an einen Auftragsverarbeiter (Dienstleister) auslagert wird.	

IAM	englische Bezeichnung	Identity- und Access Management
	deutsche Bezeichnung	Identitäts- und Zugriffsverwaltung
Beschreibung	IAM-Systeme dienen zur Verwaltung von digitalen Identitäten (Nutzer:innen, Maschinen, Geräte) und den diesen Identitäten zugewiesenen (Zugriffs)Rechten.	

ISMS	englische Bezeichnung	Information Security Management System
	deutsche Bezeichnung	Managementsystem für Informationssicherheit“
Beschreibung	In einem ISMS werden alle Verfahren und Regeln (Policies) festgehalten, um in einem Unternehmen IT- und Datensicherheit zu gewährleisten. Diese ganzheitliche Darstellung der Informationssicherheitsrisiken ist regelmäßig zu evaluieren und entsprechend dem Stand der Technik zu adaptieren	

MDR	englische Bezeichnung	Managed Detection and Response
	deutsche Bezeichnung	verwaltetes Erkennen und Reagieren
Beschreibung	MDR beschreibt das Prinzip einer ausgelagerte IT-Security Abteilung (im datenschutzrechtlichen Sinn ein Auftragsverarbeiter), welche dann für die Verwaltung der Sicherheitsfälle eines Unternehmens verantwortlich ist.	

MFA	englische Bezeichnung	Multi-factor authentication
	deutsche Bezeichnung	Multi-Faktor-Authentifizierung
Beschreibung	Bei der Multi-Faktor-Authentifizierung wird die Zugriffsberechtigung eines:r Nutzer:in für ein IT-System anhand mehrerer (zumindest zwei) voneinander getrennter Faktoren geprüft. Neben dem Passwort kann dies zB ein SMS-Code sein, der an ein dem/der Nutzer:in zugeschriebenes Smartphone (somit ein zweites Gerät) gesendet wird, oder die Bestätigung in einer App, die sich am Smartphone der/des Nutzer:in befindet.	

MSSP	englische Bezeichnung	Managed security service provider
	deutsche Bezeichnung	Anbieter von Sicherheitsdiensten
Beschreibung	MSSP bezeichnet einen externen Anbieter, der beauftragt wird, die Cybersicherheit in einem Unternehmen sicherzustellen.	

PaaS	englische Bezeichnung	Platform as a Service
	deutsche Bezeichnung	Plattform als Dienstleistung
Beschreibung	Bei diesem Service wird von Anbietern neben der Infrastruktur auch das Betriebssystem oder eine Entwicklungsumgebung für Anwendungen über das Internet/in der Cloud zur Verfügung gestellt.	

SaaS	englische Bezeichnung	Software as a service
	deutsche Bezeichnung	Software als Dienstleistung
Beschreibung	Bei diesem Service verwenden Nutzer:innen Apps (Software), die über eine Cloud-Plattform zur Verfügung gestellt werden (zB Microsoft 365).	

SIEM	englische Bezeichnung	Security Information and Event Management
	deutsche Bezeichnung	Sicherheitsinformations- und Ereignisverwaltung
Beschreibung	SIEM-Systeme sammeln und analysieren Protokolldaten unterschiedlichster IT-Systeme (Quellen) in einer gesonderten Datenbank- und Systemumgebung. Durch die Zusammenführung von Protokolldaten aus unterschiedlichen (Quell)Systemen ergibt sich ein umfassendes Bild, wie diese IT-Systeme im Unternehmen genutzt werden. Aus der Analyse der dabei gesammelten Informationen können Auffälligkeiten („Events“) erkannt werden, die auf eine Bedrohung schließen lassen können.	

SOAR	englische Bezeichnung	Security Orchestration, Automation and Response
	deutsche Bezeichnung	Sicherheits-Orchestrierung, Automatisierung und Reaktion
Beschreibung	SOAR-Systeme erweitern den SIEM-Ansatz (siehe oben) der Analyse und des Aufzeigens von aktuellen Bedrohungen. In diesen Systemen werden - abhängig von den erkannten Bedrohungen - automatische Systemreaktionen ohne menschlichen Eingriff (der IT-Fachabteilung) definiert und durchgeführt, dadurch kann die Reaktionszeit eines Unternehmens auf aktuell erkannte Bedrohungen beschleunigt werden.	

SOC	englische Bezeichnung	Security Operations Center
	deutsche Bezeichnung	Zentrale Stelle, die Dienstleistungen für die IT-Sicherheit anbietet:
Beschreibung	Diese zentrale Stelle (interner Fachbereich oder extern dafür beauftragtes Team) ist für alle Aktivitäten rund um die IT- und Datensicherheit zuständig.	

XDR	englische Bezeichnung	Extended Detection and Response
	deutsche Bezeichnung	Erweitere Erkennung und Reaktion
Beschreibung	XDR-Systeme erfassen und analysieren automatisiert Daten mehrerer Bereiche der betrieblichen IT-Landschaft (E-Mail, Endpunkte, Netzwerk) um Bedrohungen erkennen, untersuchen und angemessen darauf regieren zu können.	

Zero Trust	englische Bezeichnung	Zero Trust
	deutsche Bezeichnung	Null Vertrauen
Beschreibung	Das Prinzip „Zero Trust“ beruht auf dem organisatorischen Konzept keiner Person, keinem Gerät (PC, Laptop, Tablet, Smartphone) und keiner Anwendung (App, Software) uneingeschränkt zu vertrauen, unabhängig davon, ob es sich um interne oder externe Nutzer:innen, Geräte oder Anwendungen handelt. Das Vertrauen muss jeweils (mit technischer Unterstützung) neu überprüft werden.	

14 ABKÜRZUNGSVERZEICHNIS

AaaS	Access as a Service
AD	Active Directory
App	Application
APT	Advanced Persistent Threats
ArbVG	Arbeitsverfassungsgesetz
Art	Artikel
BSI	deutsches Bundesamt für Sicherheit in der Informationstechnik
CaaS	Cybercrime as a Service
CISO	Chief Information Security Officer
DDoS	Distributed-Denial-of-Service
DIN	Deutsche Institut für Normung
DLP	Data Leakage/Loss Prevention
DoS	Denial-of-Service
DSG	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
EDR	Endpoint Detection and Response
ENISA	Agentur der Europäischen Union für Cybersicherheit
GPS	Global Positioning System
Iaas	Infrastructure as a Service
IAM	Identity- und Access Management
ID	Identifikation
IEC	International Electrotechnical Commission
IM	Instant Messaging
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Information Technology

MFA	Multi-Faktor-Authentifizierung
MIT	Massachusetts Institute of Technology
MSSP	Managed security service provider
NIS-RL	Netz- und Informationssicherheitsrichtline
NISG	Netz- und Informationssystemsicherheitsgesetz
NIST	US National Institute of Standards and Technology
NISV	Netz- und Informationssystemsicherheitsverordnung
NPO	Non-Profit-Organisation
PaaS	Platform as a service
PDCA	Plan-Do-Check-Act
PII	personally identifiable information
SaaS	Software as a service
SIEM	Security Information and Event Management
SOA	Security Orchestration, Automation and Response
SOC	Security Operations Center
TISAX	Trusted Information Security Assessment Exchange
TOM	technische und organisatorische Maßnahmen
UWG	Bundesgesetz gegen den unlauteren Wettbewerb
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
XDR	Extended Detection and Response

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

GEFÖRDERT DURCH
Digifonds
AK WIEN

Im Spannungsfeld von IT- und Datensicherheit und versteckter Kontrolle am (Home-)Office Arbeitsplatz

Ein Leitfaden zur Mitbestimmung für die betriebliche Interessenvertretung (Betriebsrat und Personalvertretung)