Information Security

Compliance in der Sicherheitstechnik

Normen, Gesetze und Verträge im Sicherheitstechnikbereich

Diplomarbeit

zur Erlangung des akademischen Grades

Diplom-Ingenieurin

eingereicht von

Bianca Danczul, BSc
1510619504

im Rahmen des
Studiengangs Information Security an der Fachhochschule St. Pölten

Betreuung
Betreuer: Dipl.-Ing. Herfried Geyer

St. Pölten,
01.06.2018

(Unterschrift Autorin)

(Unterschrift Betreuer)

Ehrenwörtliche Erklärung

Ich versichere, dass

- ich diese Diplomarbeit selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich sonst keiner unerlaubten Hilfe bedient habe.
- ich dieses Diplomarbeitsthema bisher weder im Inland noch im Ausland einem Begutachter / einer Begutachterin zur Beurteilung oder in irgendeiner Form als Prüfungsarbeit vorgelegt habe.
- diese Arbeit mit der vom Begutachter beurteilten Arbeit übereinstimmt.

Die Studierende/Absolventin räumt der FH St. Pölten das Recht ein, die Diplomarbeit für Lehr- und Forschungstätigkeiten zu verwenden und damit zu werben (z.B. bei der Projektevernissage, in Publikationen, auf der Homepage), wobei die Absolventin als Urheberin zu nennen ist. Jegliche kommerzielle Verwertung/Nutzung bedarf einer weiteren Vereinbarung zwischen der Studierenden/Absolventin und der FH St. Pölten.

St. Pölten,
01.06.2018

(Unterschrift Autorin)

Kurzfassung

Die vorliegende Masterarbeit beschäftigt sich mit den Möglichkeiten, Compliance-Anforderungen im Sicherheitstechnikbereich umzusetzen, wobei hierbei sowohl die Anforderungen an Hersteller/innen als auch an Anwender/innen in Betracht gezogen wurden. Die Identifikation der relevanten, gesetzlichen Grundlagen entspricht der ersten Prozessaktivität des *COBIT ME3 Schemas* „Stelle Compliance mit Vorgaben sicher". [1, p. 42] Die konkrete Unterteilung der rechtlichen Vorgaben wurde anhand des *House of Compliance* nach Klotz [2, p. 21] erstellt.

Um dieses Ziel zu erreichen, wurden zunächst mittels einer theoretischen Analyse die wichtigsten Bereiche der mechanischen und elektronischen Sicherheitstechnik samt anzuwendender Normen identifiziert, da Normen und Standards als unternehmensexterne Regelwerke ein wichtiger Grundpfeiler einer erfolgreichen Compliance-Strategie sind. Zudem wurde die Funktionsweise der Systeme, die der elektronischen Sicherheitstechnik zuzuordnen sind – wie Gefahrenmeldeanlagen, Zutrittskontrollsysteme, Videoüberwachungsanlagen und GPS-Systeme – genauer erklärt, um einen Überblick zu bekommen und die spätere Anwendung der rechtlichen Grundlagen besser nachvollziehen zu können.

Nach der Identifikation und Definition der sicherheitstechnischen Grundlagen beschäftigt sich die Masterarbeit mit den relevanten rechtlichen Vorgaben, insbesondere der neuen Datenschutzgrundverordnung, im Folgenden DSGVO genannt, und dem Arbeitsrecht, um daraus die Richtlinien für den gesetzeskonformen Einsatz und Vertrieb ableiten zu können. Das letzte Kapitel gibt schließlich einen Überblick, wie sowohl unternehmensinterne Regelwerke als auch Verträge gestaltet werden könnten, um den hohen Compliance-Maßstäben Genüge zu tun.

Abstract

This master's thesis is looking into the details of implementing compliance requirements in the field of safety technology, whereby both the requirements of manufacturers and users have been considered. The identification of the relevant legal regulations corresponds to the first point of the *COBIT ME3 scheme* [7, p. 42] and the concrete subdivision of the legal requirements was based on the *House of Compliance* according to Klotz [2, p. 21].

In order to achieve this goal, the most important areas of mechanical and electronic safety technology, including applicable external regulations like standards, were identified, as external regulations are an important keystone of a successful compliance strategy. In addition, the functionality of the electronic security systems - such as alarm systems, access control systems, video surveillance systems and GPS systems - has been explained in more detail in order to get a rough overview and a better understanding of the later application of the legal basis.

Following the identification and definition of the basic safety principles, this master's thesis deals with the relevant legal requirements, in particular the new General Data Protection Regulation, also known as GDPR, and employment law, in order to derive the guidelines for acting conformable to law. Finally, the last chapter gives an overview of how to design both internal policies and contracts to meet the high compliance standards.

Inhaltsverzeichnis

1. Einleitung

Die in weiterer Folge präsentierten Statistiken zeigen, dass einerseits das Interesse der Bevölkerung an Sicherheitstechnik (insbesondere elektronischer) stetig wächst und somit auch in Unternehmen Videoüberwachungssysteme oder Zutrittskontrollsysteme immer häufiger eingesetzt werden, um das Unternehmen bzw. dessen Daten zu schützen. Andererseits steigen dadurch die Anforderungen an die Hersteller, gesetzeskonforme Produkte anzubieten.

Basierend auf einer von Statista in den Jahren 2015 und 2016 durchgeführten Prognose, welche den Umsatz im Segment der Gebäudesicherheit in Österreich zwischen 2016 und 2022 behandelt, wird der Umsatz in diesem Segment relativ linear von 21 Millionen Euro im Jahr 2016 auf 81 Millionen Euro im Jahr 2022 ansteigen und 2018 bei rund 40 Millionen liegen. [3] In Deutschland, wo der Markt wesentlich größer ist, ist sogar eine Umsatzsteigerung von 246 Millionen Euro im Jahr 2016 auf 904 Millionen Euro im Jahr 2022 prognostiziert. [4]

Betrachtet man nun den Umsatz elektronischer Sicherungstechnik nach Segment in Deutschland im Jahr 2016 so zeigt sich, dass der Brandmeldetechnikbereich mit 1805 Millionen Euro mit Abstand der Größte ist, gefolgt von der Einbruchmeldetechnik mit 800 Millionen, der Videoüberwachungstechnik mit 511 Millionen und den Zutrittssteuerungssystemen mit 307 Millionen Euro. [5]

Um nun die Einhaltung von internationalen, nationalen oder innerbetrieblichen Gesetzen, Verordnungen, Verträgen und Richtlinien zu gewährleisten und Regelbrüche sowie etwaige Strafen zu vermeiden, ist es für alle Beteiligten wichtig, geeignete Compliance-Maßnahmen zu setzen. [6]

1.1. Der Begriff der (IT-) Compliance und dessen Abgrenzung

Um eine ordnungsgemäße Führung und Kontrolle eines Unternehmens und der dazugehörigen (IT-) Systeme zu gewährleisten, ist es wichtig, Vorgaben einzuhalten und Betrugsvergehen oder Missmanagement zu verhindern, wodurch sich die Verbindung zwischen Governance und Compliance ergibt. [2]

Beachtenswert ist dabei insbesondere, dass eine Non-Compliance ein wirtschaftliches Risiko für das Unternehmen darstellt und durch entsprechende Compliance-Maßnahmen verhindert werden muss. [2]

1.1.1. (IT-) Governance

IT-Compliance ist ein Teilbereich der Corporate Compliance und Bestandteil der IT-Governance, welche wiederum unter den Oberbegriff der Corporate Governance fällt. Unter Corporate Governance versteht man die ordnungsgemäße Führung und Überwachung eines Unternehmens, während die IT-Governance nach ISO/IEC 38500 die aktuelle und zukünftige Verwendung der IT steuert und kontrolliert. Dies beinhaltet Definition, Kenntnis und Akzeptanz der Verantwortlichkeiten sowie eine geeignete IT-Strategie, welche sich an der Unternehmensstrategie orientiert. [2]

Weitere wichtige Prinzipien der IT-Governance nach ISO/IEC 38500 sind die bedarfsgerechte Beschaffung von IT-Systemen, eine entsprechende Performanz ebenjener Systeme und eine „Konformität der IT mit rechtlichen Vorgaben, Normen, professionellen Standards etc." sowie die „Beachtung der Bedürfnisse von Personen, die in irgendeiner Weise von der im Unternehmen eingesetzten IT betroffen sind (als Nutzer, IT-Spezialisten, Kunden, Lieferanten etc.)". [2, p. 15]

Eine weitere, an das COBIT Framework angelehnte Definition der IT-Governance liefert das IT Governance Institute (ITGI), welches eine Tochterorganisation der ISACA ist. In diesem Kontext werden die Ziele des IT-Governance insofern definiert, als sich die IT an den Anforderungen des Unternehmens ausrichten muss und der versprochene Nutzen von IT-Investitionen realisiert werden sollte, um den Gewinn durch die IT zu definieren. Weitere Ziele sind ein „verantwortungsvoller Umgang mit IT-Ressourcen" sowie ein „angemessenes Management von IT-Risiken". [2, p. 16]

1.1.2. IT-Compliance

Die IT-Compliance, als Unterbegriff der Corporate Compliance, behandelt nun konkret die Sicherheit und den Umgang mit Daten, das „Vorhandensein und Funktionieren informations- und kommunikationstechnischer Einrichtungen" sowie die Dokumentation von Programmen, Notfallplänen oder Kontrollergebnissen und kann nach Klotz wie folgt definiert werden [2, p. 20]:

> *„IT-Compliance bezeichnet einen Zustand, in dem alle die IT des Unternehmens betreffenden und verbindlich vorgegebenen bzw. als verbindlich akzeptierten Vorgaben nachweislich eingehalten werden." [2, p. 20]*

Zu beachten ist hierbei, dass es aufgrund der Fülle an sich regelmäßig verändernden Vorgaben weder wirtschaftlich noch erstrebenswert ist, eine hundertprozentige Compliance erreichen zu wollen und somit das Risiko einer Non-Compliance definiert und akzeptiert werden muss. Zudem müssen Compliance-Maßnahmen nicht nur definiert und durchgeführt, sondern auch dokumentiert werden, um im Falle einer Prüfung oder eines Streitfalles nachweisbar zu sein.

Konkrete rechtliche Vorgaben können nach Klotz anhand des *House of IT-Compliance,* welches in Abbildung 1 zu sehen ist, grafisch wie folgt unterteilt werden. [2, p. 21]

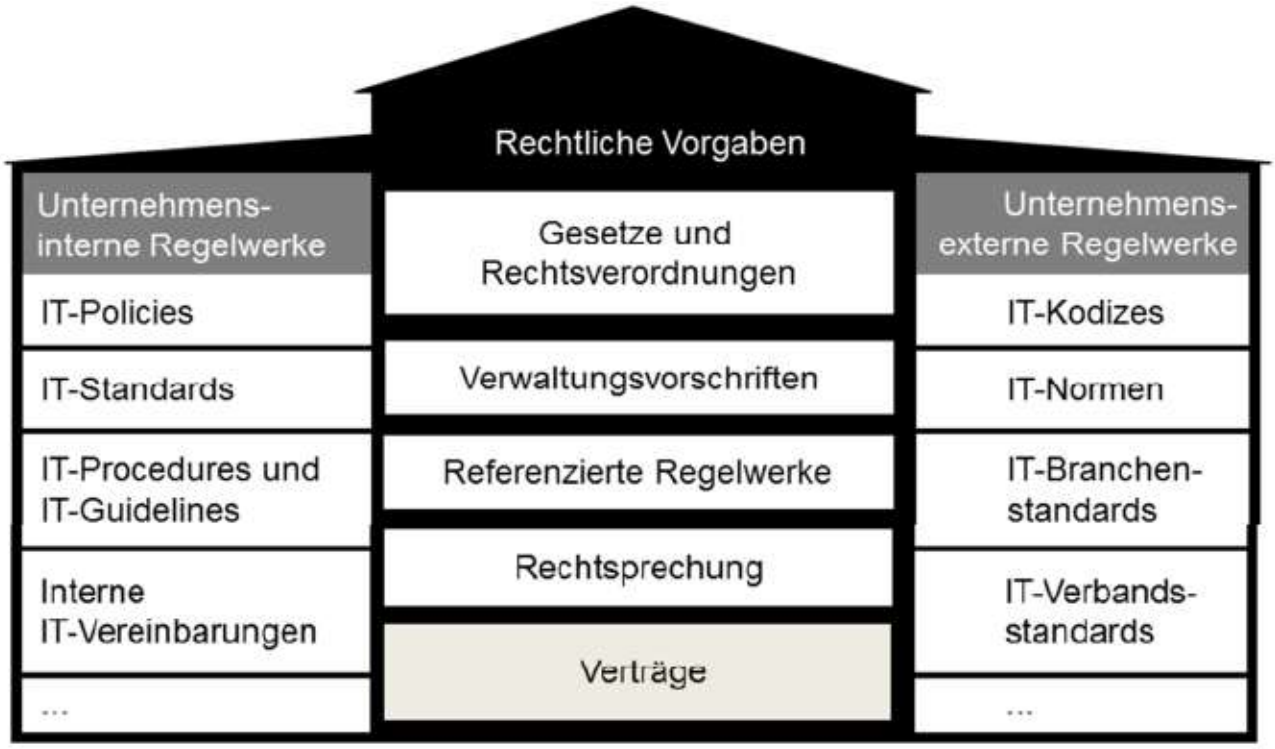

Abbildung 1: House of Compliance nach Klotz [2, p. 21]

- Unternehmensinterne Regelwerke, wie z.B. IT-Policies, Procedures oder Service Level Agreements (SLAs), weisen bei einer Non-Compliance sowohl die geringste Bindung als auch das geringste Risiko für das Unternehmen auf, da sie ihre Anwendung primär innerhalb des Unternehmens finden, welches das Regelwerk definiert hat. Da diese Regelwerke die Befolgung von anderen Regelwerken und rechtlichen Vorgaben innerhalb des Unternehmens definieren, erfüllen sie zugleich die zuvor erwähnte Dokumentationspflicht. [7]

- Unternehmensexterne Regelwerke, wie z.B. Normen oder Branchenstandards, weisen bei einer Non-Compliance das zweitniedrigste Risiko und die zweitniedrigste Bindung für ein Unternehmen auf. Sie helfen diesem allerdings bei der Definition von relevanten Best-Practice Lösungen oder können eine Basis für Zertifizierungen sein. [7]

- Verträge mit Kunden oder Lieferanten fallen unter die rechtlichen Vorgaben, da im Falle einer Vertragsverletzung mit hohen Vertragsstrafen oder Schadenersatzansprüchen zu rechnen ist. Daher besitzen sie das zweithöchste Risiko und die zweithöchste Bindung. [7]

- Zu den relevanten rechtlichen Vorgaben zählen einerseits die für die jeweilige Branche relevanten Gesetze und Rechtsverordnungen (in Österreich sind das im Bereich der Sicherheitstechnik z.B. die DSGVO, das Produkthaftungsgesetz oder das Arbeitsrecht), andererseits sind auch aktuelle Rechtsprechungen relevant, da diese die Auslegung von Rechtsnormen betreffen. Zudem können auch Branchenstandards oder Normen rechtlich verpflichtend sein, wenn auf diese ausdrücklich verwiesen wird. [2]

1.1.3. IT-Compliance Prozess

Um nun die Compliance-Vorgaben nachweislich einzuhalten „ist ein gezieltes Management der IT-Compliance notwendig“, welches „in Form eines ganzheitlichen IT-Compliance-Prozesses, der langfristig im Unternehmen zu etablieren ist, erfolgen [kann]“. [1, p. 42]

Ein Beispiel für solch einen IT-Compliance Prozess ist im COBIT Framework des ITGI unter der Domäne „Monitor and Evaluate“ im Unterpunkt ME3 „Stelle Compliance mit Vorgaben sicher“ beschrieben und beinhaltet die nachfolgenden fünf Prozessaktivitäten. [1, p. 42]

(1) Identifikation relevanter nationaler und internationaler Vorgaben, wie z.B. Gesetze und Normen;

(2) nachweisliche Einhaltung der relevanten Vorgaben samt „regelmäßige[r] Überprüfung, Beurteilung und Optimierung von IT-Richtlinien, -Standards und -Verfahren“;

(3) „Evaluierung der Einhaltung von IT-Richtlinien, -Standards und Verfahren sowie rechtlicher und regulatorischer Vorgaben“;

(4) „Definition und Implementierung von Verfahren zur positiven Bestätigung von Compliance“;

(5) integrierte Berichterstattung, um den Status der Compliance festzustellen

1.2. Ziel dieser Diplomarbeit

Anhand der obenstehenden Definitionen soll nun – analog zur IT-Compliance – der Grundpfeiler gelegt werden, um Compliance sowohl beim Einsatz als auch beim Vertrieb von Sicherheitstechnik mittels geeigneter Maßnahmen zu gewährleisten. Dies inkludiert einerseits die Identifikation relevanter rechtlicher Vorgaben und aktueller unternehmensexterner Regelwerke, wobei hierbei insofern deswegen kein Anspruch auf Vollständigkeit erhoben wird, als dass diese Arbeit nur eine Momentaufnahme der aktuellen Rechtslage zeigen kann. Zudem ist zu beachten, dass sich Standards und Gesetze stetig verändern, um sich den aktuellen Gegebenheiten anzupassen. Andererseits zeigt diese Arbeit konkrete Beispiele von Verträgen und unternehmensinternen Regelwerken.

Das Kapitel 3 (Einführung in die Sicherheitstechnik) definiert und identifiziert zunächst einige der wichtigsten Begriffe, Anwendungsgebiete und Normen aus dem Bereich der mechanischen und elektronischen Sicherheitstechnik und legt anschließend das Hauptaugenmerk auf die Funktionsweise von Alarmanlagen, Videoüberwachungs- sowie Zutrittskontrollsystemen und GPS-Systemen. Zu erwähnen ist hierbei, dass sich diese Diplomarbeit auf Normen der ÖNORM und DIN sowie Richtlinien von OVE beschränkt. Weitere Normen, Standards und Richtlinien, wie VdS oder ISO/IEC wurden aus Platzgründen nicht inkludiert, sind aber bei einer vollständigen Compliance-Strategie natürlich ebenso in Betracht zu ziehen.

Das darauffolgende Kapitel 4 (Rechtliche Grundlagen in Bezug auf Sicherheitstechnik) behandelt einige der beim Einsatz oder der Wartung von (elektronischer) Sicherheitstechnik zu beachtenden rechtlichen Grundlagen, wobei hier das Arbeitsrecht, die DSGVO samt Datenschutzrecht und die rechtliche Bewertung der in Kapitel 3 vorgestellten Systeme die Kernthemen bilden.

Im Kapitel 5 (Compliancemaßnahmen für unternehmensinterne Regelwerke und Verträge) werden die Verwendung und der Nutzen verschiedenster Verträge und unternehmensinterner Regelwerke genauer betrachtet und mittels eines anschaulichen Beispiels die Möglichkeit der Haftungsfreizeichnung im Vertragsrecht erklärt. Dabei stehen insbesondere die Gewährleistung, die Produkthaftung und der Schadenersatz im Mittelpunkt.

Schließlich wird in Kapitel 6 (Beispielverträge) anhand von Beispielverträgen und -vereinbarungen gezeigt, welche konkreten Möglichkeiten es für ein Unternehmen gibt, beim Einsatz oder der Wartung von Sicherheitstechnik Compliancemaßnahmen zu setzen. Dabei besteht kein Anspruch auf Vollständigkeit. Diese Verträge können einerseits Musterverträge von Juristen – wie das Beispiel einer Vereinbarung über eine Auftragsverarbeitung oder das Muster einer Rahmenbetriebsvereinbarung – und andererseits selbst entwickelte Verträge – wie ein Beispiel-SLA – sein.

Die Arbeit endet mit einer Zusammenfassung der Ergebnisse gefolgt von einem Ausblick.

1.3. Problemstellung

Im Normalfall werden in der elektronischen Sicherheitstechnik die Anlagen vor der Übergabe an den/die Nutzer/in zwar korrekt installiert und programmiert, jedoch werden bei der weiteren Betreuung dieser Systeme meist Kosten eingespart, wodurch die Systeme viele Jahre ohne Wartung oder Updates in Betrieb sind. Durch das fehlende Patch-, Identitäts-, oder Netzwerkmanagement sinkt die Sicherheit in Bezug auf IT-Security und Informationssicherheit daher stetig. Dies birgt unter anderem die Gefahr, dass bei Nichtkonformität der im Mai 2018 in Kraft getretenen DSGVO, welche das österreichische Datenschutzgesetz verschärft, hohe Strafen auf Unternehmen zukommen.

Gerade im Gesundheits- und Cloudbereich wurde die neue Datenschutzgrundverordnung bereits ausführlich behandelt. [8] [9] [10] Eine Forschungslücke gibt es jedoch im Bereich der Anforderungen an Unternehmen im Sicherheitstechnikbereich. Einzig die datenschutzrechtlichen Anforderungen an Videoüberwachungssysteme wurden bereits mehrfach aufgegriffen. [11] [12]

Zudem existiert zwar eine Diplomarbeit, welche die Überwachung der Mitarbeiter am Arbeitsplatz samt zu beachtender, arbeitsrechtlicher Vorgaben behandelt [13], eine gesamtheitliche Abhandlung, welche die Funktionsweise von wichtigen sicherheitstechnischen Systemen umfasst und auf die anzuwendenden Gesetze und Normen fokussiert ist, konnte jedoch nicht gefunden werden.

1.4. Forschungsfragen

Aus der zuvor beschriebenen Problemstellung ergeben sich die folgenden Forschungsfragen, welche mittels dieser Arbeit beantwortet werden sollen:

- Welche gesetzlichen Grundlagen sind beim Vertrieb oder dem Einsatz von Sicherheitstechnik zu beachten?
- Wie müssen AGBs und Verträge gestaltet sein, damit die rechtlichen Rahmenbedingungen eingehalten werden?
- Was ist im Fall eines Datendiebstahls durch kompromittierte Systeme zu tun? Und wer haftet für Schäden innerhalb der gesetzlichen Gewährleistung, wenn die Systeme kompromittiert wurden?

1.5. Methodik

Für die Beantwortung der Forschungsfragen wird zunächst eine theoretische Analyse der vorhandenen Literatur durchgeführt, welche Fachliteratur (wie Fachzeitschriften oder Fachbücher), Gesetzestexte und aktuelle Internetquellen (wie Zeitungsartikel oder Zeitschriftenartikel), miteinbezieht. Die Recherche umfasst die wichtigsten Bereiche der elektronischen und mechanischen Sicherheitstechnik zum einen und den Anwendungsbereich sowie die wesentlichsten Inhalte der Datenschutzgrundverordnung und des Arbeitsrechts zum anderen. Zudem werden weitere relevante unternehmensinterne und unternehmensexterne Gesetze sowie Normen, die den Bereich der Sicherheitstechnik betreffen, behandelt und anhand von Musterverträgen anschaulich gemacht.

Die Identifikation der relevanten gesetzlichen Grundlagen entspricht Punkt 1 des COBIT ME3 Schemas. Für eine erfolgreiche Compliance im Bereich der Sicherheitstechnik müssen anschließend die weiteren Punkte, die in Kapitel 1.1.3 erklärt wurden, angewendet werden.

2. Begriffsdefinitionen und Abkürzungsverzeichnis

ABGB – Allgemeines bürgerliches Gesetzbuch

AGB – Allgemeine Geschäftsbedingungen

ArbVG – Arbeitsverfassungsgesetz

BSI – Bundesamt für Sicherheit in der Informationstechnik

c't – Magazin für Computer und Technik

COBIT – Control Objectives for Information and Related Technology; Framework zur IT-Governance

DIN – Deutsches Institut für Normung

DSG 2000 – Datenschutzgesetz 2000

DSB – Datenschutzbehörde

DSGVO – Datenschutz-Grundverordnung

EMRK – Europäische Menschenrechtskonvention

EN – Europäische Norm

GPS – Global Positioning System

GPA-djp – Gewerkschaft der Privatangestellten, Druck, Journalismus, Papier

IKT – Informations- und Kommunikationstechnik

ISACA – Information Systems Audit and Control Association

IEC – Internationale Elektrotechnische Kommission

ISO – Internationale Organisation für Normung

KSchG – Konsumentenschutzgesetz

OGH – Oberster Gerichtshof

ÖNORM – Nationale österreichische Norm

OVE – Österreichischer Verband für Elektrotechnik

SLA – Service Level Agreement

StGB – Strafgesetzbuch

StGG – Staatsgrundgesetz

TKG – Telekommunikationsgesetz 2003

UrhG – Urheberrechtsgesetz

UN-Kaufrecht – Übereinkommen der Vereinten Nationen über Verträge über den internationalen Warenkauf

VdS – Vertrauen durch Sicherheit (Institution für Unternehmenssicherheit)

VOI – Verband Organisations- und Informationssysteme e.V.

WKO – Wirtschaftskammer Österreich

3. Einführung in die Sicherheitstechnik

Die Sicherung eines Gebäudes und der dazugehörigen Freifläche ist sowohl für Unternehmen als auch für Privatpersonen wichtig, um unbefugten Zutritt zu verhindern oder gegen Gefahren, wie Rauch oder Wasser, geschützt zu sein. Verstärkt der Einsatz von Sicherheitstechnik bei privaten Haushalten eher das subjektive Sicherheitsgefühl, so ist in Unternehmen der Einsatz ebendieser oftmals vorgeschrieben. [14]

Das nachfolgende Kapitel 3 gibt somit zunächst einen allgemeinen Überblick über die Einsatzmöglichkeiten von Sicherheitstechnik und beschreibt anschließend die technischen Grundlagen der jeweiligen Systeme sowie deren Einsatzgründe.

3.1. Konventionelle Gründe für den Einsatz von Sicherheitstechnik

Betrachtet man die polizeiliche Kriminalstatistik zwischen 2008 und 2017 so zeigt sich, dass die Zahl der angezeigten Wohnraumeinbrüche mit 11802 im Jahr 2017 den niedrigsten Wert der letzten zehn Jahre aufweist und seit 2014 stetig sinkt. Dies hat nicht zuletzt mit den richtigen Präventionsmaßnahmen und gutem Eigenschutz der Bevölkerung zu tun; blieb es im Jahr 2017 doch bei knapp 44 Prozent aller Wohnraumeinbruchsdelikte in Österreich bei dem Versuch. [15]

Während in Einfamilienhäusern meist die Fenster, die Fenstertüren oder die Haustüren im Erdgeschoss aufgehebelt werden, verschaffen sich Einbrecher/innen in Mehrfamilienhäusern vermehrt Zutritt über die Wohnungstüren, wobei es keine Rolle spielt, um welches Stockwerk es sich handelt. In Wohnungen oder Einfamilienhäusern wird zudem meist in den Wintermonaten in der Dämmerung eingebrochen, da eine Anwesenheit der Bewohner/innen aufgrund der Lichtverhältnisse leichter festzustellen ist. Gewerbeobjekte sind hingegen zum größten Teil nachts oder am Wochenende gefährdet sind, da Einbrecher/innen bei Nichtvorhandensein von Wachpersonal oder einer automatischen Alarmeinrichtung oftmals bis zum nächsten Tag Zeit haben. Auch bei Gewerbeobjekten werden überwiegend Türen oder Fenster im Erdgeschoss aufgebrochen. Lohnende Objekte sind hierbei Arztpraxen, Boutiquen oder Elektromärke. [16]

Da die meisten Einbrecher/innen Gelegenheitstäter/innen sind und mit einfachen Hilfsmitteln unter hohem Zeitdruck arbeiten, wirken geeignete mechanische und elektronische Sicherungen oft abschreckend. Zudem wird durch den Einsatz der genannten Sicherungen der Einbruchsversuch verlangsamt, was meist zur Folge hat, dass Einbrecher/innen nach einigen Minuten von ihrem Vorhaben ablassen. [17]

Beispiele für geeignete Sicherungen sind gut sichtbare Alarmanlagen und einbruchhemmende Fenster mit mehreren Pilzkopfzapfen, sowie Sicherheitstüren, die mit einem Türschloss mit Mehrpunktverriegelung und Zusatzschlössern ausgestattet sind. Auch Videoüberwachungsanlagen, Bewegungsmelder und Glasbruchmelder, sowie der Einsatz von Alarmweiterverfolgungssystemen, welche einerseits einen Alarm auslösen und andererseits eine externe Alarmempfangsstelle kontaktieren, können helfen, die Wahrscheinlichkeit eines erfolgreichen Einbruches signifikant zu verringern und die Aufklärungsquote zu erhöhen. [17]

Auch wenn die unbefugte Person bereits Zugang zu dem Gebäude erlangt hat, gibt es weitere Möglichkeiten, wertvolle Gegenstände oder Daten mit Hilfe von Wertbehältnissen zu sichern. Erwähnenswert sind hierbei Datensicherungsschränke, Wertschutzschränke oder Möbeltresore, deren Einsatz ebenfalls unter den Begriff der Sicherheitstechnik fällt. [16]

Weitere Einsatzmöglichkeiten für die Sicherheitstechnik sind Gefahrenwarnanlagen, die beispielsweise dazu dienen, Feuer rechtzeitig zu bemerken, Wasseraustritt zu erkennen oder vor Gaslecks zu warnen. [17] Der Einsatz von Zutrittskontrollsystemen oder Videoüberwachung kann ferner helfen, den Zugang zu Geschäfts- oder Privaträumen zu protokollieren oder zu schützen. [13]

3.2. Gründe für den Einsatz von Sicherheitstechnik in Bezug auf die DSGVO

Betrifft der Diebstahl keine Privatperson, sondern ein Unternehmen, können zusätzlich zu dem Wert der gestohlenen Gegenstände und den Kosten für die Wiederherstellung des Normalbetriebs – samt Beseitigung etwaiger Einbruchsspuren – weitere Probleme auf das Unternehmen zukommen. Wurden beispielsweise Laptops oder Smartphones mit sensiblen Kundendaten gestohlen, ergibt sich zusätzlich zum Vermögensschaden potentiell ein starker Reputationsverlust. Zudem haben Unternehmer nach dem Datenschutzgesetz und der neuen DSGVO für die Sicherheit von Kundendaten zu sorgen und sind bei einem Datenverlust somit einerseits haftbar und müssen andererseits die betroffenen Personen über den Datenverlust informieren. [18]

Für den Schutz von Daten mittels technischer oder organisatorischer Maßnahmen können zudem gemäß Art. 38 DSGVO beispielsweise bauliche Maßnahmen eingesetzt werden, welche Zutrittskontrollanlagen, Videoüberwachungssysteme oder Einbruchmeldeanlagen inkludieren. [19]

3.3. Definition Sicherheitstechnik

Der Begriff der Sicherheitstechnik kann wie folgt definiert werden:

> *„‘Sicherheitstechnik‘ bezeichnet alle technischen und elektronischen Vorrichtungen, die der Sicherheit von Personen und Gütern dienen. Sicherheitstechnik beugt einerseits Risiken vor, etwa durch das Vorhandensein von Alarmanlagen oder Videoüberwachung. Andererseits melden diese Vorrichtungen Gefahrensituationen, beispielsweise einen Brand oder einen unerlaubten Zutritt zu einem Raum.“ [14]:*

Oder anders gesagt:

> *„Unter Sicherheitstechnik werden vorrangig Maßnahmen verstanden, welche die Verbesserung der Sicherheit von Gebäuden gewährleisten, die auf haustechnischen Maßnahmen beruhen um physische Sicherheit und körperliche Unversehrtheit der Nutzer zu erreichen.“ [20]*

Wie man der Definition entnehmen kann, ist Sicherheitstechnik ein breit gefächerter Begriff, welcher sich grob in zwei Arten – die elektronische und die mechanische Sicherheitstechnik – unterteilen lässt, die auch miteinander kombiniert werden können und sollen. Zudem gibt es noch die Möglichkeit der personellen Bewachung eines Gebäudes [16], die in dieser Arbeit allerdings nicht weiter behandelt wird.

3.4. Unternehmensexterne Regelwerke in der Sicherheitstechnik

Im Folgenden werden einige der identifizierten anzuwendenden, unternehmensexternen Regelwerke, welche die mechanische und elektronische Sicherheitstechnik betreffen, kurz erklärt und übersichtlich dargestellt. Um die Übersichtlichkeit zu wahren, beschränkt sich diese Arbeit auf Normen der ÖNORM und DIN sowie Richtlinien von OVE. Zudem wurde das BSI IT-Grundschutz-Kompendium der Vollständigkeit halber kurz erwähnt. Weitere Normen, Standards und Richtlinien, wie VdS oder ISO/IEC wurden aus Platzgründen nicht inkludiert, sind aber bei einer vollständigen Compliance-Strategie natürlich ebenso in Betracht zu ziehen.

3.4.1. Definition und Anwendungsbereich von Standards, Normen und Richtlinien

Standards sind als Oberbegriff von Richtlinien sowie Normen zu sehen [21] und werden von Austrian Standards wie folgt definiert:

> *„Standards (z. B. ÖNORMEN und ISO-Standards) sind von Fachleuten entwickelte Empfehlungen. Sie sind Lösungen für konkrete Anwendungsfälle und branchenübergreifende Herausforderungen der Wirtschaft und des öffentlichen Bereichs. Als aktuelles und anerkanntes Praxiswissen stellen Standards sicher, dass eins zum anderen passt und unser modernes Leben täglich funktioniert.“ [22]*

Klotz [21, p. 10] hingegen definiert Standards als „ein Regelwerk, das beschreibt, wie etwas zu tun, zu lösen oder handzuhaben ist“ und dabei „breit akzeptiert und angewendet werden kann“ und wird.

Normen beschreiben nach VOI (zitiert nach [21, p. 10]) „wissenschaftlich begründete Arbeitsmethoden zur Bewältigung rationeller, meist wiederholbarer Arbeitsprozesse … bzw. Qualitäts- und Sicherheitsanforderungen“. Richtlinien schließlich stellen generelle Empfehlungen dar, um einen Prozess durchzuführen oder Probleme zu lösen. [2]

Der Unterschied zwischen Normen und Richtlinien auf der einen und Standards auf der anderen Seite ist nun, dass eine Norm oder eine Richtlinie ein Standard ist, „der von einer offiziellen Normungsorganisation als Ergebnis eines systematischen, festgelegten Normungsverfahrens beschlossen und veröffentlicht wurde“. [21, p. 10]

Erwähnenswert ist hierbei, dass Standards, Normen oder Richtlinien in Normalfall keine rechtliche Verbindlichkeit haben, außer „sie werden vertraglich vereinbart oder der Gesetzgeber erklärt sie für verbindlich“. [22] Sie können aber sehr wohl von Gutachtern oder vor Gericht herangezogen werde, „um festzustellen, ob Sorgfaltspflichten eingehalten wurden“. [21, p. 11]

Leider ist der Zugang zu Normen und Richtlinien meist kostenpflichtig.

3.4.2. Normen der mechanischen Sicherheitstechnik

Die Normen DIN EN 1627-1630 und die ergänzenden Bestimmungen in der ÖNORM B 5338 betreffen einbruchhemmende Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse, während sich die ÖNORM B 5351 mit einbruchhemmenden Baubeschlägen, wie Schlössern, Schließblechen, Schutzbeschlägen, Schließzylindern und Nachrüstprodukten für Fenster und Türen befasst. [23]

In weiterer Folge werden die DIN und ÖNORMEN, die in der mechanischen Sicherheitstechnik angewendet werden können und sollten, kurz übersichtlich dargestellt.

- **DIN EN 1627:2011 09**
  Diese Norm definiert die Anforderungen an und Klassifizierungen „für einbruchhemmende Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse“. [24]

- **DIN EN 1628:2016 03**
  Diese Norm definiert die „Prüfverfahren für die Ermittlung der Widerstandsfähigkeit für einbruchhemmende Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse unter statischer Belastung“. [25]

- **DIN EN 1629:2016 03**
  Diese Norm definiert die „Prüfverfahren für die Ermittlung der Widerstandsfähigkeit für einbruchhemmende Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse unter dynamischer Belastung“. [26]

- **DIN EN 1630:2016 03**
  Diese Norm definiert die „Prüfverfahren für die Ermittlung der Widerstandsfähigkeit für einbruchhemmende Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse gegen manuelle Einbruchversuche“. [27]

- **ÖNORM B 5338:2011 08 01**
  Diese ÖNORM gilt für einbruchhemmende Türen, Fenster und zusätzliche Abschlüsse. Die anzuwendenden Prüfmethoden sind den Normen EN 1627 bis EN 1630 zu entnehmen. [28]

- **ÖNORM B 5351: 2011 08 01**
  Diese ÖNORM betrifft die Ausführung, Prüfung und Kennzeichnung von Elementen, die in einbruchhemmende Türen verbaut oder für deren Nachrüstung verwendet werden. [29]

3.4.3. Normen und Richtlinien die Einbruch- und Überfallmeldeanlagen betreffend

Die ÖNORMEN 50130 bis 50134 sowie 50136 betreffen Anforderungen an Einbruch- und Überfallmeldeanlagen sowie dazugehörige Komponenten. Zudem werden in der Richtlinie OVE-R2 verschiedene Sicherheitsklassen definiert. [30]

In weiterer Folge werden die ÖNORMEN und OVE-Richtlinien, die bei Einbruch- und Überfallmeldeanlagen angewendet werden können und sollten, kurz übersichtlich dargestellt.

Normen

- **ÖNORM 50130 Teil 4 und 5**
  Diese ÖNORM regelt die Errichtung von Alarmanlagen. [30]

- **ÖNORM 50131 Teil 1, 2 und 6**
  Diese ÖNORM legt Anforderungen an Einbruch- und Überfallmeldeanlagen fest. [30]

- **ÖNORM 50132 Teil 2, 4, 5 und 7**
  Diese ÖNORM definiert Mindestanforderungen für Überwachungsanlagen für Sicherheitsanwendungen. [30]

- **ÖNORM 50133 Teil 1, 2 und 7**
  Diese ÖNORM definiert Mindestanforderungen für Zutrittskontrollanlagen für Sicherheitsanwendungen. [30]

- **ÖNORM 50134 Teil 2, 3 und 7**
  Diese ÖNORM behandelt Personen-Hilferufanlagen. [30]

- **ÖNORM 50136 Teil 1, 2, 4 und 7**
  Diese ÖNORM legt Anforderungen an Leistungsmerkmale, Zuverlässigkeit und Sicherheitsmerkmale von Alarmübertragungsanlagen fest. [30]

Richtlinie OVE R2

Die Richtlinie OVE R2 behandelt unter anderem die notwendigen Voraussetzungen für die Planung und Errichtung von Einbruch- und Überfallmeldeanlagen und teilt diese in fünf Klassen ein [31]:

- PS: Privat/Standard
- GS-N: Gewerbestandard-Nieder
- GS-H: Gewerbestandard-Hoch
- WS: Werteschutz
- HS: Hochsicherheit
- Zusatzschutz Überfall

Während Alarmanlagen der Klasse PS nur über einen geringen Schutz gegen Manipulationsversuche im scharfgeschalteten Zustand verfügen und daher nur im privaten Haushalt oder in Familienbetrieben ohne besondere Wertgegenstände eingesetzt werden dürfen, verfügen die Klassen GS-N und GS-H über einen mittleren Manipulationsschutz und dürfen daher in Handels-, Gewerbe- oder Produktionsbetrieben mit geringem oder mittleren Risiko eingesetzt werden. In den zuvor genannten Klassen wird von einem Einbrecher ohne besondere Kenntnisse oder Werkzeuge ausgegangen. Die Klassen WS und HS gehen von einem gut organisierten Einbrecher aus, der über höhere Kenntnisse Einbruchmeldeanlagen betreffend verfügt und ausreichend passendes Werkzeug besitzt. Die Klasse WS wird bei Haushalten oder Gewerbebetrieben eingesetzt, die Gegenstände mit hohem Wert verwahren, während die Klasse HS für Hochsicherheitsanlagen konzipiert ist. Der Zusatzschutz Überfall entspricht der Schutzklasse GS, ist aber zusätzlich mit einem spezifischen Überfallschutz und Überfallmeldern ausgestattet und daher insbesondere als Mindeststandard für Geschäfte empfohlen. [30]

3.4.4. Normen und Richtlinien elektronische Zutrittskontrollanlagen betreffend

Die ÖNORMEN 50133 und 60839 betreffen Anforderungen an elektronische Zutrittskontrollanlagen. Weitere relevante Anforderungen sind die in dem Kapitel 3.4.2 für mechanische Sicherheitstechnik definierten Normen für einbruchhemmende Türen und Fenster. Zudem werden in der Richtlinie OVE-R10 verschiedene Mindestvoraussetzungen und Sicherheitsklassen für die Errichtung von Zutrittskontrollanlagen definiert. [32]

In weiterer Folge werden die ÖNORMEN und OVE-Richtlinien, die bei elektronischen Zutrittskontrollanlagen angewendet werden können und sollten, kurz übersichtlich dargestellt.

Normen

- **ÖNORM 50133 Teil 1,2 und 7**
  Diese ÖNORM definiert Mindestanforderungen für Zutrittskontrollanlagen für Sicherheitsanwendungen. [32]

- **ÖNORM 60839-11-1 und 60839-11-2**
  Diese ÖNORM definiert Anforderungen und Anwendungsregeln für elektronische Zutrittskontrollanlagen. [32]

Richtlinie OVE R10

Die Richtlinie OVE R10 behandelt unter anderem die notwendigen Mindestvoraussetzungen für die Planung und Errichtung von Zutrittskontrollanlagen. Die Risikoklassen sind – wie bei Alarmanlagen – PS, GS-N, GS-H, WS und HS und werden hier daher nicht mehr gesondert behandelt. [33]

3.4.5. Normen und Richtlinien Videoüberwachungsanlagen betreffend

Die ÖNORMEN 50132 und 62676 betreffen Anforderungen an Videoüberwachungsanlagen. Zudem werden in der Richtlinie OVE-R2 verschiedene Mindestvoraussetzungen an CCTV-Überwachungsanlagen definiert.

In weiterer Folge werden die ÖNORMEN und OVE-Richtlinien, die bei Videoüberwachungsanlagen angewendet werden können und sollten, kurz übersichtlich dargestellt.

Normen

- **ÖNORM 50132 Teil 2, 4, 5 und 7**
  Diese ÖNORM definiert Mindestanforderungen für Überwachungsanlagen für Sicherheitsanwendungen. [30]

- **ÖNORM EN 62676-4**
  Diese ÖNORM definiert Anwendungsregeln für Videoüberwachungsanlagen und unterteilt Objekte in verschiedene Klassen. [34]

Richtlinie OVE R9

Die Richtlinie OVE R9 behandelt unter anderem die notwendigen Mindestvoraussetzungen für die Planung und Errichtung von CCTV-Überwachungsanlagen für Sicherungsanwendungen. [31]

3.4.6. Exkurs – BSI IT-Grundschutz

Der Vollständigkeit halber sei erwähnt, dass das BSI in dem IT-Grundschutz-Kompendium eine Vielzahl von Bausteinen festgelegt hat, welche „standardisierte Sicherheitsanforderungen für typische Geschäftsprozesse, Anwendungen und IT-Systeme“ beschreiben und zur Erhöhung der Informationssicherheit in Unternehmen beitragen sollen. [60] Ein Vorteil des Bausteinprinzips ist, dass für die jeweiligen Bausteine bereits eine Risikoanalyse durchgeführt wurde und es daher möglich ist, die Anforderungen mittels eines Soll-Ist-Vergleiches einfach zu detektieren und umzusetzen. Außerdem werden in jedem Baustein bereits die Personen definiert, die die Anforderungen idealerweise umsetzen sollten. Nach der Erfüllung der Basis- und Standardanforderungen des jeweiligen Bereiches ist zudem eine Zertifizierung nach ISO 27001 möglich. [35]

Um die Wirksamkeit eines Sicherheitssystems zu gewährleisten, ist es sehr wichtig, dass dieses durch ein strukturiertes Sicherheitskonzept geschützt wird und nicht einfach umgangen werden kann. [36] Ein strukturiertes Sicherheitskonzept umfasst lt. BSI insbesondere Integrität, Vertraulichkeit, welche lt. dem Glossar des BSI Grundschutzhandbuches wie folgt definiert werden können [37]:

- **Integrität**
  „Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf ‚Daten‘ angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. […]“

- **Vertraulichkeit**
  „Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein."

- **Verfügbarkeit**
  „Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können."

Die Basisanforderungen des IT-Grundschutz-Kompendiums – welche vorrangig umgesetzt werden müssen – schreiben daher für Rechenzentren und Serverräume (INF.2) den Einsatz einer Zutrittskontrolle (INF.2.A6) sowie einer Brandmeldeanlage (INF.2.A8) als Muss-Kriterium vor. [35]

In den als Soll-Kriterium definierten Standard-Anforderungen ist vorgeschrieben, dass eine adäquate Gefahrenmeldeanlage (INF.2.A13) sowie ein umfangreicher Perimeterschutz (INF.2.A12), inklusive Personenidentifikation und Umzäunung installiert und umgesetzt werden sollte. [35]

Weiters gibt es bei besonderem Schutzbedarf die Möglichkeit, die vorhandenen Zutritts- und Einbruchmeldeanlagen durch Videoüberwachungsanlagen (INF.2.A24) zum Schutz der Integrität und Verfügbarkeit zu ergänzen. [35]

3.5. Mechanische Sicherheitstechnik

Das nächste Unterkapitel behandelt den Stand der Technik sowie etwaige Normen und Sicherheitsklassen, welche Türen, Fenster samt Verglasungen, Industrietore, Vergitterungen und Rolläden betreffen. [16]

Der Vollständigkeit halber sei erwähnt, dass die mechanische Sicherheitstechnik eine Voraussetzung für die erfolgreiche Anwendung der elektronischen Sicherheitstechnik darstellt. Beispielsweise ist die beste elektronische Zutrittskontrolle wertlos, wenn die zu sichernde Türe einfach aufgehebelt oder das Fenster durchbrochen werden kann. Daher ist eine Befolgung der Normen und der Einsatz der mechanischen Sicherheitstechnik gemäß dem aktuellen Stand der Technik in Bezug auf Beweispflichten unbedingt erforderlich.

3.5.1. Türen

Eine einbruchhemmende Tür zeichnet sich durch „verstärkte Rahmenbauteile, spezielle Beschläge und einbruchhemmende Verglasungen“ aus [23] und kann wie folgt definiert werden:

> *„Eine Tür weist einbruchhemmende Wirkung auf, wenn sie die Eigenschaft hat, eine bestimmte Zeit (Widerstandszeit, Widerstandswert) dem Versuch zu widerstehen, sich unter Einsatz von körperlicher Gewalt und unter Zuhilfenahme von Werkzeugen gewaltsam Zutritt zu dem geschützten Raum oder Bereich zu schaffen (EN 1627:2011).“ [38]*

Die europäischen Normen EN 1627-1630, die 1999 eingeführt und 2011 das letzte Mal überarbeitet wurden, definieren Anforderungen beziehungsweise Prüfverfahren, um die Einbruchsicherheit einer Tür festzustellen. [38] In Österreich sollten einbruchhemmende Türen nach der ÖNORM B 5338 zertifiziert sein, welche eine nationale Erweiterung zu den europäischen Normen darstellt. [39]

Die Widerstandsfähigkeit einer einbruchhemmenden Tür wird in der EN 1627:2011 mittels sechs Widerstandsklassen definiert, wobei RC 1 die geringste und RC 6 die höchste Widerstandsklasse darstellt. Das Sicherheitsniveau steigt bei den einzelnen Widerstandsklassen exponentiell an. Während die Widerstandsklassen RC 1, RC 2 und RC 3 gegen Gelegenheitstäter schützen und daher ein geringes Sicherheitsniveau aufweisen, schützen die Widerstandsklassen RC 4, RC 5 und RC 6 gegen professionell vorgehende Täter. [38]

Es wird empfohlen, mindestens eine einbruchhemmende Tür der Widerstandsklasse 2, welche nach ÖNORM B 5338 zertifiziert ist, von Fachpersonal montieren zu lassen, da die Sicherheit der Türen ab dieser Sicherheitsklasse mit einem Werkzeugsatz geprüft wird. [23]

Prinzipiell wird die Einbruchsicherheit einer Tür mittels dreier Schritte sichergestellt – zunächst erfolgt eine statische Prüfung nach EN 1628, danach eine dynamische Prüfung nach EN 1629 und schließlich ein manueller Einbruchversuch mit Hilfe von verschiedenen Werkzeugen, welcher in EN 1630 genauer definiert ist. In der nachfolgenden Tabelle 1 sind die verschiedenen Widerstandsklassen samt Täterprofil übersichtlich dargestellt. [38]

Widerstands-klassen nach DIN EN 1627	Werkzeugsatz	Einbrecher/in	Widerstandszeit/ Gesamtprüfzeit
RC 1 N	A1	Gelegenheitseinbrecher/in ohne Kenntnis über die Tür, setzt körperliche Gewalt ein.	Keine manuelle Einbruchprüfung
RC 2 N / RC 2	A2 Verwendet einfache Werkzeuge wie Schraubendreher, Zange und Keil (In der RC2N gibt es im Gegensatz zur RC2 keine Anforderungen an die Verglasung)	Gelegenheitseinbrecher/in mit geringer Kenntnis über die Tür, setzt einfaches Werkzeug ein.	3 Min. / 15 Min.
RC 3	A3 Verwendet zusätzlich Werkzeuge wie Brecheisen, mechanische Bohrer, kleinen Hammer, weitere Schraubendreher und Splinttreiber	Gelegenheitseinbrecher/in mit etwas Kenntnis über die Tür, setzt zusätzlich Hebelwerkzeug ein.	5 Min. / 20 Min.
RC 4	A4 Verwendet zusätzlich Werkzeuge wie einen 1,25 kg Hammer, Äxte, Bolzenschneider und Akkubohrer	Erfahrene/r Einbrecher/in, setzt zusätzlich Schlagwerkzeug ein.	10 Min. / 30 Min.
RC 5	A5 Verwendet zusätzlich Werkzeuge wie Loch- und Stichsäge, eine elektrische Bohrmaschine und einen Winkelschleifer mit einer Scheibe von max. 125 mm DM.	Sehr erfahrene/r, gut organisierte/r Einbrecher/in mit elektrischem Werkzeug.	15 Min. / 40 Min.
RC 6	A6 Verwendet zusätzlich Werkzeuge wie Spalthämmer und leistungsstarke Elektrowerkzeuge, wie einen Winkelschleifer mit einer Scheibe von max. 230 mm DM und Bohrer.	Sehr erfahrene/r, gut organisierte/r Einbrecher/in mit elektrischem Werkzeug.	20 Min. / 40 Min.

Tabelle 1: Beschreibung der Widerstandsklassen nach EN 1627 nach [38]

Zudem besteht die Möglichkeit, die einbruchhemmende Wirkung bestehender Türen nachträglich durch die Montage von Baubeschlägen zu erhöhen. In Österreich werden die einbruchhemmenden Baubeschläge in der ÖNORM 5351 genauer definiert. Die wichtigsten Schutzziele sind hierbei „Schutz gegen Anbohren, Abreißen, Abschlagen sowie Schutz gegen Zurückdrücken der Verriegelung“. [40]

Wieser [23] empfiehlt hierzu folgende Produkte samt anzuwendender Normen:

- „Einbruchhemmendes Einsteckschloss oder Mehrfachverriegelung, geprüft gemäß ÖNORM B 5351“ [23]
- „Einbruchhemmende Schutzbeschläge geprüft gemäß ÖNORM B 5351 oder DIN 18257“ [23]
- „Einbruchhemmende Schließzylinder geprüft gemäß ÖNORM B 5351 oder DIN 18252 in Verbindung mit einem Schutzbeschlag (Zylinder soll max. 3 mm über Schutzbeschlag vorstehen)“ [23]
- „Zusatzkastenschlösser geprüft gemäß ÖNORM B 5351“ [23]
- „Panzerriegelschlösser (Querbalken oder Längsbalkenschlösser) geprüft gemäß ÖNORM B 5351 oder DIN 18104-1“ [23]

3.5.2. Fenster

Einbruchhemmende Fenster zeichnen sich – ebenso wie einbruchhemmende Türen – dadurch aus, dass sie „über verstärkte Rahmenbauteile, spezielle Beschläge und einbruchhemmende Verglasungen“ verfügen [23] und wie folgt definiert werden können:

> *„‘Einbruchhemmung ist die Eigenschaft eines Fensters (Türe, Vorhangfassade, Gitter oder Abschluss) dem Versuch, sich gewaltsam Zutritt in den zu schützenden Raum oder Bereich zu verschaffen, Widerstand zu leisten‘ (DIN EN 1627). Einbruchhemmende Fenster sind also Bauteile, die neben den üblichen Funktionsaufgaben Einbruchsversuchen einen definierten Widerstand entgegensetzen.“ [38]*

Auch für einbruchhemmende Fenster gilt, dass diese nach ÖNORM B 5338 bzw. EN 1627-1630 geprüft sowie zertifiziert sein müssen. Ebenso gelten die Widerstandsklassen RC1 bis RC6, welche bereits im Unterkapitel 3.5.1 Türen definiert wurden, auch für Fenster. Es ist daher empfehlenswert, Fenster einzubauen, die mindestens die Widerstandsklasse RC2 aufweisen. [41]

Zusätzlich zu der Widerstandsfähigkeit der Rahmen und Beschläge werden bei einbruchhemmenden Fenstern auch Anforderungen an die Verglasungen nach EN 356 gestellt. In den Widerstandsklassen RC1N und RC2N werden die Anforderungen nicht europaweit vorgegeben, können aber national hinzugefügt werden – das N steht hierbei in Österreich für Normalglas. [41]

In der nachfolgenden Tabelle 2 werden die Widerstandsklassen samt der Prüfkriterien für das Glas noch einmal übersichtlich dargestellt. [26]

WK	Verglasung nach EN 356	Widerstandszeit	Prüfkriterien Glas	Eigenschaft Glas
RC1N	Float	Keine	Keine	Normalglas
RC2N	Float	3 Min.	Keine	Normalglas
RC2	P4A 1.52 PVB-Folie Typ BG R15	3 Min.	Fallhöhe der 4.11 kg Stahlkugel: 9 Meter (3 Treffer)	durchwurf-hemmend
RC3	P5A 2.28 PVB-Folie Typ BG R15	5 Min.	Fallhöhe der 4.11 kg Stahlkugel: 9 Meter (9 Treffer)	durchwurf-hemmend
RC4	P6B	10 Min.	Axtschläge: mindestens 30 Schläge	durchbruch-hemmend
RC5	P7B	15 Min.	Axtschläge: mehr als 50 Schläge	durchbruch-hemmend
RC6	P8B	20 Min,	Axtschläge: mehr als 70 Schläge	durchbruch-hemmend

Tabelle 2: Beschreibung der Widerstandsklassen für Fensterverglasungen nach [42]

Zudem besteht die Möglichkeit, die einbruchhemmende Wirkung bestehender Fenster und Terassentüren nachträglich durch die Montage von Baubeschlägen zu erhöhen. Wieser [23] empfiehlt hierzu folgende Produkte samt anzuwendender Normen:

- „Aufschraubbare Fenstersicherungen (z.B. Stangenschloss, Fenstergriff mit Sperrriegel) geprüft gemäß ÖNORM B 5351 oder DIN 18104-1“ [23]
- „Scharnierseitensicherungen geprüft gemäß ÖNORM B 5351 oder DIN 18104-1“ [23]
- „Absperrbare Fenstergriffe“ [23]
- „Im Falz eingelassene Pilzzapfenverriegelungssysteme geprüft gemäß ÖNORM B 5351 oder DIN 18104-2“ [23]
- „Einbruchhemmende Schließzylinder geprüft gemäß ÖNORM B 5351 oder DIN 18252 in Verbindung mit einem Schutzbeschlag (Zylinder soll max. 3 mm über Schutzbeschlag vorstehen)“ [23]

3.5.3. Tore, Vergitterungen und Rolläden

Da auch für Tore, Vergitterungen und Rolläden ebenfalls die Anforderungen der EN 1627-1630 gelten, welche in den vorherigen Abschnitten bereits ausführlich behandelt wurden, werden diese in diesem Kapitel nicht weiter ausgeführt. Der Vollständigkeit halber sei hier erwähnt, dass es bei den Vergitterungen eine Unterscheidung in fest- und freistehende Gitter gibt und dass man Rolläden in einbruchhemmende Rolläden, Rolläden mit Hochschiebesicherung und Rolläden mit innenliegender Sicherung unterteilen kann. [16]

3.6. Elektronische Sicherheitstechnik

Der Bedarf an elektronischer Sicherheitstechnik wächst jährlich, was nicht zuletzt an dem immer größer werdenden Interesse der Bevölkerung an vernetzen Systemen, wie beispielsweise Smart Home oder Smart Building, liegt. Betrachtet man den Umsatz der elektronischen Sicherheitstechnik im Jahr 2016 in Deutschland so zeigt sich, dass beispielsweise das Segment der Brandmeldetechnik einen Umsatzanstieg von 6,8 Prozent verzeichnen konnte und somit die 1,8 Milliarden Euro-Marke erreicht hat. Aber auch das Segment der Einbruchmeldetechnik konnte durch ein Plus von 8,0 Prozent auf 800 Millionen Euro steigen und steht somit an zweiter Stelle. Vertreiber von Videoüberwachungstechnik konnten eine Umsatzsteigerung von 8,0 Prozent auf 511 Millionen Euro verzeichnen und auch die Zutrittssteuerungssysteme erfreuen sich mit einem Plus von 4,8 Prozent immer größerer Beliebtheit; der Umsatz in diesem Segment lag 2016 bei 307 Millionen Euro. [43]

Der Vorteil der elektronischen Sicherheitstechnik gegenüber der mechanischen ist, dass durch den Einsatz dieser Gefahren im Idealfall frühzeitig erkannt und automatisch ausgewertet werden können. Zudem können beispielsweise Zugangsberechtigungen verhältnismäßig einfach erteilt und entzogen werden und bleiben – je nach Art der Zugangskontrolle – auch bei Schlüsselverlust bestehen, da die Zugangsberechtigung für den verlorenen Schlüssel einfach gelöscht werden kann. [44]

Für einen Rundumschutz ist daher eine Ergänzung der mechanischen Sicherheitstechnik mit der elektronischen Sicherheitstechnik empfehlenswert. Die elektronische Sicherheitstechnik wird wie folgt definiert:

> *„Elektronische Sicherheitstechniken umfassen Sicherheitslösungen durch Videoüberwachung, elektronischen Alarmtechniken, (Video-) Türsprechsystemen und Gefahrenmeldern. Alles, was elektronisch zur Sicherheit von Personen, Gebäuden und Co eingesetzt wird, wird unter dem Begriff der elektronischen Sicherheitstechnik zusammengefasst.“ [45]*

Längst werden die sicherheitstechnischen Systeme nicht mehr getrennt betrachtet, viele Unternehmen kombinieren z.B. digitale oder biometrische Zutrittskontrollsysteme mit Alarmanlagen – auch Gefahrenmeldeanlagen (GMA) genannt – und setzen Videoüberwachungssysteme ein, um das subjektive Sicherheitsgefühl zu erhöhen und ihr Eigentum samt Kundendaten zu schützen.

Um den aktuellen Stand der Technik sowie etwaige Probleme in Bezug auf den Datenschutz oder das Arbeitsrecht verstehen zu können, beschreibt das nachfolgende Kapitel 3.6.1 kurz die Funktionsweise von Gefahrenmeldeanlagen, Zutrittskontrollsystemen und Videoüberwachungsanlagen. Anschließend werden anwendbare Normen aufgezeigt.

Die rechtlichen Rahmenbedingungen für den Einsatz und die Wartung solcher Systeme werden in den nachfolgenden Kapiteln 4 und 5 behandelt.

3.6.1. Gefahrenmeldeanlagen

Die erste elektro-magnetische Alarmanlage wurde 1853 von Augustus Russell Pope in Amerika patentiert. Die Funktionsweise war vergleichsweise simpel, da Türen und Fenster mittels einer Parallelschaltung so miteinander verbunden waren, dass beim Öffnen dieser ein Stromkreislauf geschlossen wurde, der elektromagnetische Schwingungen auf einen Hammer übertrug, welcher daraufhin auf eine Glocke schlug. Auch das erneute Schließen der Türen und Fenster konnte die Alarmanlage nicht deaktivieren, da eine Schaltfeder den Kontakt weiterhin unterbrochen hielt. [46]

Edwin Holmes kaufte daraufhin 1857 die Rechte an dieser Alarmanlage und begann, diese zu vermarkten. Er integrierte sie zudem in das New Yorker Telefonnetz und erfand somit das erste Alarmleitsystem. [46]

Die erste zentrale Notrufstelle wurde schließlich Ende der 1960er Jahre von Edward A. Calahan in New York erfunden, indem er New York in Distrikte unterteilte und für jeden Distrikt eine zentrale Notrufstelle einrichtete, welche im Falle eines Alarms einen Laufburschen aussendete, der so Hilfe holte. Gegen Ende des 20ten Jahrhunderts wurden schließlich Alarmanlagen mit Bewegungsmeldern kombiniert und die ersten Funkalarmanlagen kamen auf den Markt. [46]

Heutzutage werden Gefahrenmeldeanlagen dazu eingesetzt, Häuser und Flächen auf unbefugtes Eindringen zu überwachen und vor externen Einflüssen, wie Wasser oder Rauch, zu schützen. Kombiniert mit Videoüberwachung und Zutrittskontrolle bieten sie ein universales Sicherheitskonzept.

Arten von Gefahrenmeldeanlagen

Gefahrenmeldeanlagen werden eingesetzt, um beispielsweise austretendes Wasser oder Brände beziehungsweise einen Einbruch rechtzeitig erkennen zu können. Im Falle einer Gefahr geben sie meist einen lauten Signalton von sich, um gefährdete Personen zu informieren. Auch bei personeller Abwesenheit wird die Meldezentrale informiert, um die Gefahr rasch einzudämmen. [47]

Prinzipiell kann man Gefahrenmeldeanlagen in Brandmeldeanlagen, Einbruchmeldeanlagen und Überfallmeldeanlagen unterteilen.

- **Brandmeldeanlagen** erkennen mittels automatischer (wie Rauchmelder oder Gasmelder) oder manueller Melder Feuer oder Rauch frühzeitig und melden das Auftreten dieser an die Brandmeldezentrale. [48] Für die Planung, Errichtung, Änderung und Verwendung von Brandmeldeanlagen gilt die europäische Norm EN 54, welche in Österreich der ÖNORM EN 54 entspricht. [49]

- **Einbruchmeldeanlagen** überwachen im scharfgeschalteten Zustand Türen und Fenster auf deren unbefugte Öffnung mittels Öffnungsmeldern und detektieren Bewegungen innerhalb des überwachten Bereichs mittels Bewegungsmeldern. [16] Sie dienen aber nicht primär der Verhinderung von Einbrüchen, sondern sollen Gegenstände auf unbefugte Wegnahme sowie Flächen und Räume auf unbefugtes Eindringen zu überwachen. [50]

- **Überfallmeldeanlagen** sind meist in eine Einbruchmeldeanlage inkludiert und dienen „dem direkten Hilferuf von Personen bei einem Überfall“. [48] Im Gefahrenfall kann die gefährdete Person den Alarm durch die Betätigung eines manuellen Melders auslösen, der über die Meldezentrale an Einsatzkräfte weitergeleitet wird. [50]

Bestandteile einer Gefahrenmeldeanlage

Der Aufbau einer Gefahrenmeldeanlage ist gemäß Schnabel [48] wie folgt:

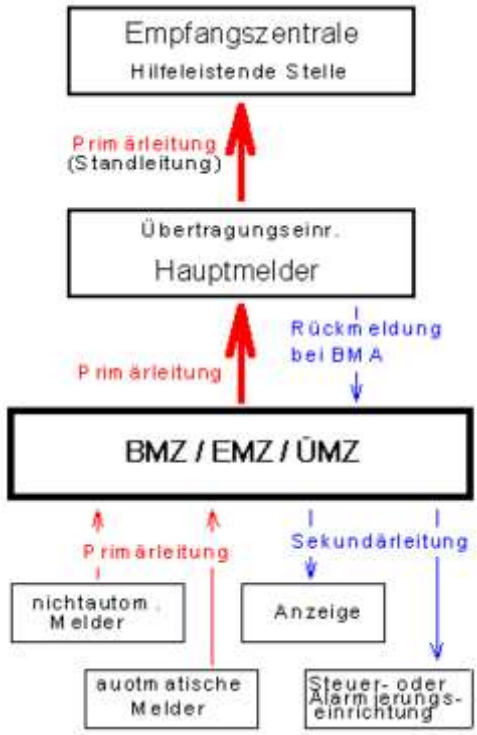

Abbildung 2: Aufbau einer Gefahrenmeldeanlage nach [48].

- **Primär- und Sekundärleitungen**

  In einer Gefahrenmeldeanlage werden zwei Arten von Leitungen eingesetzt – die Primär- und die Sekundärleitung. Während durch eine Primärleitung immer Ruhestrom fließt, um Unterbrechungen und Kurzschlüsse rechtzeitig erkennen und melden zu können, werden Sekundärleitungen nicht überwacht und sind daher nicht als Steuerleitungen geeignet. [51]

- **Automatische und nichtautomatische Melder**

  Melder (z.B. Glasbruch- oder Bewegungsmelder) sind an Primärleitungen angeschlossene Bauteile, welche im Falle eines Einbruchsversuches oder Brandes den Stromkreis unterbrechen und so einen Alarm auslösen. Werden mehrere Melder in einem Stromkreis zusammengefasst, spricht man von sogenannten Meldergruppen, wobei zu beachten ist, dass maximal 20 Melder zu einer Meldergruppe zusammengefasst werden dürfen. [50]

- **Alarmierungseinrichtungen**

  Prinzipiell wird bei der örtlichen Alarmierung zwischen optischen und akustischen Signalgebern unterschieden, wobei bei einer Einbruchmeldeanlage meist zwei akustische Signalgeber, wie beispielsweise Alarmsirenen, und ein optischer Signalgeber, wie Blitz- oder Blinkleuchten, außen an dem überwachten Gebäude montiert werden. [50] Hierbei muss beachtet werden, dass kein Blickkontakt zwischen den Signalgebern bestehen darf. [48]

Bei einer Überfallmeldeanlage wird ein sogenannter stiller Alarm eingesetzt, welcher an eine Alarmempfangsstelle gemeldet wird. [50] Die Alarmauslösung geschieht ohne optische und akustische Signalgeber, um „die sich in Gefahr befindenden Personen zu schützen“. [48]
Ein weiterer Alarmtyp – welcher vermieden werden sollte – ist der Fehlalarm, welcher „durch Fehlverhalten oder durch ein defektes Gerät ausgelöst wird“. [48]

- **Brand-, Einbruch-, oder Überfallmeldezentrale (BMZ / EMZ, ÜMZ)**
  In der Meldezentrale werden die von den Meldern gesendeten Signale ausgewertet und Maßnahmen, wie eine Alarmierung von hilfeleistenden Stellen, eingeleitet. [50]

- **Übertragungseinrichtung**
  Übertragungseinrichtungen leiten den Alarm im Ernstfall über eine Standleitung, über das Telefonnetz oder über das GSM-Netz an die hilfeleistende Stelle, wie Wachdienste, Feuerwehr, Polizei oder an Privatpersonen weiter. [48]

Überwachungsbereiche und -typen

Der Sicherungsbereich ist der gesamte Bereich, der von einer Gefahrenmeldeanlage überwacht wird. In einem Sicherungsbereich gibt es normalerweise mehrere Meldebereiche, welche eine oder mehrere Meldergruppen umfassen. Der Überwachungsbereich ist der Bereich, der von einem Melder überwacht wird. [50]

Der Überwachungsbereich wird in die Flächenüberwachung, die Außenhautüberwachung und die Innenraumüberwachung unterteilt, zudem ist auch eine Sabotageüberwachung ein wichtiger Bestandteil eine Gefahrenmeldeanlage.

Während die Innenraumüberwachung geschlossene Bereiche mittels Infrarot-, Ultraschall, oder Dualmeldern auf unbefugte Bewegungen überprüft [48], überwacht die Flächenüberwachung Glasflächen auf Durchbruch, Durchstieg oder Durchgriff [50]. Unter einer Außenhautüberwachung versteht man schließlich die Überwachung aller nach außen führenden Zugänge auf Verschluss oder Öffnung. [50]

Eine Verschlussüberwachung setzt Schließblechkontakte ein, um den verschlossenen Zustand aller Zugänge zu überwachen, da es ansonsten nicht möglich ist, eine Alarmanlage scharfzuschalten. Bei einer Öffnungsüberwachung werden hingegen Magnetkontakte eingesetzt, um Zugänge auf unbefugte Öffnung zu überwachen und gegebenenfalls die Alarmanlage zu aktivieren. [50]

Die Sabotageüberwachung überwacht die Leitungen und Anlageteile, um den Versuch einer Sabotage der Einbruchmeldeanlage zu erkennen und mittels eines Alarms zu melden. [50]

Scharfschaltung

Um eine Einbruchmeldeanlage scharfschalten zu können, muss die Zwangsläufigkeit gewahrt sein. Das bedeutet, dass alle nach außen führenden Zugänge auf ihren verschlossenen Zustand überprüft werden müssen und die Bewegungsmelder keine Bewegungen registrieren dürfen. [50]

Erst die Scharfschaltung einer Alarmanlage mittels einer elektromechanischen, „geistigen“1 oder berührungslosen Scharfschalteinrichtung oder einer Kombination aus den eben genannten führt zu einer aktivierten Alarmanlage und in weiterer Folge zu einer Alarmierung bei einem Einbruch. [50]

- **Elektromechanische Scharfschalteinrichtung**
  „Eine elektromechanische Scharfschalteinrichtung besteht aus einem Schaltschloss, das mit einer mechanischen Verriegelung der Zugangstür verbunden ist.“ [50]

- **„Geistige“ Scharfschalteinrichtung**
  Die „geistige“ Scharfschalteinrichtung wird beispielsweise durch die Eingabe eines Codes scharfgeschaltet, muss jedoch ebenfalls mit „einer mechanischen Verriegelung der Zugangstür verbunden sein.“ [50]

- **Berührungslose Scharfschalteinrichtung**
  Bei der berührungslosen Scharfschalteinrichtung werden z.B. elektronische Schlüssel oder Magnetkarten eingesetzt. „Zusammen mit dem Einsatz eines Sperrelements (ESPE) im Türrahmen, sowie eines Riegelschaltkontaktes (WRK) zur Verschlussüberwachung des Schlosses, wird die mechanische Verriegelung der Zugangstür gewährleistet“. [50]

Wahrung von Integrität, Verfügbarkeit und Vertraulichkeit der Gefahrenmeldeanlage

Die folgenden Funktionen muss die Gefahrenmeldeanlage in jedem Fall erfüllen, um Integrität, Verfügbarkeit und Vertraulichkeit zu wahren.

[1] Geistig ist ein ungünstig gewählter Begriff, welcher jedoch in mehreren Fachquellen vorgekommen ist. Da das Ziel der Arbeit keine neue Begriffsdefinition war, wurde dieser so übernommen und in Anführungszeichen gesetzt.

- **Ereignisspeicher der Übertragungseinrichtung**
  Ein Zugriff auf den Ereignisspeicher ist nur dem Wartungsdienst erlaubt, welcher die Einträge jeder weder löschen noch verändern können darf. Im Speicher muss mindestens Platz für 100 Ereignisse sein, welche Störungen, Fernzugriffe oder Auslösungen samt etwaiger Folgen beinhalten können. [52]

- **Anforderungen an Meldungen**
  Meldungen an die Empfangszentrale müssen quittiert werden und dürfen nicht verloren gehen. Trifft keine Quittierung über den Empfang der Meldung ein, muss diese wiederholt werden, gleichzeitig muss jedoch bei über zehn Meldungen pro Minute eine Meldungsbegrenzung sichergestellt sein, um eine Überlastung der Empfangseinrichtung durch Mehrfachmeldungen im Störungsfall zu vermeiden. [52]

- **Mögliche Steuerung mittels Netzwerkschnittstelle**
  Wenn die Gefahrenmeldeanlage eine Netzwerkschnittstelle aufweist und somit mittels Smartphone oder über das Internet steuerbar ist, ist unter anderem darauf zu achten, dass das Standardpasswort vor Inbetriebnahme in jedem Fall geändert wird.
  Dies ist insbesondere von Relevanz, da eine im Jahr 2016 von der Zeitschrift *c't* durchgeführte Studie ergeben hat, dass die IP-Adresse von Alarmsystemen, die über das Internet erreichbar sind, über Scanner-Portale wie Shodan gefunden werden kann. Sind die Systeme nur mit dem Standardpasswort versehen, kann über das Web-Interface die gesamte Alarmanlage gesteuert werden. Laut dem Artikel wurde dieses Problem den Herstellern gemeldet und es sollte nun nicht mehr möglich sein, die Alarmanlagen mit Standardpasswort ins Netz zu stellen, was dennoch sicherheitshalber vor Inbetriebnahme überprüft werden sollte. [75]

Besonders in Bezug auf die Verfügbarkeit ist es empfehlenswert, kabelgebundene Alarmanlagen an Stelle von Funkalarmanlagen zu verwenden, da es bei Funkalarmanlagen, die auf gewissen defacto Standards aufbauen, möglich ist, mit Störsendern die Bewegungssensoren außer Kraft zu setzen und deren Funktionsweise zu beeinträchtigen. Problematisch ist besonders, dass weder eine Alarmierung erfolgt noch die Störung protokolliert wird – das System verhält sich so, als wäre nichts passiert. [74]

3.6.2. Zutrittskontrollsysteme

Ein Zutrittskontrollsystem ist ein elektronisches Hilfsmittel, welches dazu dient, den Zutritt zu Gebäuden oder besonders schützenswerten Bereichen nach bestimmten Kategorien, wie Person, Zeit und Ort, zu regeln. Die Personen identifizieren sich hierbei mit einem Identifizierungsmerkmal, wie

einer Karte, einem Ausweis, einem Code oder einem bestimmten biometrischen Merkmal. Es ist auch möglich, mehrere Identifizierungsmerkmale zu kombinieren. Das Ziel eines Zutrittskontrollsystems ist es, Berechtigten den Zutritt zu gewähren, Unbefugte an einem Zutritt zu hindern und potenzielle Täter/innen abzuschrecken. Weiters gibt es die Möglichkeit, Zutrittskontrollsysteme mit Zeiterfassungssystemen, Alarmanlagen oder Videoüberwachungssystemen zu koppeln. [36]

Aufbau von Zutrittskontrollsystemen

Ein Zutrittskontrollsystem besteht aus einem Sensor (Leser), einem Aktor (Türöffner) und der Zutrittskontrollzentrale. Während der Sensor die Person identifiziert und diese an die Zentrale übermittelt, prüft die Zutrittskontrollzentrale nach bestimmten Parametern, ob die Person zutrittsberechtigt ist. Ist die Prüfung erfolgreich, wird der Zutritt durch den Aktor freigeschaltet. [36]

Abbildung 3 zeigt den schematischen Aufbau eines Zutrittskontrollsystems. Die grünen Personen haben gültige und die roten Personen ungültige Zutrittsrechte auf dem Medium. Nachdem die Leseeinheit (oder der Sensor) die berechtigte Person identifiziert und die Zentrale die Erlaubnis erteilt hat, entriegelt das Verriegelungselement (Aktor) die Tür. [36]

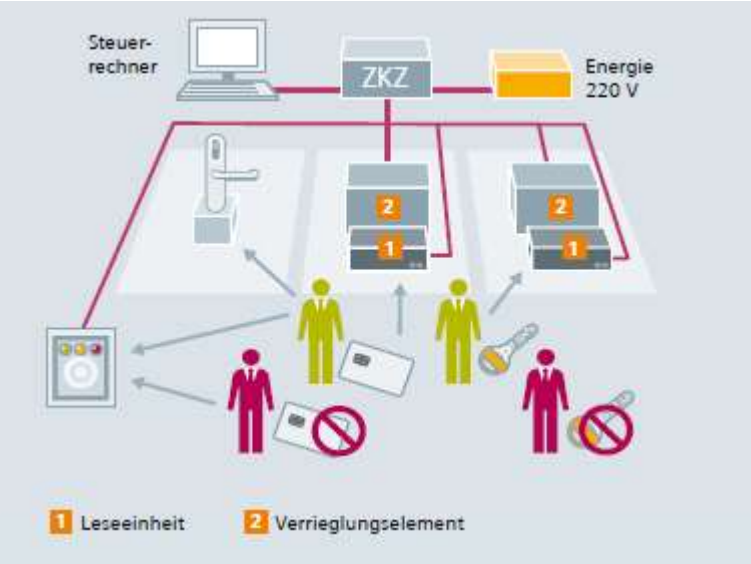

Abbildung 3: Moderne Zutrittskontrolle mit Online- und Offline-Lösung nach Siemens [36]

Arten des Zutrittskontrollsystems

Es gibt Offline- oder Online-Zutrittskontrollsysteme, welche in weiterer Folge kurz beschrieben werden. Der Unterschied zwischen den Systemen ist, dass bei Offline-Systemen die Zutrittsberechtigungen direkt in den digitalen Türkomponenten oder auf dem ID-Medium gespeichert sind und somit keine Netzwerkverbindung notwendig ist, während bei Online-Systemen die

Zutrittsberechtigungen auf einem Server gespeichert werden, welcher mittels Netzwerkverbindung die aktuellen Daten an die Zentrale liefert. Da bei Online-Systemen die Abfrage der Zutrittsrechte direkt über den Server geschieht, sind Sperren oder Änderungen sofort wirksam, wodurch eine sehr hohe Sicherheit und Flexibilität gegeben ist. Online-Systeme sollten für die Außenhautsicherung verwendet werden, während Offline-Systeme für eine Absicherung von Türen innerhalb des Gebäudes, welche geringe Sicherheitsansprüche haben, ausreichend sind. [36]

- **Offline-Zutrittskontrolle**

  Bei einem Offline-Zutrittskontrollsystem, welches aus digitalen Zylindern, Beschlägen und Zutrittslesern besteht, können die Zutrittsrechte in den digitalen Türkomponenten, auf dem ID-Medium oder autonom gespeichert sein. Zu beachten ist hierbei jedoch, dass weder Zutrittsrechte noch Kartensperrungen sofort wirksam sind. [36]

  - Werden die Zutrittsrechte in den digitalen Türkomponenten gespeichert, können die Zutrittsrechte mit Hilfe einer Software direkt auf diese Komponenten geladen werden. Der Vorteil hierbei ist, dass keine Netzwerkverkabelung notwendig ist und dass Türen einfach nachgerüstet werden können. [36]
  - Bei einer Speicherung der Zutrittsrechte auf einem ID-Medium, wie einer Karte oder einem Schlüssel, werden die Zutrittsrechte mittels Software zentral verwaltet und mit Hilfe eines Lesers auf das Medium geschrieben. Die Zutrittsrechte können hierbei jederzeit verändert werden, sind aber nicht sofort wirksam. [36]
  - Werden autonome Zutrittskontrollsysteme eingesetzt, müssen die Zutrittsrechte, die zentral mittels einer Software verwaltet werden, in eine Zentrale geladen werden, bevor sie wirksam sind. [36]

- **Online-Zutrittskontrolle**

  Setzt man ein Online-Zutrittskontrollsystem ein, „wird die Entscheidung, ob eine Person Zutritt oder keinen Zutritt erhält, in der Zentrale gefällt“. [36, p. 317] Die Erteilung von Zutrittsrechten oder Kartensperrungen sind somit sofort wirksam, da die Zutrittsrechte über eine Software verwaltet und mittels Netzwerkverbindung sofort in die Zentrale übertragen werden. Ein Nachteil bei der Online-Zutrittskontrolle ist der Verkabelungsaufwand. [36]

  - Bei einer zentralen Installation gibt es eine Zentrale, welche sowohl mit allen Sensoren und Aktoren als auch mit dem Zutrittsserver verbunden ist. Diese ist meist in einem gesicherten Bereich untergebracht und trifft die Zutrittsentscheidungen für alle Türen. [36]
  - Bei der dezentralen Installation gibt es mehrere Zentralen, welche die Zutrittsberechtigungen für die Türen regeln, die ihnen zugeordnet sind. Dabei können die Zentralen miteinander verbunden sein oder komplett eigenständig agieren. [36]

Protokollierung des Zutritts im Zutrittskontrollsystem

Die Protokollierung des Zutritts im Zutrittskontrollsystem ist nur bei der Online-Zutrittskontrolle mittels der entsprechenden Software möglich. Hierbei kann mit Hilfe der Wartungsfunktion auf die jeweiligen Logs zugegriffen werden, welche im Normalfall Zutritts- und Manipulationsversuche speichern. [53]

Identifizierungsmerkmal

Um Zugang zu dem gesicherten Bereich zu erlangen, muss sich die zutrittsberechtigte Person mit Hilfe eines bestimmten Identifizierungsmerkmales beim Sensor ausweisen. Die Verifikation kann entweder mittels Wissen2, also z.B. durch Codeeingabe, mittels Besitz3, wie einer Chip- oder RFID Karte, oder mittels eines biometrischen Merkmales, wie z.B. einem Fingerabdruck, erfolgen. [36]

Gemäß Siemens haben Verfahren, die nur den Besitz oder das Wissen einer Person in Bezug auf die Zutrittsmethode prüfen, die niedrigste Sicherheitsstufe da beides Merkmale sind, welche leicht weitergegeben oder entwendet werden können. [36]

Werden die beiden Verfahren kombiniert, erhöht sich die Sicherheitsstufe etwas, wobei Verfahren, die auf biometrischen Merkmalen basieren, dennoch gemäß Siemens sicherer sind, da diese zu den personenbezogenen Merkmalen zählen. [36]

Darüber kann man insofern diskutieren, als dass die Kombination zweier Faktoren zumindest gemäß dem aktuellen Stand der Technik im Normalfall immer sicherer ist, als die Verwendung eines Faktors, da auch biometrische Zutrittssysteme überlistet werden können. Daher empfiehlt es sich, wenn möglich, zumindest zwei der zuvor genannten Identifizierungsmerkmale bei einem Zutrittskontrollsystem zu kombinieren.

In weiterer Folge werden die zuvor genannten Identifizierungsmerkmale genauer erklärt.

- **Code**

  Die Codeeingabe zählt zu den unsichersten Verifikationsmethoden, da ein Code einfach ausspioniert oder weitergegeben werden kann. Bei einer Codeeingabe ist ein Lesegerät mit Tastatur erforderlich, wobei es auch sogenannte Scramble Code-Leser gibt, welche die Zahlenposition nach jeder Eingabe zufällig verändern und somit die Sicherheit erhöhen. [36]

[2] Auch „Wissen“ ist ein ungünstig gewählter Begriff, welcher in der Fachterminologie vermehrt vorkommt und daher übernommen würde. Das reine „Wissen“ von etwas reicht nicht aus, um eine Zutrittskontrolle zu überwinden, da man ja ein bestimmtes Wissen – eben beispielsweise den Code – erlangen muss.
[3] Ebenso ungünstig gewählt ist der Begriff des „Besitzes“, der ebenfalls aufgrund der Verwendung in facheinschlägigen Papers übernommen wurde, aber viel zu ungenau in der Definition ist.

- **Kontaktbehaftete Karten**

  Die häufigste Form einer kontaktbehafteten Karte ist die der Chipkarte, welche gleichzeitig auch als Sichtausweis dienen kann. Um die auf dem Chip gespeicherten Daten lesen zu können, werden Einsteckleser benötigt [36].

- **Kontaktlose Medien**

  Kontaktlose Medien können die Form einer Karte, eines Schlüssels, eines Anhängers oder eines Armbandes haben. Wird der NFC-Standard verwendet, können die Zutrittsrechte auch auf dem Mobiltelefon gespeichert sein. Man unterscheidet zwischen der Identifizierung mittels der RFID-Technologie, welche auf elektromagnetischen Wellen basiert, dem NFC-Standard, welcher Funkwellen verwendet, oder der RCID-Technologie, welche statische, elektrische Felder nutzt. [36]

- **Biometrie**

  Der große Vorteil bei der Identifizierung mittels biometrischen Merkmalen liegt darin, dass eine im Normalfall eindeutige, personenbezogene Verknüpfung zwischen Merkmal und Person besteht und dass das Medium weder vergessen werden noch verloren gehen kann. Zudem ist es mittels biometrischer Merkmale einerseits möglich, die Identität einer Person über das Merkmal festzustellen, indem ein 1:n Vergleich durchgeführt wird. Anderseits besteht auch die Möglichkeit der Verifikation mittels eines 1:1 Vergleiches der aktuellen und aufgenommenen Daten, wodurch die Identität der Person nur bestätigt wird, nicht aber festgestellt wird. [36]

  - Die wichtigsten Anforderungen an ein biometrisches Merkmal sind, dass es einzigartig, dauerhaft, leicht zugänglich und universal sein muss. [36]
  - Man kann bei biometrischen Merkmalen zudem zwischen physiologischen Charakteristika, wie Fingerabdruck oder Venenmuster, und verhaltensspezifischen Charakteristika, wie einer Unterschrift, unterscheiden. [36]
  - Diese Merkmale werden von einem Algorithmus in ein Template umgewandelt und anschließend gespeichert. Bei einem versuchten Zutritt wird die Person dann durch einen Vergleich der gespeicherten Daten und den Personendaten entweder verifiziert oder identifiziert. [54]
  - Wird eine Zutrittskontrolle mittels Biometrie realisiert, sind verschiedene Vorgaben – insbesondere in Bezug auf den Datenschutz und das Arbeitsrecht – zu beachten, welche in Kapitel 4.4 genauer behandelt werden.

3.6.3. Videoüberwachung

Das folgende Kapitel beschäftigt sich mit den Grundlagen der Videoüberwachung samt aktueller Technologien und Datenspeicherung. Die rechtlichen Probleme bei und Voraussetzungen für den Einsatz von Videoüberwachungsanlagen werden in den darauffolgenden Kapiteln genauer behandelt.

Gründe für den Einsatz von Videoüberwachung

Sowohl im öffentlichen als auch im privaten Raum nimmt die Anzahl an Videoüberwachungsanlagen jährlich zu. Wurden zu Beginn der 1980er die Daten noch analog auf Band gespeichert [55], ist eine digitale Speicherung der Daten samt der Möglichkeit, eine Bildanalyse durchzuführen, heutzutage bereits der Stand der Technik und daher aus modernen Videoüberwachungssystemen – die oftmals mit Gefahrenmelde- oder Zutrittskontrollanlagen kombiniert werden – nicht mehr wegzudenken. [34]

Gründe für den Einsatz von Videoüberwachung gibt es viele. Beispiele sind – sowohl im privaten und öffentlichen Raum als auch in Unternehmen – die Überwachung und der Schutz des Eigentums vor Diebstahl, Vandalismus oder Einbruch sowie der Schutz von Personen gegen Überfälle oder Gewalt. Dabei soll die Videoüberwachung einerseits potentielle Straftäter abschrecken und andererseits Straftaten mittels der Aufnahmen aufklären. [56]

Weitere Ziele von Videoüberwachung können die Detektion von Wärme, das Erfassen von Zustandsänderungen oder die Zeichen- oder Gesichtserkennung sein. [34]

Technische Grundlagen

Die Beleuchtung dient bei einer Videokamera dazu, die zu überwachenden „Objekte sichtbar zu machen“. Während sichtbares Licht bei normalen Verhältnissen ausreicht, wird bei schlechten Lichtverhältnissen oder bei einer diskreten Überwachung die Infrarotbeleuchtung angewandt. Um Infrarotbeleuchtung verwenden zu können, benötigt man infrarottaugliche Kameras mit einem passenden infrarottauglichen Objektiv, welche unter normalen Bedingungen ein normales Farbbild liefern und bei schlechten Lichtbedingungen auf den „IR-sensitiven Schwarzweissmodus“ umschalten. [34, p. 274]

Neben der Beleuchtung ist die Auswahl des richtigen Objektives essenziell für den erfolgreichen Einsatz von Videoüberwachung, da dieses unter anderem das genaue Sichtfeld definiert, die Lichtmenge steuert und das Bild scharfstellt. [34]

In weiterer Folge werden die wichtigsten Bestandteile einer Videokamera kurz erklärt, um das technische Verständnis in Bezug auf die Funktionsweise zu erhöhen.

- **Arten von Objektiven**

  Nach Siemens gibt es drei verschiedene Arten von Objektiven – das Objektiv mit Festbrennweite, welches nur ein Sichtfeld bietet und eine unveränderliche Brennweite von meist 4 mm hat, das Variofokusobjektiv, bei dem die Brennweite zwischen 3-8 mm einstellbar ist und somit eine variable Einstellung des Sichtfelds ermöglicht, und das Zoom-Objektiv, welches ebenfalls eine variable Einstellung der Brennweite, welche meist zwischen 6-48 mm liegt, und des Sichtfelds bietet und zudem bei einer Änderung den Fokus neu adjustiert. [34]

- **Sichtfeld**

  Das Sichtfeld definiert die Detailgenauigkeit und den Aufnahmebereich einer Kamera und wird u.a. durch die Brennweite des Objektives sowie die Bildsensoren der Kamera definiert. Man unterscheidet zwischen dem Normal View, welcher dem Sichtfeld des menschlichen Auges entspricht, dem Tele View, welcher genauere Details zeigt und eingesetzt wird, wenn das zu überwachende Objekt weiter weg ist, und dem Weitwinkel, welcher eine gute Übersicht bietet, aber für die Identifizierung von Personen nicht geeignet ist. [34]

- **Bildsensor**

  Bildwandlerelemente auf Bildsensoren, welche heutzutage mit Halbleiterelementen wie CCD oder CMOS realisiert werden, erzeugen unterschiedlich große Pixel, indem das Licht, das durch das Objektiv auf die Sensoren gerichtet ist, in elektrische Ladung umgewandelt wird. Je mehr Licht darauf fällt, desto größer ist die Anzahl der erzeugten Elektroden und desto größer ist somit das Pixel. [55]

- **Wärmebildsensor**

  Ein Wärmebildsensor benötigt keine Lichtquelle wie ein herkömmlicher Bildsensor, sondern misst die von einer Person oder einem Objekt ausgehenden Wärmestrahlen. Wärmebildkameras sind zum größten Teil wetterunabhängig und können daher für den Perimeterschutz eingesetzt werden. Zudem besteht die Möglichkeit einer automatischen Alarmierung, wenn eine bestimmte, zuvor definierte Temperatur überschritten wird. [34]

- **Auflösung**

  Bei analogen Videobildern wird die Auflösung in Zeilen gemessen, während digitale Videobilder aus quadratischen Pixeln bestehen, welche je nach Art der Auflösung in unterschiedlicher Anzahl eingesetzt werden. Man unterscheidet hierbei NTCS- und PAL-

Auflösung als analoge und VGA- und HDTV-Auflösungen als digitale Videostandards, wobei die analogen Standards auch bei aktuellen IP-Kameras eingesetzt werden können. [34]

- **Datenspeicherung**
  Die Art der Datenspeicherung ist insbesondere für datenschutzrechtliche Fragen interessant und kann in flüchtige (volatile) und nicht-flüchtige (persistente) Speicher unterteilt werden. Der Unterschied ist, dass bei volatilen Speichern, die für eine Videobeobachtung verwendet werden, die Daten verloren gehen, während sie bei persistenten – wieder- oder einmal beschreibbaren – Speichern dauerhaft auf dem Medium gespeichert werden. Als Medium kann beispielsweise ein mechanisches – wie Lochstreifen –, ein optisches – wie CDs oder DVDs –, ein magnetisches – wie Videokassetten und Festplatten – oder ein elektronisches – wie SSDs oder USB-Sticks – Speichermedium dienen. [55]

Klassifizierung nach DIN EN 62676-4

Die im Jahr 2015 eingeführte Norm DIN EN 62676-4 definiert Anwendungsregeln für Videoüberwachungsanlagen und unterteilt die Klassifikation von Objekten wie folgt [34, p. 275]:

- **„Überwachen**: Um zu überwachen oder für die Kontrolle von Menschenansammlungen darf das Beobachtungsziel nicht weniger als 5 % der Bildhöhe betragen (oder mehr als 80 mm/Pixel).“
- **„Detektieren**: um zu detektieren, darf das Beobachtungsziel nicht weniger als 10 % der Bildhöhe betragen (oder mehr als 40 mm/Pixel).“
- **„Beobachten**: um zu beobachten, muss das Beobachtungsziel 25 % der Bildhöhe betragen (oder mehr als 16 mm/Pixel).“
- **„Erkennen**: um zu erkennen, darf das Beobachtungsziel nicht weniger als 50 % der Bildhöhe betragen (oder mehr als 8 mm/Pixel).“
- **„Identifizieren**: um zu identifizieren, darf das Beobachtungsziel nicht weniger als 100 % der Bildhöhe betragen (oder mehr als 4 mm/Pixel).“
- **„Begutachten**: um zu überprüfen, darf das Beobachtungsziel nicht weniger als 400 % der Bildhöhe betragen (oder mehr als 1 mm/Pixel).“

Kameratypen

Prinzipiell kann man Kameras nach ihrer Auflösung, der Bauform, der Kameratechnik und der Art der Aufnahme, sprich Farbe oder Schwarz-Weiß, unterscheiden. [34]

Zudem gibt es analoge Kameras, welche das Abbild chemisch auf Band speichern und digitale Kameras, welche ein elektronisches Signal speichern und heutzutage weit häufiger eingesetzt werden. [55]

In weiterer Folge werden die wichtigsten Kameratechniken und Bauformen, die dem aktuellen Stand der Technik entsprechen, kurz erklärt.

- **Kameratechnik**

  Gemäß Siemens kann man zwischen IP-Kameras und HD-SDI Kameras unterscheiden. Während IP-Kameras direkt mit dem Netzwerk verbunden sind und – vereinfacht gesagt – eine Mischung aus einer Kamera und einem Computer darstellen, kann mittels HD-SDI Kameras ein analoges Signal in Echtzeit übertragen werden. IP-Kameras besitzen zudem ein Objektiv, einen Bildsensor, Prozessoren und einen Speicher, welcher für die Aufzeichnung der Bilddaten und für das Betriebssystem der Kamera zuständig ist. Mittels einer IP-Kamera können die Daten zudem über das Netzwerk übertragen und anschließend auf einem Bildschirm angezeigt und/oder persistent gespeichert werden. [34]

- **Bauformen**

  Man unterscheidet verschiedene Bauformen für Kameras, welche je nach Einsatzzweck unterschiedlich sind. So gibt es Boxkameras für Innen- oder Außenbereiche, die sich im verwendeten Gehäuse in Bezug auf die beispielsweise die Wasserdichtigkeit unterscheiden. Weiters gibt es sogenannte Mini-Domes, die aufgrund ihres unauffälligen Designs den Vorteil haben, dass die genaue Kameraausrichtung nur schwer erkennbar ist, sowie PTZ-IP-Kameras, welche sich automatisch schwenken lassen und einen ausgewählten Bereich verkleinern oder vergrößern können. [34]

Übertragungsarten

Signale können entweder per Funk oder mittels Kabel übertragen werden, wobei bei der Funkübertragung zu beachten ist, dass die Reichweite geringer ist und eine geeignete Verschlüsselung während der Übertragung eingesetzt werden muss. Die Übertragung analoger Videosignale ist streng mittels der Videonorm geregelt, wodurch es möglich ist, Kameras

unterschiedlicher Arten und Hersteller an ein analoges Videoüberwachungssystem anzuschließen. Nach Siemens unterscheidet man bei den Übertragungsarten die Übertragung analoger Signale über Koaxialkabel, die Zweidrahtübertragung analoger Signale, die Funkübertragung analoger Signale, die Glasfaserübertragung und die Übertragung im Netzwerk. [34]

Videomanagementsysteme

Videomanagementsysteme können für verschiedene Aufgaben eingesetzt werden, die wichtigsten sind hierbei die Wiedergabe von Live- und Speicherbildern sowie die Speicherung der Bilder, die komplexe Alarmverwaltung, das Vergeben von Nutzer- und Zugriffsrechten, die Protokollierung von Ereignissen, Aktivitäten und Zuständen sowie die Steuerung der Kameras und die intuitive Bedienung des Systems. Zudem ist es möglich, mittels forensischer Suche, welche die Metadaten der gefilmten Objekte verwendet, gezielt Ereignisse oder Daten zu finden. [34]

Intelligente Bildanalyse

Ein großer Vorteil der intelligenten Bildanalyse besteht darin, dass es möglich ist, die Bilder von der Kamera zu den Überwachungsräumen erst im Ereignisfall zu übertragen, wodurch die Gefahr, ein Ereignis zu übersehen, sinkt. Zudem kann die Bildanalyse eingesetzt werden, um bestimmte Muster, Objekte oder Personen zu detektieren. Geeignete Einsatzmöglichkeiten sind daher die Objektklassifizierung oder -erkennung, der Perimeterschutz, die Gesichtserkennung, die Personenzählung oder die Kennzeichenerkennung. [34]

3.6.4. Exkurs – GPS-Systeme

1973 beschloss das US-amerikanische Verteidigungsministerium die Entwicklung eines Ortungssystems, welches damals aus 24 Satelliten bestand und die Aufgabe hat, die genaue Position des Empfängers zu bestimmen. Ursprünglich NAVSTAR genannt, kennt es heutzutage jeder nur unter dem Begriff Global Positioning System oder kurz GPS. Heutzutage gibt es etwa 30 aktive Satelliten, welche in 20200 km Höhe die Erde umkreisen und die Bestimmung der Position eines GPS-Empfängers ermöglichen. [57]

Bestandteile

Das GPS-System besteht aus dem Weltraumsegment mit mindestens 24 (heutzutage meist 30) Satelliten, dem Kontrollsegment mit mehreren Bodenstationen, die vom US Militär verwaltet werden, und dem Benutzersegment, welches als GPS-Empfänger bekannt ist und der Positionsbestimmung dient. [58]

Positionsbestimmung

Um nun die genaue Position des GPS-Empfängers bestimmen zu können, „vergleicht der GPS-Empfänger die Zeit, zu der das Signal ausgesamdt [sic!] wurde mit der Zeit, zu der das Signal empfangen wurde“ und errechnet so die Entfernung zu den Satelliten. [59]

Mindestens drei Satelliten sind für die zweidimensionale Positionsbestimmung von Nöten, mit mindestens vier oder fünf Satelliten kann zusätzlich auch die Höhe des GPS-Empfängers bestimmt werden. Wenn die Messungen regelmäßig erfolgen, kann man mittels GPS Bewegungsabläufe und -richtungen sowie die genaue Geschwindigkeit ermitteln. [59]

Genauigkeit

Die Positionsgenauigkeit ist stark von der Anzahl und dem Standort, also der Geometrie der verwendeten Satelliten, abhängig. Prinzipiell gilt, dass der Standort genauer ist, je mehr Satelliten in der Nähe zur Verfügung stehen, da bei mehr als fünf Satelliten dank der zusätzlichen Informationen eine Integritätsprüfung der Signale durchgeführt und etwaige Fehler entdeckt werden können. Zudem unterscheidet sich die Positionsgenauigkeit durch die verwendete Technik; im Zivilbereich können dank der differenziellen GPS-Technik Genauigkeiten von bis zu 3-5 Metern erreicht werden. [60]

Anwendungsgebiete

Für diese Arbeit relevante Anwendungsgebiete sind beispielsweise der Einsatz von GPS-Peilsendern in Mobiltelefonen oder Autos, um Positionen festzustellen oder Geschwindigkeiten zu berechnen. [13]

4. Rechtliche Grundlagen in Bezug auf Sicherheitstechnik

Die Einhaltung und Beachtung von rechtlichen Vorgaben, wie Gesetzen und Rechtsverordnungen samt aktueller Rechtsprechung, ist eine wesentliche Grundlage einer funktionierenden Compliance-Strategie. Daher stellt sich mit der am 25.05.2018 in Kraft getretenen Datenschutzgrundverordnung (DSGVO) und der daraus folgenden Novellierung des DSG 2000 die Frage, was ab diesem Zeitpunkt beim Einsatz oder der Wartung von Sicherheitstechnik, insbesondere von Zutrittskontrollsystemen oder Videoüberwachungsanlagen, in Bezug auf die verwendeten Daten rechtlich zu beachten ist, da solche Systeme zum Teil personenbezogene Daten verarbeiten. Zudem muss beim Einsatz von Sicherheitstechnik im Beschäftigtenkontext auch das Arbeitsrecht beachtet werden, insbesondere wenn die Gefahr besteht, dass die Menschenwürde berührt oder verletzt wird.

Um einen ganzheitlichen Blick auf das Thema zu ermöglichen, werden daher in weiterer Folge relevante Grundrechte definiert und anschließend die zuvor genannten Gesetze inklusive etwaiger Beispiele aktueller Rechtsprechung mit Bezug auf die Sicherheitstechnik behandelt.

Im letzten Teil dieses Kapitels werden schließlich die in Kapitel 3.6 vorgestellten sicherheitstechnischen Produkte in Verbindung mit den in diesem Kapitel definierten Gesetzen gebracht, um festzustellen, was bei deren Einsatz und Vertrieb zu beachten ist.

4.1. Relevante Grundrechte und Definitionen

Gemäß § 16 AGBG [61] hat „[j]eder Mensch […] angeborne, schon durch die Vernunft einleuchtende Rechte, und ist daher als eine Person zu betrachten.“ Die Grundrechte sind in Österreich in verschiedenen Gesetzen, wie dem StGB, dem ABGB, dem DSG 2000 und dem UrhG sowie der EMRK geregelt und sind im Kontext dieser Arbeit [13, p. 18]:

- „das Grundrecht auf Gleichbehandlung (Art 7 B-VG, Art 2 STGG, Art 14 EMRK)“
- „der Schutz vor unmenschlicher Behandlung (Art 3 EMRK)“
- „das Recht auf Achtung des Privat- und Familienlebens (Art 8 EMRK)“
- der Schutz personenbezogener Daten (§ 1 DSG 2000)

4.1.1. Definition personenbezogener Daten

Nach Voigt und von dem Bussche spricht man von personenbezogenen Daten, „sobald die Zuordnung der Daten zu einem oder mehreren Charakteristika, die Ausdruck der physischen, physiologischen, psychischen, genetischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, möglich ist“ [19, p. 13].

Gemäß Art. 4 Abs. 1 DSGVO sind personenbezogene Daten:

> *„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.“ [62, p. 33]*

Im Zuge dieser Arbeit sind dies beispielsweise Standortdaten, Namen, Ausweisnummern oder Videoaufnahmen der betroffenen Person. [19]

Besondere Kategorien personenbezogener Daten, die besonders schutzwürdig sind, definiert die DSGVO in Art. 9 Abs. 1 als:

> *„[…] Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.“ [62, p. 38]*

Prinzipiell ist es nach der DSGVO untersagt, besondere Kategorien personenbezogener Daten zu verarbeiten, außer die „betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt“ oder es ist erforderlich, um die Umsetzung der Rechte aus dem Arbeitsrecht zu gewährleisten oder „lebenswichtige Interessen der betroffenen Person“, zu schützen. [62, pp. 38-39]

Im Kontext dieser Arbeit sind besondere Kategorien personenbezogener Daten beispielsweise biometrische Daten nach Art. 9 DSGVO. [62]

4.1.2. Kontrollmaßnahmen

Eine Kontrollmaßnahme dient dazu, vorliegende Fakten mit dem gewünschten Sollzustand zu vergleichen. Greift nun eine Person in die Grundrechte – insbesondere den Privatbereich, die Privatsphäre oder das Grundrecht auf Datenschutz – einer anderen Person ein, müssen die

Interessen der auftraggebenden Person, wie die Unverletzlichkeit des Eigentums nach Art 5 StGG, den Grundrechten der betroffenen Person gegenübergestellt werden. [13]

4.1.3. Menschenwürde

Die Menschenwürde einer jeden Person muss geschützt werden. Prinzipiell unterscheidet man daher gem. Schnepfleitner „Maßnahmen, die die Menschenwürde nicht berühren“, „Maßnahmen, die die Menschenwürde berühren“ und „Maßnahmen, die die Menschenwürde verletzen“. [13, pp. 19, 21]

Unter die Menschenwürde nicht berührende Kontrollmaßnahmen fallen beispielsweise Zeiterfassungssysteme. Diese Maßnahmen dienen dazu, die ordnungsgemäße Pflichterfüllung des Personals zu kontrollieren und unterliegen gemäß § 97 Abs 1 Z 1 ArbVG der erzwingbaren Mitbestimmung. [13]

Berühren Kontrollmaßnahmen die Menschenwürde, wird also ein Persönlichkeitsrecht des Betroffenen eingeschränkt, aber nicht verletzt, ist im arbeitsrechtlichen Kontext für die Einführung und Änderung dieser die Zustimmung des Betriebsrats oder jedes/jeder einzelnen Betroffenen erforderlich. Unter solche Maßnahmen fällt unter anderem der Einsatz einer Videoüberwachung, eines Zutrittskontrollsystems oder einer Überwachung mittels GPS-Peilsendern. [13]

Maßnahmen, die das angestrebte Kontrollziel überschreiten und somit die Menschenwürde des Personals oder das Grundrecht auf Datenschutz verletzten, sind ebenfalls seitens des Betriebsrats oder jedes/jeder einzelnen Betroffenen zustimmungspflichtig. Hierbei ist jedoch anzumerken, dass in diesem Fall die Zustimmung nur verweigert werden darf und solche Maßnahmen – darunter fällt zum Beispiel Leibesvisitation – generell rechtswidrig sind. [13]

4.1.4. Interessensabwägung und Verhältnismäßigkeitsprinzip

Diese Gegenüberstellung zwischen den Rechten des/der Auftraggebers/Auftraggeberin und dem Eingriff in die Grundrechte des/der Betroffenen ist im Zuge einer Interessensabwägung durchzuführen. Hierbei ist zu beachten, dass der/die Auftraggeber/in durchaus Kontrollmaßnahmen durchführen kann, allerdings die Persönlichkeitsrechte des/der Betroffenen hierbei beachten muss, um eine Verletzung der Menschenwürde zu verhindern. Zudem muss das Prinzip der Verhältnismäßigkeit beachtet werden, welches besagt, dass die Kontrollmaßnahmen nur in dem Ausmaß durchgeführt werden dürfen, sodass die Ziele des/der Auftraggebers/Auftraggeberin mit der geringsten Beschränkung der Persönlichkeitsrechte des/der Betroffenen erreicht werden können. [13]

4.1.5. Judikatur zur Verletzung der Grundrechte

Der OGH definiert im Fall 6Ob38/13a vom 04.07.2013 die grundrechtlichen Probleme beim Einsatz von Videoüberwachung wie folgt:

> *„Eine Videoüberwachung ist in datenschutzrechtlicher Sicht zwar grundsätzlich nur dann relevant, wenn sie für die Überwachung und somit zur Kontrolle von Menschen eingesetzt wird […]. Systematische, verdeckte, identifizierende Videoüberwachung stellt aber grundsätzlich einen Eingriff in das geschützte Recht auf Achtung der Geheimsphäre dar. Die Videoaufzeichnung ist dabei identifizierend, wenn sie aufgrund eines oder mehrerer Merkmale letztlich einer bestimmten Person zugeordnet werden kann. Muss sich jemand ständig kontrolliert fühlen, wenn er sein Haus betritt oder verlässt oder sich in seinem Garten aufhält, so bewirken getroffene Maßnahmen (selbst wenn das Gerät nur eine Attrappe einer Videokamera sein sollte) eine schwerwiegende Beeinträchtigung der Geheimsphäre des Betreffenden […]. Geheime Bildaufnahmen im Privatbereich, fortdauernde unerwünschte Überwachungen und Verfolgungen stellen eine Verletzung der Geheimsphäre dar (RIS-Justiz RS0107155). Nach der Entscheidung 6 Ob 256/12h kann bei Bildaufnahmen schon ausreichen, wenn sie vom Aufgenommenen als unangenehm empfunden werden und ihn an der freien Entfaltung seiner Persönlichkeit hindern.“ [63]*

Diesbezüglich wurde am 21.03.2018 eine Grundstückseigentümerin vor dem OGH im Fall 3Ob195/17y schuldig gesprochen, in die Privatsphäre ihres Nachbarn einzugreifen, da sie eine Videoüberwachungsanlage installieren ließ, die teilweise auch das Grundstück des Nachbarn erfasste. Die Bereiche außerhalb ihres Grundstückes waren zwar mittels geeigneter technischer Maßnahmen verpixelt und es wurde durch Schilder auf die Videoüberwachung hingewiesen. Das Gericht stellte jedoch fest, dass es auch möglich gewesen wäre, die Videokameras so anzubringen, „dass ausschließlich das Grundstück der Beklagten gefilmt werde, wozu sie verpflichtet gewesen wäre. Die eingerichtete Videoüberwachung sei keinesfalls das schonendste Mittel zur Zweckerreichung“. Daher wurde durch die durchgeführte Interessensabwägung festgestellt, „dass das Interesse des Klägers an der Entfernung oder zumindestens der Änderung der Ausrichtung der Kameras das Interesse der Beklagten an einer effizienten Überwachung ihres Grundstücks überwiege“ und die Beklagte sowohl eine Überwachung der Bereiche außerhalb ihres Grundstückes künftig zu unterlassen habe als auch zur Zahlung der halben Pauschalgebühr für die Verfahren verpflichtet wurde. [64]

Die zuvor genannten Beispiele der aktuellen Judikatur in Bezug auf die Verletzung der Privatsphäre und anderer relevanter Menschenrechte zeigen, dass es auch als Privatperson wichtig ist, die aktuellen Gesetze und zuvor genannten Prinzipien genau einzuhalten, um einen Gesetzesbruch und die Zahlung von Geldstrafen zu vermeiden.

4.2. Einsatz von Sicherheitstechnik im Kontext der DSGVO

Gerade im Bereich des Datenschutzes kommt es zu einer immer engeren Verknüpfung zwischen IT und Recht, da in der DSGVO vorgegeben ist, personenbezogene Daten (darunter fallen unter Umständen auch personenbezogene Daten von Sicherheitssystemen) bei einer Datenverarbeitung mittels geeigneter technischer und organisatorischer Maßnahmen – wie z.B. Zutrittskontrollsysteme, Alarmanlagen oder Videoüberwachungssystemen – zu schützen. [65]

4.2.1. DSGVO und DSG 2000

Die DSGVO ging am 25.05.2018 unmittelbar in das nationale Recht jedes EU-Staates über, was bedeutet, dass die darin enthaltenen Vorgaben ab diesem Tag (rückwirkend!) eingehalten werden müssen, auch wenn die einzelnen Mitgliedstaaten durch sogenannte Öffnungsklauseln die Möglichkeit haben, manche Bereiche selbst zu regeln [65]. Daher war auch eine Anpassung der Datenschutzgesetze der jeweiligen EU-Staaten erforderlich, im Falle von Österreich wurden die Öffnungsklauseln und die Anpassung des DSG 2000 an die Vorgaben der DSGVO durch das Datenschutz-Anpassungsgesetz und das Datenschutz-Deregulierungs-Gesetz 2018 geregelt [66].

Am Rande sei hierbei erwähnt, dass einerseits in dem neuen Datenschutz-Anpassungsgesetz grundlegende Begriffe, wie der Begriff einer öffentlichen Stelle, nicht definiert wurden. Andererseits wurde versucht, andere Gesetze anzupassen, welche neue Verfassungsbestimmungen enthalten sollen, die in Widerspruch mit der neuen DSGVO stehen. „Unter anderem wurden Betroffenenrechte massiv beschnitten, sensible Datensammlungen sollen generell zu ‚*Forschungszwecken*' freigegeben werden und Informationspflichten der Behörden sollen aufgehoben werden." [67]

Da „sowohl EU-Grundrechtecharta, als auch DSGVO Vorrang vor österreichischen Verfassungsbestimmungen haben" [67], beschäftigt sich das folgende Kapitel primär mit den für diese Arbeit relevanten Artikeln der DSGVO. Inwieweit sich die neuen Gesetze mit dem Europarecht vereinbaren lassen, wird sich früher oder später zeigen.

Als für diese Arbeit relevante Bereiche wurden zum einen die Rechte der betroffenen Person sowie die Rechte und Pflichten der Verantwortlichen und Auftragsverarbeiter/innen, und zum anderen die möglichen Sanktionen bei einer Nichteinhaltung der rechtlichen Vorgaben identifiziert.

4.2.2. Anwendungsbereich der DSGVO

Der Anwendungsbereich der DSGVO lässt sich grob in den sachlichen, den persönlichen und den räumlichen Anwendungsbereich unterteilen, wobei alle Anwendungsbereiche das gemeinsame Ziel verfolgen, die Verarbeitung personenbezogener Daten von natürlichen Personen zu schützen. Erwähnenswert ist hierbei zudem, dass für die Verarbeitung personenbezogener Daten prinzipiell ein Verbot mit Erlaubnisvorbehalt gilt, was bedeutet, dass die Datenverarbeitung so lange verboten ist, bis die betroffene Person dieser explizit zustimmt. [19]

Sachlicher Anwendungsbereich

Art. 2 der DSGVO definiert den sachlichen Anwendungsbereich wie folgt:

> *„Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.“ [62, p. 32]*

Der sachliche Anwendungsbereich ist sehr weit gefasst und betrifft quasi jedweden Umgang mit Daten. „Beispiele sind das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, das Löschen oder die Vernichtung von Daten“ [19, pp. 11-12].

Im Zuge dieser Arbeit ist der sachliche Anwendungsbereich insofern relevant, als dass die Aufnahme personenbezogener Daten durch eine Kamera oder die Anzeige oder Verarbeitung durch ein Computersystem darunterfällt. [19]

Persönlicher Anwendungsbereich

Die DSGVO ist sowohl auf den/die Verantwortliche/n, also die Person, „die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, Art. 4 Nr. 7“ als auch auf den/die Auftragsverarbeiter/in, also die Person, „die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, Art. 4 Nr. 8 DSGVO“ anwendbar [19, pp. 21, 24] und soll natürliche Personen schützen.

Beispielsweise können im Kontext dieser Arbeit Unternehmen, die Sicherheitstechnik einsetzen, als Verantwortliche definiert werden, während Unternehmen, welche personenbezogene Daten im Auftrag der erstgenannten Unternehmen verarbeiten, als Auftragsverarbeiter angesehen werden.

Räumlicher Anwendungsbereich

Art. 3 der DSGVO definiert den räumlichen Anwendungsbereich wie folgt:

> *„Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.“ [62, p. 32]*

Dies bedeutet, dass die DSGVO auch die Verarbeitung personenbezogener Daten europäischer Bürger/innen betrifft, wenn diese außerhalb der Europäischen Union durchgeführt wird. [19]

Anonymisierung und Pseudonymisierung

„Anonymisierung ist eine Technik zur Veränderung personenbezogener Daten mit dem Ergebnis, dass keine Verbindung der Daten zu einer natürlichen Person (mehr) besteht“ [19, p. 16]. Eine Anonymisierung kann beispielsweise durch Randomisierung, also einer Veränderung der Genauigkeit der Daten, oder durch Verallgemeinerung, also einer Veränderung des Bezugspunktes der Daten, geschehen. Werden personenbezogene Daten anonymisiert, ist also eine Identifizierung der betroffenen Person nicht mehr möglich, fallen die verarbeiteten Daten nicht mehr unter den Anwendungsbereich der DSGVO. [19]

Bei einer Pseudonymisierung werden die Daten hingegen so verarbeitet, dass „die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, Art. 4 Nr. 5 DSGVO“ [19, p. 18]. Die Informationen, die zur Identifikation der betroffenen Person verwendet werden können, müssen dabei gesondert aufbewahrt und durch „den Einsatz technischer und organisatorischer Mittel“ – wie Verschlüsselung samt Zutrittskontrolle – „zusätzlich gesichert werden“ [19, p. 18]. Auch wenn Daten pseudonymisiert werden, fallen sie immer noch unter den Anwendungsbereich der DSGVO, die Vorteile bei der Verwendung von Pseudonymisierung liegen jedoch darin, „dass der Verantwortliche von seiner Pflicht zur Meldung von Datenschutzverletzungen bzgl. der pseudonymisierten Daten entbunden wird“ [19, p. 18].

4.2.3. Rechte der betroffenen Person und Pflichten der Verantwortlichen und Auftragsverarbeiter/innen

Die DSGVO definiert verschiedene Rechte, die eine von einer Verarbeitung personenbezogener Daten betroffene Person gegenüber des mit der Verarbeitung beauftragten Unternehmens oder dessen Auftraggeber/in hat. Darunter fallen beispielsweise Informationspflichten des/der

Verantwortlichen über die Erhebung der personenbezogenen Daten nach Art. 13 und 14 bzw. Auskunftsrechte der betroffenen Person über die Maßnahmen, die nach dem Antrag auf Auskunft, Löschung oder Berichtigung der Daten ergriffen wurden nach Art. 15-22. [19]

Informationspflichten

Für die betroffene Person ist es wichtig, über die Verarbeitung ihrer Daten informiert zu sein. Daher wird die Informationspflicht in Art. 12 wie folgt definiert:

> *„Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.“ [62, p. 39]*

Wie nun genau die Information übermittelt werden muss, ist weit gefasst, lt. Art. 12 DSGVO ist eine schriftliche, mündliche oder elektronische Übermittlung zulässig. [62]

Genau definiert ist hingegen, dass bei der Erhebung personenbezogener Daten nach Art. 13 DSGVO die betroffene Person über die Dauer der Datenspeicherung sowie den Sinn und Zweck der Datenverarbeitung informiert werden muss. Zudem muss so eine Information die Kontaktdaten des/der Verantwortlichen sowie die genauen Rechte der betroffenen Person beinhalten. [62]

Eine Möglichkeit, eine Einwilligung in die Verarbeitung personenbezogener Daten zu erhalten und gleichzeitig die Informationspflichten zu erfüllen, ist der Abschluss eines Vertrags über eine Auftragsverarbeitung gemäß Art. 28 DSGVO, welcher in weiterer Folge näher behandelt und in Kapitel 6.4 beispielhaft dargestellt wird.

Möchte eine Person nun wissen, welche personenbezogene Daten ein Unternehmen verarbeitet, hat diese Person gem. Art. 15 DSGVO einerseits das Recht auf eine Auskunft, welche die Verarbeitungszwecke, die Datenkategorien und die Herkunft der Daten inkludiert, und andererseits das Recht, die verarbeiteten Daten anzufordern, unrichtige Daten gem. Art. 16 DSGVO berichtigen zu lassen oder eine Löschung der Daten gem. Art. 17 DSGVO anzufordern, sofern die Daten z.B. unrechtmäßig verarbeitet wurden oder nicht mehr benötigt werden. [62]

Aufgrund der umfangreichen Rechte, die eine betroffene Person hat, ist es für Unternehmen wichtig, geeignete Maßnahmen zu setzen, um die Informationspflichten zu erfüllen und den Datenschutz zu gewährleisten. Hierzu gehören beispielsweise das Einführen von technischen und organisatorischen

Maßnahmen für den Schutz der Daten samt der Anwendung datenschutzfreundlicher Voreinstellungen, die genaue Dokumentation von Verarbeitungsvorgängen und die Durchführung einer Datenschutzfolgenabschätzung bei der Einführung neuer Technologien, wie beispielsweise GPS- oder Videoüberwachung.

Allgemeine Pflichten der Verantwortlichen und Auftragsverarbeiter/innen

Die allgemeinen Pflichten der Verantwortlichen und Auftragsverarbeiter/innen werden in den Art. 24-31 DSGVO behandelt, wobei im Kontext dieser Arbeit die Auftragsverarbeitung (Art. 28), die Verarbeitungsvorgänge (Art. 30) und der Schutz der Daten durch Technikgestaltung samt datenschutzfreundlicher Voreinstellung (Art. 25) in weiterer Folge näher betrachtet werden. [62]

- **Art. 25 – Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen**

  Beim Prinzip des Datenschutzes durch *Technikgestaltung* sollen Hersteller/innen und Entwickler/innen dazu angehalten werden, geeignete Maßnahmen zu setzen, die sicherstellen, dass nur das absolute Minimum der für den jeweiligen Zweck notwendigen, personenbezogenen Daten gesammelt und diese Daten nach Möglichkeit pseudonymisiert werden. [19]

  Hingegen betrifft das Prinzip des Datenschutzes durch datenschutzfreundliche *Voreinstellung* die konkrete Verarbeitung der personenbezogenen Daten und soll dazu führen, dass nur das absolute Minimum der für den jeweiligen Zweck notwendigen Daten verarbeitet wird. [19]

  Ein dazu verwandtes Konzept ist die Sicherheit durch Technikgestaltung, welche zum Beispiel Hersteller/innen von sicherheitstechnischen Systemen, wie Alarmanlagen und Zutrittskontrollen, betrifft und dazu führen soll, dass nur die Funktionen implementiert werden, die das jeweilige System wirklich benötigt, um so das Auftreten von Sicherheitslücken zu minimieren. Dadurch soll unter anderem sichergestellt werden, dass bei mit dem Internet verbundenen Systemen keine Standard-Login-Daten verwendet werden, um einen unbefugten Zugriff zu erschweren. [68]

- **Art. 28 – Auftragsverarbeiter/in**

  Wird eine natürliche oder juristische Person mit der Verarbeitung personenbezogener Daten von einem/einer Verantwortlichen mittels eines Vertrages beauftragt, spricht man von einer Auftragsverarbeitung im Sinne des Art. 28 DSGVO [62]. Ein solcher Vertrag über die Auftragsverarbeitung muss den Gegenstand, die Dauer und den Sinn und Zweck der

Verarbeitung sowie die Kategorien und Arten der Daten und die zum Schutz der Daten ergriffenen, technischen oder organisatorischen Maßnahmen beinhalten und dient dazu, eine Verletzung der Verordnung und somit hohe Geldstrafen zu vermeiden. [19]

Umstritten ist derzeit noch, ob reine (Fern-)Wartungsarbeiten als Auftragsverarbeitung anzusehen sind.

Das Bayrische Landesamt für Datenschutzaufsicht äußert sich dazu insofern, als dass es zwischen der rein technischen Wartung (ohne den möglichen Zugriff auf personenbezogene Daten) und der Wartung mit Zugriff auf personenbezogene Daten unterscheidet. Während bei ersterer davon auszugehen ist, dass Art. 28 keine Anwendung findet, muss bei zweiterer in jedem Fall eine Vereinbarung über die Auftragsverarbeitung abgeschlossen werden. [69]

Schmidt und Freund hingegen gehen davon aus, dass bei einer (Fern-)Wartung in der Regel ein Zugriff auf personenbezogene Daten möglich ist und daher Art. 28 in jedem Fall anwendbar ist. [70]

Bitkom hingegen ist der Meinung, dass Wartungs- oder Prüfungsarbeiten keine Auftragsverarbeitung darstellen, „sofern Gegenstand des Vertrages keine Datenverarbeitung ist, sondern [dieser] allein auf die Supportleistung abzielt“ – auch wenn im Zuge der Wartungsarbeiten „personenbezogene Daten durch den IT-Dienstleister zur Kenntnis genommen werden“. Als Beispiele werden hier die „Installation und Wartung von Netzwerken, Hardware […] sowie Pflege von Software“ angeführt [71, pp. 22-23].

Um sicherzugehen und hohe Geldstrafen zu vermeiden, sollten Dienstleister/innen, bis das Thema rechtskräftig geklärt wird, vor Wartungsarbeiten in jedem Fall zusätzlich zu der bestehenden Vertraulichkeitsvereinbarung einen Vertrag zur Auftragsverarbeitung abschließen.

- **Art. 30 – Verzeichnis von Verarbeitungsvorgängen**

  Verantwortliche und Auftragsverarbeiter/innen müssen prinzipiell nach Art. 30 DSGVO ein Verzeichnis über die Verarbeitungsvorgänge die personenbezogenen Daten betreffend führen, welche in jedem Fall die Kontaktdaten und den Namen des/der Auftragsverarbeiters/Auftragsverarbeitern und/oder des/der Verantwortlichen sowie die gesetzten technischen und organisatorischen Maßnahmen beinhaltet. Zudem haben Verantwortliche weitere Punkte in das Verzeichnis zu inkludieren, wie Löschfristen und die Kategorien der betroffenen Personen und Daten. [19]

  Dieses Verzeichnis soll dazu dienen, im Falle einer Anfrage oder Prüfung eine korrekte Auskunft an die Datenschutzbehörde oder die betroffene Person zu geben und somit nachzuweisen, dass die Vorgaben der DSGVO eingehalten wurden. [19]

Nach Art. 5 DSGVO sind klein- und mittelständische Unternehmen (KMUs) mit einer Mitarbeiter/innenanzahl von weniger als 250 Mitarbeitenden von der Pflicht, ein Verzeichnis über die Verarbeitungsvorgänge zu führen, ausgenommen, wenn der Jahresumsatz unter 50 Millionen Euro liegt. [19]

Gewährleistung der Sicherheit personenbezogener Daten

Die zu ergreifenden Maßnahmen, um die Sicherheit personenbezogener Daten zu gewährleisten, werden in den Art. 32-34 DSGVO behandelt und inkludieren die Setzung geeigneter technischer und organisatorischer Maßnahmen, sowie die Meldung von Datenschutzverstößen an die Datenschutzbehörde und die betroffene Person. [62]

- **Art. 32 – Sicherheit der Verarbeitung**

  Sowohl der/die Auftragsverarbeiter/in als auch der/die Verantwortliche müssen die Sicherheit der personenbezogenen Daten bei der Verarbeitung mittels geeigneter Maßnahmen sicherstellen. Dazu gehören gemäß Art. 32 DSGVO beispielsweise [62, pp. 51-52]:
  - „die Pseudonymisierung und Verschlüsselung personenbezogener Daten“;
  - die Wahrung der Integrität, Vertraulichkeit, Verfügbarkeit und Belastbarkeit der datenverarbeitenden Systeme und
  - die Wiederherstellung der Verfügbarkeit der personenbezogenen Daten im Falle eines Zwischenfalles;

  Gemäß Voigt und von dem Bussche gehören im Kontext dieser Arbeit zu diesen Maßnahmen auch „[b]auliche Maßnahmen zur Verhinderung eines unbefugten physischen Zugriffs auf personenbezogene Daten, wie bspw. gesicherte Räume, Wachpersonal, passwortgesicherter Zugang oder Mitarbeiterkennungsmaßnahmen, etc.“. [19, p. 48]
  Kurz gesagt kann der Einsatz von Sicherheitstechnik die Sicherheit bei der Verarbeitung personenbezogener Daten erhöhen.

- **Art. 33 – Meldung von Datenschutzverstößen**

  Art. 4 Abs. 12 versteht unter der „‘*Verletzung des Schutzes personenbezogener Daten‘* eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden“. [62, p. 34]
  Wird nun – unabhängig ob durch Vorsatz oder Fahrlässigkeit – ein Datenschutzverstoß durch technische oder physische Zwischenfälle – wie dem Verlust eines USB-Sticks mit

Kundendaten oder aufgrund kompromittierter Systeme – verursacht, sieht Art. 33 DSGVO eine Meldung des/der Verantwortlichen an die zuständige Aufsichtsbehörde innerhalb von 72 Stunden vor. Dies ist eine große Verbesserung der bisherigen Rechtslage, da es bisher in den meisten EU-Staaten keine Meldeplicht bei der Verletzung des Schutzes personenbezogener Daten gab. [19]
Die Meldung an die Aufsichtsbehörde muss in jedem Fall eine Folgenabschätzung, etwaige Maßnahmen, Kontaktdaten des/der Verantwortlichen und die genaue Beschreibung samt Anzahl der betroffenen Personen, Kategorien und Datensätze enthalten. [62]
Der/Die Auftragsverarbeiter/in muss einen Datenschutzverstoß gem. Art 33 DSGVO zwar nicht der Aufsichtsbehörde, wohl aber dem/der Verantwortlichen unverzüglich melden, wobei nicht genauer definiert ist, was unter unverzüglich zu verstehen ist. [19]

- **Art. 34 – Benachrichtigung der betroffenen Person**
  Zusätzlich zu der Meldung an die Aufsichtsbehörde muss die betroffene Person unverzüglich über eine Datenschutzverletzung, die „ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge“ hat, informiert werden [62, p. 52]. Diese Information muss zumindest eine Folgenabschätzung, etwaige Maßnahmen und Kontaktdaten des/der Verantwortlichen enthalten. [62]
  Ausnahmen von der Informationspflicht bestehen, wenn höchstwahrscheinlich kein hohes Risiko mehr besteht oder die Daten durch geeignete Maßnahmen – wie Verschlüsselung oder Pseudonymisierung – geschützt wurden. [62]

Durchführung einer Datenschutz-Folgenabschätzung

Gem. Art. 35 DSGVO ist eine Datenschutz-Folgeabschätzung dann durchzuführen, wenn:

> „[…] eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien [wie GPS-Systeme oder biometrische Zutrittskontrollanlagen], aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge [hat].“ *[62, p. 53]*

Es ist einerseits möglich, bei ähnlichen Verarbeitungsvorgängen nur eine einzige Datenschutz-Folgenabschätzung durchzuführen [62], andererseits können auch bereits in Kraft gesetzte Verarbeitungsvorgänge erneut Gegenstand einer Datenschutz-Folgenabschätzung werden, wenn sich deren Risiko durch eine Veränderung der verarbeiteten Daten oder der Verarbeitungszwecke erhöht. [19]

Die Datenschutz-Folgenabschätzung soll dazu dienen, die personenbezogenen Daten der betroffenen Personen zu schützen und zugleich die Vorgaben der DSGVO nachweislich einzuhalten. Als erster Schritt ist daher jedenfalls eine unternehmensinterne Risikoabschätzung durchzuführen, wenn die Rechte und Freiheiten der betroffenen Person unter Umständen gefährdet sind. Wird in der vorgeschriebenen, unternehmensinternen Risikoabschätzung ein hohes Risiko identifiziert, ist zudem die Aufsichtsbehörde hinzuzuziehen, die ebenfalls eine Bewertung des Risikos abgibt. [19]

Beinhalten muss eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO in jedem Fall eine Beschreibung und den Zweck der Verarbeitungsvorgänge samt Bewertung der Notwendigkeit ebenjener, sowie eine Risikobewertung samt zu treffender Schutzmaßnahmen die Rechte der betroffenen Person betreffend. [62]

Bestellung einer/eines Datenschutzbeauftragten

Wenn der/die Verantwortliche oder der/die Auftragsverarbeiter/in im täglichen Betrieb eines privaten Unternehmens (sensible) personenbezogene Daten verarbeitet oder „eine regelmäßige und systematische Überwachung von betroffenen Personen“ durchführt, ist ein/e Datenschutzbeauftragte/r gem. Art. 37 DSGVO zu ernennen. [62, p. 55]

Als Beispiel sei hier genannt, dass ein Unternehmen, welches sicherheitstechnische Produkte, wie Videoüberwachungssysteme oder (biometrische) Zutrittskontrollanlagen, verkauft, aller Voraussicht nach keine/n Datenschutzbeauftragte/n benötigt, wenn es nur mit der Montage der Systeme, nicht aber mit der Aufbewahrung und Analyse der Logfiles oder Videodaten betraut ist, da das Kerngeschäft in diesem Beispiel im Verkauf und nicht in der Verarbeitung personenbezogener Daten oder einer systematischen Überwachung besteht. Auch bei einer Durchführung von sporadischen (Fern-) Wartungstätigkeiten ist zwar eventuell ein Vertrag über eine Auftragsverarbeitung abzuschließen – insbesondere dann, wenn die Möglichkeit besteht, auf personenbezogene Daten zuzugreifen; ein/e Datenschutzbeauftragte/r sollte jedoch nicht von Nöten sein.

Anders ist der Fall, wenn das Unternehmen zusätzlich zur Implementierung der Produkte auch für die Analyse der personenbezogenen Daten – wie z.B. der Videoaufnahmen – zuständig ist oder unbeschränkten Zugriff auf die personenbezogenen Daten der betroffenen Personen hat. In diesem Fall ist zu klären, ob das Hauptgeschäft die Verarbeitung der personenbezogenen Daten ist und in weiterer Folge ein/e Datenschutzbeauftragte/r nach Art. 37 DSGVO benannt werden muss.[4]

[4] Diese Ansicht sollte gem. einer am 29.05.2018 beim Datenschutzbeauftragten der KPMG Wien, Reinhard Fiegl, telefonisch eingeholten Auskunft der aktuellen Rechtslage entsprechen.

Zusätzlich besteht die Möglichkeit, eine/n Datenschutzbeauftragte/n auf freiwilliger Basis zu ernennen. Dies macht insbesondere dann Sinn, wenn nicht eindeutig geklärt ist, ob man als Verantwortliche/r oder Auftragsverarbeiter/in unter die zuvor genannten Regeln fällt. [19]

Egal ob die Ernennung des/der Datenschutzbeauftragten auf freiwilliger oder unfreiwilliger Basis erfolgt, er/sie muss in jedem Fall die fachliche und berufliche Qualifikation mitbringen, um gem. Art. 39 DSGVO gegebenenfalls die Verarbeitungstätigkeiten des/der Verantwortlichen oder Auftragsverarbeiters/Auftragsverarbeiterin mittels einer Datenschutz-Folgeabschätzung bewerten und in weiterer Folge die Einhaltung der Vorgaben der DSGVO überwachen zu können. Zudem ist er/sie im Anlassfall die erste Ansprechperson der Aufsichtsbehörde. [62]

Sowohl der/die Auftragsverarbeiter/in als auch der/die Verantwortliche sind gem. Art. 38 DSGVO verpflichtet, den/die Datenschutzbeauftrage/n in seiner Tätigkeit zu unterstützen und „frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen“ einzubinden. [62, pp. 55-56]

4.2.4. Rechtsbehelfe, Haftung und Sanktionen

Die Einhaltung der zuvor genannten Artikel und Vorgaben der DSGVO ist essenziell, um Verstöße gegen den Schutz personenbezogener Daten und in weiterer Folge zivilrechtliche Haftung und Schadenersatzansprüche zu vermeiden. Art. 82 DSGVO regelt die „Haftung und [das] Recht auf Schadenersatz“, während Art. 83 „Allgemeine Bedingungen für die Verhängung von Geldbußen“ definiert. [62, pp. 81-82]

Art. 82 – Haftung und Recht auf Schadenersatz

Nach Art. 82 DSGVO hat „[j]ede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, […] Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter“. [62, p. 81]

Im Art. 82 DSGVO wird der Begriff des Schadens sehr weit gefasst und umfasst materielle (finanzielle) Schäden zum einen und immaterielle Schäden (wie psychische Belastungen) zum anderen, wobei jede betroffene Person anspruchsberechtigt ist. [19]
Sowohl der/die Auftragsverarbeiter/in als auch der/die Verantwortliche können weiters im Falle eines Verstoßes gegen die Vorschriften der DSGVO zur Rechenschaft gezogen werden. Dies ist eine signifikante Verschärfung der vorherigen Rechtslage, da bisher nur der/die Verantwortliche, nicht aber der/die Auftragsverarbeiter/in unmittelbar haftbar war. [19]

Zu erwähnen ist hierbei weiters, dass der/die Verantwortliche bei einem Verstoß gegen die Verordnung in jedem Fall haftbar ist, während der/die Auftragsverarbeiter/in nur dann haftbar gemacht werden kann, „wenn er [oder sie] seinen [oder ihren] speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat“. [62, p. 81]

Wird von einem/einer Verantwortlichen oder Auftragsverarbeiter/in der gesamte Schadenersatz bezahlt, hat diese/r nach Art. 82 Abs. 5 DSGVO das Recht, den Schadenersatz anteilsmäßig von den anderen, ebenfalls an der Verarbeitung beteiligen Parteien, einzufordern. [19]

Eine Haftungsfreistellung tritt nur dann ein, wenn nachweisbar ist, dass der/die Auftragsverarbeiter/in oder der/die Verantwortliche „in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“. [62, p. 81] Dies wird in der Praxis jedoch schwer zu beweisen sein, wie das nachfolgende Beispiel nach Voigt und von dem Bussche anschaulich zeigt:

> *„Ein Verantwortlicher erfüllt alle seinen materiellen und organisatorischen Pflichten nach der DSGVO in Bezug auf seine Verarbeitungsvorgänge. Dennoch gelingt es einem unbefugten Dritten, Zugang zu den personenbezogenen Daten zu erhalten. Dem Verantwortlichen gelingt es nicht festzustellen, warum eine solche Zugriffsmöglichkeit bestand. Infolge der Offenlegung der Daten entsteht bei den betroffenen Personen ein Schaden.*
>
> *In diesem Beispiel hat der Verantwortliche seine Pflichten nach der DSGVO erfüllt, aber konnte dennoch nicht verhindern, dass ein Dritter Zugriff auf die von der Verarbeitung betroffenen personenbezogenen Daten erhält. Es kann nicht mit Sicherheit ausgeschlossen werden, dass der Verantwortliche für den Zugriff durch Dritte in keinerlei Hinsicht verantwortlich ist. Aus diesem Grund ist der Verantwortliche unter Art. 82 DSGVO haftbar.“ [19, p. 275]*

Art. 83 – Allgemeine Bedingungen für die Verhängung von Geldbußen

Während die maximale Höhe von Schadenersatzansprüchen in der DSGVO nicht definiert wurde, gibt es sehr klare Angaben über die maximale Höhe der zu verhängenden Geldbußen im Falle eines Verstoßes gegen die Verordnung. Hierbei unterscheidet man – bei Auftragsverarbeitern/Auftragsverarbeiterinnen und Verantwortlichen – zwischen den zwei folgenden Varianten von Verstößen.

Bei der ersten Variante, die in Art. 83 Abs. 4 DSGVO definiert ist, werden „Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist“. [62, p. 82]

Die Voraussetzungen dafür, dass dieser Fall eintritt, ist beispielsweise eine Verletzung der Datensicherheitsvorschriften gem. Art. 11, Art. 25-39 und 42-43 DSGVO, welche auf den vorherigen Seiten bereits zum größten Teil behandelt wurden. [62]

Bei der zweiten Variante werden bei einem Verstoß „Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist“. [62, p. 83]

Dies betrifft beispielsweise Verstöße gegen „die Grundsätze für die Verarbeitung“ gem. Art. 5, 6, 7, 9 oder eine Verletzung der Betroffenenrechte gem. Art. 12-22. [62, p. 83]

Die genaue Höhe hängt dabei von verschiedenen Faktoren, wie Vorsätzlichkeit oder Fahrlässigkeit, der Schwere des Verstoßes, den betroffenen Datenkategorien, etwaigen gesetzten Maßnahmen und eventuellen vorherigen Verstößen ab. [62]

In Österreich wird zusätzlich durch das Datenschutz-Anpassungsgesetz 2018 und das Datenschutz-Deregulierungs-Gesetz 2018 geregelt, dass die Datenschutzbehörde Bußgelder in Höhe von max. 50.000 Euro verhängen kann, wenn einer der folgenden Fälle vorsätzlich eintritt und dieser nicht bereits durch die DSGVO oder andere Gesetze mit einem höheren Bußgeld versehen werden kann. Erwähnenswert ist zudem, dass auch der reine Versuch strafbar ist [72]:

- unbefugter Zugriff auf eine Datenverarbeitung
- unbefugte Datenübermittlung
- unbefugtes Beschaffen personenbezogener Daten
- unbefugtes Betreiben von Bildverarbeitung

Die zuvor diskutierten Bereiche der DSGVO zeigen, dass der Schutz personenbezogener Daten sowohl für Auftragsverarbeiter/innen als auch für Verantwortliche wichtiger ist denn je und die Judikatur in naher Zukunft beschäftigen wird. Erwähnenswert ist zudem, dass die DSGVO auch rückwirkend gilt, also auch die bisher erfassten Daten ab Zeitpunkt des Inkrafttretens den Vorschriften der Verordnung Genüge tun müssen. Zusammenfassend gesagt ist eine Einhaltung der gesetzlichen Vorschriften daher sehr wichtig, um hohe Strafen und Schadenersatzansprüche zu vermeiden.

4.3. Einsatz von Sicherheitstechnik im arbeitsrechtlichen Kontext

Es kommt immer öfter vor, dass Sicherheitstechnik im Beschäftigungskontext eingesetzt wird, um die Sicherheit des Unternehmens zu erhöhen. Beispiele sind der Einsatz einer Zutrittskontrolle mittels RFID Chip oder einem biometrischen Erkennungsmerkmal oder die Überwachung des Werksgeländes mittels Videoüberwachung. Doch auch ein/e Arbeitgeber/in muss bestimmte Vorgaben und Gesetze einhalten, bevor er/sie Sicherheitstechnik in seinem/ihrem Unternehmen einsetzen kann, um eine Verletzung der Persönlichkeitsrechte seines/ihres Personals zu vermeiden. Das nächste, kurze Kapitel beschäftigt sich daher zunächst mit dem Zusammenhang zwischen Arbeitsrecht und DSGVO und geht anschließend auf die Möglichkeiten eines/einer Arbeitgebers/Arbeitgeberin ein, Sicherheitstechnik gesetzeskonform einzusetzen.

4.3.1. Datenverarbeitung im Beschäftigungskontext

Die Datenschutzgrundverordnung beschäftigt sich in Art. 88 DSGVO mit der Datenverarbeitung im Beschäftigungskontext und erlaubt mittels einer Öffnungsklausel, dass die einzelnen Mitgliedsstaaten festlegen können, wie sie den Schutz „der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext [gewährleisten]“. [62, p. 84]

Nach Art. 88 Abs. 2 DSGVO müssen diese spezifischen Datenschutzbestimmungen „angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz [umfassen]“. [62, p. 84]

In Österreich können sowohl die spezifischen Datenschutzbestimmungen als auch der Einsatz von Kontrollmaßnahmen – was oftmals Hand in Hand geht – durch das Individual- und das Kollektivarbeitsrecht festgelegt werden. [13]

4.3.2. Individualarbeitsrecht

Der Arbeitsvertrag regelt die individuellen Arbeitsbeziehungen zwischen Arbeitgeber/in und Arbeitnehmer/in. Es ist durchaus möglich, gesetzeskonforme Arbeitsbedingungen oder den Einsatz von Kontrollmaßnahmen im Arbeitsvertrag näher zu regeln, sofern dies nicht dem Kollektivvertrag oder einer Betriebsvereinbarung widerspricht. Berühren diese Kontrollmaßnahmen jedoch die Menschenwürde, muss mit jedem/jeder Arbeitnehmer/in eine schriftliche Vereinbarung getroffen werden, welche im Falle einer Abänderung der Kontrollmaßnahme angepasst werden muss. [13]

Zudem gibt es im Individualarbeitsrecht sogenannte Weisungen, welche dazu dienen, eine Willenserklärung des/der Arbeitgebers/Arbeitgeberin umzusetzen. Weisungen sind einseitige Rechtsgeschäfte, welche jedoch nicht gegen Betriebsvereinbarungen, Kollektivverträge oder Gesetze verstoßen dürfen. Da der Betriebsrat Kontrollmaßnahmen im Sinne des § 96 ArbVG zustimmen muss, ist es nicht zulässig, ebenjene durch Weisungen einzuführen. [13]

4.3.3. Kollektivarbeitsrecht

Auf der sicheren Seite ist man, wenn man den Einsatz von Kontrollmaßnahmen oder genauere Datenschutzvereinbarungen mittels einer Betriebsvereinbarung – oder im Falle des Fehlens eines Betriebsrates mittels einer Einzelvereinbarung – regelt. [13] [19]

Gemäß Voigt und von dem Bussche sind Betriebsvereinbarungen „Vereinbarungen zwischen einem Arbeitgeber und, sofern im nationalen Recht vorgesehen, dem Betriebsrat, der die Arbeitnehmer des besagten Arbeitgebers vertritt […], welche die Arbeitsbedingungen für die Arbeitnehmer des Betriebs kollektiv regeln“. [19, p. 298]

Schnepfleitner sieht die Betriebsvereinbarung als adäquates Mittel an, um Kontrollmaßnahmen in österreichischen Betrieben einzuführen, wobei zu beachten ist, dass „Inhalt einer notwendigen Betriebsvereinbarung […] nicht alle Arten von Kontrollmaßnahmen [sind], sondern lediglich solche, die die Menschenwürde berühren. Die Menschenwürde verletzende Kontrollmaßnahmen sind immer unzulässig […]“ [13, pp. 10-11].

Auch wenn nach § 40 Abs 1 Satz 1 ArbVG ein Betriebsrat zu bilden ist, wenn ein Betrieb dauerhaft mehr als fünf wahlberechtige Beschäftigte hat [13], trifft den/die Arbeitgeber/in keine Pflicht, einen Betriebsrat einzuführen. Er/Sie muss dessen Wahl zwar dulden, jedoch sind nur die Arbeitnehmenden dafür zuständig, einen Betriebsrat zu errichten. Da es nach der aktuell gültigen Rechtslage in Österreich keine Sanktionen für den/die Arbeitgeber/in gibt, wenn kein Betriebsrat eingerichtet wurde, gibt es nach wie vor Betriebe mit weit mehr als fünf Mitarbeitern, die keinen Betriebsrat haben. [73]

In Kapitel 6.5 wird ein Muster einer Rahmenbetriebsvereinbarung gezeigt, die die Verarbeitung und Verwendung personenbezogener Daten im Beschäftigungskontext regelt und dabei Rücksicht auf die Vorgaben der DSGVO nimmt.

4.3.4. Rechtliche Folgen für den/die Arbeitgeber/in bei der unerlaubten Durchführung von Kotrollmaßnahmen

Werden nun Kontrollmaßnahmen unrechtmäßig durchgeführt, beispielsweise aufgrund einer fehlenden oder rechtswidrigen Betriebsvereinbarung, können dem/der Arbeitgeber/in Konsequenzen seitens der Mitarbeiter/innen oder seitens des Betriebsrates drohen.

Ein/e Mitarbeiter/in hat beispielsweise die Möglichkeit, Schadensersatzansprüche zu stellen, wenn sein/ihr Persönlichkeitsrecht durch die Kontrollmaßnahme verletzt wurde. Nach bisherigem Recht stand dem/der Mitarbeiter/in „ein Schadenersatzanspruch nach den allgemeinen Schadenersatzregeln, zB bei Verletzung der Privatsphäre gem § 1328a ABGB, zu“ [13, pp. 51-52].

Dies wird nun durch die Schadenersatzansprüche durch Art. 82 DSGVO ergänzt, wenn personenbezogene Daten ohne die Einwilligung der Betroffenen verarbeitet wurden, da der/die Arbeitgeber/in im Normalfall als der/die Verantwortliche anzusehen ist.

Weiters können sowohl der Betriebsrat als auch ein/e Arbeitnehmer/in Beseitigungs- oder Unterlassungsklagen einbringen sowie eine einstweilige Verfügung erwirken, sofern Gefahr in Verzug ist. Erwähnenswert ist jedoch, dass das Personal seine Rechtsansprüche nach Möglichkeit immer über den Betriebsrat durchsetzen sollte, da andernfalls eine eventuelle Entlassung oder Kündigung des/der Mitarbeiter/in drohen könnte. [13]

4.4. Rechtliche Bewertung sicherheitstechnischer Systeme

In diesem Kapitel werden die zuvor definierten, rechtlichen Grundlagen auf die in Kapitel 3.6 vorgestellten, elektronischen, sicherheitstechnischen Systeme angewendet. Dies umfasst konkrete Probleme und Besonderheiten der einzelnen Systeme, wobei auf eine genaue Erklärung der Systeme und Rechtsbegriffe in diesem Kapitel zum größten Teil verzichtet wird, da die meisten Grundlagen bereits in den vorherigen Kapiteln behandelt wurden.

Für alle angeführten Systeme gilt in jedem Fall, dass im Falle eines Verstoßes gegen die Datenschutzbestimmungen einerseits eine Meldung des/der Verantwortlichen an die Datenschutzbehörde innerhalb von 72 Stunden erforderlich ist und andererseits der/die Auftragsverarbeiter/in gegebenenfalls einen Verstoß unverzüglich dem/der Verantwortlichen melden muss. Dies inkludiert insbesondere den unbefugten Zugriff auf oder den Verlust von personenbezogenen Daten, unabhängig davon, ob leichte oder grobe Fahrlässigkeit die Ursache ist.

4.4.1. Videoüberwachung

Im österreichischen Datenschutz-Anpassungsgesetz und dem Datenschutz-Deregulierungsgesetz 2018 wird die Bildverarbeitung geregelt, unter welche auch die Videoüberwachung fällt. Die Definition einer Bildaufnahme ist gemäß WKO folgende:

> *„Unter einer ‚Bildaufnahme' versteht das DSG ‚die durch Verwendung technischer Einrichtungen zur Bildverarbeitung vorgenommene Feststellung von Ereignissen im öffentlichen oder nicht-öffentlichen Raum zu privaten Zwecken. Zur Bildaufnahme gehören auch dabei mitverarbeitete akustische Informationen'." [74]*

Gemäß WKO ist eine Bildaufnahme zulässig, wenn [74]:

- "sie im lebenswichtigen Interesse einer Person erforderlich ist,
- die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,
- sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder
- im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist."

Dementsprechend ist eine Videoüberwachung[5] zum Schutz von Personen oder dem Eigentum auf privaten oder öffentlichen Plätzen nach der Durchführung einer Interessensabwägung prinzipiell zulässig. Unzulässig ist sie in jedem Fall, wenn die betroffenen Personen dieser nicht zugestimmt haben oder damit überwacht werden. Eine verdeckte Überwachung ist ebenfalls immer unzulässig, auch wenn nur Kameraattrappen eingesetzt werden. Weiters ist eine Videoüberwachung unzulässig, wenn dadurch ein Abgleich mit anderen personenbezogenen Daten durchgeführt wird. [74]

Zudem müssen beim Einsatz von Videoüberwachung besondere Kennzeichnungs- und Sorgfaltspflichten gewahrt werden, da sonst Geldstrafen bis zu 50.000 Euro anfallen können, „sofern die Tat nicht unter die Strafbestimmungen der Datenschutz-Grundverordnung fällt oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist." Darunter fallen [74]:

- Die Löschung der Aufnahmen innerhalb von 72 Stunden, sofern die personenbezogenen Daten nicht mehr benötigt werden. Ist eine Aufbewahrung von mehr als 72 Stunden erforderlich, muss ein begründetes Interesse diesbezüglich nachgewiesen werden;

[5] Genaueres zur Funktionsweise von Videoüberwachungssystemen ist Kapitel 3.6.3 zu entnehmen.

- Die Kennzeichnung des Bereiches, der videoüberwacht wird, um die Informationspflichten gegenüber der betroffenen Personen zu erfüllen, da eine direkte Erhebung personenbezogener Daten stattfindet;
- Die Protokollierung eines jeden Verarbeitungsvorganges;
- Die sichere Aufbewahrung der Aufnahmen durch geeignete technische und organisatorische Maßnahmen, wie Zutritts-, Zugangs-, und Zugriffsmaßnahmen

Wird die Videoüberwachung in einem Betrieb durchgeführt, muss zudem beachtet werden, dass diese zwar nicht mehr beim Datenverarbeitungsregister gemeldet, stattdessen jedoch in ein Verzeichnis von Verarbeitungstätigkeiten gem. Art. 30 DSGVO inkludiert werden muss. Zudem ist gegebenenfalls eine Datenschutz-Folgeabschätzung gem. Art. 35 DSGVO durchzuführen, wenn ein großes Risiko für die Rechte und Freiheiten der betroffenen Personen zu erwarten ist. [75]

Vor der Einführung der Videoüberwachung ist zudem entweder eine Einzelvereinbarung mit jeder betroffenen Person – bei Unternehmen ohne Betriebsrat – oder eine Betriebsvereinbarung abzuschließen, da durch den Einsatz dieser die Menschenwürde berührt werden kann. [75]

Diese Betriebsvereinbarung muss in jedem Fall die Transparenzpflichten gem. Art. 88 erfüllen, wobei noch nicht eindeutig geklärt ist, ob sie alle Informationen enthalten muss oder ob ein Verweis auf die entsprechenden Regelungen der DSGVO ausreicht. In jedem Fall „können [Anlagen zur Betriebsvereinbarung] ein probates Mittel sein, um die hohen Transparenzanforderungen der DS-GVO umzusetzen und im Falle einer Überprüfung durch die Datenschutzbehörden die entsprechenden internen Standards nachzuweisen“. [76]

Sollte bei der (Fern-)Wartung von Videoüberwachungsanlagen zudem die Möglichkeit bestehen, auf die Aufnahmen, welche personenbezogene Daten darstellen, zuzugreifen, ist in jedem Fall ein Vertrag zur Auftragsverarbeitung abzuschließen.

Ein Vertrag zur Auftragsverarbeitung ist außerdem jedenfalls abzuschließen, wenn das Unternehmen, welches die Videoüberwachungsanlage vertreibt auch gleichzeitig mit der Überwachung betraut ist. In diesem Fall ist das Sicherheitsunternehmen der/die Verarbeiter/in und das Unternehmen, in dem die Videoüberwachung eingesetzt wird, der/die Auftraggeber/in. Den Verarbeiter trifft in diesem Fall zudem die Pflicht, eine Datenschutz-Folgeabschätzung gem. Art. 35 DSGVO durchzuführen.

4.4.2. Zutrittskontrolle

Eine Zutrittskontrolle ist gem. DSGVO ein geeignetes, technisches oder organisatorisches Mittel, um den unbefugten Zugriff auf personenbezogene Daten zu verhindern, da damit genau definiert werden kann, wer wann in welche Räume darf[6].

Prinzipiell muss man in Hinblick auf den Datenschutz und das Arbeitsrecht zwischen einer Zutrittskontrolle mittels Wissen und der Zutrittskontrolle zwischen Besitz oder biometrischem Merkmal unterscheiden. Da bei einer Zutrittskontrolle mittels Wissen normalerweise nur ein Code zum Einsatz kommt, sind hierbei weder eine Betriebsvereinbarung noch sonstige Maßnahmen gemäß DSGVO erforderlich, da weder eine Beschränkung des Persönlichkeitsrechts noch eine Erhebung personenbezogener Daten durchgeführt wird. Dies ist damit begründet, dass im Normalfall mehrere Personen den Code wissen und somit nicht eindeutig zugeordnet werden kann, wer zu welcher Zeit die Türe mittels Code geöffnet hat[7].

Anders ist der Fall jedoch, wenn für die Zutrittskontrolle ein Medium, wie eine Karte oder ein Code, oder ein biometrisches Merkmal verwendet wird, welches dieser Person eindeutig zugeordnet werden kann. In diesem Fall ist durch die Logs eine genaue Zuordnung möglich, welche Person wann welchen Raum betreten hat, was wiederum unter den Begriff der personenbezogenen Daten fällt.

Im Normalfall gelten bei der Zutrittskontrolle durch personenbezogene Daten dieselben Regeln wie schon bei der Videoüberwachung, nämlich dass sie zulässig ist, wenn [74]:

- “sie im lebenswichtigen Interesse einer Person erforderlich ist,
- die betroffene Person zur Verarbeitung ihrer personenbezogenen Daten eingewilligt hat,
- sie durch besondere gesetzliche Bestimmungen angeordnet oder erlaubt ist, oder
- im Einzelfall überwiegende berechtigte Interessen des Verantwortlichen oder eines Dritten bestehen und die Verhältnismäßigkeit gegeben ist.”

Das Prinzip der Verhältnismäßigkeit ist insbesondere dann zu beachten, wenn die Zutrittskontrolle mittels biometrischer Daten umgesetzt werden soll, da diese gem. Art. 9 DSGVO unter den Begriff der besonderen Kategorien personenbezogener Daten fallen [62].

Gem. Schmidt ist das berechtigte Interesse des/der Arbeitgebers/Arbeitgeberin zum Einsatz von biometrischen Daten nur dann gegeben, „wenn es sich um Branchen handelt, bei denen

[6] Genaueres zur Funktionsweise von Zutrittskontrollsystemen ist Kapitel 3.6.2 zu entnehmen.
[7] Vorausgesetzt natürlich, dass die Tür nicht zusätzlich videoüberwacht wird.

Sicherheitsaspekte eine große Rolle spielen, insbesondere bezogenen auf Leib und Leben z. B. Hochsicherheitslabore oder Tresore die hohe Wertbeträge enthalten“. Daraus folgt, dass „die Zugangskontrolle durch biometrische Verfahren in normalen Bürobereichen […] deshalb regelmäßig unzulässig [ist]“. [54]

Auch der OGH sah 2006 den Einsatz eines biometrischen Zutrittssystems im Krankenhausumfeld als unzulässig an, da dieses einerseits ohne Zustimmung des Betriebsrates eingeführt wurde und andererseits der/die Arbeitgeber/in nicht argumentieren konnte, „dass das schonendste oder zielführendste Kontrollmittel verwendet wurde“. [13, p. 27]

Unabhängig davon empfiehlt es sich aus datenschutzrechtlicher Sicht, beim Einsatz eines biometrischen Zutrittskontrollsystems eine Offline-Zutrittskontrolle einzusetzen, bei der das Template direkt auf einer Karte gespeichert ist und der Abgleich mittels einer Kombination aus Besitz und Biometrie stattfindet. Ist eine Online-Zutrittskontrolle notwendig, muss gewährleistet sein, dass die Daten zumindest verschlüsselt abgelegt werden und somit vor unbefugtem Zugriff geschützt sind. [54]

In jedem Fall muss bei der Einführung einer Zutrittskontrolle durch Karte oder biometrischem Merkmal eine Datenschutz-Folgeabschätzung gem. Art. 35 DSGVO durchgeführt und eine Betriebsvereinbarung darüber abgeschlossen werden, da die Menschenwürde durch solch eine Kontrollmaßnahme berührt wird. [13] [54] [76]

Sollte bei der (Fern-)Wartung von Zutrittskontrollsysteme zudem die Möglichkeit bestehen, auf die Logfiles oder gar die biometrischen Daten, welche personenbezogene Daten darstellen, zuzugreifen, ist in jedem Fall ein Vertrag zur Auftragsverarbeitung abzuschließen.

4.4.3. GPS bei Firmenhandy oder Firmenfahrzeug

Setzt ein Unternehmen GPS-Systeme ein, um die Position eines/einer Arbeitnehmers/Arbeitnehmerin nachzuvollziehen[8], ist in jedem Fall die Menschenwürde des/der Arbeitnehmers/Arbeitnehmerin berührt, wodurch der Abschluss einer Betriebsvereinbarung erforderlich ist. [13]

Außerdem muss bei der Einführung der Überwachung mittels GPS eine Datenschutzfolgeabschätzung gemäß Art. 35 DSGVO durchgeführt werden, um die Auswirkungen auf die persönlichen Rechte und Freiheiten des Personals zu evaluieren. [76]

[8] Genaueres zur Funktionsweise von GPS-Systemen ist Kapitel 3.6.4 zu entnehmen.

4.4.4. Gefahrenmeldeanlagen

Werden Gefahrenmeldeanlagen ohne Zusatz von Videoüberwachungs- oder Zutrittskontrollsystemen eingesetzt und erfolgt die Scharfschaltung ausschließlich mittels Code, ist aufgrund der Funktionsweise, welche keine Speicherung personenbezogener Daten vorsieht, die Menschenwürde nicht berührt[9]. Es ist daher in einem solchen Fall weder eine Datenschutz-Folgeabschätzung noch eine Betriebsvereinbarung nötig.

Sollte die Gefahrenmeldeanlage mit oben genannten Verfahren kombiniert werden, kommen jedoch die Vorgaben dieser Systeme zur Anwendung, wodurch gegebenenfalls eine Datenschutz-Folgeabschätzung oder eine Betriebsvereinbarung erforderlich ist.[10]

[9] Genaueres zur Funktionsweise von Gefahrenmeldeanlagen ist Kapitel 3.6.1 zu entnehmen.
[10] Genaueres kann den Kapiteln 4.4.1 und 4.4.2 entnommen werden.

5. Compliancemaßnahmen für Verträge und unternehmensinterne Regelwerke

Eine ganzheitliche Compliance-Strategie betrifft nicht nur die Einhaltung internationaler und nationaler Gesetze, sondern auch die Beachtung verschiedenster Verträge und unternehmensinterner Regelwerke. Darunter zählen sowohl SLAs, Betriebsvereinbarungen oder Datenschutz-Folgeabschätzungen als auch AGBs und Verträge zur Auftragsverarbeitung.

Dieses Kapitel beschäftigt sich daher mit dem Nutzen und den Möglichkeiten von Vertragsabschlüssen mittels Verträgen und AGBs – insbesondere im Hinblick auf die Haftungsfreizeichnung – und weiteren Compliancemaßnahmen die DSGVO betreffend.

5.1. Übersicht über verschiedene unternehmensexterne Vertragsarten

Das folgende Unterkapitel widmet sich verschiedenen unternehmensexternen Vertragsarten, genauer gesagt AGBs, Rahmenverträgen und SLAs einerseits sowie der Vereinbarung über die Auftragsvereinbarung andererseits.

5.1.1. AGBs

Die Allgemeinen Geschäftsbedingungen – oder kurz AGBs – sind eine weitverbreitete Möglichkeit, einen standardisierten Vertragsinhalt zu formulieren und somit Zeit und Geld zu sparen. Dies hat insbesondere den Vorteil, dass für alle Kunden/Kundinnen dieselben Rahmenbedingungen gelten, der Nachteil ergibt sich jedoch aus einer Ungleichbehandlung beider Vertragspartner/innen, da der/die Ersteller/in der AGBs oft gegenüber der anderen Partei in Bezug auf die Interessensdurchsetzung im Vorteil ist. [77]

Normalerweise werden in AGBs Dinge wie „Erfüllungszeit und -ort“, „Fälligkeit und Mahnung“, „Lieferfristen“, „Zahlungsmodalitäten“ und „Gewährleistungs- und/oder Schadensersatzansprüche“ geregelt, wobei auf eine rechtskonforme Formulierung ebenjener zu achten ist, da Teile davon im Zweifelsfall auch als ungültig erklärt werden können. [77, p. 365]

Wichtig ist zunächst, dass ABGs sowohl zwischen Unternehmer/in und Kunden/Kundin als auch zwischen zwei Unternehmern/Unternehmerinnen ihre Anwendung finden können, wobei zu beachten ist, dass der Vertragsinhalt explizit von beiden Vertragspartnern/Vertragspartnerinnen akzeptiert werden muss. Der Hinweis auf die geltenden AGBs muss vor Vertragsabschluss schriftlich oder mündlich erfolgen und eindeutig sein, ein nachträgliches Verweisen auf ebenjene – beispielsweise auf dem Lieferschein oder der Rechnung – ist nach aktuell gültiger Rechtsprechung unzulässig. [77]

Wenn nach Vertragsabschluss Teile der abgeschlossenen AGBs vom Gericht als gesetzes- oder sittenwidrig erklärt werden, werden diese Teile ungültig. Der Rest der Vereinbarung bleibt jedoch Vertragsinhalt. [77]

Beispiele für unzulässigen Vertragsinhalt sind gemäß Barta [77, p. 367]:

- „Überstrenge Zugangserfordernisse
- Ausschluß von Schadenersatz für vorsätzliche und grob fahrlässige Schädigung
- Beweislastverträge
- Unangemessen kurze Verfallszeiten für überlassene Sachen
- § 6 Abs 2 KSchG: ‚sofern ... sie [nicht] im einzelnen ausgehandelt[11]' wurden, gilt das gleiche auch für folgende Klauseln:
  - Ungerechtfertigtes Rücktrittsrecht des Unternehmers
  - Vertragsüberbürdung an ungenannte Dritte
  - Einseitige Leistungsänderungen
  - Ausschluß von Schadenersatz für Schäden an übernommenen Sachen"

Gemäß der WKO dürfen in AGBs zudem Gewährleistungsansprüche in keinem Fall ausgeschlossen[12] werden, wenn einer der Vertragspartner/innen als Unternehmer/in und der/die andere als Konsument/in gilt, da dann das KschG zur Anwendung kommt. [78]

In Bezug auf die Zustimmungserklärung zur Verarbeitung personenbezogener Daten gem. Art. 7 DSGVO gilt, dass diese freiwillig, eindeutig und – aufgrund der einfacheren Nachweisbarkeit – nach Möglichkeit schriftlich zu erfolgen hat [62].

Demensprechend ist es verlockend, eine Einwilligungserklärung in die AGBs zu inkludieren, jedoch gibt es ob der Gültigkeit verschiedene Ansichten.

Ein Artikel auf der Website *Help.gv.at* empfiehlt, „(vorformulierte) Einwilligungserklärungen nicht in Allgemeine Geschäftsbedingungen zu integrieren. Stattdessen sollten zusätzlich zu den AGB separate Einwilligungen der betroffenen Personen eingeholt werden. Der Grund dafür ist, dass eine in AGB enthaltene Einwilligungserklärung gegen das Prinzip der Freiwilligkeit verstoßen könnte (Koppelungsverbot)". [79]

---

[11] „Als nicht im einzelnen „ausgehandelt" iSd § 6 Abs 2 KSchG gelten Klauseln /Vertragsbestimmungen vor allem dann, wenn sie nur in AGB oder Vertragsformblätter aufgenommen und nicht im einzelnen erörtert wurden".

[12] Genauere Möglichkeiten zur Haftungsfreizeichnung im Vertragsrecht werden in Kapitel 5.3 genannt.

Die *WKO*, auf der anderen Seite, ist der Meinung, dass eine Inkludierung der Einwilligungserklärung in AGBs zulässig ist, sofern diese „in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache“ formuliert ist und sich von anderen Inhalten klar unterscheiden lässt. [79]: Der Praxistipp das Thema betreffend besagt:

> *„Das kann entweder durch eine Separierung erfolgen oder – weniger empfehlenswert (u.a. wegen des „Koppelungsverbots“) - durch eine optische Hervorhebung innerhalb der AGB […].“ [79]*

Beispielhafter Formuliervorschlag nach WKO

> *„Der Vertragspartner stimmt zu, dass seine persönlichen Daten, nämlich … (die Datenarten genau aufzählen, z.B. ‚Name‘, ‚Adresse‘ etc.) zum Zweck der… (genaue Zweckangabe […]) bei der Firma NN verarbeitet werden und die Daten … (die Datenarten genau aufzählen, z.B. ‚Name‘, ‚Adresse‘ etc.) zum Zweck der … (genaue Zweckangabe, z.B. ‚zur zentralen Abwicklung des Kunden-Beschwerdemanagements‘) an … (genaue Angabe des Übermittlungsempfängers, z.B. Name der Konzernmutter mit Anschrift) weitergegeben werden.*
>
> *Diese Einwilligung kann jederzeit bei … (Angabe der entsprechenden Kontaktdaten) widerrufen werden. Durch den Widerruf wird die Rechtmäßigkeit der bis dahin erfolgten Verarbeitung nicht berührt.“ [79]*

Um auf Nummer sicher zu gehen, sollten Unternehmen, bis die Rechtslage eindeutig geklärt ist, auf eine Aufnahme der Einwilligungserklärung in die AGBs verzichten und stattdessen die Einwilligung beispielsweise mittels eines Rahmenvertrags von den betroffenen Personen einholen.

5.1.2. Rahmenvertrag

Ein Rahmenvertrag ist eine Möglichkeit, Vetragsinhalte gemeinsam mit dem/der Vertragspartner/in zu regeln. Wichtig ist, dass der Rahmenvertrag weder zu einer Leistung oder Abnahme verpflichtet, noch als Vorvertrag gem. § 936 AGBG zu sehen ist, sondern nur die Rahmenbedingungen für künftige Verträge regelt. Darin kann alles, „was sonst auch in AGB oder Verträgen geregelt werden kann“, geregelt werden. Der Vorteil gegenüber den AGBs ist insbesondere, dass dieser „nicht nur von einem, sondern von beiden Vertragsteilen gemeinsam erstellt“ wird und somit „von einem vereinbarten Rahmenvertrag auch nicht einseitig abgegangen werden“ kann. [77, pp. 368-369]

Ein Rahmenvertrag ist daher eine gute Möglichkeit, um die Auftragsverarbeitung zu regeln oder eine Zustimmung zur Verarbeitung personenbezogener Daten zu erhalten.

5.1.3. Service-Level-Agreement

Insbesondere in Hinblick auf die DSGVO, welche besonderen Wert auf den Schutz personenbezogener Daten legt, wird es immer wichtiger, eingesetzte Systeme auf dem aktuellen Stand zu halten und somit deren Informationssicherheit zu gewährleisten. Eine Möglichkeit dies umzusetzen ist, verschiedene Services zu definieren und ein Service-Level-Agreement, oder kurz SLA genannt, darüber abzuschließen.

Das SLA regelt die Rahmenbedingungen für die Durchführung der Services zwischen dem/der Auftraggeber/in und dem/der Auftragnehmer/in, also kurz gesagt den Leistungsinhalt, das Qualitätslevel und die Kosten. [80]

Ein SLA kann dabei sowohl intern, also innerhalb eines Unternehmens zum Beispiel zwischen der IT-Abteilung und einer weiteren Abteilung, als auch extern, also zwischen zwei Unternehmen vereinbart werden und dient dazu, einerseits die Durchführung bestimmter Leistungen zu definieren und vereinbaren und andererseits eine Entscheidungsgrundlage bei Streitfällen zu liefern. [80]

Wichtige Inhalte eines SLAs sind in jedem Fall gemäß Gadatsch die [80]:

- **„Leistungsspezifikation“**; also die Beschreibung, welche Leistung zu welchen Konditionen durchgeführt wird;
- **„Termine und Fristen“**; also der Zeitpunkt, bis wann oder innerhalb welcher Frist welche Leistung durchgeführt werden muss;
- **„Konditionen“**; also bis wann welcher Betrag bezahlt werden muss;
- **„Rahmenbedingungen“**; also wie die Meldungen eintreffen müssen und zu welchen Zeiten diese bearbeitet werden
- Definition den „**Nachweis der Leistungserbringung**“ betreffend; also wie die Durchführung der Leistung gemessen und nachgewiesen werden kann;
- **„Zulässige Ausreißerquote“**; also der „[m]aximale[.] Anteil der Leistungseinheiten, die außerhalb des vereinbarten Qualitäts- / Terminrasters liegen dürfen“;
- **„Konsequenzen von SLA-Verletzungen“**; also die Maßnahmen, die der Auftraggeber gegenüber den Auftragnehmer bei Überschreitung der zulässigen Ausreißerquote setzen kann;
- **„Maßnahmen bei SLA-Verletzungen“**; also beispielsweise die Reduzierung des Leistungspreises „für entstandene Schäden, die durch die SLA-Verletzung eingetreten sind“.

Für die Einführung des SLAs ist es wichtig, dass zunächst der Auftraggeber und der Auftragnehmer gemeinsam die Anforderungen des Auftraggebers in Bezug auf Leistung und Servicelevel definieren. Nachdem der Auftragnehmer im Anschluss daran seine Leistungen in Form eines Leistungskataloges zu Papier gebracht hat und sich beide Parteien über den Preis einig geworden sind, kann der Vertrag abgeschlossen werden. [80]

Ein konkretes Beispiel über ein SLA eines Wartungsvertrags ist in Kapitel 6.1 zu finden.

5.1.4. Auftragsverarbeitung

Gem. Art. 28 DSGVO muss ein/e Auftragsverarbeiter/in dann einen Vertrag über eine Auftragsverarbeitung abschließen, wenn personenbezogene Daten verarbeitet werden[13]. Da noch nicht rechtskräftig geklärt wurde, ob es sich bei (Fern-)Wartung um eine Auftragsverarbeitung handelt, sollte im Zweifelsfall zusätzlich zur bestehenden Vertraulichkeitsvereinbarung ein Vertrag über ebenjene abgeschlossen werden.

Ein solcher Vertrag über die Auftragsverarbeitung muss den Gegenstand, die Dauer und den Sinn und Zweck der Verarbeitung sowie die Kategorien und Arten der Daten und die zum Schutz der Daten ergriffenen, technischen oder organisatorischen Maßnahmen beinhalten und dient dazu, eine Verletzung der Verordnung und somit hohe Geldstrafen zu vermeiden. [19]

Ein Mustervertrag nach WKO [81] ist in Kapitel 6.4 zu finden.

5.2. Übersicht über verschiedene unternehmensinterne Vertragsarten

Das folgende Unterkapitel widmet sich einerseits der Betriebsvereinbarung als unternehmensinterne Vertragsart. Andererseits werden die Datenschutz-Folgeabschätzung und das Verarbeitungsverzeichnis ebenso kurz behandelt und erklärt, da diese gemäß Art. 35 bzw. Art. 30 in manchen Fällen verpflichtet erstellt werden müssen.

5.2.1. Datenschutz-Folgeabschätzung

Bei der Einführung von neuen Technologien, welche die Persönlichkeitsrechte einer Person in Hinblick auf den Datenschutz betreffen können, muss gem. Art. 35 DSGVO eine Datenschutz-Folgeabschätzung durchgeführt werden[14].

[13] Genaueres in Kapitel 4.2.3.
[14] Wie in Kapitel 4.2.3 genauer beschrieben.

Beinhalten muss eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO in jedem Fall eine Beschreibung und den Zweck der Verarbeitungsvorgänge samt Bewertung der Notwendigkeit ebenjener, sowie eine Risikobewertung samt zu treffender Schutzmaßnahmen die Rechte der betroffenen Person betreffend. [62]

Ein Muster-Datenschutz-Folgeabschätzung nach Feiler und Horn [82] ist in Kapitel 6.2 zu finden.

5.2.2. Verarbeitungsverzeichnis

Werden personenbezogene Daten verarbeitet, müssen Verantwortliche und Auftragsverarbeiter in Unternehmen mit mehr als 250 Mitarbeitern/Mitarbeiterinnen oder einem Jahresumsatz über 50 Millionen Euro ein Verarbeitungsverzeichnis über ebenjene Daten führen [19]. Dieses dient insbesondere dazu, die Sorgfaltspflichten gegenüber der Datenschutzbehörde nachzuweisen[15].

Das Verzeichnis über die Verarbeitungsvorgänge die personenbezogenen Daten betreffend muss in jedem Fall die Kontaktdaten und den Namen des/der Auftragsverarbeiters/Auftragsverarbeitern und/oder des/der Verantwortlichen sowie die gesetzten technischen und organisatorischen Maßnahmen beinhaltet. Zudem haben Verantwortliche weitere Punkte in das Verzeichnis zu inkludieren, wie Löschfristen und die Kategorien der betroffenen Personen und Daten. [19].

Ein Muster-Verarbeitungsverzeichnis nach Feiler und Horn [83] ist in Kapitel 6.3 zu finden.

5.2.3. Betriebsvereinbarung

Eine Möglichkeit, sicherheitstechnische Systeme rechtskonform in einem Betrieb einzusetzen, ist, eine Betriebsvereinbarung[16] darüber abzuschließen.

Es gibt nun mehrere Möglichkeiten, wie solch eine Betriebsvereinbarung umgesetzt werden kann. Entweder man schließt für jedes System eine vollständige Betriebsvereinbarung ab, in welcher auch jeweils die allgemein gültigen Rahmenbedingungen enthalten sind, oder man erstellt eine Rahmenbetriebsvereinbarung über die allgemeinen Regelungen. Die spezifischeren Regelungen für jedes System – wie beispielsweise einer Zutrittskontrolle oder Videoüberwachung – werden dann in jeweils eigenen Betriebsvereinbarungen definiert, welche beispielsweise immer den aktuellen Ist-Stand des Systems samt technischer Beschreibung beinhalten muss. [84]

---

[15] Wie in Kapitel 4.2.3 ausführlicher beschrieben.
[16] Genaueres zur Rechtslage siehe Kapitel 4.3.

Die sinnvollere Variante ist gemäß der Gewerkschaft der Privatangestellten – Druck, Journalismus – kurz *GPA-djp* [84] „die Teilung in eine übergreifende, allgemein gültige Rahmenbetriebsvereinbarung (RBV) zur Verwendung personenbezogener Daten im Betrieb und Zusatzbetriebsvereinbarungen zu den konkreten im Einsatz befindlichen bzw. geplanten IKT“, da die Systeme wesentlich schnelllebiger sind als die übergreifenden Rahmenbedingungen. [84, p. 1]

Kapitel 6.5 zeigt ein Muster über eine Rahmenbetriebsvereinbarung, welche die Verwendung der personenbezogenen Beschäftigungsdaten betrifft, bereits DSGVO konform ist und von der GPA-djp erstellt wurde [84, pp. 2-13]:

5.3. Haftungsfreizeichnung im Vertragsrecht

Ein für Unternehmen wichtiger Bestandteil in Verträgen ist eine etwaige Haftungsfreizeichnung, also die Einschränkung oder der Ausschluss von Haftung in Bezug auf die Gewährleistung, das Schadenersatzrecht oder die Produkthaftung. Hierbei ist aufgrund der unterschiedlichen Regelungen insbesondere die Unterscheidung von Verträgen zwischen zwei Konsumenten/Konsumentinnen oder zwei Unternehmern/Unternehmerinnen sowie zwischen Unternehmer/in und Konsument/in wichtig.

5.3.1. Gewährleistung

Nach der *WKO* versteht man unter der Gewährleistung „die verschuldensunabhängige Haftung für Sach- und Rechtsmängel, die zum Übergabe- bzw. Lieferzeitpunkt schon vorhanden sind“ [85], wobei zu beachten ist, dass gem. Art. 928 ABGB jedoch „für Mängel, die offensichtlich sind („ins Auge fallen“) grundsätzlich keine Gewähr zu leisten [ist]“ [86]. „Allerdings haftet der Verkäufer trotz Offenkundigheit, wenn er die fehlende Eigenschaft ausdrücklich zugesichert oder arglistig verschwiegen hat“ [86].

Die Gewährleistung darf insbesondere nicht mit der Garantie verwechselt werden. Der wesentliche Unterschied ist, dass eine Gewährleistung prinzipiell gesetzlich vorgeschrieben ist, während eine Garantie freiwillig gewährt werden kann. Eine Garantie kann dabei zudem „an Bedingungen und Auflagen geknüpft werden“ und gilt unabhängig davon, ob der Mangel bereits zum Übergabezeitpunkt vorhanden war oder nicht. [85]

Bei beweglichen Sachen verjährt die Gewährleistung grundsätzlich zwei, bei unbeweglichen Sachen drei Jahre nach Lieferdatum, wobei sie bei gebrauchten Sachen auf ein Jahr verkürzt werden kann. Nach sechs Monaten gilt zudem die Beweislastumkehr, was bedeutet, dass innerhalb der ersten sechs Monate der Verkäufer beweisen muss, dass der Mangel nicht bei Lieferung vorlag, während nach sechs Monaten der Käufer beweisen muss, dass der Mangel bei Übergabe bereits vorlag. [85]

Die Gewährleistung umfasst dabei prinzipiell das Recht, den Mangel entweder beheben oder das Produkt austauschen zu lassen, wobei hier immer die Verhältnismäßigkeit gewahrt und somit die genaue Vorgehensweise im Einzelfall entschieden werden muss. Ist weder ein Austausch noch eine Reparatur möglich, kann auch eine Preisminderung oder eine Wandlung, also ein Rücktritt vom Vertrag inklusive Rückerstattung des bezahlten Betrags, durchgeführt werden. [85]

Beim Ausschluss der Gewährleistung in Verträgen und AGBs sind folgende Dinge zu beachten:

Verhältnis Unternehmer/in zu Unternehmer/in oder Privatperson zu Privatperson

Wird ein Vertrag zwischen zwei Unternehmern/Unternehmerinnen oder zwei Privatpersonen abgeschlossen, findet das KSchG keine Anwendung, wodurch die Gewährleistung prinzipiell eingeschränkt oder ausgeschlossen werden kann, wenn dies im Vertrag explizit erwähnt und von beiden Seiten akzeptiert wurde und keine Sittenwidrigkeit vorliegt. [87] [88]

Uneinigkeit besteht darin, ab wann bei einem Ausschluss oder einer Einschränkung der Gewährleistung eine Sittenwidrigkeit vorliegt.

Nach Nosko ist ein gänzlicher Ausschluss der Gewährleistung auch zwischen Unternehmern/Unternehmerinnen sittenwidrig, es müssen vertraglich zumindest vier Wochen als Untergrenze gesetzt werden. Anders sieht es jedoch mit der Beweislastumkehr zugunsten des/der Käufers/Käuferin aus, hier ist es möglich, diese vertraglich auszuschließen. [89]

Gemäß einem Artikel auf der Website *Recht Einfach* wird die Gewährleistung nach § 929 ABGB jedoch ausgeschlossen, „wenn der Übernehmer wissentlich eine fremde Sache kauft oder auf die Gewährleistung ausdrücklich verzichtet“ [86]

Auf der sicheren Seite ist man, wenn man vertraglich eine kürzere Laufzeit der Gewährleistung vereinbart, diese aber nicht gänzlich ausschließt.

Verhältnis Unternehmer/in zu Konsument/in

Bei einem Vertrag zwischen einem/einer Unternehmer/in und einem/einer Konsumenten/Konsumentin kommt das KSchG zur Anwendung, welches einen kompletten Ausschluss der Gewährleistung untersagt. Daher sollte auf einen allgemeinen Ausschluss der Gewährleistung in den AGBs verzichtet werden. [87]

Bei gebrauchten beweglichen Sachen ist jedoch, wie bereits oben erwähnt, die Verkürzung der gesetzlichen Gewährleistung auf ein Jahr zulässig. Diese muss jedoch explizit vertraglich vereinbart werden, da ein reines Verweisen auf die AGBs ist auch in diesem Fall rechtlich nicht zulässig ist. [87]

Beispiele für Mängel in Bezug auf die Sicherheitstechnik

Die Website *Konsument.at* gibt ein anschauliches Beispiel, wann eine sogenannte Mängelrüge im Sicherheitstechnikbereich im Zuge der gesetzlichen Gewährleistungsfest erfolgreich und rechtmäßig sein kann:

> *„Herr Bernegger lässt an der Eingangstüre eine (bewegliche) Alarmanlage montieren. Als er wenige Wochen später feststellen muss, dass diese nicht funktioniert, rügt er den Mangel sofort und verlangt Verbesserung. Er kündigt an, den Kaufpreis von rund 1500 Euro so lange nicht zu bezahlen, als der Mangel nicht behoben ist. Die Firma rührt sich nicht. Herr Bernegger hat keine Zeit, sich um eine Ersatzvornahme durch eine andere Firma zu bemühen und wartet einfach ab. Nach 30 Monaten bekommt er ein Mahnschreiben der Montagefirma. Er möge den Rechnungsbetrag samt Zinsen und Mahnspesen bezahlen, ansonsten würde er geklagt. Herr Bernegger verweist auf seine – fristgerechte – Mängelrüge und verweigert die Zahlung. Als die Firma ihn klagt , wendet er bei Gericht ein, dass er den Mangel innerhalb der zweijährigen Gewährleistungsfrist gerügt und Verbesserung verlangt habe. Bis zu einer Verbesserung habe er das Recht, den Kaufpreis zurückzubehalten. Das Gericht wird daher die Klage der Montagefirma abweisen.“ [90]*

Wichtig ist in Bezug auf den Gewährleistungsanspruch in jedem Fall die rechtzeitige Bekanntgabe der Mängel sowie die rechtzeitige Forderung der Behebung. Für Unternehmen empfiehlt es sich, dem Gewährleistungsanspruch innerhalb der ersten sechs Monate im Zweifel zu entsprechen, da sie in diesem Zeitpunkt nach derzeit gültiger Rechtslage beweisen müssen, dass der Mangel zum Übergabezeitpunkt noch nicht bestanden hat, was in der Praxis schwierig ist.

5.3.2. Schadenersatz

Wenn dem/der Käufer/in aus einem Mangel ein Schaden entsteht, ist der/die Verkäufer/in unter bestimmten Umständen gemäß den Bestimmungen des Schadenersatzrechts dafür haftbar.

Nach der WKO ist im § 1293 AGBG der Begriff des Schadens als ein „Nachteil, der jemandem am Vermögen, an seinen Rechten oder an seiner Person zugefügt worden ist“, definiert. [91]

Ein Schaden kann dabei einerseits ein Vermögensschaden und andererseits ein ideeller Schaden sein, zudem unterscheidet man im Vertragsrecht noch zwischen dem Nichterfüllungsschaden – also dem Schaden, der aus der Nichterfüllung vertraglicher Pflichten entsteht – und dem Vertrauensschaden – also dem Schaden, der daraus entsteht, dass ein Vertrag nicht zustande gekommen ist. [91]

Schadenersatz gemäß ABGB ohne Verstöße gegen das Grundrecht auf Datenschutz

Wurde der Schaden nun durch ein rechtswidriges Verhalten, sprich leichte oder grobe Fahrlässigkeit oder Vorsatz, verursacht, kann innerhalb von 30 Jahren ein Schadenersatz eingefordert werden, wobei zu beachten ist, dass dies ab Kenntnis des Schadens nur für 3 Jahre möglich ist. [91]

In den ersten 10 Jahren muss zudem der Verkäufer beweisen, dass er nicht für den Schaden verantwortlich ist, danach besteht eine Beweislastumkehr. [88]

Zusätzlich besteht nach der Vereinbarung nach dem UN-Kaufrecht „ein Schadenersatzanspruch unabhängig vom Verschulden des Schädigers“, was bedeutet, dass ein/e Verkäufer/in selbst dann Schadenersatz für einen eingetretenen Schaden zu leisten hat, wenn er/sie den Schaden selbst nicht schuldhaft verursacht hat, sondern nur beispielsweise als Zwischenhändler/in diente. Es empfiehlt sich daher, die Anwendung des UN-Kaufrechts in jedem Fall vertraglich auszuschließen. [89]

Folgendes ist beim Haftungsausschluss in Bezug auf den Schadenersatz vertraglich zu beachten.

- **Verhältnis Unternehmer/in zu Unternehmer/in**
  Zwischen Unternehmern/Unternehmerinnen ist der Ausschluss oder die Einschränkung von Haftungsansprüchen in Bezug auf den Schadenersatz bei leichter Fahrlässigkeit prinzipiell zulässig, außer es entstand daraus ein Personenschaden. [88]
  Ob der Haftungsausschluss für grobe Fahrlässigkeit zulässig ist, muss im Einzelfall beurteilt werden, da der oberste Gerichtshof diesbezüglich bereits unterschiedliche Entscheidungen gefällt hat. Bei Vorsatz ist weder ein Ausschluss noch eine Einschränkung von Haftungsansprüchen erlaubt. [88]
  Eine weitere vertragliche Gestaltungsmöglichkeit sieht vor, dass die Beweislastumkehr vertraglich ausgeschlossen werden kann. Zudem können die Verjährungsfristen im Einzelfall verkürzt werden, der OGH entschied beispielsweise in einem konkreten Fall, dass die Verkürzung der Meldefrist ab Kenntnisnahme von 3 Jahren auf 6 Monate zulässig war. [88]

- **Verhältnis Unternehmer/in zu Konsument/in**
  Auch bei einem Vertragsverhältnis zwischen einem/einer Unternehmer/in und einem/einer Konsumenten/Konsumentin kann die Haftung im Falle einer leichten Fahrlässigkeit vertraglich zum Teil ausgeschlossen oder eingeschränkt werden, sofern kein Personenschaden vorliegt. Voraussetzungen dafür sind, dass der/die Konsument/in dem Haftungsausschluss freiwillig zugestimmt hat, keine große wirtschaftliche Übermacht in Bezug auf den/die Unternehmer/in besteht und dass der Haftungsausschluss konkret begründet werden kann. [88]
  Haftungseinschränkungen oder Ausschlüsse in Bezug auf grobe Fahrlässigkeit, Vorsatz oder die Anspruchsdauer sind gegenüber Konsumenten/Konsumentinnen auf jeden Fall unzulässig, ebenso wie generelle Haftungseinschränkungen oder Ausschlüsse in AGBs. [88]

Schadenersatz bei Verstößen gegen das Grundrecht auf Datenschutz

Wird der Schaden durch eine Verletzung des Grundrechts auf Datenschutz verursacht, gelten die strengeren Bestimmungen gemäß der DSGVO.

Prinzipiell haftet der/die Verantwortliche in jedem Fall, außer er kann nachweisen, dass er nicht für den Schaden verantwortlich ist. Der/Die Auftragsverarbeiter/in haftet nur, wenn er/sie nicht nachweisen kann, dass er/sie seine/ihre Pflichten gegenüber dem/der Verantwortlichen erfüllt hat. [92]

Derzeit gibt es bezüglich der Haftungseinschränkung oder des Haftungsausschlusses in Österreich weder Rechtsprechungen noch Lehrmeinungen, „[n]ach deutscher Ansicht ist ein vertraglicher Haftungsausschluss [jedoch] nicht möglich." [93]

5.3.3. Produkthaftung

Im Zuge der Produkthaftung werden sowohl Personenschäden als auch Sachschäden ersetzt, wobei bei Sachschäden nur die Schäden ersetzt werden, die das fehlerhafte Produkt nicht direkt betreffen. Zudem gilt bei privaten Sachschäden ein Selbstbehalt von 500 Euro. [94]

Gemäß der Produkthaftung haftet der/die Hersteller/in, der/die Quasi-Hersteller/in oder der/die Importeur/in für Schadenersatzansprüche, die aus fehlerhaft in den Verkehr gebrachten Produkten entstehen. Sind diese Personen oder Unternehmen nicht feststellbar, kann auch der/die Händler/in haftbar gemacht werden. Gemäß WKO kommen „als Fehlerarten […] Konstruktionsfehler, Produktionsfehler […] und Instruktionsfehler […] in Betracht." [94]

Die Haftung ist verschuldensunabhängig, sprich es wird sowohl für Fahrlässigkeit als auch für Versehen gehaftet. Ein Haftungsausschluss ist prinzipiell nicht möglich, außer:

- „der Hersteller, Importeur oder Händler kann nachweisen, dass das Produkt im Zeitpunkt des Inverkehrbringens keinen Fehler hatte“; [94]
- „der Fehler des Produkts ist auf die Einhaltung zwingender Rechtsvorschriften zurückzuführen, die im Zeitpunkt des Inverkehrbringens gegolten haben;“ [94]
- „das Produkt entsprach im Zeitpunkt des Inverkehrbringens dem Stand der Technik, sodass zu diesem Zeitpunkt der Fehler nicht als solcher qualifiziert werden konnte.“ [94]

Nach 10 Jahren verjähren Schadenersatzansprüche aus der Produkthaftung. Zudem muss ab Kenntnis des Schadens ein Anspruch innerhalb von drei Jahren geltend gemacht werden. [94]

Haftungsausschluss

Es ist sowohl zwischen Unternehmern/Unternehmerinnen als auch zwischen einem/einer Unternehmer/in und einem/einer Konsumenten/Konsumentin unzulässig, Ansprüche aus der Produkthaftung vertraglich auszuschließen. [88]

5.3.4. Fiktives Beispiel zur Haftung

Ausgangslage: Ein/e Hersteller/in verkauft ein Sicherheitssystem, welches eine biometrische Zutrittskontrollanlage, eine Gefahrenmeldeanlage und ein Videoüberwachungssystem umfasst, an eine/n Unternehmer/in, welche/r dieses System in seinem/ihrem Unternehmen einsetzt. Die Übertragung der Daten von der Gefahrenmeldeanlage und dem Videoüberwachungssystem werden aus Sicherheitsgründen über Kabel abgewickelt und auch die Zutrittskontrollanlage ist aufgrund der schnelleren Wirksamkeit der Zutrittsrechte als Online-Zutrittskontrolle konzipiert.

Gemäß SLA muss der/die Hersteller/in die gesamte Verkabelung und das Aufsetzen der Systeme erledigen, die Software, der Server und die Daten liegen jedoch bei dem/der Unternehmer/in. Der/Die Hersteller/in hat nur bei der vertraglich vereinbarten Fernwartung Zugriff auf die Systeme. Vertraglich vereinbart ist ebenfalls, dass der/die Unternehmer/in für die Sicherheit der Daten auf seinem System mittels geeigneter Maßnahmen, wie Schutz vor Zugriff oder Verschlüsselung, selbst zu sorgen hat. Im Vertrag wurde die Haftung in Bezug auf Schadenersatz bei leichter Fahrlässigkeit ausgeschlossen, die Gewährleistungsfristen blieben jedoch mangels eindeutiger Rechtslage unberührt.

Daraus ergeben sich folgende Rollen: Der Vertrag wurde zwischen zwei Unternehmern/Unternehmerinnen abgeschlossen, wodurch eine Haftungseinschränkung bei

Schadenersatz zulässig ist. [88] In Bezug auf die Verarbeitung personenbezogener Daten ist der/die Hersteller/in bei der Wartung mangels derzeit eindeutiger Rechtslage vermutlich als Auftragsverarbeiter/in und der/die Unternehmer/in in jedem Fall als Verantwortliche/r zu sehen, wodurch die beiden einen Vertrag über eine Auftragsverarbeitung gem. Art. 28 DSGVO abschließen müssen. [62] Der/Die Unternehmer/in hat zudem die Pflicht, eine Datenschutz-Folgeabschätzung gem. Art 35 DSGVO durchzuführen, da er/sie durch das biometrische Zutrittssystem eine besonders schützenswerte Kategorie personenbezogener Daten verarbeitet [62].

Beispiel 1: Gewährleistung und Schadenersatz

Macht nun der/die Hersteller/in bei der Verkabelung einen Fehler und bemerkt der/die Unternehmer/in diesen innerhalb der ersten sechs Monate der gesetzlichen Gewährleistungsfrist, muss der/die Hersteller/in den Fehler in jedem Fall beheben, sofern der/die Unternehmer/in den/die Hersteller/in fristgerecht darauf aufmerksam gemacht hat [90].

Tritt aufgrund der mangelnden Verkabelung zusätzlich ein Schaden ein, da beispielsweise ein Einbruch aufgrund des Nicht-Auslösens der Gefahrenmeldeanlage nicht oder zu spät erkannt wurde, ist zu beurteilen, ob eine leichte oder grobe Fahrlässigkeit vorliegt.

Lag nur eine leichte Fahrlässigkeit vor und trat dadurch weder ein Personenschaden noch eine Datenschutzverletzung ein, ist der/die Hersteller/in nicht haftbar, da der Schadenersatz bei leichter Fahrlässigkeit vertraglich ausgeschlossen wurde.

Hat der/die Hersteller/in jedoch grob fahrlässig gehandelt, muss er im Sinne des Schadenersatzrechts für den Schaden, der durch die nicht ordnungsgemäße Verkabelung eingetreten ist, aufkommen.

Werden personenbezogene Daten entwendet, die beispielsweise auf einem USB-Stick gespeichert wurden, muss die Datenschutzverletzung in jedem Fall der Datenbehörde angezeigt werden. Der/Die Verantwortliche ist dafür haftbar, kann sich aber gem. Art. 82 DSGVO einen Teil des entrichteten Schadenersatzes von dem/der Hersteller/in holen, die genaue Höhe ergibt sich aus dem Mitverschulden des/der Herstellers/Herstellerin und den sonstigen getroffenen Sicherheitsmaßnahmen, wie einer etwaigen Verschlüsselung der Daten [62].

Beispiel 2: Schadenersatz bei kompromittiertem System

Der/Die Hersteller/in hat die Systeme ordnungsgemäß installiert und an den/die Unternehmer/in übergeben. Diese/r speichert die biometrischen Templates für das Zutrittskontrollsystem mitsamt der Software auf einem Server, auf den nur autorisiertes Personal Zugriff hat. Der Server steht in einem

zutritts-, zugriffs-, und zugangsgesichertem Bereich, auf eine Pseudonymisierung der gespeicherten Daten wurde jedoch verzichtet. Zusätzlich ist die Festplatte gemäß dem aktuellen Stand der Technik verschlüsselt, nicht jedoch die Daten selbst.

Erlangt nun ein/e unbefugte/r Dritte/r Zugriff auf den Server und kann personenbezogene Daten stehlen, liegt in jedem Fall eine Datenschutzverletzung vor, wodurch eine Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden nach Kenntnisnahme erfolgen muss [62].

In Bezug auf den zu leistenden Schadenersatz unterscheidet man nun im Wesentlichen die folgenden Möglichkeiten:

(1) Den/Die Hersteller/in, der/die gleichzeitig Auftragsverarbeiter/in ist, trifft keine Schuld, da er/sie nachweisen kann, dass er/sie zu diesem Zeitpunkt keinen Zugriff auf das System hatte. Den/Die Verantwortliche/n trifft somit die alleinige Schadenersatzpflicht, da er/sie nicht nachweisen kann, alle technischen und organisatorischen Maßnahmen getroffen zu haben, um die Daten zu schützen.

(2) Der/Die Hersteller/in führte im Zeitraum des Datendiebstahls Wartungsarbeiten durch und kann nicht eindeutig beweisen, dass er/sie an der Kompromittierung des Systems keine Schuld trägt. Beide Parteien sind schadenersatzpflichtig.

(3) Die Kompromittierung des Systems erfolgte aufgrund eines Fehlers der Software. In diesem Fall ist einerseits der/die Verantwortliche haftbar, da er/sie nicht nachweisen kann, alle technischen und organisatorischen Maßnahmen getroffen zu haben, um die Daten zu schützen. Zusätzlich können jedoch Ansprüche aus der Produkthaftung geltend gemacht werden, wenn nachgewiesen werden kann, dass ohne den Softwarefehler der Datendiebstahl nicht eingetreten wäre.

Wie das vorherige Beispiel zeigt, ist es wichtig, die gesetzlichen Vorgaben genau zu befolgen und insbesondere geeignete Maßnahmen zu setzen, um personenbezogene Daten zu schützen.

6. Beispielverträge

Im folgenden Kapitel werden schließlich einige zuvor beschriebenen Vertragsarten (SLA, Auftragsvereinbarung, Rahmenbetriebsvereinbarung, Verzeichnis der Verarbeitungstätigkeiten und Datenschutzfolgeabschätzung) mittels konkreter Beispiele anschaulich gemacht. Im Falle des SLAs wurde das Muster selbst erstellt, bei den restlichen Verträgen wurde auf Quellen zurückgegriffen.

6.1. Beispiel eines Service-Level-Agreements [17]

Der Auftraggeber: [NN] (im Folgenden Auftraggeber)	Der Auftragnehmer: [NN] (im Folgenden Auftragnehmer)

(1) Präambel

Im Zuge dieses SLAs kann der Auftraggeber nach dem Kauf eines Systems zwischen einem oder mehreren Wartungs-Dienstleistungen wählen:

- Wartung und/oder Instandhaltung der Alarmanlage
- Wartung und/oder Instandhaltung des Zutrittskontrollsystems
- Wartung und/oder Instandhaltung der Videoüberwachungsanlage

Die nachfolgend beschriebenen Services und Leistungen gelten mit dem zu Stande kommen des Vertrags als akzeptiert.

(2) Dauer der Vereinbarung

Der Vertrag über das gewählte Service kommt nach einer Einigung über die Kosten am Tag der Vertragsunterzeichnung beider Parteien zu Stande.

„Der Instandhaltungsvertrag wird auf eine Mindestlaufzeit von drei Jahren abgeschlossen und verlängert sich nach Ablauf dieses Zeitraums jeweils um ein weiteres Jahr, sofern er nicht von einem der Vertragsparteien drei Monate vor Ablauf der Mindestlaufzeit oder des jeweiligen Verlängerungszeitraumes mit eingeschriebenem Brief gekündigt wird, wobei das Datum des Einlangens des Briefes für die Rechtzeitigkeit maßgeblich ist.“ [95, p. 4]

[17] Als Leitfaden für den Aufbau diente das von Dina Knorr erstellte SLA der Firma Ordana [98].

(3) Leistungsbeschreibung

Folgende Leistungen können im Zuge des SLAs vereinbart werden:

(1) Inspektion der Alarmanlage gemäß OVE R2
   a. [Beschreibung der genauen Maßnahmen einfügen]

(2) Inspektion des Zutrittskontrollsystems gemäß OVE R9
   a. [Beschreibung der genauen Maßnahmen einfügen]

(3) Inspektion der Videoüberwachungsanlage gemäß OVE R10
   a. [Beschreibung der genauen Maßnahmen einfügen]

(4) (Fern-) Wartung der Alarmanlage
   a. Allgemeine Problemannahme durch den Help-Desk
   b. Änderung der Konfiguration
   c. Durchführen von Wartungsarbeiten
   d. Einspielen von Updates/Patches
   e. Behebung von Störungen
   f. [Durch zusätzliche Maßnahmen ergänzen]

(5) (Fern-) Wartung des Zutrittskontrollsystems
   a. Allgemeine Problemannahme durch den Help-Desk
   b. Änderung der Konfiguration
   c. Durchführen von Wartungsarbeiten
   d. Einspielen von Updates/Patches
   e. Behebung von Störungen
   f. [Durch zusätzliche Maßnahmen ergänzen]

(6) (Fern-) Wartung der Videoüberwachungsanlage
   a. Allgemeine Problemannahme durch den Help-Desk
   b. Änderung der Konfiguration
   c. Durchführen von Wartungsarbeiten
   d. Einspielen von Updates/Patches
   e. Behebung von Störungen
   f. [Durch zusätzliche Maßnahmen ergänzen]

(4) Verfügbare Servicelevel

Parameter	SLA 0		SLA 1	SLA 2
Verfügbarkeit pro Jahr	99,5 %		99,7 %	99,85 %
Störungsannahme	Mo-Do	Fr	Mo-So	Mo-So
	[Zeitraum]	[Zeitraum]	[Zeitraum]	[Zeitraum]
Servicebereitschaft	Mo-Di	Fr	Mo-So	Mo-So
	[Zeitraum]	[Zeitraum]	[Zeitraum]	[Zeitraum]
Reaktionszeit	[Reaktionszeit]		[Reaktionszeit]	[Reaktionszeit]
Entstördauer	[Entstördauer]		[Entstördauer]	[Entstördauer]
Wartungsfenster	Mo-So		Mo-So	Mo-So
	[Zeitraum]		[Zeitraum]	[Zeitraum]
Kostenpflichtige Entstördienstleistungen	Exkludiert		Exkludiert	Inkludiert

(5) Leistungsvergütung

„Die vereinbarte jährliche Wartungspauschale wird quartalsweise im voraus in Rechnung gestellt und ist lt. den Zahlungsbedingungen nach Vereinbarung zur Zahlung fällig. Im Falle des Zahlungsverzuges gelten Verzugszinsen in der Höhe von 5% über dem jeweiligen Diskontzinssatz der Österreichischen Nationalbank als vereinbart. Zahlungsziel ist 14 Tage netto ohne jeden Abzug. Preisangaben immer netto ohne USt.“ [95]

„Im Falle des Zahlungsverzuges ist [der Auftragnehmer] nach Verstreichen einer 14tägigen Nachfrist von sämtlichen Verpflichtungen aus diesem Instandhaltungsvertrag entbunden, ohne daß dadurch der Anspruch von [dem Auftragnehmer] auf die laufende Bezahlung der Wartungspauschale beeinträchtigt wird.“ [95]

[Ort], am [Datum]	[Ort], am [Datum]
Für den Auftraggeber:	Für den Auftragnehmer:
.....	.....
[Name samt Funktion]	[Name samt Funktion]

6.2. Muster einer minimalistischen Datenschutz-Folgenabschätzung nach [82] [18]

Inhalt

I. Allgemeine Information zur Organisation

1. Name und Kontaktdaten der Organisation	
Name/Firmenwortlaut der Organisation:	
Adresse:	
E-Mail-Adresse:	
2. Name und Kontaktdaten des Datenschutzbeauftragten (sofern bestellt)	
Name:	
Adresse:	
E-Mail-Adresse:	
Telefonnummer:	

II. Beschreibung der Verarbeitungstätigkeit

Bezeichnung der Verarbeitungstätigkeit	*Bezeichnung, wie sie auch im Verzeichnis der Verarbeitungstätigkeiten angegeben wurde; zB Kundenbeziehungsmanagement.*
Datenkategorien, Verarbeitungszwecke, Übermittlungsempfänger, Speicherdauer	*zB Verweise auf eine anbei befindliche Kopie des Eintrags im Verzeichnis der Verarbeitungstätigkeiten.*

[18] Diese Datenschutz-Folgeabschätzung wurde von Feiler und Horn erstellt und als Beispiel in dieser Arbeit wörtlich übernommen. [93]

Art, Umfang und Kontext der Verarbeitung	*zB Wie viele Betroffene wird es geben? Was ist der unternehmerische Kontext der Verarbeitung? (zB Teil einer größeren Digitalisierungsstrategie)*
Funktionale Beschreibung der Datenverarbeitung	*zB Verweis auf eine beiliegende funktionale Dokumentation des Systems, wie sie hoffentlich die IT-Abteilung liefern kann.*
Verwendete Ressourcen (Software, Hardware, Personal)	*zB Aufstellung der verwendeten Software-Produkte sowie der eingesetzten Hardware bzw Verweis auf Cloud-Dienste von Drittanbietern.*

III. Prüfung der Rechtmäßigkeit

1. Grundsätze der Datenverarbeitung einschließlich Rechtsgrundlage für die Verarbeitung	
Rechtmäßigkeit – Welche Rechtsgrundlage?	*Identifikation einer anwendbaren Rechtsgrundlage (siehe Schritt 8, Zwischenschritt A des Umsetzungsplans)*
Zweckbindung	*Beschreibung der Maßnahmen, mit denen zweckwidrige Datenverarbeitungen verhindert werden.*
Datenminimierung	*Prüfung, ob tatsächlich nicht mehr Daten als erforderlich erhoben werden*
Speicherbegrenzung	*Prüfung, ob die Daten tatsächlich nicht länger als erforderlich aufbewahrt werden.*
Sicherheit	*zB Verweise auf eine anbei befindliche Kopie des Eintrags im Verzeichnis der Verarbeitungstätigkeiten*
2. Eingesetzte Auftragsverarbeiter	
Welche Auftragsverarbeiter und Sub-Auftragsverarbeiter werden eingesetzt und (i) hat sich der Verantwortliche von ihrer Zuverlässigkeit überzeugt und (ii) sind rechtskonforme Auftragsverarbeitervereinbarungen geschlossen worden?	*Auflistung der eingesetzten Auftragsverarbeiter und Bestätigung ihrer Zuverlässigkeit sowie der Rechtskonformität der Auftragsverarbeitervereinbarungen, die in Kopie beigelegt werden sollten.*

3. Internationale Datenübermittlungen	
Gibt es Datenübermittlungen in Drittländer oder an internationale Organisationen?	*Beschreibung allfälliger internationaler Datenübermittlungen und Beschreibung ihrer Absicherung (siehe Schritt 8, Zwischenschritt C des Umsetzungsplans).*
4. Datenschutzmitteilung an Betroffene	
Ist die entworfene Datenschutzmitteilung rechtskonform?	*Beschreibung, wie die Datenschutzmitteilung den Betroffenen zugänglich gemacht wird sowie Bestätigung, dass diese rechtskonform ist; Verweis auf die anbei befindliche Kopie der Datenschutzmitteilung.*
5. Betriebsvereinbarung	
Ist eine Betriebsvereinbarung erforderlich?	*Erklärung weshalb (nicht) sowie gegebenenfalls ein Verweis auf eine anbei befindliche Kopie der Betriebsvereinbarung.*
6. Möglichkeit für die Betroffenen, ihre Rechte geltend zu machen	
Wie sieht der Prozess zur Geltendmachung der Betroffenenrechte	*Beschreibung des Prozesses zur Geltendmachung und Umsetzung*
und ihrer Umsetzung beim Verantwortlichen aus?	*der Betroffenenrechte auf Auskunft, Datenportabilität, Berichtigung, Löschung, Widerspruch und Einschränkung der Verarbeitung*

IV. Involvierung des Datenschutzbeauftragten und der Betroffenen

In welcher Form wurde der Datenschutzbeauftragte involviert?	*Entweder (i) Hinweis, dass kein Datenschutzbeauftragter bestellt wurde oder (ii) Beschreibung der Involvierung des Datenschutzbeauftragten sowie gegebenenfalls Verweis auf seine anbei befindliche Stellungnahme (falls er die Folgenabschätzung nicht ohnedies selbst durchgeführt hat). Sofern der Verantwortliche von der Empfehlung des Datenschutzbeauftragten abweicht, sollte dies gesondert dokumentiert und begründet werden.*

In welcher Form wurde der Standpunkt der Betroffenen erhoben und berücksichtigt?	*zB wenn die Betroffenen die Arbeitnehmer sind, Verweis auf eine anbei befindliche Kopie einer Betriebsvereinbarung; wird der Standpunkt der Betroffenen nicht eingeholt oder wird der Standpunkt im Ergebnis nicht berücksichtigt, ist dies zu begründen (siehe Frage 27).*

V. Risiken für die Betroffenen

1. Identifikation und vorläufige Bewertung der Risiken für die Betroffenen		
Beschreibung des Risikos	Vorläufige Bewertung (niedrig/mittel/hoch)	Risikominderungsmaßnahme (allenfalls mit Umsetzungsfrist)
…	…	…
…	…	…
2. Bewertung des Restrisikos		
Risikoklassifizierung (niedrig/mittel/hoch)	*niedrig/mittel/hoch*	
Erläuterung der Risikoklassifizierung	*Beschreibung des Restrisikos“*	

6.3. Muster eines minimalistischen Verarbeitungsverzeichnisses nach [83][19]

Inhalt

I. Allgemeine Information zur Organisation

1. Name und Kontaktdaten der Organisation	
Name/Firmenwortlaut der Organisation:	
Adresse:	
E-Mail-Adresse:	
2. Name und Kontaktdaten des Datenschutzbeauftragten (sofern bestellt)	
Name:	
Adresse:	
E-Mail-Adresse:	
Telefonnummer:	

II. Verarbeitungstätigkeiten, für welche die Organisation Verantwortlicher ist

[Nachfolgende Tabelle ist für jede Verarbeitungstätigkeit zu reproduzieren]

1. Allgemeine Angaben zur Verarbeitungstätigkeit	
LfNr:	*zB 1*
Name der Verarbeitungstätigkeit:	*zB Kundenbeziehungsmanagement*
2. Allfällige gemeinsam Verantwortliche	

[19] Dieses Verzeichnis von Verarbeitungstätigkeiten wurde von Feiler und Horn erstellt und als Beispiel in dieser Arbeit wörtlich übernommen. [93]

Firmenwortlaut	Adresse	E-Mail-Adresse
…	…	…
3. Verarbeitungszwecke		
Liste der Verarbeitungszwecke, zB Erfüllung eines mit dem Kunden geschlossenen Vertrages.		
4. Kategorien Betroffener		
Liste der Kategorien betroffener Personen, zB Arbeitnehmer, Kunden.		
5. Datenkategorien		
Datenkategorie	Speicherdauer	
zB Name	*zB bis drei Jahre nach Vertragsbeendigung*	
…	…	
6. Kategorien von Empfängern (Verantwortliche und Auftragsverarbeiter)		
Kategorie von Empfängern	Typ (Verantwortlicher oder Auftragsverarbeiter)	Land (sofern außerhalb des EWR)
zB IT-Dienstleister	*zB Auftragsverarbeiter*	*zB EWR*
zB Konzerngesellschaften	*zB Verantwortlicher*	*zB EWR, USA, Kanada*
…	…	…
7. Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen		
…		

III. Verarbeitungstätigkeiten, für welche die Organisation Auftragsverarbeiter ist

[Nachfolgende Tabelle ist für jede Verarbeitungstätigkeit zu reproduzieren]

1. Allgemeine Angaben zur Verarbeitungstätigkeit	
LfNr:	*zB 1*
Name der Verarbeitungstätigkeit:	*zB Hosting von Websites*

2. Verantwortliche, in deren Auftrag diese Verarbeitungstätigkeit durchgeführt wird				
Firmenwortlaut	Adresse	E-Mail-Adresse	Kontaktdaten des Datenschutzbeauftragten*	Kontaktdaten des Vertreters**
…	…	…	…	…

* Sofern der jeweilige Verantwortliche einen Datenschutzbeauftragten bestellt hat: Name, Adresse, E-Mail-Adresse und Telefonnummer
** Sofern der jeweilige Verantwortliche nicht im EWR niedergelassen ist und einen inländischen Vertreter bestellt hat: Name, Adresse und E-Mail-Adresse

3. Datenübermittlungen an Sub-Auftragsverarbeiter				
Firmenwortlaut	Adresse	E-Mail-Adresse	Kontaktdaten des Datenschutzbeauftragten*	Kontaktdaten des Vertreters**
…	…	…	…	…

* Sofern der jeweilige Sub-Auftragsverarbeiter einen Datenschutzbeauftragten bestellt hat: Name, Adresse, E-Mail-Adresse und Telefonnummer
** Sofern der jeweilige Sub-Auftragsverarbeiter nicht im EWR niedergelassen ist und einen inländischen Vertreter bestellt hat: Name, Adresse und E-Mail-Adresse

4. Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen
…“

6.4. Vereinbarung über eine Auftragsverarbeitung nach [81][20]

Der Verantwortliche:	Der Auftragsverarbeiter:
[NN]	[NN]
[Anschrift]	[Anschrift]
(im Folgenden Auftraggeber)	(im Folgenden Auftragnehmer)

(1) Gegenstand der Vereinbarung

(1) Gegenstand

☐ Der Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben durch den Auftragnehmer: _____[21]

☐ Der Gegenstand des Auftrags ergibt sich aus einem Rahmenvertrag, Werkvertrag, Leistungsvereinbarung, _____ vom _____, auf die hier verwiesen wird. Diese Vereinbarung ist als Ergänzung zu _____[22] zu verstehen.

(2) Art und Zweck der Verarbeitung von Daten

☐ Nähere Beschreibung des Auftrages in Hinblick auf Art und Zweck der vorgesehenen Verarbeitung durch den Auftragnehmer: _____

☐ Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben in der Leistungsvereinbarung vom _____.

(3) Art der Daten

Folgende Datenkategorien werden verarbeitet: _____[23]

[20] Dieses Muster einer Vereinbarung über eine Auftragsverarbeitung wurde von der WKO erstellt und als Beispiel in dieser Arbeit wörtlich übernommen. [95]
[21] Detaillierte Beschreibung der Aufgaben des Auftragnehmers
[22] Vertrag etc. samt Datum ergänzen
[23] Datenkategorien aufzählen, z.B. Personenstammdaten, Kontaktdaten, Vertragsdaten, Verrechnungsdaten, Bonitätsdaten, Bestelldaten, Entgeltdaten, Kundenhistorie, usw.

(4) Kategorien betroffener Personen

Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: _____[24]

(2) Dauer der Vereinbarung

☐ Einmalige Durchführung

Die Vereinbarung endet mit einmaliger Durchführung der Arbeiten.

☐ Befristete Laufzeit

Die Vereinbarung ist befristet abgeschlossen und endet mit _____[25].

☐ Unbefristete Laufzeit

Die Vereinbarung ist auf unbestimmte Zeit geschlossen und kann von beiden Parteien mit einer Frist von _____[26] zum _____[27] gekündigt werden. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

(3) Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

---

[24] Betroffenenkategorien ergänzen, z.B. Kunden, Interessenten, Lieferanten, Ansprechpartner, Beschäftigte, etc.
[25] Fristende eintragen.
[26] Kündigungsfrist eintragen, z.B. ein Monat.
[27] Kündigungstermin eintragen, z.B. Kalenderviertaljahr.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(6) Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.

(7) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, der Datenverarbeitungseinrichtungen eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(8) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.

(9) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

(4) Technisch-organisatorische Maßnahmen

Die technischen und organisatorischen Maßnahmen (TOMs) unterliegen dem technischen Fortschritt und der Weiterentwicklung. Es ist dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen, soweit das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen sind zu dokumentieren. Einzelheiten sind der Anlage ./1 zu entnehmen.

(5) Ort der Durchführung der Datenverarbeitung

☐ Ausschließliche Durchführung innerhalb der EU/des EWR

Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw des EWR durchgeführt.

☐ Bei Durchführung, wenn auch nur teilweise, außerhalb der EU/des EWR

Datenverarbeitungstätigkeiten werden zumindest zum Teil auch außerhalb der EU bzw des EWR durchgeführt, und zwar in _____[28]. Das angemessene Datenschutzniveau ergibt sich aus[29]

- ☐ einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
- ☐ einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO.
- ☐ verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO.
- ☐ Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
- ☐ genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
- ☐ einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO.
- ☐ von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO.
- ☐ einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.

(6) Sub-Auftragsverarbeiter

☐ Verbot der Hinzuziehung eines Sub-Auftragsverarbeiters

Der Auftragnehmer ist nicht berechtigt, einen Sub-Auftragsverarbeiter heranzuziehen.

☐ Zulässigkeit der Hinzuziehung eines bestimmten Sub-Auftragsverarbeiters

---

[28] Staaten aufzählen.
[29] Siehe im Allgemeinen Merkblatt Internationaler Datenverkehr nach der EU-DSGVO.

Der Auftragnehmer ist befugt folgendes Unternehmen als Sub-Auftragsverarbeiter zur unmittelbaren Erbringung der Hauptdienstleistung hinzuziehen: _____ [30]

Beabsichtigte Änderungen des Sub-Auftragsverarbeiters sind dem Auftraggeber so rechtzeitig schriftlich bekannt zu geben, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

☐ Zulässigkeit der Hinzuziehung von Sub-Auftragsverarbeitern

Der Auftragnehmer kann Sub-Auftragsverarbeiter _____ [31] hinzuziehen.

Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters.

[Ort], am [Datum]	[Ort], am [Datum]
Für den Auftraggeber:	Für den Auftragnehmer:
.....	.....
[Name samt Funktion]	[Name samt Funktion]

[30] Firmenname und Sitz ergänzen, Art der Tätigkeiten.
[31] Tätigkeiten.

ANLAGE./1 [der Vereinbarung] - TECHNISCH-ORGANISATORISCHE MASSNAHMEN [32]

Vertraulichkeit

- **Zutrittskontrolle**: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Schlüssel, Magnet- oder Chipkarten, elektrische Türöffner, Portier, Sicherheitspersonal, Alarmanlagen, Videoanlagen;
- **Zugangskontrolle**: Schutz vor unbefugter Systembenutzung, z.B.: Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
- **Zugriffskontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf ‚need to know-Basis', Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten;
- **Pseudonymisierung**: Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert aufbewahrt.
- **Klassifikationsschema für Daten**: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

Integrität[33]

- **Weitergabekontrolle**: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
- **Eingabekontrolle**: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

[32] Entsprechend den Realitäten anpassen!
[33] Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.

Verfügbarkeit und Belastbarkeit

- **Verfügbarkeitskontrolle**: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
- Rasche **Wiederherstellbarkeit**;
- **Löschungsfristen**: Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen;
- Incident-Response-Management;
- Datenschutzfreundliche Voreinstellungen;
- Auftragskontrolle: Keine Auftragsdatenverarbeitung im Sinne von Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, Auswahl des Auftragsverarbeiters, Vorabüberzeugungspflicht, Nachkontrollen.“

6.5. Rahmenbetriebsvereinbarung über die Verwendung personenbezogener Beschäftigtendaten nach [84, pp. 2-13][34]

abgeschlossen zwischen dem Unternehmen XY einerseits und dem zuständigen Betriebsrat[35] andererseits.

(1) GELTUNGSBEREICH

Diese Betriebsvereinbarung gilt:

- **Personell**: für alle Beschäftigten, VoluntärInnen und freien DienstnehmerInnen sowie natürliche Personen im Sinne des § 36 ArbVG.[36]
- **Sachlich**: allgemeine organisatorische Regelungen für die Planung, Einführung, Verwendung und Veränderung bestehender und zukünftiger Informations- und Kommunikationssysteme (IKT-Systeme), die personenbezogene Daten von Beschäftigten verwenden.

Die Grundsätze dieser Rahmenbetriebsvereinbarung gelten für alle (auch zukünftige) Einzel-Betriebsvereinbarungen, die den konkreten Einsatz von Informations- und Kommunikationssystemen beschreiben (Betriebsvereinbarungen im Sinne der §§ 96, 96a und 97 ArbVG).

(2) RECHTSGRUNDLAGEN UND BEGRIFFSDEFINITIONEN

Die rechtliche Basis bilden insbesondere

- die Bestimmungen des Arbeitsverfassungsgesetzes (ArbVG) im Besonderen die §§ 89, 91, 92, 96, 96a und 97
- die Bestimmungen der EU-Datenschutzgrundverordnung und des Datenschutzanpassungsgesetzes 2018
- die Bestimmungen des ArbeitnehmerInnenschutzgesetzes (ASchG)[37]
- das Kommunikationsgeheimnis nach § 93 Abs 3 Telekommunikationsgesetz (TKG)

Die Definitionen aus der Europäischen Datenschutzgrundverordnung (DSGVO) und des Datenschutzanpassungsgesetzes 2018 (DSAG) finden in dieser Betriebsvereinbarung Anwendung.

---

[34] Das nachfolgende Beispiel zeigt ein Muster über eine Rahmenbetriebsvereinbarung, welche bereits DSGVO konform ist und von der GPA-djp erstellt wurde [96, pp. 2-13].
[35] Das kann sein: der Arbeiter- und/oder Angestelltenbetriebsrat, der Betriebsausschuss oder auch der Zentralbetriebsrat [nach Kompetenzübertragung]
[36] d.h. Zeitarbeitskräfte, überlassene ArbeitnehmerInnen sowie HeimarbeiterInnen sind eingeschlossen.
[37] Im Zusammenhang mit IKT-Einsatz ist insbesondere §68 zur benutzergerechten Gestaltung von Bildschirmarbeitsplätzen wichtig, wobei auch die Bildschirme von diversen mobilen Geräten gemeint sind.

(3) ZIELSETZUNG

Diese Betriebsvereinbarung dient zur rechtlichen Qualitätssicherung und Transparenz bei der Verwendung personenbezogener Daten beim Einsatz von Informations- und Kommunikationssystemen (IKT-Systemen). Sie kann Betriebsvereinbarungen zu einzelnen IKT-Systemen nicht ersetzen, gibt aber einen Rahmen vor. Personenbezogene Daten von Beschäftigten dürfen nur verwendet werden, soweit der Verwendungszweck rechtlich gedeckt ist.[38]

Daher sind bei jeder IKT, die personenbezogene Beschäftigtendaten verwendet, folgende Prüfungsmaßstäbe (in dieser Reihenfolge) anzuwenden:

a) Prüfung, ob eine rechtliche Grundlage nach Art 5 Abs 1 lit a DSGVO vorliegt.
b) Prüfung, ob ein berechtigter Zweck nach Art 5 Abs 1 lit b DSGVO vorliegt. Der Zweck der geplanten Datenverarbeitung ist detailliert zu beschreiben. Unbestimmte und allgemeine Aussagen sind nicht zulässig.
c) Prüfung, ob die Datenerhebung und -verarbeitung auf das notwendige Mindestmaß beschränkt wird (Art 5 Abs 1 lit c DSGVO). Dazu sind Maßnahmen im Sinne der Modelle ‚Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen' (Art 25 DSGVO) zu setzen.

Bereits bei Planung und Einführung der IT-Systeme wird dokumentiert, wie die Datenschutzgrundsätze eingehalten werden (Rechenschaftspflicht Art 5 Abs 2 DSGVO).

(4) UMGANG MIT PERSONENBEZOGENEN DATEN

Daten über Benutzeraktivitäten dürfen nur zu folgenden Zwecken verwendet werden:

- Einhaltung der Bestimmungen der DSGVO zur Datensicherheit (Art 5 Abs 1 lit f);
- Überprüfung der Einhaltung von Betriebsvereinbarungen;
- Gewährleistung der Systemsicherheit;
- Analyse und Korrektur von technischen Fehlern im IKT System;
- Optimierung des Computersystems;
- Leistungsverrechnung für den Betrieb der Hardware, Software und Netzwerkserver

[38] Falls innerbetriebliche Verhaltensrichtlinien (z.B. Governance und Compliance) vorhanden sind, empfiehlt es sich, diese im Hinblick auf die nationalen Gesetze und diese Rahmenbetriebsvereinbarung zu überprüfen und miteinander in Einklang zu bringen.

Protokolldaten dürfen ausschließlich dahingehend geprüft werden, ob die Zugriffsberechtigungen vorhanden waren. Eine Auswertung der Protokolle im Hinblick auf das Benutzerverhalten einzelner Personen ist jedenfalls rechtlich unzulässig (Art 5 Abs 1 lit f, 25, 30 Abs 1 lit f, 40 ff iVm Art 12-14 DSGVO). Die Geschäftsführung verzichtet ausdrücklich darauf, Informationen, die unter Verletzung der Bestimmungen dieser Betriebsvereinbarung gewonnen wurden, als Beweismittel zur Begründung arbeitsrechtlicher Maßnahmen zu verwenden.

4.1 Stufenweise Kontrollverdichtung

Grundsätzlich wird die Protokollierung von Daten aus technischen Gründen maschinen- und damit auch personenbezogen vorgenommen. Der direkte Personenbezug wird aber nur unter bestimmten Bedingungen einer bestimmten Personengruppe zugänglich gemacht.

Stufe 1: Die Kontrolle erfolgt allerdings im Sinne einer stufenweisen Kontrollverdichtung vorerst nur durch die IT-Abteilung und ohne konkreten Personenbezug.

Stufe 1a: Sollte sich das auftretende Problem nicht rein technisch lösen lassen, wird der betroffene Personenkreis (z.B. Abteilung, Team, Bürobereich,...) informiert und zur Verhaltensänderung aufgefordert.

Stufe 2: Im Fall des Weiterbestehens einer Gefahr für die betriebliche IKT-Infrastruktur (z.B. Virenattacke) oder einer hohen Wahrscheinlichkeit, dass tatsächlicher Schaden für die Firma entstehen wird (z.B. Datenverlust) ist die/der einzelne Betroffene zu informieren.

Stufe 3: Erst bei fortgesetzter pflichtwidriger und System gefährdender Nutzung kann die Offenlegung der personenbezogenen Daten gegenüber der vorgesetzten Person unter Hinzuziehen des Betriebsrates erfolgen.

Der Prozess der stufenweisen Kontrollverdichtung ist zu protokollieren, ebenso wie begründete Verdachtsmomente schriftlich festzuhalten sind. Wird jemand zu Unrecht verdächtigt, sind die Protokolle sofort zu löschen, erhärten sich Verdachtsmomente sind die Protokolle maximal drei Jahre nach dem ersten Verdachtsmomentzeitpunkt aufzubewahren (Art 10 ff DSGVO). Ausgenommen von den ersten beiden Stufen der Kontrollverdichtung sind nur die Fälle einer konkreten unmittelbaren Gefährdung für die IKT-Infrastruktur oder ihre korrekte Funktionsfähigkeit. Darüber hinaus für all diejenigen Fälle, in denen ein begründeter Verdacht eines Verstoßes gegen strafrechtliche Bestimmungen vorliegt, der durch rasches Eingreifen vermieden werden kann.

4.2 Kategorisierung personenbezogener Daten nach verschiedenen Datenschutz- und Datensicherheitsniveaus

Es ist eine Differenzierung nach Datenarten/-kategorien vorzunehmen (Art 9, 10), um die erhöhten Schutzanforderungen für die Verarbeitung besonderer Datenkategorien (ethnische Herkunft, politische Meinung, Religion, sexuelle Orientierung, Gewerkschaftszugehörigkeit, genetische oder biometrische Daten, Daten über Verurteilungen und Straftaten[39]) zu gewährleisten.[40]

Die Datenkategorisierung erfolgt nach der in Anhang 2 beschriebenen Vorgangsweise.

(5) BETRIEBLICHE PERSONALDATENSCHUTZKOMMISSION (PDSK)

Zur Beratung aller Fragen, die sich im Zusammenhang mit der Einführung, dem Betrieb, der Auslegung und den Änderungen von IKT-Systemen ergeben, wird eine innerbetriebliche Personaldatenschutzkommission (PDSK) gebildet. Die Beratungen, Ergebnisse und Erkenntnisse der PDSK dienen Unternehmensleitung und Betriebsrat als Entscheidungsgrundlagen.

Die Entscheidungskompetenzen der Unternehmensleitung als Organ des Unternehmens und die des Betriebsrates als Körperschaft gemäß ArbVG bleiben davon unberührt.

5.1 Zusammensetzung

Dieser Kommission gehören paritätisch an[41]:

- zwei bis vier von der Unternehmensleitung nominierte VertreterInnen
- zwei bis vier vom Betriebsrat nominierte VertreterInnen
- so vorhanden: der betriebliche Datenschutzbeauftragte (DSB)

Unternehmensleitung und Betriebsrat haben jeweils das Recht, bei Bedarf Fachpersonal ihrer Wahl zur Beratung bei zu ziehen.

---

[39] ACHTUNG: Nach Vorstrafen und laufenden Ermittlungsverfahren darf der Arbeitgeber idR gar nicht fragen, geschweige denn darf er solche Daten speichern. Ausnahme: Wenn zwischen dem Tätigkeitsbereich des Arbeitnehmers und einem begangenen Delikt ein Zusammenhang besteht (z.B. KassierIn in einem Geldinstitut und Vermögensdelikte; LehrerInnen und Kindesmissbrauchsdelikte).

[40] Die folgende Einstufung ist eine wichtige Grundlage für das Verarbeitungsverzeichnis, die interne Dokumentation der Datenanwendungen (Art 30 DSGVO), für eine allfällige Datenschutzfolgeabschätzung (Art 35 DSGVO) und für die Frage, bei welchen Systemen eine Mitbestimmung nach ArbVG vorliegt (manchmal B, immer C und D).

[41] je nach Unternehmensgröße

Die Tätigkeit der PDSK-Mitglieder erfolgt während der bezahlten Arbeitszeit und ihnen dürfen aus dieser Tätigkeit keine Nachteile entstehen.

Die PDSK legt eine Geschäftsordnung nach dem Muster im Anhang 3 fest.

5.2 Aufgaben der PDSK

Aufgabe der PDSK ist es, einen Interessenausgleich zwischen Unternehmensleitung und Betriebsrat herbeizuführen. Auch eine Nichteinigung im Zusammenhang mit dieser Betriebsvereinbarung ist in der PDSK zu behandeln. Die PDSK schlägt vor, wie die personenbezogenen Daten in Anlehnung an Pkt.4.2 dieser Vereinbarung kategorisiert werden. Sie schlägt geeignete technische und organisatorische Maßnahmen vor, um die Einhaltung dieser Betriebsvereinbarung sowie der jeweils geltenden gesetzlichen Bestimmungen zu überprüfen und sicherzustellen.

Alle zum Zeitpunkt des Abschlusses dieser Rahmenbetriebsvereinbarung bestehenden und nicht mit Betriebsvereinbarung geregelten IKT-Systeme, die personenbezogene Daten verwenden, sind der PDSK unter Angabe der in Anhang 1 beschriebenen Informationen umgehend zu melden und haben das folgende Prozedere zu durchlaufen.

In der PDSK ist für jedes IKT-System zu klären, bei welchen Daten ein Personenbezug im Sinne der Bestimmungen des Art 4 DSGVO vorliegt (z.B. durch Kostenstellennummer o.ä.).

Von den Systemverantwortlichen ist zu prüfen, ob das angestrebte Ziel der Datenverwendung auch ohne Personenbezug mit vertretbarem Aufwand erreicht werden kann.

Ist dies nicht der Fall, überprüft die PDSK die Notwendigkeit des Abschlusses einer Zusatzbetriebsvereinbarung für das konkrete IKT-System im Sinne der §§ 96, 96a bzw. 97 ArbVG.

Die PDSK schlägt bei Einführung neuer IKT-Systeme Maßnahmen vor, die Datensparsamkeit durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art 25 DSGVO) garantieren.

Weiters prüft die PDSK, ob eine geplante Datenverarbeitung für die Betroffenen risikoreich ist und eine Datenschutz-Folgenabschätzung nach Art 35 DSGVO erforderlich ist. Ist das der Fall, wird eine DS-Folgenabschätzung durchgeführt und allfällige Maßnahmen zur Eindämmung des Risikos in der PDSK erarbeitet, dabei werden schriftliche Empfehlungen der Aufsichtsbehörde einbezogen.

Die gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten nach Art 37 DSGVO wird von der PDSK geprüft.

Die PDSK entwickelt gemeinsam mit dem Datenschutzbeauftragten, der Unternehmensleitung und dem Betriebsrat ein Datenschutzkonzept und erstellt einmal jährlich einen Datenschutzreport. Dieser Datenschutzreport dient der Unternehmensleitung und dem Betriebsrat zur Diskussion, Evaluation und Weiterentwicklung der bestehenden Betriebsvereinbarungen. In diesem Datenschutzreport werden die wesentlichen Problembereiche betreffend Datensicherheit und Datenschutz dargestellt, wobei auch die Anwendbarkeit und die mögliche Ergänzung der bestehenden Betriebsvereinbarungen untersucht werden.

(6) MASSNAHMEN BEI DER VERWENDUNG PERSONENBEZOGENER DATEN

6.1 Übertragung von Daten auf PCs, Laptops, mobile Geräte oder dgl.

Bei der Übertragung von personenbezogenen Daten auf Personal Computer (PC), Laptop, mobile Geräte (z.B.: Smartphone, Tablet-PC, USB-Stick, externe Festplatten) oder dgl. gilt im Hinblick auf alle Daten eine besondere Sorgfaltspflicht. Für die Verarbeitung besonderer Kategorien personenbezogener Daten ist für jedes System eine Regelung in der Zusatzvereinbarung zu treffen.

6.2 Aufbewahren und Löschen personenbezogener Daten

Für alle personenbezogenen Daten ist in der jeweiligen Zusatzvereinbarung eine Frist zu vereinbaren, bis wann diese Daten zu löschen sind. Die Löschung ist vorzunehmen, wenn die Datenverwendung ihren Zweck erfüllt hat.

6.3 Simulationsdaten (Testdaten)

Bei der Entwicklung und Erweiterung von IKT-Systemen muss mit Simulationsdaten (Testdaten) gearbeitet werden. Falls eine Anonymisierung oder Pseudonymisierung nicht möglich ist, werden Echtdaten verwendet und es gelten die Regelungen dieser Rahmenvereinbarung bzw. der jeweiligen Einzelvereinbarung.

6.4 Auftragsverarbeiter

Alle zum Einsatz kommenden Auftragsverarbeiter müssen eine ausreichende Gewähr für die rechtmäßige und sichere Datenverwendung im Sinne des Art 28 DSGVO bieten.

Der Verantwortliche hat dazu mit jedem Auftragsverarbeiter eine Vereinbarung zu treffen und auf die Regelungen dieser Betriebsvereinbarung und der betreffenden Zusatzvereinbarung(en) nachweislich hinzuweisen. Dem Betriebsrat ist eine Kopie der jeweiligen Verträge zur Verfügung zu stellen.

6.5 Benutzerservice / Auskunftsperson / Helpdesk

Hard- und Software der IKT-Systeme werden durch ein Benutzerservice betreut. Es ist sicherzustellen, dass für an Bildschirmarbeitsplätzen Beschäftigte Ansprechpartner zur Verfügung stehen.

Sollte eine Hilfestellung durch Aufschalten in die aktuelle Arbeitsumgebung erfolgen, ist dies nur nach

Aufforderung durch die Betroffenen und deren Zustimmung für jeden einzelnen Fall erlaubt. Der Ferneinstieg des/r Systembetreuers/-in in eine fremde Anwendung ist durch Signal zu kennzeichnen. Der Ausstieg des/r Systembetreuers/-in nach erfolgter Hilfestellung wird ebenfalls auf dem Bildschirm angezeigt.

Eine Auswertung, welche Beschäftigten zu welchem Zeitpunkt das Help-Desk-System in Anspruch genommen haben, findet nicht statt. Es wird lediglich anonym die Art der Hilfestellung dokumentiert, um Hinweise für zukünftige Schulungsinhalte zu bekommen.

6.6 Fernwartung

Bei Fernwartung ist sicherzustellen, dass personenbezogene Daten nicht missbräuchlich verwendet werden können (z.B. über vertragliche Regelungen zur Datensicherheit). Dem Betriebsrat ist eine Kopie der jeweiligen Verträge zur Verfügung zu stellen.

Der PDSK ist über den Stand der Fernwartungseinrichtungen auf Verlangen, mindestens aber einmal jährlich, Bericht zu erstatten.

(7) RECHTE des BETRIEBSRATES

7.1 Informationspflichten des Unternehmens

- Das Unternehmen verpflichtet sich, dem Betriebsrat folgende Übersicht zur Verfügung zu stellen, die laufend aktualisiert wird (§§ 89 ff, 91 ArbVG):
- alle Systeme, die personenbezogene Daten verwenden, inklusive einer allgemein verständlichen Kurzbeschreibung und dem Verzeichnis von Verarbeitungstätigkeiten nach Art 30 DSGVO.
- Personaldatenübermittlung und Auftragsdatenverarbeitung.
- Einladungen zu Veranstaltungen/Sitzungen, die in Zusammenhang mit der Einführung oder Änderung von IKT-Systemen mit personenbezogenen Datenverwendungen stehen.

- Protokolle aller Sitzungen und Veranstaltungen, die in Zusammenhang mit der Einführung oder Änderung von IKT-Systemen zur personenbezogenen Datenverwendung im Sinne der §§ 96 und 96a ArbVG stehen.

7.2 Informationsrechte des Betriebsrates

Bei allen eingesetzten IKT-Systemen sind auf Anforderung des Betriebsrates die Informationen laut Anhang 1 zur Verfügung zu stellen:

Für zukünftige (geplante) IKT-Systeme und Verwendungen sind zusätzlich folgende Informationen zur Verfügung zu stellen:

- geplante Auswirkungen des Projektes (z.B. Personalausmaß, Veränderung von Arbeitsabläufen)
- den Zeitplan des Projektablaufes bis zur Umsetzung
- Bekanntgabe der Projektleiter, System-Verantwortlichen und etwaiger Teilprojektleiter, sowie der involvierten Projekt-Team-Mitglieder
- Bekanntgabe eventueller externer Berater und Programmierer
- Gesamtkosten des Projektes

Sofern ein IKT-System die Verwendung von personenbezogenen Beschäftigtendaten möglich macht, ist bereits in der Planungsphase, d.h. vor Einführung bzw. Veränderung des IKT-Systems die PDSK (vgl. Pkt. 4) und der Betriebsrat einzubinden. Diese Systemänderungen oder -entwicklungen sind vor ihrer Implementierung zu dokumentieren und der PDSK zur Verfügung zu stellen.

7.3 Kontrollrechte des Betriebsrates

Der Betriebsrat hat das Recht, in sämtliche Protokolle und Auswertungen Einsicht nehmen bzw. solche anzufordern.[42]

Dem Betriebsrat sind neben der entsprechende[n] Hard- und Software Zugriffsberechtigungen (Leseberechtigung) zur Verfügung zu stellen, die ihm die Kontrolle der IKT-Systemen ermöglicht.

Es steht dem Betriebsrat zu, externe ExpertInnen hinzuzuziehen. Diese ExpertInnen sind zur Verschwiegenheit verpflichtet. Sie sind von den zuständigen Fachabteilungen zu unterstützen. Das

[42] Ausnahme: Die Einsicht in einen Personalakt bedarf der Zustimmung des/der betroffenen Beschäftigten.

Unternehmen trägt die anfallenden Kosten – insbesondere, wenn ein Verstoß gegen Bestimmungen dieser RBV oder einer Zusatzvereinbarung festgestellt wurde.

7.4 Besonderes Schulungsrecht des Betriebsrates

Die Mitglieder des Betriebsrates haben unter Fortzahlung des Entgeltes das Recht

- sowohl innerbetriebliche als auch außerbetriebliche einschlägige Fort- und Weiterbildungsangebote in Anspruch zu nehmen und die Kosten trägt der Arbeitgeber.

Es wird vereinbart, dass die Ausübung des Besonderen Schulungsrechts nicht auf einen Anspruch gemäß § 118 ArbVG angerechnet wird.

(8) RECHTE der BESCHÄFTIGTEN

8.1 Information über Rechte und Pflichten

Alle Beschäftigten sind über ihre Rechte und Pflichten in Bezug auf die elektronische Datenverwendung und die dazu abgeschlossenen Betriebsvereinbarungen zu informieren.

Der Verantwortliche stellt den betroffenen Beschäftigten klare und leicht verständliche Informationen über geplante Datenverarbeitungen zur Verfügung. Über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling muss ausdrücklich informiert werden, in diesem Fall sind den Betroffenen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung zu übermitteln (Art 12-14 DSGVO) und die Betroffenen sind auf deren Widerspruchsrecht (Art 21-22 DSGVO) hinzuweisen.

Verwenden Beschäftigte personenbezogene Daten, haben sie vorher durch Unterschrift zu bestätigen, dass sie über ihre datenschutzrechtlichen Verpflichtungen im Sinne der betreffenden Betriebsvereinbarung(en) informiert wurden.

Die Konsequenzen eines Datenmissbrauches sollten in der PDSK genauer geregelt werden (z.B. zeitweiser Entzug der Zugriffsberechtigung oder Abmahnung) – idealer Weise bevor ein Anlassfall eintritt.

8.2 Schriftlicher Arbeitsauftrag bei Verdacht auf unzulässige Verwendung

Klargestellt wird: Verstößt die Weisung hinsichtlich der Zulässigkeit einer Verarbeitung oder Übermittlung gegen höherrangige Bestimmungen (insb DSGVO und Datenschutz-Anpassungsgesetz), so ist sie nichtig und muss nicht befolgt werden. Sind Beschäftigte über die

Zulässigkeit einer Verarbeitung oder Übermittlung im Zweifel, sind sie berechtigt, von ihren Vorgesetzten einen schriftlichen Arbeitsauftrag einzufordern.

8.3 Auskunftsrecht

Alle Beschäftigten erhalten auf Anforderung einmal jährlich eine kurze, allgemein verständliche Auflistung im Sinne des Art 15 DSVGO.

Die Art der Auflistung (z.B. Intranet-Veröffentlichung) kann für die jeweiligen IKT-Systeme in der PDSK beschlossen werden.

8.4 Richtigstellungs- bzw. Löschungsrecht (Art 16 ff DSGVO)

Alle Beschäftigten haben das Recht, Daten richtig stellen bzw. löschen zu lassen, wenn sie nicht berechtigt ermittelt wurden wenn sie nicht richtig sind, oder für den vorgesehenen Zweck nicht (mehr) erforderlich sind. Diesen Beschäftigten und dem zuständigen Betriebsrat ist eine Überprüfungsmöglichkeit über die Korrektur bzw. Löschung einzuräumen. Entsteht Uneinigkeit über die Richtigkeit von Daten und kann das Unternehmen die Richtigkeit nicht nachweisen, so sind diese Daten zu löschen. Bis zur Klärung eines allfällig vorliegenden Sachverhalts hat die betroffene Person das Recht auf Einschränkung der Verarbeitung (Art 18 DSGVO).

8.5 Umgang mit privaten Dokumenten und E-Mails

Die Nutzung der betrieblichen IKT-Systeme für private Zwecke ist in angemessenem Ausmaß zulässig. Es können alle Beschäftigten, auf ihren Arbeitsspeichern bzw. im verwendeten Kommunikationssystem einen Ordner ‚privat' anlegen, dessen Inhalt keinesfalls von dritter Seite ohne Zustimmung der Betroffenen eingesehen oder ausgewertet werden darf. Die ArbeitnehmerInnen haben dabei jedoch betriebliche Regelungen im Hinblick auf Daten- und Netzwerksicherheit zu berücksichtigen, die den uneingeschränkten Gebrauch von Daten unterbinden (z.B. Download aus dem Internet, Installieren neuer Software).

(9) BESTEHENDE und NEUE SYSTEME

In den Zusatzvereinbarungen sind je IKT-System zumindest folgende Informationen zu vereinbaren

- Verwendungszweck(e)
- Systemteile, Module
- verwendete Datenarten inklusive Kategorisierung
- Auswertungen

- Berechtigungskonzept
- Schnittstellen, Empfängerkreise und mögliche Dienstleister
- Löschfristen

(10) INKRAFTTRETEN und VERTRAGSDAUER

Diese Betriebsvereinbarung tritt mit Unterzeichnung in Kraft und gilt unbefristet.

Sie kann jedoch bei Übereinstimmung zwischen Arbeitgeber und Betriebsrat, jederzeit ergänzt werden.

Zeichnungsbevollmächtigte

Für das Unternehmen:	Für den Betriebsrat:
.....	.....
[Name]	[Name]

ANHANG 1 [zur Rahmenbetriebsvereinbarung]: Information zu IKT-System

Je Informations- und Kommunikationssystem (IKT-System) sind, sofern vorhanden, folgende Informationen zur Verfügung zu stellen:

(1) Name des IKT-Systems (Datenanwendung), Versionsbezeichnung und Anbieter
(2) die jeweiligen Systembeschreibungen / Benutzerhandbücher
(3) betriebliche(r) Verantwortliche(r) / Ansprechperson(en)
(4) Dokumentation aus dem Verzeichnis von Verarbeitungstätigkeiten nach Art 30 DSGVO
(5) Mandanten, die personenbezogene Echtdaten verwenden (z.B. Testsystem, Konsolidierungssystem, Produktivsystem)
(6) eingesetzte Systemteile/Module
(7) Verwendungszweck der Datenanwendung
(8) Ort der Datenhaltung/-verwaltung (bei Dienstleister, nähere Angaben zum Dienstleister)
(9) betroffene Personengruppe
(10) Standort und Art der Datenerfassungsgeräte (z.B. Terminals, Kameras, Automaten, ...)
(11) die verwendeten Datenarten und Datenkategorien

(12) ein Verzeichnis personenbezogener Auswertungen mit Beispielen
(13) Schnittstellen (Import und Export) zu anderen IKT-Systemen
(14) Zugriffsberechtigungsverzeichnis und mögliche Empfängerkreise
(15) Löschfristen
(16) Technische und organisatorische Maßnahmen gemäß Art 32 Abs 1 DSGVO
(17) Die Ergebnisse der allfällig durchgeführten Datenschutzfolgenabschätzung sowie der Konsultation der Datenschutzbehörde (gem Art 35 f DSGVO)
(18) Auflistung der allfällig getroffenen Maßnahmen im Zusammenhang mit Datenschutz durch Technik und allfällig eingeführte datenschutzfreundliche Voreinstellungen
(19) Auflistung allfällig eingeführter Verfahrensregeln und Zertifizierungen
(20) Name des/der allfällig bestellten betrieblichen Datenschutzbeauftragten (gem 37 ff DSGVO)
(21) Allfällig vorhandener Tätigkeitsbericht des betr. DSB
(22) Form der Protokollierung

ANHANG 2 [zur Rahmenbetriebsvereinbarung]: Datenkategorisierung

Zwecke der Kategorisierung sind

- Aufbereitung der personenbezogenen Daten für die interne Dokumentation der Datenanwendungen (Art 30 DSGVO) und für eine allfällige Datenschutzfolgeabschätzung (Art 35 DSGVO)
- Grundlage für organisatorische und technische Regelungen bei der Datenverwendung
- Sensibilisierung der Führungskräfte und der Beschäftigten für Datenschutz und Datensicherheit

Die personenbezogenen Beschäftigtendaten werden für jedes eingesetzte IKT-System nach den folgenden vier Kategorien unterteilt.

Da idente Datenfelder in verschiedenen IKT-Systemen unterschiedliche Bedeutung besitzen können, hat diese Unterteilung für jedes IKT-System, für das eine Zusatzvereinbarung abgeschlossen wird, zu erfolgen. Der Vorschlag, welches Datenfeld in welche Kategorie fällt, kann in der innerbetrieblichen Personaldatenschutzkommission (vgl. Pkt.4) erfolgen

Folgende vier Kategorien werden eingeführt:

Kategorie A: Allgemeine Daten zur Person.

Diese Daten umfassen die geschäftlichen Kommunikationsdaten (z.B.: Name, Organisationseinheit, Firmenanschrift, Büroraum, Telefonnummer, E-Mail-Adresse). Diese Daten können in einem Unternehmensadressbuch gefunden werden. Sie stehen zwar mit den einzelnen Beschäftigten in Verbindung, gehören aber zu den Arbeitsmitteln im Unternehmen.

Kategorie B: Daten zur Person die verpflichtend aus Gesetz, Normen der kollektiven Rechtsgestaltung oder Arbeitsvertrag für einen eindeutigen Zweck verwendet werden müssen.

Diese Daten müssen vom Unternehmen verwendet werden. In diesen Fällen werden die Daten benötigt, um gesetzlichen Forderungen bzw. vertraglichen Verpflichtungen (eindeutiger und rechtmäßiger Zweck im Sinne von Art 5 Abs 1 lit a und b DSGVO) nachkommen zu können. Darüber hinaus können in dieser Kategorie weitere Datenarten in Abstimmung zwischen Arbeitgeber – Betriebsrat angeführt werden. (z.B.: Anschrift, Arbeitszeit, Urlaubsanspruch, Bankverbindung, Qualifikationen, betriebliche Funktion.)

Kategorie C: Schutzwürdige Daten der Beschäftigten sowie Daten, für die keine gesetzliche Verpflichtung zur Verwendung besteht.

Diese Daten gehören zum Teil zu den Stammdaten (werden daher auch für einzelne Verarbeitungen wie z.B. zur Entgeltberechnung benötigt), sind aber primär dem Privatbereich der Beschäftigten zuzuordnen und stehen nicht direkt mit dem Unternehmen in Verbindung (z.B.: Familienstand, Zweitwohnsitz). Hierunter fallen auch Daten, die aus Sicht der betroffenen Beschäftigten einem erhöhten Schutzinteresse unterliegen (z.B.: Pfändungen, betriebliche Darlehen).

Weiters fallen in diese Kategorie Daten, die Aussagen über das Verhalten einzelner Beschäftigter enthalten können (z.B.: Fehlzeiten und Mehrarbeit, Leistungsstunden für diverse Aufträge/Projekte die Vergleiche zulassen, leistungsabhängige Entgeltbestandteile, Beurteilungen, vereinbarte Ziele aus Mitarbeitergesprächen, ...)

Kategorie D: Sensible Daten. Besondere Kategorien personenbezogener Daten und Daten mit erhöhten Schutzanforderungen im Sinn des Art 9 und 10 DSGVO

Darunter fallen Daten der Beschäftigten über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben, sowie biometrische (z.B. Irisscan, Fingerprint) und genetische Daten sowie Daten über strafrechtliche Verurteilungen und Straftaten.

ANHANG 3 [zur Rahmenbetriebsvereinbarung]: Geschäftsordnung

Zur Bewältigung der organisatorischen Abläufe hat die PDSK (nach ihrer Konstituierung) eine Geschäftsordnung mit folgendem Mindestinhalt festzulegen, die dieser Betriebsvereinbarung angehängt wird, ohne allerdings Bestandteil zu sein:

- Vorsitzführung
- Protokollführung
- Art der Beschlussfassung
- Art der Einberufung
- Tagungsintervall

Mögliche Inhalte der Geschäftsordnung:

- Die Konstituierung hat innerhalb drei Monaten nach Abschluss dieser Betriebsvereinbarung durch Wahl eines/-r Vorsitzenden zu erfolgen.
- Die PDSK ist beschlussfähig, wenn sowohl von Seite der Unternehmensleitung, als auch von Seite des Betriebsrats zwei Mitglieder anwesend sind. Gültige Beschlüsse können nur einstimmig gefasst werden und sind zu protokollieren.
- Die PDSK tagt vierteljährlich.
- Der/die Vorsitzende hat auch auf Verlangen eines Kommissionsmitgliedes, unter Angabe des Grundes, binnen fünf Arbeitstagen eine Sitzung einzuberufen. Jede Einberufung hat eine schriftliche Tagesordnung zu enthalten und ist spätestens zwei Arbeitstage vor der Sitzung allen Kommissionsmitgliedern zu übergeben.
- Zwischenzeitliche Einberufungen durch den/die Vorsitzende/n sind möglich.“

7. Zusammenfassung

Ziel der vorliegenden Diplomarbeit war es, geeignete Compliance-Maßnahmen für den Einsatz und Vertrieb von Sicherheitstechnik zu identifizieren. Zu diesem Zweck wurde zunächst der Begriff der Sicherheitstechnik definiert und anschließend in Hinblick auf die Unterteilung in mechanische und elektronische Sicherheitstechnik genauer erörtert, wobei hierbei einerseits auf die anzuwendenden Normen und andererseits auf die Funktionsweise der einzelnen Systeme eingegangen wurde.

Im Anschluss daran wurden relevante rechtliche Grundlagen, welche den Einsatz der Sicherheitstechnik betreffen, identifiziert und erklärt. Dabei ergab sich, dass sowohl die Beachtung des Arbeitsrechts als auch der Datenschutzgrundverordnung wichtig ist, um solche Systeme gesetzeskonform einsetzen zu können.

Dies hatte den Hintergrund, dass sowohl das Wissen über die Funktionsweise von Alarmanlagen, Zutrittskontrollsystemen, Videoüberwachungsanlagen und GPS-Systemen als auch das Wissen über die eben genannten Gesetze essentiell ist für das Verständnis der Systeme und deren anschließenden rechtlichen Bewertung in Bezug auf die rechtskonforme Einsetzbarkeit. Das gilt besonders bei der Verarbeitung von personenbezogenen Daten.

Kommen diese Systeme nun zur Verarbeitung personenbezogener Daten zum Einsatz, lässt sich zeigen, dass bei der Implementierung einer Alarmanlage weder eine Betriebsvereinbarung noch eine Datenschutz-Folgeabschätzung oder eine Vereinbarung über eine Auftragsverarbeitung erforderlich ist, da diese Systeme im Normalfall keine personenbezogenen Daten verarbeiten. Das gilt jedoch nicht für den Fall, wenn man Zutrittskontrollanlagen, GPS-Systeme oder Videoüberwachungsanlagen einsetzen möchte. Hier musste festgestellt werden, dass unter Umständen die oben genannten Vereinbarungen abgeschlossen und eine Datenschutz-Folgeabschätzung durchgeführt werden muss. Dies trifft besonders dann zu, wenn biometrische Zutrittskontrollanlagen eingesetzt werden.

Um das Verständnis für die abzuschließenden Verträge und Vereinbarungen zu erhöhen, wurden einerseits die Möglichkeiten von AGBs, Rahmenverträgen und SLAs genauer unter die Lupe genommen und andererseits die Vorgaben der DSGVO in Bezug auf die Auftragsverarbeitung, das Verarbeitungsverzeichnis und die Datenschutz-Folgeabschätzung genauer betrachtet. Daraus ergab sich, dass es unter Umständen bestimmte Möglichkeiten zur Einschränkung oder zum Ausschluss der Haftung bei Gewährleistungs- oder Schadenersatzansprüchen, nicht jedoch bei Ansprüchen aus der Produkthaftung gibt. Zudem musste festgestellt werden, dass die Haftung bei einer Verletzung des Schutzes personenbezogener Daten nicht ausgeschlossen werden kann.

7.1. Fazit

In weiterer Folge werden die konkreten Forschungsfragen noch einmal kurz beantwortet. Als relevante unternehmensexterne Richtlinien konnten einerseits verschiedene EN-Normen und OVE-Richtlinien definiert werden, deren Anwendung insbesondere dann wichtig ist, wenn nachgewiesen werden soll, dass der aktuelle Stand der Technik angewendet wurde. Andererseits wurde sowohl das Arbeitsrecht als auch die Datenschutzgrundverordnung als wesentliche Voraussetzung für den gesetzeskonformen Einsatz von elektronischer Sicherheitstechnik identifiziert.

Was die Gestaltung von AGBs und Verträgen betrifft, so konnte anhand der identifizierten rechtlichen Grundlagen gezeigt werden, dass es wichtig ist, bei der Verarbeitung personenbezogener Daten eine explizite Einstimmungserklärung der betroffenen Person zu erhalten. Unklar blieb hierbei jedoch, ob ein Hinweis in den AGBs ausreicht oder ob eine konkrete Vereinbarung abgeschlossen werden muss. In jedem Fall kann jedoch gesagt werden, dass die Formulierung in den Verträgen einerseits klar und verständlich sein muss und andererseits keine versteckten Formulierungen erlaubt sind, wie z.B. eine Information über den Datenschutz in dem Bereich über die Zahlungsmodalitäten.

Abschließend kann festgestellt werden, dass die Frage, wer für Schäden bei kompromittierten Systemen innerhalb der gesetzlichen Gewährleistung haftet, differenziert beantwortet werden muss. Zunächst muss unterschieden werden, ob auch eine Verletzung des Schutzes personenbezogener Daten vorliegt. Ist dies nicht der Fall, so gibt es für den/die Hersteller/in unter anderem die Möglichkeit, die Haftung aus Schadenersatzansprüchen im Falle einer leichten Fahrlässigkeit vertraglich einzuschränken oder auszuschließen. Eine andere Möglichkeit wäre die vertragliche Verkürzung der Gewährleistung bei Verträgen zwischen zwei Unternehmer/innen, wobei nicht festgestellt werden konnte, ob ein kompletter Ausschluss der Gewährleistung ebenfalls rechtskonform ist.

Resultiert aus den kompromittierten Systemen jedoch eine Verletzung des Schutzes der personenbezogenen Daten, so ist nach der derzeitigen Auslegung der Gesetzeslage kein Haftungsausschluss möglich – der/die Verarbeiter/in ist sogar für leichte Fahrlässigkeit haftbar, außer er/sie kann nachweisen, dass er alle Möglichkeiten ergriffen hat, um die Daten zu schützen, und auch den/die Auftragsverarbeiter/in können Haftungsansprüche treffen, je nachdem welche Rolle er/sie in Bezug auf die Datenschutzverletzung hatte.

7.2. Ausblick

Zusammenfassend kann gesagt werden, dass insbesondere Fragen zu Haftung komplex zu beantworten sind, da eindeutige Rechtsprechungen und Urteile bezüglich der korrekten Auslegung der Datenschutzgrundverordnung derzeit noch fehlen.

Es bleibt daher zu hoffen, dass in naher Zukunft durch OGH-Urteile Klarheit in die genaue Auslegung der Datenschutzgrundverordnung gebracht werden kann. Bis dahin sollte man auf Nummer sicher gehen und die Vorgaben der Datenschutzgrundverordnung in Bezug auf den Schutz der Systeme und die abzuschließenden Verträge genau einhalten.

Literaturverzeichnis

[1] A. Strasser und M. Wittek, „IT-Compliance," *Informatik-Spektrum,* Bd. 35, Nr. 1, pp. 39-44, Februar 2012.

[2] M. Klotz, „IT-Compliance: Begrifflichkeit und Grundlagen," 2014. [Online]. Available: http://nbn-resolving.de/urn:nbn:de:0226-simat06140289. [Zugriff am 04 05 2018].

[3] Statista, „Prognose zum Umsatz im Segment Gebäudesicherheit in Österreich in den Jahren 2015 bis 2021 (in Millionen Euro)," Oktober 2017. [Online]. Available: https://de-statista-com.ezp.sub.su.se/statistik/daten/studie/729962/umfrage/umsatz-im-segment-gebaeudesicherheit-in-oesterreich/. [Zugriff am 15 04 2018].

[4] Statista, „Prognose zum Umsatz im Segment Gebäudesicherheit in Deutschland in den Jahren 2016 bis 2022 (in Millionen Euro)," Oktober 2017. [Online]. Available: https://de-statista-com.ezp.sub.su.se/statistik/daten/studie/479203/umfrage/umsatzprognose-im-bereich-gebaeudesicherheit-in-deutschland/. [Zugriff am 15 04 2018].

[5] Statista, „Umsatz mit elektronischer Sicherungstechnik in Deutschland nach Segment im Jahr 2016 (in Millionen Euro)," Juni 2017. [Online]. Available: https://de-statista-com.ezp.sub.su.se/statistik/daten/studie/274362/umfrage/umsatz-der-elektronischen-sicherungstechnikbranche-in-deutschland-nach-segment/. [Zugriff am 15 04 2018].

[6] K. Mossanen und M. Amberg, „IT-Outsourcing & Compliance," *HMD Praxis der Wirtschaftsinformatik,* Bd. 45, Nr. 5, pp. 58-68, Oktober 2008.

[7] M. Klotz und D. W. Dorn, „IT-Compliance – Begriff, Umfang und relevante Regelwerke," *HMD Praxis der Wirtschaftsinformatik,* Bd. 45, Nr. 5, pp. 5-14, Oktober 2008.

[8] European Society of Radiology, „The new EU General Data Protection Regulation: what the radiologist should know," *Insights into Imaging,* Bd. 8, Nr. 3, p. 295–299, Juni 2017.

[9] T. Weichert, „Gesundheitsdatenschutz in vernetzten Zeiten," *Wiener klinisches Magazin,* p. 1–6, April 2018.

[10] D. Müller, „Cloud Computing," *Datenschutz und Datensicherheit - DuD,* Bd. 41, Nr. 6, p. 371–376, Juni 2017.

[11] E. Rose, „Datenbrillen, Drohnen, Dashcams …," *Datenschutz und Datensicherheit - DuD,* Bd. 41, Nr. 3, p. 137–141, März 2017.

[12] J. Taeger, „Smart Cams — Videoüberwachung 4.0?," *Datenschutz und Datensicherheit - DuD,* Bd. 41, Nr. 3, p. 129–130, März 2017.

[13] S. Schnepfleitner, „Überwachung der Mitarbeiter am Arbeitsplatz," 2008. [Online]. Available: http://forschungsnetzwerk.at/downloadpub/Schnepfleitner_Graz_Mitarbeiter_am_Arbeitsplatz.pdf. [Zugriff am 05 04 2018].

[14] W&R Sicherheitstechnik, [Online]. Available: https://www.wr-sicherheitstechnik.at/leistungen/sicherheitstechnik/. [Zugriff am 28 04 2018].

[15] Bundeskriminalamt, „Polizeiliche Kriminalstatistik 2017," 2017. [Online]. Available: http://bundeskriminalamt.at/501/files/PKS_17_Broschuere_Web.pdf. [Zugriff am 05 04 2018].

[16] W. J. Friedl, Effektiver Einbruchschutz : Mechanische, mechatronische und elektronische Gebäudesicherung, Stuttgart: Richard Boorberg Verlag, 2016.

[17] H. Rieche, „Einbruchsicherheit - so schützen Sie sich und Ihr Zuhause," [Online]. Available: https://www.baufi24.de/documents/ebook-optimaler-einbruchschutz-praevention.pdf. [Zugriff am 05 04 2018].

[18] K. Peyerl, „Unternehmer haften bei Kundendatenklau!," 2006 Dezember 2011. [Online]. Available: http://www.wirtschaftsanwaelte.at/unternehmer-haften-bei-kundendatenklau/. [Zugriff am 16 03 2018].

[19] P. Voigt und A. von dem Bussche, EU-Datenschutz-Grundverordnung (DSGVO), Berlin: Springer, 2018.

[20] Sikom Essra, „Sicherheitstechnik," [Online]. Available: http://www.sikom-essra.at/sicherheitstechnik/. [Zugriff am 05 03 2018].

[21] M. Klotz, „Regelwerke der IT-Compliance - Klassifikation und Übersicht, Teil 2: Normen," 2013. [Online]. Available: nbn-resolving.de/urn:nbn:de:0226-simat05130240. [Zugriff am 04 05 2018].

[22] Austrian Standards, „Über Standards," [Online]. Available: https://www.austrian-standards.at/ueber-standards/. [Zugriff am 18 04 2018].

[23] M. Wieser, „Einbruchhemmende Fenster und Türen," 2009. [Online]. Available: www.sicherheitszentrale.at/download.php?id=17. [Zugriff am 28 04 2018].

[24] DIN EN 1627:2011 09, *Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Anforderungen und Klassifizierung.*

[25] DIN EN 1628:2016 03, *Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Prüfverfahren für die Ermittlung der Widerstandsfähigkeit unter statischer Belastung.*

[26] DIN EN 1629:2016 03, *Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Prüfverfahren für die Ermittlung der Widerstandsfähigkeit unter dynamischer Belastung.*

[27] DIN EN 1630:2016 03, *Türen, Fenster, Vorhangfassaden, Gitterelemente und Abschlüsse - Einbruchhemmung - Prüfverfahren für die Ermittlung der Widerstandsfähigkeit gegen manuelle Einbruchversuche.*

[28] ÖNORM B 5338:2011 08 01, *Einbruchhemmende Fenster, Türen und zusätzliche Abschlüsse - Allgemeine Festlegungen - Ergänzende Bestimmungen zu den ÖNORMEN EN 1627 bis EN 1630.*

[29] ÖNORM B 5351:2011 08 01, *Einbruchhemmende Baubeschläge - Schlösser, Schließbleche, Schutzbeschläge, Schließzylinder und Nachrüstprodukte für Fenster und Türen - Maße, Ausführung, Prüfung und Kennzeichnung.*

[30] WKO Elektrotechniker, „Die Vorschriftensammlung für Errichter von Alarmanlagen," 10 2014. [Online]. Available: https://kfe.at/medien/brosch%C3%BCren/79-vorschriftensammlung-f%C3%BCr-errichter-von-alarmanlagen/file.html. [Zugriff am 04 05 2018].

[31] WKO, „OVE Richtlinien," [Online]. Available: http://elektrotechniker.at/gesetze-und-normen/ove-richtlinien.html. [Zugriff am 04 05 2018].

[32] dormakaba, „Zutrittskontrolle," [Online]. Available: https://www.dormakaba.com/at-de/produkte-loesungen/systemloesungen/zutrittskontrolle. [Zugriff am 04 05 2018].

[33] C. Pleschberger, „Neue OVE-Richtlinie R 10 für größere Sicherheit bei Zutrittskontrollanlagen," 09 03 2016. [Online]. Available: http://www.pqrm.at/2016/03/09/neue-ove-richtlinie-r-10-fuer-groessere-sicherheit-bei-zutrittskontrollanlagen/. [Zugriff am 04 05 2018].

[34] Siemens, „Videoüberwachung," 2016. [Online]. Available: https://w1.siemens.ch/buildingtechnologies/ch/de/gebaeudesicherheit/Videoueberwachung/Documents/07_ext_Videoueberwachung_de.pdf. [Zugriff am 10 05 2018].

[35] Bundesamt für Sicherheit in der Informationstechnik, IT-Grundschutz-Kompendium, Köln: Bundesanzeiger Verlag GmbH, 2018.

[36] Siemens, „Zutrittskontrolle," [Online]. Available: https://w3.siemens.at/buildingtechnologies/at/de/loesungen/sicherheit/zutrittskontrolle/Documents/Portfolio_Zutrittskontrolle.pdf. [Zugriff am 10 05 2018].

[37] B. f. S. i. d. Informationstechnik, „IT Grundschutzhandbuch - Glossar und Begriffsdefinitionen," 2016. [Online]. Available: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/glossar/04.html. [Zugriff am 05 04 2018].

[38] Secupedia, „Einbruchhemmende Tür," 14 Mai 2016. [Online]. Available: http://www.secupedia.info/wiki/Einbruchhemmende_T%C3%BCr. [Zugriff am 28 04 2018].

[39] Riha-Sicherheit, „Einbruchschutz," [Online]. Available: http://www.riha-sicherheit.at/servicemenue/wissenswertes/technisches-lexikon/einbruchschutz/. [Zugriff am 28 04 2018].

[40] M. Wieser, „Einbruchhemmende Fenster und Türen," 01 2008. [Online]. Available: http://www.holzforschung.at/uploads/media/HFA_Mag0108_Wieser.pdf. [Zugriff am 28 04 2018].

[41] Secupedia, „Einbruchhemmende Fenster," 14 05 2016. [Online]. Available: http://www.secupedia.info/wiki/Einbruchhemmende_Fenster. [Zugriff am 28 04 2018].

[42] Flachglas Schweiz, „Vergleichstabelle neue Widerstandsklassen," 09 09 2015. [Online]. Available: https://flachglas.ch/fileadmin/user_upload/fgs_download/Widerstandsklassen_Dokument_von_HUF/Neue_Widerstandsklassen_RC_und_Panikverglasung.pdf. [Zugriff am 28 04 2018].

[43] Intersec Forum, „Elektronische Sicherheitstechnik: Die Branche wächst mit dem Bedarf an vernetzten Systemen in Gebäuden und Infrastruktur," [Online]. Available: https://intersec-forum.messefrankfurt.com/frankfurt/de/press/press-releases/intersec-forum/branche-wachstum-press.html. [Zugriff am 01 05 2018].

[44] Schonert, „Elektronische Sicherheitstechnik," [Online]. Available: https://www.schonert.org/elektronische-sicherheitstechnik.html. [Zugriff am 01 05 2018].

[45] Securityszene, „Elektronische Sicherheitstechnik," [Online]. Available: https://www.securityszene.de/sicherheitslexikon/elektronische-sicherheitstechnik/. [Zugriff am 28 04 2018].

[46] Abus, „Die Geschichte der Alarmanlage," [Online]. Available: http://www.abus.com/Ratgeber/Einbruchschutz/Alarmanlagen/Geschichte-der-Alarmanlage#mechatronik. [Zugriff am 01 05 2018].

[47] Abus, „Gefahrenmelder," [Online]. Available: https://www.abus.com/at/Sicherheit-Zuhause/Alarmanlagen/Gefahrenmelder. [Zugriff am 01 05 2018].

[48] P. Schnabel, „Grundlagen Sicherheitstechnik," 1999. [Online]. Available: http://www.tuf-ev.de/inhalt/a_hefte/Sicherheitstechnik.pdf. [Zugriff am 05 04 2018].

[49] Secupedia, „Brandmeldeanlage (BMA)," [Online]. Available: http://www.secupedia.info/wiki/Brandmeldeanlage_(BMA). [Zugriff am 01 05 2018].

[50] ABB, „Einbruch-Meldesysteme," [Online]. Available: http://www.knx-gebaeudesysteme.de/sto_g/Deutsch/Oesterreich_Schweiz/Sicherheitstechnik/PROJEKTIERUNG/PROJEKTIERUNG-EMA_PH_DE_V4-0_2CDC541100D0101.pdf. [Zugriff am 15 04 2018].

[51] ABB, „ABB i-bus KNX,“ [Online]. Available: http://mailing.knx-gebaeudesysteme.de/pdf/2CDC500074M0101_ApplikationsHB_Sicherheit.pdf. [Zugriff am 28 04 2018].

[52] VdS, „Übertragungseinrichtungen für Gefahrenmeldungen (ÜE),“ 08 2007. [Online]. Available: https://vds.de/fileadmin/vds_publikationen/vds_2463_web.pdf. [Zugriff am 20 05 2018].

[53] TCS, „Anwenderhandbuch: Anwenderprogramm-Zutrittskontrolle,“ 01 2013. [Online]. Available: https://www.tcsag.de/fileadmin/user_upload/TCS_DE/Metanavigation/Downloads/Handbuecher/ahb_PCitACC.pdf. [Zugriff am 20 05 2018].

[54] N. Schmidt, „Nutzung von Biometrischen Zugangssystemen am Arbeitsplatz,“ Südwest-Datenschutz, 10 10 2016. [Online]. Available: https://www.suedwest-datenschutz.com/nutzung-von-biometrischen-zugangssystemen-am-arbeitsplatz/. [Zugriff am 20 05 2018].

[55] M. Desoi, Intelligente Videoüberwachung, Wiesbaden: Springer Vieweg, 2017.

[56] K.-H. Böker, Videoüberwachung, Düsseldorf: Setzkasten GmbH, 2009.

[57] kowoma.de, „NAVSTAR GPS - Geschichtliches,“ 30 09 2008. [Online]. Available: http://www.kowoma.de/gps/Geschichte.htm. [Zugriff am 15 04 2018].

[58] kowoma, „Kontrollsegment (Bodenstationen),“ 18 11 2008. [Online]. Available: http://www.kowoma.de/gps/Bodenstationen.htm. [Zugriff am 15 04 2018].

[59] kowoma, „Positionsbestimmung,“ 29 11 2007. [Online]. Available: http://www.kowoma.de/gps/Positionsbestimmung.htm. [Zugriff am 15 04 2018].

[60] kowoma, „Genauigkeit,“ 18 06 2007. [Online]. Available: www.kowoma.de/gps/Genauigkeit.htm. [Zugriff am 15 04 2018].

[61] RIS, „Allgemeines bürgerliches Gesetzbuch für die gesammten deutschen Erbländer der Oesterreichischen Monarchie“.

[62] Europäisches Parlament, „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,“ 2016.

[63] OGH, *6Ob38/13a,* 2013.

[64] OGH, *3Ob195/17y,* 2018.

[65] B. A. Mester, „Auswirkungen der DSGVO auf die IT,“ *Wirtschaftsinformatik & Management,* pp. 12-14, 04 2017.

[66] RIS, „Datenschutz-Anpassungsgesetz 2018,“ 2018.

[67] Arge Daten, „DSGVO - Österreichs Politik agiert zunehmend chaotisch," 19 04 2018. [Online]. Available: http://www.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=67628gpo. [Zugriff am 05 03 2018].

[68] A. Brunne und S. Gerstl, „Security by Design," Elektronik Praxis, 31 10 2017. [Online]. Available: https://www.elektronikpraxis.vogel.de/security-by-design-sicherheit-von-anfang-an-a-657606/index2.html. [Zugriff am 10 05 2018].

[69] Bayerisches Landesamt für Datenschutzaufsicht, „EU-Datenschutz-Grundverordnung," 26 10 2016. [Online]. Available: https://www.elektronikpraxis.vogel.de/security-by-design-sicherheit-von-anfang-an-a-657606/index2.html. [Zugriff am 10 05 2018].

[70] K. Rammo, „Wartungsarbeiten – Ist das eine Auftragsverarbeitung nach der DSGVO?," Datenschutzbeauftragter-Info, 23 01 2017. [Online]. Available: https://www.datenschutzbeauftragter-info.de/wartungsarbeiten-ist-das-eine-auftragsverarbeitung-nach-der-dsgvo/. [Zugriff am 10 05 2018].

[71] Bitkom, Begleitende Hinweise zu der Anlage Auftragsverarbeitung, Berlin: Bitkom e. V., 2017.

[72] WKO, „EU-Datenschutz-Grundverordnung (DSGVO): Rechtsdurchsetzung und Strafen," 16 05 2018. [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Rechtsdurchsetzung-und-St.html. [Zugriff am 22 05 2018].

[73] T. Rauch, „Arbeitgeber muss keinen Betriebsrat einrichten," 24 09 2010. [Online]. Available: https://www.wienerzeitung.at/nachrichten/wirtschaft/international/37004_Arbeitgeber-muss-keinen-Betriebsrat-einrichten.html. [Zugriff am 20 05 2018].

[74] WKO, „EU-Datenschutz-Grundverordnung (DSGVO): Bildverarbeitung," WKO, 29 05 2018. [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-bildverarbeitung.html. [Zugriff am 29 05 2018].

[75] Dataprotect, „Videoüberwachung-Hinweisschild und Information," 18 03 2018. [Online]. Available: https://www.dataprotect.at/2018/03/18/video%C3%BCberwachung-hinweisschild-und-information/. [Zugriff am 20 05 2018].

[76] B. Dzida und T. Granetzny, „Anpassungsbedarf für Betriebsvereinbarungen unter der DS-GVO," Freshfields Bruckhaus Deringer, 09 10 2017. [Online]. Available: http://knowledge.freshfields.com/de/Germany/r/3612/anpassungsbedarf_f_r_betriebsvereinbarungen_unter_der_ds-gvo. [Zugriff am 10 05 2018].

[77] H. Barta, Zivilrecht: Grundriss und Einführung in das Rechtsdenken, Wien: WUV Universitätsverlag, 2004.

[78] WKO, „Praxistipps für Allgemeine Geschäftsbedingungen," 02 01 2018. [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/praxistipps-allgemeine-geschaeftsbedingungen.html. [Zugriff am 20 05 2018].

[79] HELP-Redaktion, 25 05 2018. [Online]. Available: https://www.help.gv.at/Portal.Node/hlpd/public/content/436/Seite.4360005.html. [Zugriff am 30 05 2018].

[80] A. Gadatsch, „Service Level Agreements (SLA)," [Online]. Available: http://org-portal.org/fileadmin/media/legacy/Prof._Dr._A._Gadatsch_SLA.pdf. [Zugriff am 25 05 2018].

[81] WKO, „Vereinbarung über eine Auftragsverarbeitung nach Art 28 DSGVO," 05 2018. [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-vereinbarung-auftragsverarbeitung.docx. [Zugriff am 29 05 2018].

[82] L. Feiler und B. Horn, „Muster einer minimalistischen Datenschutz-Folgeabschätzung," [Online]. Available: https://www.jusline.at/abfrageservices/dsgvo-mustervorlagen. [Zugriff am 14 05 2018].

[83] L. Feiler und B. Horn, „Muster eines minimalistischen Verzeichnisses der Verarbeitungstätigkeiten," [Online]. Available: https://www.jusline.at/abfrageservices/dsgvo-mustervorlagen. [Zugriff am 14 05 2018].

[84] GPA-djp, „Muster-Betriebsvereinbarung-Datenschutz-DSGVO," 07 2017. [Online]. Available: bildung.gpa-djp.at/files/2017/10/GPA-djp-Muster-Betriebsvereinbarung-Datenschutz-DSGVO.pdf. [Zugriff am 10 05 2018].

[85] WKO, „Gewährleistung und Konsumentenschutz - allgemeiner Überblick," 02 01 2018. [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Gewaehrleistung-Ueberblick.html. [Zugriff am 20 05 2018].

[86] Recht Einfach, „Gewährleistung," 14 07 2015. [Online]. Available: http://www.rechteinfach.at/rechtslexikon/gewaehrleistung-64.html. [Zugriff am 20 05 2018].

[87] WKO, „Gewährleistung - Garantie - Schadenersatz - Produkthaftung - FAQs," 02 01 2018. [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Gewaehrleistung_-_Garantie_-_Schadenersatz_-_Produkthaftun.html. [Zugriff am 20 05 2018].

[88] WKO, „Haftungsfreizeichnung im Vertragsrecht im Detail," 02 01 2018. [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Haftungsfreizeichnung_im_Vertragsrecht_im_Detail.html. [Zugriff am 20 05 2018].

[89] H.-P. Nosko, „Wissenslücken bei Gewährleistung," 08 02 2006. [Online]. Available: https://www.wienerzeitung.at/nachrichten/wirtschaft/international/122561_Wissensluecken-bei-Gewaehrleistung.html. [Zugriff am 20 05 2018].

[90] Konsument.at, „Gewährleistung und Garantie Extra," 16 10 2015. [Online]. Available: https://www.konsument.at/gew%C3%A4hrleistung?pn=9. [Zugriff am 20 05 2018].

[91] WKO, „Unter welchen Voraussetzungen ist Schadenersatz zu leisten?," 29 11 2017. [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Unter_welchen_Voraussetzungen_ist_Schadenersatz_zu_leisten_.html. [Zugriff am 20 05 2018].

[92] WKO, „EU-Datenschutz-Grundverordnung (DSGVO): Rechtsdurchsetzung und Strafen," 29 05 2018. [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Rechtsdurchsetzung-und-St.html. [Zugriff am 29 05 2018].

[93] WKO, „EU-Datenschutz-Grundverordnung (DSGVO): Die wichtigsten Fragen und Antworten," 23 04 2018. [Online]. Available: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/datenschutz-grundverordnung-fragen-und-antworten.html#heading_14__Kann_ich_die_Haftung_mit_dem_Kunden_einvernehmlich_ausschliessen_. [Zugriff am 20 05 2018].

[94] WKO, „Produkthaftung," 03 10 2016. [Online]. Available: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/Produkthaftung.html. [Zugriff am 20 05 2018].

[95] Sikom Essra, *Inspektionsvertrag für die Alarmanlage.*

[96] RIS, „Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000), Fassung vom 23.04.2018".

[97] D. Knorr, „Service Level Agreement für Wartungsverträge," 2013 09 2018. [Online]. Available: https://www.ordana.de/wp-content/uploads/2015/07/DOK-QMS-SLA.pdf. [Zugriff am 25 05 2018].

Abbildungsverzeichnis

Tabellenverzeichnis