UNIVERSITÄTSLEHRGANG
STRAFRECHT, WIRTSCHAFTSSTRAFRECHT UND KRIMINOLOGIE

Sanktionsrisikominimierungsmaßnahmen in Unternehmen durch die Verwendung moderner Managementsysteme

Master-Thesis

zur Erlangung des akademischen Grades

Master of Arts (M.A.)

im Universitätslehrgang „Strafrecht, Wirtschaftsstrafrecht und Kriminologie, Master of Arts (MA)“

eingereicht von

Ing. Günther Neukamp, MSc

am Department für Wirtschaftsrecht und Europäische Integration

an der Donau-Universität Krems

Betreuer: Univ.-Prof. DDr. Thomas Ratka, LL.M.

Eidesstattliche Erklärung

Ich, Ing. Günther Neukamp MSc., geboren am 25.06.1967 in Wien erkläre,

1. dass ich meine Master-Thesis selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfen bedient habe,

2. dass ich meine Master-Thesis bisher weder im In- noch im Ausland in irgendeiner Form als Prüfungsarbeit vorgelegt habe,

3. dass ich, falls die Arbeit mein Unternehmen oder einen externen Kooperationspartner betrifft, meinen Arbeitgeber über Titel, Form und Inhalt der Master-Thesis unterrichtet und sein Einverständnis eingeholt habe.

_____ Wien, am 17.9.2018

1 Inhaltsverzeichnis

1 INHALTSVERZEICHNIS 3

1.1 ABSTRAKT / ABSTRACT (ENGL.) 6

2 ABKÜRZUNGSVERZEICHNIS 7

3 EINLEITUNG 8

3.1 VERBANDSVERANTWORTLICHKEITSGESETZ (VBVG) 10

3.1.1 VERBÄNDE IM SINNE DES VBVG 10

3.1.2 VERBÄNDE IM SINNE DER GEGENSTÄNDLICHEN ARBEIT 11

3.1.3 VERANTWORTUNG FÜR STRAFTATEN VON VERBÄNDEN 11

3.1.4 ENTSCHEIDUNGSTRÄGER_INNEN UND MITARBEITER_INNEN 12

3.1.5 BEMESSUNG DER VERBANDSGELDBUßE 13

3.1.6 STRAFRECHTLICHES RISIKOMANAGEMENT 13

3.2 RISIKOMANAGEMENT 17

3.2.1 RISIKO DEFINIERT 17

3.2.2 RISIKOBEWÄLTIGUNG 20

3.2.3 RISIKOÜBERWACHUNG UND RISIKOÜBERPRÜFUNG 25

3.3 STANDARDS/NORMEN 26

3.3.1 INTEGRIERTE MANAGEMENTSYSTEME (IMS) 28

3.3.2 ISO 9001:2015 29

3.3.3 ISO 27001:2005 34

3.3.4 ONR 49.001:2014 RISIKOMANAGEMENT FÜR ORGANISATIONEN UND SYSTEME 38

3.4 DATENSCHUTZGRUNDVERORDNUNG (DSGVO) 41

3.4.1 173 ERWÄGUNGSGRÜNDE 41

3.4.2 DER SCHUTZ NATÜRLICHER PERSONEN 41

3.4.3 GEGENSTAND UND ZIELE DER DSGVO 41

3.4.4 SACHLICHER ANWENDUNGSBEREICH DER DSVGO 42

3.4.5 BEGRIFFSBESTIMMUNGEN DSVGO 42

3.4.6 PERSONENRECHTE AUS DER DSGVO 43

3.4.7 BESCHRÄNKUNGEN DER PERSONENRECHTE DURCH NATIONALE GESETZGEBUNGSMAßNAHMEN 44

3.4.8 Pflichten für Verantwortliche und Auftragsverarbeiter 45
3.4.9 Geldbußen bei Verstößen gegen die DSGVO/DSG 46
3.5 Datenschutzrichtlinie für Polizei und Justiz (DSRL-PL) 47
3.6 Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) 48
3.6.1 Besondere Strafbestimmungen im ab 25.5.2018 geltenden DSG 48
3.7 Personenbezogene Daten 50
3.8 Liegen personenbezogenen Daten vor? 50
3.9 Besondere Kategorien personenbezogener Daten 51
3.10 Dateisystem 51
3.11 Pseudonymisierung 52

4 HAUPTTEIL 53

4.1 Beispiel "Datenvernichtung von Ausdrucken mit personenbezogenen Daten" 53
4.1.1 Sachverhalt 53
4.1.2 Sicherheitsstufen der Aktenvernichtung 55
4.1.3 Wie kann man den Schutzbedarf / Stand der Technik der Datenträgervernichtung ermitteln? 57
4.1.4 Informationssicherheitsverordnung 59
4.1.5 Wie überprüft man Datenvernichtungsprozesse? 63
4.1.6 Ermittlung der Prozessrisiken Datenvernichtung 66
4.1.7 Ermittlung der Schutzziele personenbezogener Daten für den Prozess der Datenträgervernichtung 66
4.1.8 Ermittlung der Prozessrisiken auf Basis der festgelegten Schutzziele 70
4.1.9 Risikobewertung von (Prozess)Risiken 75
4.1.10 Risikobewältigung im fiktiven Fallbeispiel 82
4.1.11 Auswirkungen der Risikobewältigungsmaßnahmen am fiktiven Fallbeispiel 95
4.2 Schlussfolgerungen aus der Bearbeitung des Fallbeispiels für die Forschungsfrage 96
4.2.1 Risikoanalyse nach ISO 31000 bzw. ONR 49001 96
4.2.2 Integrierte Managementsysteme auf Basis der Logik der ISO 9001:2015 96
4.2.3 ISO 27001 Informationssicherheitsnorm 97
4.2.4 DIN 66399 Norm für Datenvernichtungsprozesse 97
4.2.5 ONR 19 20 50 Compliance 99

5 ZUSAMMENFASSUNG MEINER ERKENNTNISSE 100

6 LITERATURVERZEICHNIS 101

7 ABBILDUNGSVERZEICHNIS 105

1.1 Abstrakt / Abstract (engl.)

Abstrakt

Die gegenständliche Master Thesis untersucht die Möglichkeiten der Nutzung gängiger normierter Managementsysteme (ISO 31000, ISO 9001, ISO 27001,...) zur Bestimmung und Reduzierung von Sanktionsrisiken für Unternehmen aus dem Verbandsverantwortlichkeitsgesetz, der DSGVO /DSG am Beispiel der methodischen Analyse eines Datenvernichtungsprozesses von Datenträgern mit personenbezogenen Daten in Papierform durch und an einem Standort eines externen Dienstleisters.

Abstract

This Master thesis explores possible usages of common certified management systems (ISO 31000, ISO 9001, ISO 27001,...) to evaluate and reduce the sanction risks for corporates out of the (Austrian)Act of corporate liability, the GDPR/DPL with an example of a methodical analysis of a data destruction process of data files in paper form through and at an external service company premises.

2 Abkürzungsverzeichnis

AG...Aktiengesellschaft

BGBLA...Datenschutz Anpassungsgesetz

BGBl...Bundesgesetzblatt

DSGVO...Datenschutzgrundverordnung

DSG...Datenschutzgesetz

DSRL-PL...Datenschutzrichtlinie für Polizei und Justiz

GmbH...Gesellschaft mit beschränkter Haftung

IFRS...International Finance and Reporting Standard

IMS...Integrierte Managementsysteme

KEG...Kommanditerwerbsgesellschaft

KFG...Kraftfahrzeuggesetz

KG...Kommanditgesellschaft

MFC...Minimum Financial Controls

ÖAMTC...Österreichischer Automobil Motorrad und Touring Club

OG...Offene Gesellschaft

ONR...Ö-Norm von Austrian Standards veröffentlicht

Pickerl...(umgangssprachlich) für Begutachtungsplakette für KFZ, gemäß §57a KFG

QM...Qualitätsmanagement

RIS...Rechts Informationssystem der Republik Österreich

TÜV...Technischer Überprüfungsverband

u.a....unter Anderem

Überprüfung

UGB...Unternehmensgesetzbuch

VbVG...Verbandsverantwortlichkeitsgesetz

VbVG ... Verbandverantwortlichkeitsgesetz

3 Einleitung

Im Zuge meiner langjährigen Tätigkeit als Führungskraft in sensiblen Bereichen der Informationssicherheit, stellt für mich der sorglose Umgang mit Datenträgern seit jeher ein erhebliches Risiko für Unternehmen dar.

Im Lichte der DSGVO [1] und DSG [2] liegt der Fokus der allgemeinen Aufmerksamkeit derzeit auf den diversen elektronischen Datenverarbeitungsprozessen und noch maximal im Bereich der Vernichtung von elektronischen Datenträgern. Die Vernichtung von Ausdrucken personenbezogener Daten in Papierform wird derzeit meines Erachtens zu wenig Bedeutung beigemessen.
Das Verbandverantwortlichkeitsgesetz verpflichtet, wie die DSGVO und das DSG Unternehmen und deren Entscheidungsträger zur Ergreifung von Maßnahmen zur Risikominimierung von bekannten Risiken um strafrechtlichen Sanktionen zu entgehen.

Als Forschungsfrage meiner gegenständlichen Arbeit möchte ich den Nutzen moderner Managementsysteme bei der Sanktionsrisikobewältigung analysieren:

Wie weit kann das diesbezügliche Sanktionsrisiko für Unternehmen, durch die Nutzung methodischer Herangehensweisen normierter Managementsysteme (ISO 31000, ISO 9001, ISO 27001,...), reduziert werden? Wie kann der Stand der Technik basierend auf Normen ermittelt werden? Dabei soll ein konkreter Vorgang - Vernichtung von Daten auf Datenträgern aus Papier - methodisch auf Sanktionsrisiken geprüft und darauf basierend Maßnahmen zur Risikobewältigung abgeleitet werden.

Im Zuge meiner Tätigkeit bei G4S, dem weltweit führenden Sicherheitsunternehmen hatte ich Einblicke in die gängige Praxis großer Aktenvernichtungsunternehmen und deren Zugang zum Thema DSGVO / DSG sowie die Anwendung und Nutzung der gegenständlichen Managementsysteme.

[1] DSGVO VO (EU) 2016/679 25.05.2018 idgF

[2] Datenschutzgesetz 2000 BGBl. I Nr. 165/1999 2000 idgF

Die generelle Beleuchtung der Prozesse der Datenvernichtung von Datenträgern in Papierform mit modernen Risikoanalyseansätzen soll auch Bewusstsein der Entscheidungsträger von Verbänden für die meiner Meinung nach eklatanten Sanktionsrisiken in diesem Bereich schaffen.

3.1 Verbandsverantwortlichkeitsgesetz (VbVG)

Das VbVG regelt unter welchen Voraussetzungen Verbände für Straftaten verantwortlich sind und wie sie sanktioniert werden.

3.1.1 Verbände im Sinne des VbVG

sind lt. §1 Z 2 und 3 VbVG juristische Personen sowie eingetragene Personengesellschaften und Europäische wirtschaftliche Interessensvereinigungen, sowie Bund, Länder, Gemeinden oder andere juristische Personen, soweit sie nicht in Vollziehung der Gesetze handeln. Anerkannte Kirchen, Religionsgesellschaften und religiöse Bekenntnisgemeinschaften, gelten soweit sie nicht seelsorgerisch tätig sind ebenfalls als Verbände. [3]

Als Beispiele führt Kienapfel/Höpfel/Kert Krankenhäuser, die als AG oder GmbH organisiert sind an. Er meint diese fallen unter die Kategorie „juristische Personen"; aber auch die Gemeinde, die ein Krankenhaus als unselbständigen Betrieb führt, hat Rechtspersönlichkeit, und sie handelt dabei nicht hoheitlich (also nicht „in Vollziehung der Gesetze"). Dagegen scheidet die Verbandsverantwortlichkeit aus, wenn die Hochschülerschaft (obzwar juristische Person) Wahlen durchführt (=Hoheitsakt). [4] .

Im Umkehrschluss wird die Grenzziehung zwischen hoheitlichen Handlungen und nicht hoheitlichen Handlungen von Maximilian Hotter und Richard Soyer bei Betrachtung der Ausstellung eines „Pickerl" durch den ÖAMTC betrachtet: Sie gehen davon aus, dass Mitarbeiter eines Unternehmens, die unter anderem mit der Vornahme öffentlicher Aufgaben betraut sind, insoweit hoheitlich tätig werden, als sie in Vollziehung der Gesetze handeln. [5]

Damit können sehr wohl auch Bund, Länder, Gemeinden und Kirchen in gewissen Bereichen umfasst sein!

---

[3] VbVG 2006 BGBl. 151/2005 idgF. 1.

[4] *Kienapfel/Höpfel/Kert*, Strafrecht Allgemeiner Teil[15] (2016) 331.

[5] vgl. *Hotter/Lunzer/Schick/Soyer*, Unternehmensstrafrecht - eine Praxisanleitung [12] (2010) 22.

3.1.2 Verbände im Sinne der gegenständlichen Arbeit

Ich konzentriere mich in meiner Arbeit auf allgemein gültige Maßnahmen für Verbände laut §1 Z 2 VbVG juristische Personen, sowie eingetragene Personengesellschaften und Europäische wirtschaftliche Interessensgemeinschaften.
Darunter fallen damit Juristische Personen wie Stiftungen, Fonds, Aktiengesellschaften, Gesellschaften mit beschränkter Haftung, Genossenschaften und Vereine,
aber auch Eingetragene Personengesellschaften wie Offene Gesellschaft (OG), Kommanditgesellschaft (KG), Kommanditerwerbsgesellschaft (KEG), Gesellschaft bürgerlichen Rechtes (§§ 1175 ff ABGB) und sogenannte Europäische wirtschaftliche Interessensgemeinschaften (EWIV) wie sie im Bundesgesetz zur Ausführung der Verordnung des Rates über die Schaffung einer Europäischen wirtschaftlichen Interessensvereinigung BGBl. Nr. 52/1995 idF BGBl. Nr. 680/1996 geregelt sind. [6]

Gegenüber Bund, Ländern, Gemeinden und Kirchen ist in dem Bereich der Juristischen Personen §1 Z 2 VbVG die Verbreitung der beleuchteten Managementsysteme sehr verbreitet.

3.1.3 Verantwortung für Straftaten von Verbänden

Kienapfel/Höpfel/Kert meinen dazu:

"*Ein Verband insbesondere eine juristische Person, kann nur durch seine Organe oder andere Mitarbeiter handeln. Soll der Verband strafrechtlich verantwortlich sein, so bedeutet das, dass er aus einer (nicht bloß stellvertretend für eine) Tat einer natürlichen Person haftet.*" [7]

Gemäß §3 Z 1 VbVG ist ein Verband für eine Straftat verantwortlich, wenn 1. die Tat zu seinen Gunsten begangen worden ist, oder 2. durch diese Tat Pflichten verletzt worden sind, die den Verband treffen und die Voraussetzungen aus Z 2 und Z 3 erfüllt sind:
Im §3 Z 2 VbVG ist die Verantwortung des Verbandes für die Straftaten eines

---

[6] vgl. VbVG 2006 BGBl. 151/2005 idgF. 1.

[7] *Kienapfel/Höpfel/Kert*, Strafrecht Allgemeiner Teil[15] (2016) 331.

Entscheidungsträgers definiert, falls dieser Entscheidungsträger die Tat rechtswidrig und schuldhaft begangen hat. Die Verantwortung des Verbandes für Straftaten von Mitarbeitern und Mitarbeiterinnen ist lt. §3 Z 3 VbVG gegeben, wenn der Sachverhalt, welcher dem gesetzlichen Tatbild entspricht rechtswidrig verwirklicht wurde; der Verband ist für eine Straftat, die vorsätzliches Handeln voraussetzt, nur verantwortlich, wenn ein Mitarbeiter vorsätzlich gehandelt hat. Für eine Straftat das fahrlässiges Handeln voraussetzt, nur, wenn Mitarbeiter_innen die nach den Umständen gebotene Sorgfalt außer Acht gelassen haben; und die Begehung der Tat dadurch ermöglicht oder wesentlich erleichtert wurde, dass Entscheidungsträger_innen die nach den gebotenen Umständen gebotene und zumutbare Sorgfalt außer Acht gelassen haben, insbesondere indem sie wesentliche technische, organisatorische und personelle Maßnahmen zur Verhinderung solcher Taten außer Acht gelassen haben. [8]

Damit fordert der Gesetzgeber im VbVG vom Verband wesentliche Maßnahmen zur Verhinderungen von Straftaten. D.h. der Verband muss solche Risiken ermitteln, bewerten und ggf. Maßnahmen zur Bewältigung ergreifen.

In diesem Zusammenhang sind die folgenden Definitionen entscheidend:

3.1.4 Entscheidungsträger_innen und Mitarbeiter_innen

Im §2 Z1und 2 VbVG werden die Gruppen der Entscheidungsträger_innen und Mitarbeiter_innen definiert:

"§ 2. Z 1 ***Entscheidungsträger_innen*** *im Sinne dieses Gesetzes ist, wer Geschäftsführer, Vorstandsmitglied oder Prokurist ist oder aufgrund organschaftlicher oder rechtsgeschäftlicher Vertretungsmacht in vergleichbarer Weise dazu befugt ist, den Verband nach außen zu vertreten, Mitglied des Aufsichtsrates oder des Verwaltungsrates ist oder sonst Kontrollbefugnisse in leitender Stellung ausübt, oder sonst maßgeblichen Einfluss auf die Geschäftsführung des Verbandes ausübt.*

§2 Z 2 ***Mitarbeiter_innen*** *im Sinne dieses Gesetzes ist, wer auf Grund eines Arbeits-, Lehr- oder anderen Ausbildungsverhältnisses, auf Grund eines dem Heimarbeitsgesetz 1960, BGBl.*

[8] vgl. VbVG 2006 BGBl. 151/2005 idgF. 1.

Nr. 105/1961, unterliegenden oder eines arbeitnehmerähnlichen Verhältnisses, als überlassene Arbeitskraft (§ 3 Abs. 4 des Arbeitskräfteüberlassungsgesetzes – AÜG, BGBl. Nr. 196/1988) oder auf Grund eines Dienst- oder sonst eines besonderen öffentlich-rechtlichen Rechtsverhältnisses Arbeitsleistungen für den Verband erbringt." [9]

3.1.5 Bemessung der Verbandsgeldbuße

Bei der Bemessung der Tagessätze gemäß §5 Z 1 VbVG ist eine Höhere Bemessung abhängig von Schädigungs- oder Gefährdungsgröße, Größe der Verbandsvorteilsnahme und Duldung und Begünstigung von gesetzeswidrigem Verhalten.
Eine geringere Bemessung ist gemäß §5 Z 2 VbVG u.a. vorgesehen, wenn seitens des Verbandes schon vor der Tat Vorkehrungen zur Verhinderung solcher Taten getroffen wurden oder Mitarbeiter_innen zu rechtstreuem Verhalten angehalten wurden, wenn der Verband lediglich für Straftaten von Mitarbeiter_innen verantwortlich ist, er wesentliche Schritte zur zukünftigen Verhinderung ähnlicher Taten unternommen hat. [10]

Damit fordert der Gesetzgeber präventive Maßnahmen des Verbandes, welche Straftaten verhindern sollen.

Um die Wirkung solcher Präventivmaßnahmen zu fokussieren bzw. abhängig von Eintrittswahrscheinlichkeit und Auswirkung auf den Verband zu priorisieren werden Methoden des Risikomanagements angewendet:

3.1.6 Strafrechtliches Risikomanagement

Die Verbandsverantwortlichkeit macht „strafrechtliches Risikomanagement“ für viele Unternehmen zur unverzichtbaren Aufgabe.
Von Hotter/Soyer wird in diesem Zusammenhang die Verbandsverantwortlichkeits-Compliance mit den Elementen: Risikoanalyse, Compliance Programm, Compliance Officer, Betriebsinterne Schulungen und Versicherungsschutz gefordert.

---

[9] vgl. VbVG 2006 BGBl. 151/2005 idgF. 1.

[10] vgl. VbVG 2006 BGBl. 151/2005 idgF. 3.

Dazu führen Hotter/Soyer wie folgt aus:

3.1.6.1 Verbandsverantwortlichkeits-Compliance

Als „strafrechtliches Risikomanagement“ werden alle Tätigkeiten bezeichnet, die gesetzt werden um potentielle Gefahren einer strafrechtlichen Verurteilung abzuwenden
Neben dem Terminus „Risikomanagement“ hat sich auch im Bereich des Unternehmensstrafrechtes der der – nicht vollständig deckungsgleiche – englische Begriff der Compliance durchgesetzt. Compliance soll die innerbetriebliche Einhaltung gesetzlicher, aber auch unternehmensinterner Vorgaben gewährleisten.
Im unternehmensstrafrechtlichen Kontext soll vor allem die Strafbarkeit des Unternehmens wegen eines Organisationsverschuldens sowie strafbaren Verhaltens von Entscheidungsträgern oder Mitarbeiter_innen vermieden werden. [11]

Als Eckpunkte einer präventiven Unternehmensorganisation, die die Einhaltung gesetzlichen Mindestanforderungen gewährleistet sehen Hotter/Soyer folgende Element der Verbandsverantwortlichkeit.

3.1.6.2 Elemente der Verbandsverantwortlichkeits-Compliance

3.1.6.2.1 Risikoanalyse

Die Notwendigkeit einer Risikoanalyse zur Identifizierung von strafrechtlichen Risiken unter Beiziehung strafrechtlich Rechtskundiger (Juristen, Anwälte) wird hier unbedingt empfohlen.[12]

3.1.6.2.2 Compliance Programm

Ein Compliance Programm sollte einen Verhaltenskodex für Entscheidungsträger_innen und Mitarbeiter_innen enthalten, welche sich zur Einhaltung dieses Verhaltenskodex verpflichten müssen. Die Nichteinhaltung sollte auch entsprechend sanktioniert werden (bspw. Kündigung des Arbeitsverhältnisses, Schadenersatzforderungen etc.).

---

[11] vgl. *Hotter/Lunzer/Schick/Soyer*, Unternehmensstrafrecht - eine Praxisanleitung [12] (2010) 30f.

[12] vgl. *Hotter/Lunzer/Schick/Soyer*, Unternehmensstrafrecht - eine Praxisanleitung [12] (2010) 32.

In diesem Zusammenhang ist auch das Krisenmanagement im Ernstfall von Verstößen zu regeln.[13]

3.1.6.2.3 Compliance Officer

Die Rolle eines allfälligen Compliance Officer, welcher die Einhaltung der Compliance Richtlinien sicherstellen soll umfasst einerseits Überwachungs-, Kontroll- und Informationspflichten, andererseits die Aufgabe als Anlauf- und Kommunikationsstelle für Mitarbeiter_innen. Darüber hinaus sollte die Unternehmensführung über Verstöße und Mängel informiert werden, Verbesserungsvorschläge unterbreitet werden und Mitarbeiter_innenschulungen und Informationsveranstaltungen organisiert werden. Gegebenenfalls steht sie in Kontakt mit Medien oder Behörden. [14]

3.1.6.2.4 Betriebsinterne Schulungen

Mitarbeiter_innen eines Unternehmens sind im Rahmen von Schulungen und Informationsveranstaltungen regelmäßig von fachkundigen Personen über Verhaltensrichtlinien zu unterrichten.

Über diese Unterweisungen sind Aufzeichnungen zu führen und Wissensüberprüfungen über Compliance (bspw. Tests) durchzuführen.[15]

Für mich stellen moderne **e-learning** Systeme und **Wissensmanagementsysteme** effiziente Instrumente zur Organisation dieser Unterweisungserfordernisse dar .

3.1.6.2.5 Versicherungsschutz

Die vom Unternehmen abgeschlossenen Versicherungen zur Abwehr von zivilrechtlichen Geschädigten Ansprüchen sollten auch auf bestimmte Vorsatzdelikte ausgeweitet werden. Damit sollten die Verfahrenskosten bei komplizierten und langwierigen Verfahren gedeckelt

---

[13] vgl. *Hotter/Lunzer/Schick/Soyer*, Unternehmensstrafrecht - eine Praxisanleitung [12] (2010) 32f.

[14] vgl. *Hotter/Lunzer/Schick/Soyer*, Unternehmensstrafrecht - eine Praxisanleitung [12] (2010) 33f.

[15] vgl. *Hotter/Lunzer/Schick/Soyer*, Unternehmensstrafrecht - eine Praxisanleitung [12] (2010) 34.

werden.[16]

Hotter und Soyer unterstreichen damit die Bedeutung von modernen Risikomanagement, welches Bestandteil oder Inhalt der normierten relevanten Managementsysteme (ISO 31000, ISO 9001, ISO 27001,...) sind.

[16] vgl. *Hotter/Lunzer/Schick/Soyer*, Unternehmensstrafrecht - eine Praxisanleitung [12] (2010) 34.

3.2 Risikomanagement

Um Risikomanagement im Kern zu verstehen werde ich in den Punkten 3.2.x vor allem aus dem diesbezüglichen Standardwerk im deutschsprachigen Raum zitieren, welches einen aktuellen Überblick über die verwendeten Risikomanagementansätze und Elemente gibt.

Dr. Bruno Brühwiler ist Experte auf dem Gebiet Risk Management und internationaler Industrieversicherungen und international anerkannter Fachbuchautor in diesem Themenbereich. [17]

Bruno Brühwiler fasst in seinem Buch „Risikomanagement als Führungsaufgabe“ (2016) den aktuellen Stand von Risikomanagementsystemen zusammen:

3.2.1 Risiko definiert

Die aufgezeichneten Quellen des Risikomanagements zeigen laut Brühwiler ein ganz unterschiedliches Verständnis von Risiko. Während bei technischen Methoden und bei Versicherungen Risiken eher von ihrer negativen Seite betrachtet werden, eröffnet die Sichtweise der Managementlehre und der modernen Finanztheorie sowie von Corporate Governance eine dynamische Perspektive. In diesem Sinn soll auch Risiko definiert werden. Diese Anforderung erfüllt der Risikobegriff laut der österreichischen Risikomanagementnorm ONR 49000:2014 [18] :

Risiko = Auswirkung von Unsicherheiten auf Ziele, Tätigkeiten und Anforderungen [19]

Der Begriff „Risiko“ im Sinne der ONR 49000:2014 umfasst demnach die folgenden Aspekte

---

[17] Schulthess Buchhandlungen - Kommentar, https://www.schulthess.com/buchshop/detail/ISBN-9783258079639/Bruehwiler-Bruno/Risikomanagement-als-Fuehrungsaufgabe (12.09.2018).

[18] *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 32.

[19] *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 33.

3.2.1.1 Die Kombination von Wahrscheinlichkeit und Auswirkung

Brühwiler sagt die Kombination von Wahrscheinlichkeit und Auswirkung laut Norm vernachlässigt aber Ereignisse mit geringer Wahrscheinlichkeit, damit finden in der Norm **Ereignisse mit hoher Wahrscheinlichkeit** in der Regel **mehr Aufmerksamkeit** als Ereignisse mit niedriger Wahrscheinlichkeit.[20]

Aber gerade **Ereignisse mit sehr niedriger Wahrscheinlichkeit** und extrem hoher Auswirkungen **stellen die Welt immer wieder auf den Kopf**. Ein „Schwarzer Schwan" ist ein Ereignis, auf das außerhalb der regulären Erwartung liegt, es hat enorme Auswirkungen und es ist letztendlich „Ungewiss". [21]

Aus diesem Grund müssen wir uns bei der DSGVO auch mit Ungewissem auseinandersetzen. Diesbezüglich müssen wir bei der Risikobewertung auch Managemententscheidungen einfließen lassen.

3.2.1.2 Auswirkungen

Laut Brühwiler können die **Auswirkungen** können positiv oder negativ sein. Als Beispiel führt er den Konsum von Medikamenten an, die eine Chance und Lebensqualität bieten aber auch Nebenwirkungen bedeuten können. [22] .

3.2.1.3 Unsicherheiten

Die **Unsicherheiten** (bzw. Ungewissheit) werden **mit Wahrscheinlichkeit geschätzt** bzw. ermittelt. In vielen Lebensbereichen, in welchen Unsicherheiten vorhanden sind, lassen sich Wahrscheinlichkeiten meist nicht mit ausreichender Information statistisch erfassen. Die Komplexität der Wirklichkeit ist enorm und sie nach zwingender Logik zu strukturieren sehr schwierig. Risikoeigner mit entsprechender Erfahrung können laut Aussage erfahrener

---

[20] *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 35.

[21] Vgl. *Taleb*, Der Schwarze Schwan - Die Macht höchst unwahrscheinlicher Ereignisse[1] (2015) 20ff.

[22] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 34.

Risikomanager bei der Festlegung der Wahrscheinlichkeit eines Ereignisses oder einer Entwicklung recht zuverlässig sein. [23]

Aus diesem Grund hat das im Hauptteil angewendete sehr verbreitete Verfahren des Brainstormings bei der Risikoermittlung eine entsprechend hohe Bedeutung.

3.2.1.4 Die Ziele der Organisation

erstecken sich lt. Brühwiler auf die strategische Entwicklung (bspw. Kundenbedürfnisse, Innovation, Marktstellung) Die Tätigkeiten umfassen die operativen Aktivitäten (bspw. Beschaffung, Produktion, Dienstleistung und Vertrieb). **Die Anforderungen beziehen sich insbesondere auf Gesetze**, Normen sowie weitere externe oder interne regulatorische Vorgaben, auch betreffend die Sicherheit von Menschen, Sachen und der Umwelt. [24]

Im Hauptteil dieser Arbeit werde ich besondere Ziele einer Organisation, in Form von sogenannten Schutzzielen aus Anforderungen von Gesetzen, nämlich VbVG, DSGVO und DSG in Zusammenhang mit dem Prozess der Datenvernichtung definieren.

3.2.1.5 Risiko ist eine Folge von Ereignissen oder von Entwicklungen

Der Begriff der Eintrittswahrscheinlichkeit bzw. der Häufigkeit, mit der ein Risiko auftreten kann, weist darauf hin, dass es sich um etwas Mögliches, Zukünftiges handelt. Die Wahrscheinlichkeit drückt die Ungewissheit aus und charakterisiert die fehlende Information zu einer bestimmten Annahme über Entwicklungen und Ereignisse in der Zukunft. [25]

---

[23] *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 33.

[24] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 36.

[25] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 36f.

3.2.2 Risikobewältigung

Ist ein Risiko einmal bewertet liegt der Fokus auf der Risikobewältigung, d.h. die Auswirkung bleibt gleich, die Eintrittswahrscheinlichkeit wird aber reduziert.

Wie in Gablers Wirtschaftslexikon beschrieben kann Risikobewältigung auch als Teil der Risikosteuerung bezeichnet werden, wobei er hier von Risikovermeidung, Risikoverminderung und Risikoüberwälzung spricht. [26]

3.2.2.1 Konzepte der Risikobewältigung

Die Risikobewältigung umfasst Strategien und Maßnahmen, welche die Organisation ergreift, um Risiken tragbar und verantwortbar zu machen. [27]

Brühwiler unterscheidet zwischen

- **Präventivem Risikomanagement,**
- **Schadenmanagement,**
- **Risikofinanzierung/Versicherungsmanagement,**
- **Restrisiko akzeptieren**.

Beim Präventiven Risikomanagement geht es ihm um die Vermeidung und die Verminderung des Eintrittes von Risiken. Die gebräuchliche Einteilung "*TOP"* (Technik – Organisation – Person) wird hier folgendermaßen definiert [28]:

Hinsichtlich Personeller Maßnahmen – fokussiert auf die Humanfaktoren und das Strafrecht finden sich hier interessante Definitionen: Brühwiler unterteilt hier menschliche Fehler in **Unvermögen** und in **Regelverstöße**. Das Unvermögen entsteht durch falsches Verhalten oder

---

[26] *Krystek/Fiege,* Gabler Wirtschaftslexikon (Stand 15.9.2018, https://wirtschaftslexikon.gabler.de/definition/risikomanagement-42454).

[27] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 165ff.

[28] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 165.

falsche Annahmen. Menschen neigen dazu, gegen gegebene Regeln und Vorschriften bewusst oder unbewusst zu verstoßen. Unbewusste Verstöße sind im Bereich von fahrlässiger Handlung, **bewusste als Absicht und Inkaufnahme qualifiziert**. Er sieht darin eine **Konfrontation mit dem Strafrecht**. **Menschen und Teams** werden von ihm klar als **Risikoquelle** in Betracht gezogen. [29]

Damit weist er in Sinne dieser Arbeit auf potentielle Sanktionsrisiken hin.

Bezüglich der **technischen Risikobewältigung** verweist Brühwiler auf die "Technische Systemgestaltung: "Das 3-Stufen-Modell"[30] auf Basis der EG – Maschinenrichtlinie:

- **Beseitigung oder Minimierung der Risiken soweit es möglich ist.** (Integration der Sicherheit in Konstruktion und Bau der Maschine)
- **Ergreifen der notwendigen Schutzmaßnahmen** gegen Risiken, die sich nicht beseitigen lassen
- **Unterrichtung der Benutzer über die Restrisiken** auf Grund der nicht vollständigen Wirksamkeit der getroffenen Schutzmaßnahmen, Hinweis auf eine eventuell erforderliche spezielle Auswirkung oder Einarbeitung und persönliche Schutzausrüstung. [31]

Brühwiler wendet dieses 3-Stufen-Modell auch auf **Organisatorische Risikobewältigung** an: Nach Brühwiler muss man Risiken vermindern, vermeiden und sich des Restrisikos bewusst sein. Er sieht hier zunächst die Analogie, dass Organisationen Prozesse und Abläufe so gestalten müssen, dass bei deren Ablauf wenige Risiken entstehen. Hier spielen nach seiner Ansicht Business Engineering, Prozessmanagement und das Qualitätsmanagement eine große Rolle. Darüber hinaus müssen Schutzmaßnahmen, d.h. Kontrollen vorhanden sein um die Restrisiken abzufangen. Er spricht hier u.a. ein „4-Augen-Prinzip“ an. [32]

---

[29] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 166f.

[30] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 170.

[31] vgl. MRL RL (EU) 2006/42/EG idgF.

[32] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 171f.

Man könnte hier weiter gefasst von einem „Internen Kontrollsystem (IKS)“ sprechen.

Die Definition eines IKS gemäß Österreichischem Rechnungshof:

„Die interne Kontrolle ist ein in die Arbeits- und Betriebsabläufe einer Organisation eingebetteter Prozess, der von Führungskräften und den Mitarbeitern durchgeführt wird, um bestehende Risiken zu erfassen, zu steuern und mit ausreichender Gewähr sicherstellen zu können, dass die betreffende Organisation im Rahmen der Erfüllung ihrer Aufgabenstellung ihre Ziele erreicht.
Sicherzustellende Ziele sind Sicherung der Vermögenswerte vor Verlust, Missbrauch und Schaden, Erreichung der Organisationsziele, Sicherstellung ordnungsgemäßer, ethischer, wirtschaftlicher, effizienter und wirksamer Abläufe, Zuverlässigkeit von betrieblichen Informationen; insbesondere Zuverlässigkeit des Rechnungswesens, die Einhaltung der Gesetze und Vorschriften; die Erfüllung der Rechenschaftspflicht („accuntability“/“answerability“).“ [33]

Im Folgenden beschreibt der gegenständliche Bericht des Rechnungshofes die Untrennbarkeit von IKS und Risikomanagement:

„Risikomanagement und IKS sind untrennbar miteinander verbunden: IKS soll sicherstellen, dass das Erreichen der Organisationsziele nicht durch interne und externe Risiken gefährdet wird. Zur Beurteilung der Qualität eines IKS ist die Kenntnis der Risiken der geprüften Organisation (der geprüften Prozesse) unabdingbar. Das Risikomanagement ist damit Grundvoraussetzung und Basis eines IKS. Interne Kontrollsysteme müssen bei Änderungen der Risikosituation angepasst werden.“[34]

Im gegenständlichen Kontext erachte ich die Erkenntnisse des Rechnungshofes bezüglich eines funktionierenden IKS für geeigneter als die Formulierung von Brühwiler hier beispielsweise auf ein „4-Augenprinzip“ zu verweisen, wenngleich ich davon ausgehe, dass

---

[33] *Rechnungshof,* Leitfaden zur Überprüfung von Internen Kontrollsystemen (2016) 8-9.

[34] *Rechnungshof,* Leitfaden zur Überprüfung von Internen Kontrollsystemen (2016) 10.

Brühwiler hier exemplarisch auch ein IKS anzuführen bereit wäre, da es die Idee eines 4-Augenprinzipes jedenfalls in sich enthält.

Weitere wichtige Element lt. Brühwiler sind Schadenmanagement, Notfall- und Krisenmanagement [35] .

Beim Schadenmanagement greifen die präventiven Maßnahmen nicht, folgert Brühwiler müssen folgende Schadenvermindernde Maßnahmen ergriffen werden: Hier wird gemäß ONR 49001:2014 zwischen Notfall und Krise unterschieden. Unter **Notfall** versteht man plötzliche und für gewöhnlich unvorhergesehene Ereignisse mit schwerwiegenden Folgen, welche in der Regel nur **auf eine Organisationseinheit begrenzt** ist, und das außerordentliche Maßnahmen erfordert. **Krisen** sind Situation, die **organisationsweit außerordentliche Maßnahmen erforderlich machen**, weil die bestehende Organisationsstruktur und die Prozesse zu ihrer Bewältigung nicht ausreichen. Dabei gibt es Krisen im engeren Sinn (diese Krise kann durch einen Notfall ausgelöst werden) und Krisen im weiteren Sinn (diese Krise kann eine problematische Entwicklung oder Entscheidungssituation bedeuten).[36]

Die **Aufgaben des Notfall- und Krisenmanagements** sind neben der Krisenkommunikation die Eindämmung der Schadensfolgen und die Bewältigung von operativen Fehlleistungen, oft verbunden mit einem Rechtsstreit und mit der Gefahr eines Reputationsverlustes. In Brühwilers Betrachtung ist die Vermeidung strafrechtlicher Folgen für den Verband und dessen Entscheidungsträger durch geeignetes Notfalls- und Krisenmanagement miteinzubeziehen[37], wobei ich diese sehr umfangreichen Maßnahmen in der gegenständlichen Arbeit bewusst ausklammere, da es für diese Bereiche in einem Unternehmen entsprechende generelle Pläne und Verfahren geben sollte.

Nach dem durch einen Notfall oder eine Krise eingetreten Schaden hat das **Kontinuitätsmanagement** die Aufgabe, den eingetretenen Schaden möglichst schnell zu

---

[35] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 172

[36] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 116ff.

[37] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 116.

überwinden bzw. die verlorenen Betriebsfunktionen mit der raschen Wiederherstellung der Produktions- und Lieferfähigkeit wieder zurückzugewinnen. [38]

Erwähnenswert sind in diesem Zusammenhang die Inhalte der ÖNORM S 2403[39] und der DIN EN ISO 22301 Sicherheit und Schutz des Gemeinwesens - Business Continuity Management System - Anforderungen [40] , welche sich intensiv mit den generellen Ansätzen zum Notfall- und Krisenmanagement befassen und den diesbezüglichen Stand der Technik zusammenfassen.

Brühwiler unterstreicht in diesem Zusammenhang auch die Notwendigkeit eines funktionierenden Kontinuitätsmanagements bei hochverfügbaren IT-Systemen. [41] In diesem Zusammenhang verweise ich auf die Methoden der ISO 27001:2005[42] , welche die Anforderungen an ein Informationssicherheits-Managementsystem definiert verweisen. Die ISO 27001:2005 wird von mir im Folgenden noch näher beleuchtet.

Der Umgang bzw. die Akzeptanz mit Restrisiken wird von Brühwiler auch erläutert, er beschreibt hier drei Arten von Restrisiken:

- Risiken, die man **nicht entdeckt** und **nicht identifiziert** hat
- Risiken, die zwar nach Verminderung von Wahrscheinlichkeit und Auswirkung geringer geworden sind, aber die Ziele der **Organisation immer noch erheblich beeinträchtigen**
- Restrisiken, die zwar immer noch über der Toleranzgrenze liegen, aber **aus technischen, wirtschaftlichen und praktischen Gründen nicht reduziert** werden können [43]

---

[38] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 116.

[39] vgl. *ONR*, ÖNORM S 2403 Business Continuity und COrporate Security Management idF 01.05.2009.

[40] vg. *DIN*, DIN 22301:2014 Sicherheit und Schutz des Gemeinwesens - Business Continuity Management System (2014).

[41] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 114f.

[42] *ONR*, ÖNORM ISO/IEC 27001 Ausgabe 2008-03-01.

[43] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 174.

3.2.3 Risikoüberwachung und Risikoüberprüfung

Die laufende Adaptierung an Rahmenbedingungen wird durch die 3 Elemente "*Risikomanagement als iterativer Prozess, Risikoüberwachung und Risikoüberprüfung"* sichergestellt.[44] Jede Maßnahme der Risikobewältigung ist nur so gut wie ihre laufende Überwachung und Adaptierung an sich ändernde Rahmenbedingungen.
Hier meint Brühwiler "*Das Risikomanagement ermittelt laufend Veränderungen und reagiert auf diese. Wenn interne oder externe Ereignisse eintreten, sich der Zusammenhang und das Wissen verändern, werden die Risiken überwacht und überprüft, treten neue Risiken auf, einige verändern sich und andere verschwinden*." und spricht in diesem Zusammenhang vom *"Risikomanagement als iterativer Prozess"*. [45]

D.h. Risikomanagement ist demgemäß ein sich wiederholender Prozess aus **Risikoüberwachung**, primär bei vorhandenen Restrisiken, welche bewusst oder gezwungenermaßen akzeptiert werden und **Risikoüberprüfung**. [46]

Die Risikoprüfung konzentriert sich auf die Umsetzung der geplanten Tätigkeiten der Risikominderung. Risiken die als nicht tragbar bewertet werden, sollten mit konkreten Maßnahmen, Terminen und Verantwortungen gesteuert werden. Die Risikoüberprüfung stellt regelmäßig fest, ob die Maßnahmen umgesetzt werden und die Risikobehandlung wirksam ist. Man kann bei der Risikoüberprüfung auch von **Risikocontrolling** sprechen. [47]

Ich schließe mich der Risikoüberprüfung nach Brühwiler an, muss jedoch methodisch auf die mittlerweile enormen Kosten von unterschiedlichsten Compliance-erfordernissen von Unternehmen verweisen.
In diesem Zusammenhang empfehle ich, vor allem aus Gründen der Reduktion der Total Cost of Compliance (TCoC), integrierten Managementsystemen (IMS) und der darin vorgesehenen gemeinsamen Behandlung von Prozessrisiken.

---

[44] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 174.

[45] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 175.

[46] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 175..

[47] vgl. *Brühwiler*, Risikomanagement als Führungsaufgabe (2016) 175.

Die ab September 2018 verbindliche Fassung der ISO 9001:2015[48] schafft in dieser Sache meiner Meinung nach interessante Möglichkeiten zur Optimierung und Zusammenführung unterschiedlicher Managementsysteme durch die Einführung international gängiger Methoden wie das PDCA (en.) Modell und risikobasiertes Denken. [49]

3.3 Standards/Normen

Auf der Webpage von AUSTRIAN STANDARDS findet sich eine treffliche Nutzendefinition zu Standards/Normen:

Standards (z.Bsp. ÖNORMEN und ISO-Standards) sind ein Signal für zuverlässige Qualität, die Erfüllung von Kundenerwartungen und die Einhaltung des Stands der Technik. Standards anzuwenden, unterstützt die fachgerechte Ausführung von Produkten und Dienstleistungen sowie Prüfmethoden oder Messverfahren. Sie machen Produktions- bzw. Arbeitsabläufe effizienter und sicherer. Das schafft Vertrauen und Vorsprung.[50]

Jährlich führt die SGS Group eine Analyse der weltweiten Zertifizierungen nach verschiedenen ISO Normen durch. Dieser sogenannte "The ISO Survey of Management System Standard Certifications 2015"[51] zeigt die Relevanz von Normen in Unternehmen:

Die international verbreitetste Norm für Unternehmen weltweit ist demnach die ISO 9001**. In der nachfolgenden Abbildung wird die weltweite Dominanz dieser Norm deutlich sichtbar.

---

[48] ISO 9001:2015 Qualitätsmanagementsysteme – Anforderungen idF 15.11.2015.

[49] vgl. ISO 9001:2015 Qualitätsmanagementsysteme – Anforderungen idF 15.11.2015 8.

[50] *Austrian Standards*, Nutzen von Standards (Stand 15.9.2018, https://www.austrian-standards.at/ueber-standards/nutzen-von-standards/).

[51] *SGS-Group,* The ISO Survey of Management System Standard Certifications, (Stand 13.9.2018, https://www.sgsgroup.com.hk/en/news/2016/10/2015-iso-survey-results).

Standard	2015	2014	Change	Change in %
ISO 9001**	1,033,936	1,036,321	-2,385	-0.20%
ISO 14001***	319,324	296,736	22,588	8%
ISO 50001	11,985	6,765	5,220	77%
ISO 27001	27,536	23,005	4,531	20%
ISO 22000	32,061	27,690	4,371	16%
ISO/TS 16949	62,944	57,950	4,994	9%
ISO 13485	26,255	26,280	-25	-0.10%
ISO 22301	3,133	1,757	1,376	78%
ISO 20000-1	2,778		2,778	
Total	1,519,952	1,476,504	43,448	3%

Abbildung 1: Zusammenfassung der 2015 ISO Befragung OV, The ISO Survey of Management System Standard Certifications 2015, (2015) <https://www.sgsgroup.com.hk/en/news/2016/10/2015-iso-survey-results>, aufgerufen am 13.09.2018

Eben diese Norm wurde 2015 komplett überarbeitet und mit entscheiden Änderungen in Richtung eines modernen risikofokussierten Managementsystems, doch dazu später. Bis September 2018 müssen Unternehmen ihre alten Zertifizierungen nach ISO 9001:2008 durch die neue Zertifizierung nach ISO 9001:2015 umstellen. Während ich diese Arbeit schreibe sind weltweit bis zu 1.000.000 Unternehmen dabei ihre Managementsysteme auf diese neue Norm umzustellen oder haben diese Umstellung bereits abgeschlossen. Zum Zeitpunkt der Untersuchung 2015 waren erst 4190 Unternehmen nach ISO 9001:2015 zertifiziert. In der ISO Befragung 2015 sieht man auch wie wenige Unternehmen derzeit nach ISO 27001 zertifiziert sind, nämlich knapp unter 30.000 Unternehmen weltweit. [52]

All diese Unternehmen haben meiner Ansicht nach einen entscheidenden Vorteil gegenüber Unternehmen, welche nicht über diese Zertifizierung verfügen.

Der Nutzen von Normen für Unternehmen wird gerne in Form von Case Studies beschrieben, eine relevante Case Study für diese Arbeit wird ebenfalls auf der Webpage von AUSTRIAN STANDARDS veröffentlicht. Hier wird auf die ONR 192050 bezuggenommen:

[52] *SGS-Group,* The ISO Survey of Management System Standard Certifications, (Stand 13.9.2018, https://www.sgsgroup.com.hk/en/news/2016/10/2015-iso-survey-results).

Die Elemente eines funktionierenden Compliancesystemes lt. 3.1.6.2 wurden mit der ONR 192050 normiert, zertifizierbar und auditierbar gemacht. Der Nutzen wird im Folgenden Zitat beschrieben: "*Compliance sichert den Wert des Unternehmens – Kärntner Energiedienstleister Kelag hat ein Compliance Management System nach ONR 192050 eingerichtet. Austrian Standards hat es zertifiziert und das Fair Business Compliance Certificate vergeben*."[53]

In diesem Artikel wird Kelag-Vorstandssprecher Univ. Prof. Dipl.-Ing. Herrmann Egger zitiert *"Die Identifizierung von und der Umgang mit rechtlichen Risiken ist Teil unseres Risikomanagements". Es wird weiter ausgeführt: „zu diesem Zweck hat das Unternehmen in Zusammenarbeit mit einer internationalen Anwaltskanzlei ein konzernweites Compliance Management System (CMS) implementiert, das die Wahrscheinlichkeit von Rechtsverstößen durch Mitarbeiter des KELAG-Konzerns so gering wie möglich hält. Vor kurzem wurde das System von Austrian Standards nach ONR 192050 „Compliance Management Systeme (CMS) – Anforderungen und Anleitungen zur Anwendung" zertifiziert."* [54]

Damit wirbt Austrian Standards für die Einführung einer eigenen Compliance Norm, vom Grundgedanken eine gute Idee, aber jede Norm ist mit hohen Aufwendungen für die Implementierung und den laufenden Betrieb verbunden.

3.3.1 Integrierte Managementsysteme (IMS)

Aus effizienzgründen müssen sich Unternehmen jedoch rasch von oft isolierten Managementsystemen für Qualitätserfordernisse, Normerfordernisse, Compliance Erfordernisse, ArbeitnehmerInnenschutzerfordernisse, IKS-Erfordernisse, MFC-Erfordernisse, IFRS-Erfordernisse, UGB-Erfordernisse und vielen anderen Erfordernissen verabschieden, da der dafür notwendige Aufwand schnell wettbewerbsgefährdende interne

[53] *Hirner*, Compliance sichert den Wert des Unternehmens (Stand 15.9.2018, https://www.austrian-standards.at/ueber-standards/nutzen-von-standards/nutzen-in-der-wirtschaft/kaerntner-energiedienstleister-kelag/).

[54] *Hirner*, Compliance sichert den Wert des Unternehmens (Stand 15.9.2018, https://www.austrian-standards.at/ueber-standards/nutzen-von-standards/nutzen-in-der-wirtschaft/kaerntner-energiedienstleister-kelag/).

und externe Kosten verursachen kann und zu zusätzlichen tlw. gesundheitsgefährdenden Arbeitsbelastungen und Demotivation von Mitarbeiter_innen und Entscheidungsträger_innen führen kann. [55]

Im Rahmen meiner Tätigkeiten in der Geschäftsleitung von G4S war ich mit einer Vielzahl ligistischer, normativer und vom Unternehmen selbstauferlegten Regulativen konfrontiert. Meine Erfahrungen in diesem Bereich bestätigen den Druck auf Mitarbeiter_innen um einerseits ihre Kernaufgaben zu erfüllen und andererseits alle diesbezüglichen Konformitätserfordernisse zu gewährleisten.

Eine Möglichkeit sehe ich in der Neufassung der ISO 9001:2015, welche in ihrer Gestaltung bereits den Ansprüchen einer Dachnorm zur Realisierung von integrierten Managementsystemen Rechnung trägt:

3.3.2 ISO 9001:2015

Die Neufassung der ISO 9001 in der Version ISO 9001:2015 stellt eine Revolution bezüglich Normenkonvergenz dar.

Die KIWA Unternehmensberatung fasst die Änderungen zusammen:
"*Am 23.9.2015 wurde die ISO 9001:2015 beschlossen. Bis 14.9.2018 müssen alle Zertifikate, die nach der ISO 9001:2008 erstellt wurden, erneuert werden, wenn sie weiterhin gültig bleiben sollen. Um die Managementsystemnormen kompatibler zu gestalten, wurde eine Grundstruktur entwickelt, die auf alle Managementsystemnormen angewendet wird: Das Modell des prozessorientierten Qualitätsmanagementsystems."* [56]

Die neuen Kapitel der ISO 9001:2015 umfassen demnach 01 Anwendungsbereich, 02 Normative Verweise, 03 Begriffe, 04 Kontext der Organisation, 05 Führung, 06 Planung, 07 Unterstützung, 08 Betrieb, 09 Bewertung der Leistung, 10 Verbesserung. Damit werden alle

---

[55] vgl. *Schmitt*, Integrierte Managementsysteme (IMS): der Geheimtipp zur Verbesserung der Unternehmensperformance, DGQ Blog, (2017).

[56] vgl. *kiwa*, ISO 9001:2015 Die Änderungen im Überblick, (2016, Stand: 13.9.2018, https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf) 1-6.

wesentlichen Elemente eines wie immer gearteten Betriebssystems umfasst, im Folgenden möchte ich diese definierten Element vertiefend betrachten [57] :

Für die Kapitel 04-10 wurde zur Veranschaulichung das Modell des prozessorientierten Qualitätsmanagementsystems erstellt [58]:

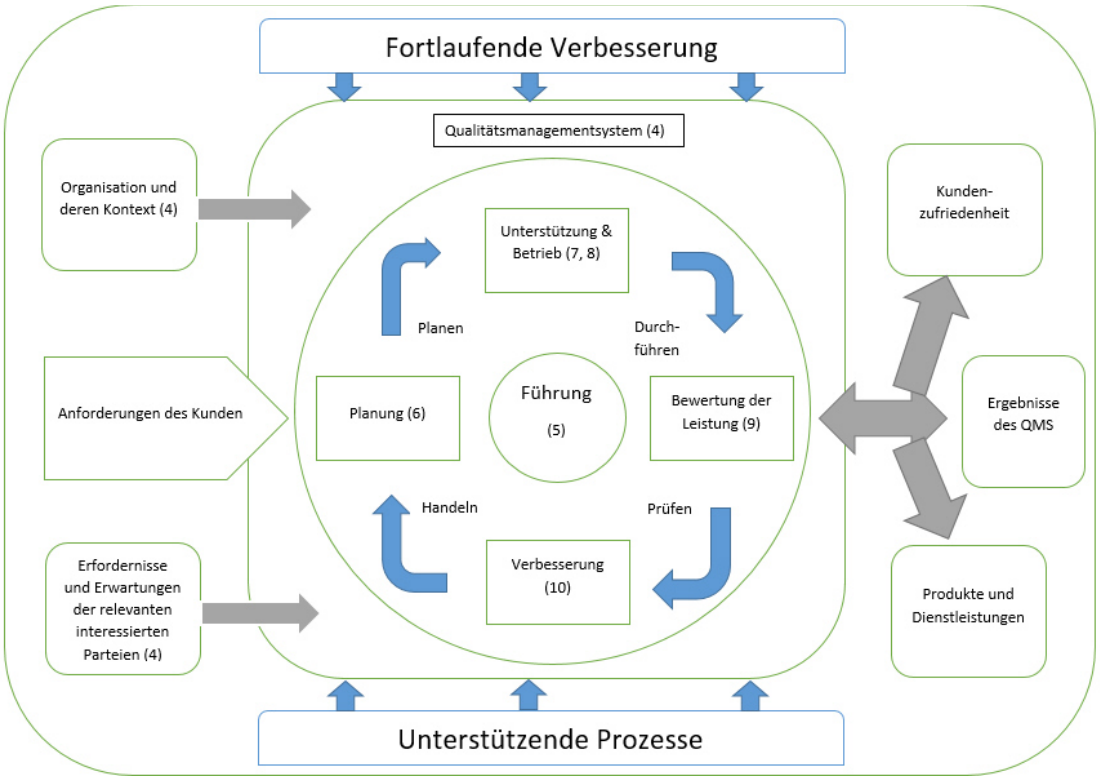


Abbildung 2: Abbildung eines Prozessorientierten Qualitätsmanagementsystems *kiwa*, ISO 9001:2015 Die Änderungen im Überblick, 2016 <https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf>, aufgerufen am 13.09.2018

Die Organisation und deren Kontext, Erfordernisse und Erwartungen der relevanten interessierten Parteien liefern Anforderungen an das Managementsystem (4), die oberste Führung (5) stellt die Verankerung dieser Anforderungen im Managementsystem sicher. Nach dem „plan/do/check/act“ Modell fließt das in die Planung (6), Unterstützung (7) & Betrieb (8), Bewertung und Leistung (9) und Verbesserung (10) ein.

---

[57] vgl. *kiwa*, ISO 9001:2015 Die Änderungen im Überblick, (2016, Stand: 13.9.2018, https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf) 2

[58] vgl. *kiwa*, ISO 9001:2015 Die Änderungen im Überblick, (2016, Stand: 13.9.2018 https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf) 2.

Im Kontext dieser Arbeit möchte ich hier besonders den Absatz über die Qualitätspolitik als wichtigen Bestandteil des Qualitätsmanagementsystems hervorheben. "*Sie ist die Basis für die zu organisierenden Abläufe und für den Anwendungsbereich des Managementsystems.*

Unternehmen müssen demnach sicherstellen, dass die Qualitätspolitik sowie die Qualitätsziele mit der strategischen Ausrichtung vereinbar sind.

In Kapitel 5.1. „Führung und Verpflichtung" manifestiert sich diese Verantwortung der obersten Führung für

- *Wirksamkeit des QM Systems*
- *Qualitätspolitik*
- *Qualitätsziele*
- *Integration in Geschäftsprozesse*
- *Prozessorientierter Ansatz*
- *Risikobasiertes Denken*
- *Ressourcen*
- *Bedeutung des QM-Systems*
- *Wichtigkeit der Erfüllung der Anforderungen*
- *Sicherstellung der Ergebnisse*
- *Personaleinsatz*
- *Verbesserung*
- *Unterstützung anderer Führungskräfte*" [59]

In vielen dieser Verantwortlichkeiten spiegeln sich schon die Erfordernisse eines guten Datenschutzmanagementsystems und der Entscheidungsträger im Sinne der DSGVO.

"Den weitergefassten Zielen der ISO 9001:2015 wird auch mit dem neuen Begriff Kontext der Organisation Rechnung getragen. Hierbei handelt es sich um interne und externe Faktoren,

[59] Vgl. *kiwa*, ISO 9001:2015 Die Änderungen im Überblick (Stand: 13.09.2018, https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf) 3.

innerhalb derer die Organisation agiert bzw. die auf sie Einfluss nehmen können. Diese Faktoren finden sich u.a. in dem

- *Gesetzlichen-,*
- *Technischen-,*
- *Wettbewerblichen-,*
- *Marktüblichen-,*
- *Kulturellen-,*
- *Sozialen-, und*
- *Wirtschaftlichem Umfeld*" [60]

Damit fordert die Norm dazu auf gesetzliche Erfordernisse wie die DSGVO in Prozesse zu integrieren, zu überwachen und zu überprüfen. Dieser prozessorientierte Ansatz ist entscheidend um die Handlungssicherheit von Mitarbeiter_innen in normativ hochkomplexen Arbeitsfeldern zu gewährleisten.

"Der prozessorientierte Ansatz und ein systematisches Prozessmanagement sind von großer Bedeutung. Die DIN EN ISO 9001:2015 fordert, dass

- *Die erforderlichen Eingaben und erwarteten Ergebnisse der Prozesse,*
- *Leistungsindikatoren zur wirksamen Lenkung der Prozess,*
- *Risiken, die einen Einfluss auf die Zielerreichung der Prozesse haben,*

bestimmt werden. Die Anforderungen an die Norm sind die Folgenden:

- *Prozessidentifikation*
- *Prozesseingabe*
- *Prozessergebnis*
- *Prozessabfolge und Wechselwirkungen*
- *Prozesssteuerung*

[60] Vgl. *kiwa*, ISO 9001:2015 Die Änderungen im Überblick (Stand: 13.09.2018, https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf) 4

- *Prozessressourcen*
- *Prozessverantwortliche*
- *Prozessrisiken*
- *Prozessbewertung*
- *Prozessänderungen*
- *Prozessverbesserungen*
- *Prozessdokumentation* [61]

Ebenfalls neu bei der ISO 9001:2015 ist die Verantwortung der obersten Leitung. Interessant ist hierbei, dass die ISO 9001:2015 keinen „(Qualitäts-) Beauftragten der obersten Leitung" mehr fordert. In der Praxis übernimmt das jeweils ressortverantwortliche Mitglied der Geschäftsleitung die Verantwortung für die ihm organisatorisch zugehörigen Prozesse. Darüber hinaus müssen Risiken und Chancen bestimmt werden um unerwünschte Auswirkungen zu vermeiden und Erwünschte zu verstärken. [62]

Das Wissen der Organisation wird in der DIN ISO 9001:2015 als eigenständige Ressource betrachtet. Die Norm erwartet Regelungen des Unternehmens bezüglich Wissensweitergabe

- Notwendiges Wissen muss
  - bestimmt
  - aufrechterhalten
  - zur Verfügung gestellt werden
- Zusatzwissen
- Aktualisierungen [63]

[61] Vgl. *kiwa*, ISO 9001:2015 Die Änderungen im Überblick (Stand: 13.09.2018, https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf) 4f.

[62] Vgl. *kiwa*, ISO 9001:2015 Die Änderungen im Überblick (Stand: 13.09.2018, https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf) 5.

[63] Vgl. *kiwa*, ISO 9001:2015 Die Änderungen im Überblick (Stand: 13.09.2018, https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf) 6.

Viele dieser Themen spielen meiner Meinung bei der Minimierung möglicher Sanktionsrisiken nach aus der Rechtsperspektive VbVG und DSGVO eine entscheidende Rolle, weil es am Ende immer um die Handlungsfähigkeit des Verbandes, seiner Mitarbeiter_innen und die Erreichung bestimmter Verbandsziele geht.

3.3.3 ISO 27001:2005

Wer ist denn bereits nach dieser ISO 27001 zertifiziert? Wie relevant ist diese Norm für Österreich? Unternehmen mit hohem Bedarf für Datensicherheit setzen ja bereits seit vielen Jahren auf die ISO 27001 Konformität um den bewussten und sorgsamen Umgang mit Daten zu dokumentieren:

Alle globale Datenverarbeiter bzw. Cloud Dienstanbieter wie Google, Apple, Amazon, Microsoft, Salesforce usw. verfügen alle bereits seit Jahren über entsprechende Zertifizierung ihrer Informations Sicherheits Managementsysteme nach ISO 27001. Die Zertifikate sind auf den Webseiten für alle abrufbar.

In Österreich verfügen zum Beispiel die ADMIRAL Casinos & Entertainment, AGRARMarkt Austia, AUVA, Austria Card, Austrian Power Grid, Bundesrechenzentrum, Energie AG Oberösterreich, Frequentis AG, GIS Gebühren Info Service, Interxion Österreich, Kapsch Business Com, MA14 der Stadt Wien, nic-at, Österreichische Nationalbank, OMV Solutions, Österreichische Staatsdruckerei, Raiffeisen Rechenzentrum & Informatik, Telekom Austria, TIWAG, Vorarlberger Illwerke, KAV aber auch die WKO Inhouse GmbH bereits über ISO 27001 Zertifizierungen [64]

Aber auch die G4S Secure Solutions GmbH, in welcher ich bis 07/2018 in der Geschäftsleitung für Business Development, Sales, IT und Risk Consulting verantwortlich war ist bereits seit gut 4 Jahren ISO 27001 zertifiziert.

[64] vgl. *Schmidhuber*, ISO 27001 zertfizierte Unternehmen - Österreich (Stand: 13.9.2018 https://www.iso-27001.at/zertifizierte-unternehmen-oesterreich/).

Der TÜV Rheinland erklärt die IT-Risiko Minimierung mittels ISO 27001 anschaulich mit folgender Grafik:

Abbildung 3: IT-Risiken minimieren mit einem ISO 27001 Zertifikat *Rheinland*, Informationssicherheit ISO 27001, (2018) <https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html>, aufgerufen am 13.09.2018

Durch die gesicherte Verfügbarkeit der IT-Systeme und Prozesse wird die Resilienz des Unternehmens gestärkt, d.h. das nach ISO 27001 zertifizierte Unternehmen kann auch feststellen ob gemäß DSGVO Z 87 eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist. Die im Rahmen der ISO 27001 überwachte Vertraulichkeit der Informationen ist im §6 DSG Datengeheimnis explizit gefordert. Wird das DSG und DSGVO als zu überwachende Complianceanforderung in die ISO 27001 integriert ist die entsprechende Einhaltung innerhalb der Unternehmensprozesse sichergestellt. In der ISO 27001 wird im

Rahmen von laufenden internen und externen Audits das systematische Aufdecken von Schwachstellen gewährleistet.
Der in der ISO 27001 beschrittene Weg der Risikoabschätzung erfolgt gemäß ISO 31000.
Durch die Erfüllung international anerkannter Anforderungen (für IT Sicherheit), die systematische Aufdeckung von Schwachstellen, die Kontrolle von IT-Risiken, die gesicherte Verfügbarkeit der IT-Systeme und Prozesse, die Vertraulichkeit von Informationen, die Minimierung von IT Risiken, mögliche Schäden und Folgekosten werden Compliance Anforderungen sichergestellt. [65]

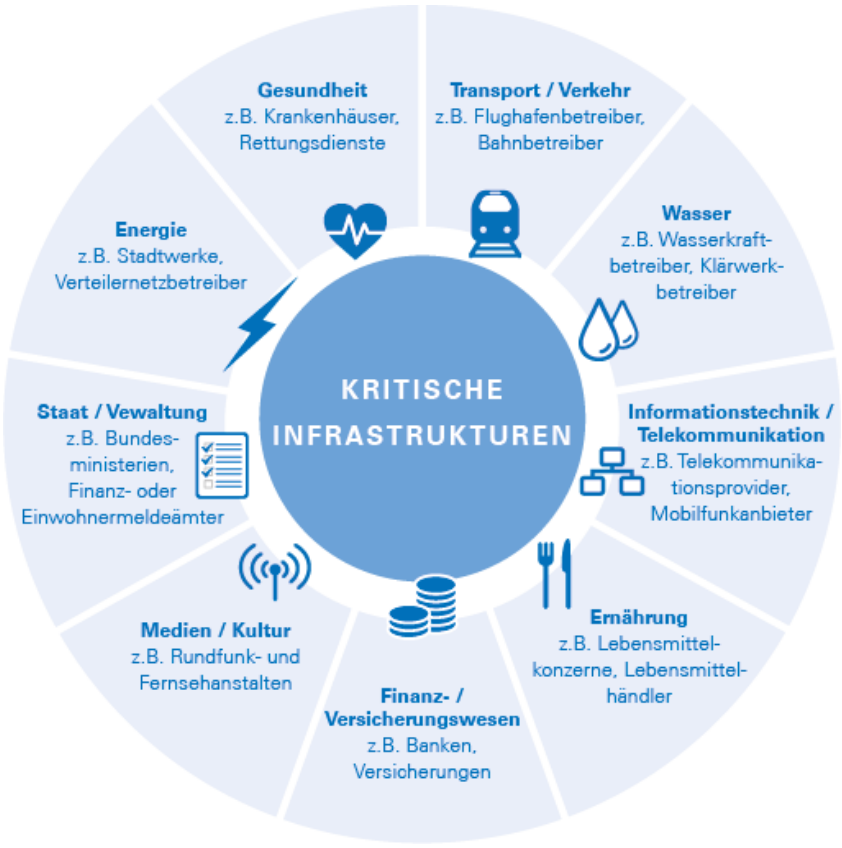


Abbildung 4: Kritische Infrastruktur (KRITIS) Vgl. *Rheinland*, Informationssicherheit ISO 27001, (Stand 13.09.2018 https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html)

[65] vgl. IT-Risiken minimieren mit einem ISO 27001 Zertifikat (Stand 13.09.2018 https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html).

Die Bedeutung der ISO 27001 wird hier besonders für KRITIS - Betreiber (Kritischer Infrastrukturen wie Staat/Verwaltung, Energie, Gesundheit, Transport/Verkehr, Wasser, IT/TELKO, Ernährung, Finanz-/Versicherungswesen, Medien/Kultur) hervorgehoben. Im Kontext dieser Arbeit ist es wichtig hervorzuheben, dass viele dieser KRITIS Betreiber „Sensible Daten“ im Sinne des DSG bzw. der DSGVO verarbeiten. [66]

Ein üblicher Zertifizierungsablauf für die ISO 27001 wird hier ebenfalls beschrieben:

Abbildung 5: Zertifizierungsablauf ISO 27001Vgl. *Rheinland*, Informationssicherheit ISO 27001(Stand 13.09.2018 https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html),

[66]vgl. IT-Risiken minimieren mit einem ISO 27001 Zertifikat (Stand 13.09.2018 https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html).

Wie in der DSGVO (Verzeichnis von Verarbeitungstätigkeiten) gefordert wird zunächst eine Bestandsaufnahme durchgeführt.

Dann werden die Unterlagen bewertet und dokumentiert und die praktische Anwendung des Managementsystems und seine Wirksamkeit überprüft (damit wird die Sicherheit der Verarbeitung im Sinne der DSGVO geprüft).
Damit werden aber auch Prozessrisiken ermittelt, welche in Verbindung mit der Datenschutz-Folgeabschätzung zum Risikomanagement herangezogen werden können.

Jährlich wird in Folge die Prozessoptimierung und Normkonformität geprüft.

Im Hauptteil meiner Arbeit werde ich an Hand einer beispielhaften Risikoanalyse gemäß ISO 31.000 bzw. ONR 49.001 die Grenzen und Möglichkeiten eines integrierten Managementsystems auf Basis der ISO 9001:2015 und der ISO 27001 als ein Risikominimierungsinstrument im Kontext DSGVO und VbVG näher beleuchten.

3.3.4 ONR 49.001:2014 Risikomanagement für Organisationen und Systeme

(Umsetzung der ISO 31.000 in Österreich)

In der ÖNORM ONR 49.001 werden die Normativen Erfordernisse eine Risikomanagementsystemes beschrieben. [67]

Die ONR 49.001 verpflichtet die Oberste Leitung zum Nachweis der Einführung und Verwirklichung und laufenden Verbesserung des Risikomanagement-Systems indem sie die Bedeutung und den Nutzen des Risikomanagements der Organisation vermittelt, die Risikomanagement-Politik, einschließlich ihrer Ziele und Strategien festlegt, das Risikomanagement an den Zielen der Organisation ausrichtet, die gesetzlichen und regulatorischen Anforderungen berücksichtigt, die Risikokommunikation plant, lenkt und leitet sowie eine offene Fehler- und Risikokultur, die Risikoakzeptanz in Einklang mit

[67] *ONR,* ONR 49001:2014 Risikomanagement für Organisationen und Systeme (Stand 1.1.2014).

anerkannten Anforderungen der interessierten Kreise bringt, die Verfügbarkeit von fachlichen, personellen und finanziellen Ressourcen sicherstellt, das Risikomanagement System in das bestehende Führungssystem integriert oder als eigenständiges System gestaltet, die Leistungsindikatoren (Früherkennung, Frühwarnung, Risikoprofile, umgesetzte Maßnahmen, quantifizierte Risikodaten, umgesetzte Systemelemente u.dgl.) für das Risikomanagementsystem festlegt und die Managementbewertung des Risikomanagementsystems in geplanten Abständen durchführt, um dessen andauernde Eignung, Angemessenheit und Wirksamkeit sicherzustellen. [68]

Bild 2 — Risikomanagement-System mit dem Risikomanagement-Prozess

Abbildung 6: Risikomanagement System mit dem Risikomanagementprozess

ONR, ONR 49001:2014 Risikomanagement für Organisationen und Systeme (Stand 1.1.2014) 6

Damit werden wie in Abbildung 6 beschrieben Risiken bearbeitet: Schutzziele der Organisation geplant, Rahmenbedingungen erfasst, Risiken identifiziert, Risiken analysiert, bewertet und die ggf. notwendige Risikobewältigung definiert.

[68] *ONR,* ONR 49001:2014 Risikomanagement für Organisationen und Systeme (Stand 1.1.2014) 7.

Die Erwägungen zur DSGVP Z 83 adressieren analog an den Verantwortlichen die Verpflichtung zur Risikoermittlung und Ergreifung von Maßnahmen zur Risikoeindämmung. Die Erwägungen zur DSGVO Z 84 zielen analog darauf ab Verantwortliche zur Durchführung einer Datenschutz-Folgenabschätzung zu verpflichten, in welcher insbesondere Verarbeitungsvorgänge zu identifizieren sind, welche ein hohes Risiko für die Freiheiten und Rechte natürlicher Personen mit sich bringen. [69]

Darüber hinaus hat die Oberste Leitung einen Beauftragten zu benennen, welcher umfassende Aufgaben, Verantwortungen mit entsprechenden Befugnissen auszuführen hat: Verantwortung für das Risikomanagementsystem, Benennung von Risikoeignern auf der Grundlage ihrer Verantwortung in der Organisation, Benennung von Risikomanagern auf der Grundlage ihrer fachlichen Befähigung, risikobasierte Abstimmung von Zielvereinbarungen und von Leistungsanreizen, Sicherstellung der notwendigen Ressourcen, Sicherstellung der Risikokommunikation in der ganzen Organisation, Sicherstellung der operativen Umsetzung der Risikomanagementpolitik, Bewertung des Risikomanagementsystems mit all seinen Elementen, Berichterstattung an die oberste Leitung über die Leistung und Wirksamkeit des Risikomanagements und über die Notwendigkeit von Verbesserungen. [70]

.

[69] DSGVO VO (EU) 2016/679 25.05.2018 idgF 16.

[70] *ONR*, ONR 49000:2014 idgF. 8.

3.4 Datenschutzgrundverordnung (DSGVO) [71]

Die Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG wird in den folgenden Kapiteln

3.4.1 173 Erwägungsgründe

173 Erwägungsgründe erläutern am Beginn des Amtsblattes der EU die der Verordnung zu Grunde liegenden Überlegungen (DSGVO).
Die Vielfalt der zu Grunde liegenden Überlegungen beleuchten die Komplexität der Entstehungsgeschichte einer europaweit einheitlichen Datenschutzregelung.[72]

3.4.2 Der Schutz natürlicher Personen

bei der Verarbeitung personenbezogener Daten ist ein EU Grundrecht.
In der Begründung zur Verordnung (EU) 2016/679 DSGVO wird gleich in (1) ausgeführt: Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) sowie Artikel 16 Absatz 1 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.[73]

3.4.3 Gegenstand und Ziele der DSGVO

Dementsprechend wird in Kapitel 1 Art. 1 DSVGO der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten zum klaren Gegenstand und Ziel erklärt.

---

[71] DSGVO VO (EU) 2016/679 25.05.2018 idgF 16.

[72] DSGVO VO (EU) 2016/679 25.05.2018 idgF 1-31.

[73] DSGVO VO (EU) 2016/679 25.05.2018 idgF 32.

3.4.4 Sachlicher Anwendungsbereich der DSVGO

Die Gültigkeit der Verordnung wird in Kapitel 1 Art. 2 Z1 DSVGO auf die ganze oder teilweise automatisierte Verarbeitung personenbezogener Daten, sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen eingeschränkt.[74]

3.4.5 Begriffsbestimmungen DSVGO

In Kapitel 1 Art. 4 DSGVO erfolgt die Begriffsbestimmung für die diversen in der Verordnung enthaltenen spezifischen Begrifflichkeiten: Personenbezogene Daten, Verarbeitung, Einschränkung der Verarbeitung, Profiling, Pseudonymisierung, Dateisystem, Verantwortlicher, Auftragsverarbeiter, Empfänger, Dritter, Einwilligung, Verletzung des Schutzes personenbezogener Daten, genetische Daten, biometrische Daten, Gesundheitsdaten, und anderen xxx.[75]

Die Definition für *personenbezogene Daten* ist zentral für diese Arbeit: Die DSVGO definiert hier in Kapitel 1 Art. 4 Z1:

"Der Ausdruck „personenbezogenen Daten" bezeichnet alle Informationen, die sich auf eine identifizierte oder identifizierbare Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einen 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."[76]

Die darauf folgenden Grundsätze der Verarbeitung personenbezogener Daten in Kapitel 2 Art. 5 DSVGO beleuchten schon recht eindrücklich die Intentionen der DSVGO. Wichtige neue

---

[74] DSGVO VO (EU) 2016/679 25.05.2018 idgF 32.

[75] DSGVO VO (EU) 2016/679 25.05.2018 idgF 33f.

[76] DSGVO VO (EU) 2016/679 25.05.2018 idgF 33.

Verpflichtungen für Datenverarbeiter werden hier festgehalten:

Rechtmäßigkeit, Verarbeitung nach Treu und Glaube, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit und Rechenschaftspflicht.[77]

3.4.6 Personenrechte aus der DSGVO

Die technischen, organisatorischen und personellen Herausforderungen an datenverarbeitenden Verbände ergeben sich u.a. aus den daraus resultierenden Personenrechten gemäß Kapitel 3 Art. 12-23 DSVGO:

Art.12: Transparente Information, Kommunikation und Modalität für die Ausübung der Rechte der betroffenen Person
Art.13: Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten
Art. 14: Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
Art.15: Auskunftsrecht der betroffenen Person
Art. 16: Recht auf Berichtigung
Art. 17: Recht auf Löschung („Recht auf Vergessen werden“)
Art. 18: Recht auf Einschränkung der Verarbeitung
Art. 19: Mitteilungspflicht in Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
Art. 20: Recht auf Datenübertragbarkeit
Art. 21: Widerspruchsrecht
Art. 22: Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
Art. 23: Beschränkungen [78]

Gerade den gegenständlichen Personenrechten muss mit der zuverlässigen Löschung von Daten(trägern) auch in Papierform Rechnung getragen werden. Die anderen angeführten

[77] DSGVO VO (EU) 2016/679 25.05.2018 idgF 35f.

[78] DSGVO VO (EU) 2016/679 25.05.2018 idgF 39-47.

Personenrechte erfordern nachvollziehbare, dokumentierte Datenverarbeitungs bzw. Datenvernichtungsprozesse.

Andererseits gibt es Beschränkungen durch nationale Gesetzgebungen.

3.4.7 Beschränkungen der Personenrechte durch nationale Gesetzgebungsmaßnahmen

Im Kapitel III Abschnitt 5 Artikel 23 DSGVO räumt die Union den Mitgliedsstaaten das Recht zu Beschränkungen der Pflichten und Rechte von Personen der Artikel 12-22 und Artikel 34 sowie Artikel 5 im Wege von Gesetzgebungsmaßnahmen ein, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt, die folgendes sicherstellt:
Die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedsstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit; den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren; die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständigen Regeln reglementierter Berufe; Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind; den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen; die Durchsetzung zivilrechtlicher Ansprüche.
Jede Gesetzgebungsmaßnahme im Sinne des Absatzes 1 muss insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf die Zwecke der Verarbeitung oder die Verarbeitungskategorien, die Kategorien personenbezogener Daten, den Umfang der vorgenommenen Beschränkungen, die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung, die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen, die jeweiligen Speicherfristen sowie die geltenden

Garantien unter Berücksichtigung von Art, Umfang und Zwecken der Verarbeitung oder der Verarbeitungskategorien, die Risiken für die Rechte und Freiheiten der betroffenen Personen und das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich ist. [79]

Damit ist bei der gegenständlichen Arbeit auch Augenmerk auf die Nationale Gesetzgebung in Österreich zu legen.

3.4.8 Pflichten für Verantwortliche und Auftragsverarbeiter

In den Artikeln 30 - 37 definiert die DSGVO neue Verpflichtungen für Verantwortliche und Auftragsverarbeiter:
Art.30 Verzeichnis von Verarbeitungstätigkeiten
Art. 31 Zusammenarbeit mit der Aufsichtsbehörde
Art. 32 Sicherheit der Verarbeitung
Art. 33 Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde
Art. 34 Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person
Art. 35 Datenschutz-Folgeabschätzung
Art. 36 Vorherige Konsultation
Art. 37 Benennung eines Datenschutzbeauftragten[80]

Die generischen Verpflichtungen von Verantwortlichen und Auftragsverarbeitung sind sehr umfassend.
Um den Umfang dieser Arbeit nicht zu sprengen beschränke ich mich im Hauptteil auf die methodische Analyse eines spezifischen Teilprozesses nämlich der Löschung, und hier im Besonderen der physischen Vernichtung von personenbezogen Daten auf Datenträgern aus Papier.

---

[79] DSGVO VO (EU) 2016/679 25.05.2018 idgF 46-47.

[80] DSGVO VO (EU) 2016/679 25.05.2018 idgF 50-55.

3.4.9 Geldbußen bei Verstößen gegen die DSGVO/DSG

Im Leitfaden der Österreichischen Datenschutzbehörde vom Juli 2017 [81] werden Geldbußen auf Basis des neuen DSG wie folgt erläutert:

"Geldbußen können auch direkt gegen juristische Personen verhängt werden und nicht nur gegenüber dem verantwortlichen Beauftragten (§ 9 des Verwaltungsstrafgesetzes 1991 – VStG); gegen Behörden und öffentliche Stellen können keine Geldbußen verhängt werden.

- *Die Datenschutzbehörde entscheidet über alle Beschwerden verbindlich (d.h. auch über solche, bei denen nach derzeitiger Rechtslage der Zivilrechtsweg zu beschreiten ist; vgl. dazu § 32 DSG 2000).*
- *Gegen verbindliche Entscheidungen der Datenschutzbehörde steht der Rechtszug an das Bundesverwaltungsgericht uneingeschränkt offen.*
- *Betroffene können sich von Einrichtungen, Organisationen oder Vereinigungen ohne Gewinnerzielungsabsicht, die im Bereich des Datenschutzes tätig sind, vor der Datenschutzbehörde und vor dem Bundesverwaltungsgericht vertreten lassen; diese Einrichtungen, Organisationen oder Vereinigungen können für Betroffene auch das Recht auf Schadenersatz gerichtlich geltend machen; ein Einschreiten der Einrichtungen, Organisationen oder Vereinigungen ohne Mandat (d.h. ohne Bevollmächtigung) ist nicht vorgesehen.*
- *Es werden – neben den Geldbußen nach der DSGVO – auch Verwaltungsübertretungen normiert, die von der Datenschutzbehörde mit Geldstrafe bis zu 50 000 Euro zu ahnden sind."* [82]

Die Art. 30 DSGVO [83] fordert vom Verantwortlichen ein Verzeichnis der Verarbeitungstätigkeiten, Art. 31 DSGVO [84] die Zusammenarbeit mit Behörden, Art. 32

---

[81] *Schmidl*, Leitfaden VO (EU) 2016/679 DSGVO, (2017)

[82] *Schmidl*, Leitfaden VO (EU) 2016/679 DSGVO, (2017) 21.

[83] DSGVO VO (EU) 2016/679 25.05.2018 idgF 50.

[84] DSGVO VO (EU) 2016/679 25.05.2018 idgF 51.

DSGVO[85] die Sicherheit der Verarbeitung, d.h. geeignete Maßnahmen und ein angemessenes Schutzniveau, die Festlegung genehmigter Verhaltensregeln gemäß Art.40 DSGVO.oder auf Grund eines genehmigten Zertifizierungsverfahrens gemäß Art. 42 DSGVO. Darüber hinaus werden im Art. 33 DSGVO Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde gefordert, sowie im Art.34 DSGVO die Benachrichtigungen der von so einer Verletzung des Schutzes personenbezogener Daten betroffenen Personen und es wird eine Datenschutz-Folgeabschätzung im Art.35 DSGVO gefordert um die Risiken zu bestimmen. Bei Datenverarbeitungsvorgängen mit hohem Risiko fordert Die Datenschutzbehörde eine vorherige Konsultation gemäß Art- 36 DSGVO. Darüber hinaus ist die Benennung eines Datenschutzbeauftragten in bestimmten Geschäftsbereichen gemäß Art. 37 DSGVO gefordert. [86]

Können diese Verpflichtungen und die Entwicklung von Maßnahmen mittels normierter Verfahren geprüft und bewertet werden? im Hauptteil dieser Arbeit werde ich die diesbezüglichen methodischen Ansätze verwenden und bewerten.

Bevor ich mich in meiner Einleitung mit dem diesbezüglichen Österreichischen Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) in der ab 25.5.2018 gültigen Fassung beschäftige werde ich zunächst noch kurz die Europäische Datenschutzrichtlinie für Polizei und Justiz im Kontext meiner Arbeit kommentieren:

3.5 Datenschutzrichtlinie für Polizei und Justiz (DSRL-PL)

Hier handelt es sich um eine Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Strafdaten oder der Strafvollstreckung sowie

[85] DSGVO VO (EU) 2016/679 25.05.2018 idgF 51f.

[86] vgl. *Schmidl*, Leitfaden VO (EU) 2016/679 DSGVO, (2017) 26-31.

zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI. [87]

Die Richtlinie nimmt in Artikel 1 (1) besonderen Bezug auf den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zweck der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit. [88]

Am Ende steht auch hier zwangsläufig auch die Vernichtung nicht mehr benötigter personenbezogener Daten. Im Zusammenhang mit meiner gegenständlichen Arbeit, werde ich die Vernichtung von personenbezogenen Daten auf Datenträgen aus Papier in der öffentlichen Verwaltung ebenfalls kurz beleuchten, um den Stand der Technik auch aus dieser Perspektive zu validieren.

3.6 Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG)

Das DSG in der ab 25.5.2018 gültigen Fassung[89]. Das DSG wurde in Österreich unter der der neuen Bundesregierung 2018 entschärft, wobei letztendlich die DSGVO den Rahmen bestimmt und bestimmen wird:

3.6.1 Besondere Strafbestimmungen im ab 25.5.2018 geltenden DSG

Im 4. Hauptstück werden besondere Strafbedingungen im Rahmen von zwei Paragraphen formuliert:

---

[87] vgl. Datenschutz RL (EU) 2016/680 ABl L 119/89 (2016) 1.

[88] vgl. Datenschutz RL (EU) 2016/680 ABl L 119/89 (2016) 1.

[89] BGBl. I Nr. 120/2017 vom 31.7.2017

3.6.1.1 Verwaltungsstrafbestimmungen gemäß §62 DSG

Sofern nicht ein Tatbestand nach Art. 83 DSGVO verwirklicht, oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, ist eine Geldstrafe in der Höhe von bis zu 50.000 € zu verhängen bei widerrechtlichem Zugang zu einer Datenverarbeitung, vorsätzlicher Verletzung des Datengeheimnisses, Datenbeschaffung durch Täuschung, illegaler Bildverarbeitung und der Verweigerung der Einschau, immer in Bezugnahme auf die verschiedenen Artikel der DSGVO.
Hier wird auch die diesbezügliche Entscheidungszuständigkeit der Datenschutzbehörde zugewiesen. [90]

3.6.1.2 Datenverarbeitung in Gewinn- oder Schädigungsabsicht gemäß §63 DSG

Besonders schwer wird hier der Geheimnisbruch von berufsmäßig Tätigen bestraft:

Freiheitsstrafen bis zu einem Jahr oder Geldstrafen bis zu 720 Tagsätzen bedrohen den vorsätzlichen Täter mit Schädigungs- oder Bereicherungsabsichten, falls ihm diese Taten auf Grund seiner berufsmäßigen Beschäftigung anvertraut (Europäisches Parlament und der Rat der europäischen Union, 2016) oder zugänglich gemacht wurden oder die er sich widerrechtlich verschafft hat, selbst benützt, oder einem Anderen zugänglich macht oder veröffentlicht. [91]

[90] DSG 2000 BGBl. 165/1999 idF BGBl. 24/2018 30f.

[91] DSG 2000 BGBl. 165/1999 idF BGBl. 24/2018 31.

3.7 Personenbezogene Daten

Der Begriff „Daten“ findet sich erstmalig mit dem Inkrafttreten am 1.1.2005 im österreichischen Strafgesetzbuch im §126 a (1) StGB „Datenbeschädigung“ verankert. Hier wird von automationsunterstützt verarbeiteten, übermittelten oder überlassenen Daten gesprochen, über die er nicht alleine verfügen darf, bzw. die er nicht verschwinden lassen darf. [92]

Die DSGVO konzentriert sich nun in ihrem Fokus auf „Personenbezogene Daten“ um die Grundrechte ihrer Bürger_innen („natürlicher Personen“) zu schützen.

3.8 Liegen personenbezogenen Daten vor?

Christian Bergauer liefert uns in einem Buchbeitrag einen Praxistipp zur Prüfung ob Personenbezogene Daten vorliegen. Er wendet hier ein Prüfschema mit folgenden Fragestellungen:

Liegt eine **Verarbeitungskomponente** vor? Werden Daten vollautomatisiert bzw. nichtautomatisiert in einem Dateisystem gespeichert, oder ist es beabsichtigt, sie in einem Dateisystem zu speichern?
Wenn nein, dann ist der sachliche Anwendungsbereich der DSGVO nicht eröffnet. Die Prüfung ist hier bereits beendet. [93]

Ist eine **Inhaltskomponente** gegeben? Liegen Daten vor die sich auf einen (lebenden) Menschen beziehen oder mit ihm in Verbindung gebracht werden können?
Wenn, nein, dann liegen anonyme bzw. anonymisierte Daten vor, die nicht oder nicht mehr der DSGVO unterliegen. [94]

---

[92] StGB BGBl. 60/1974 idF BGBl 136/2004, 01.01.2005

[93] vgl. *Bergauer,* Datenschutzgrundverordnung (2016) 43-45 .

[94] vgl. *Bergauer*, Datenschutzgrundverordnung (2016) 47-51.

Sind **Identitätskomponenten** gegeben? Ist der Mensch, auf den sich diese Daten beziehen (lassen) identifiziert oder ist es nach allgemeinem Ermessen unter Einbeziehung aller Mittel aus Sicht des Verantwortlichen sowie einer anderen Person wahrscheinlich, dass dieser identifiziert werden kann? Wenn nein, dann liegen anonyme bzw. anonymisierte Daten vor, die nicht bzw. nicht mehr der DSGVO unterliegen. Wenn ja handelt es sich um personenbezogene Daten iSd Art 4 Z 1. DSGVO. [95]

Dieses einfache Prüfschema gibt schnellen Aufschluss ob die DSGVO anwendbar ist.

3.9 Besondere Kategorien personenbezogener Daten

Wie bereits im aktuell gültigen Datenschutzgesetz kann auch in der in der Neufassung am bisherigen Begriff der „sensiblen Daten“ festgehalten werden:

Zu den sensiblen Daten gehören demnach die folgenden Informationen einer natürlichen Person: *rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, die zur Identifizierung einer natürlichen Person verarbeitet werden, Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung*.[96]

Im Zusammenhang mit dem Stand der Technik der Vernichtung wird es hier ebenfalls notwendig sein diese besonders sensible Datenkategorie besonders zu betrachten.

3.10 Dateisystem

Die Definition eines Dateisystems ist in der DSGVO prinzipiell sehr weit gefasst: "...jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird" iSd Kapitel 1 Art 4 Z 6. DSGVO [97]

---

[95] vgl. DSGVO, VO (EU) 2016/679 33.

[96] vgl. DSGVO, VO (EU) 2016/679 10.

[97] vgl. DSGVO, VO (EU) 2016/679 (2016) 5.

Ein Ausdruck eines solchen Dateisystems auf Papier, welcher vernichtet werden soll, ist Gegenstand meiner Arbeit im Hauptteil.

3.11 Pseudonymisierung

Elisabeth Hödl befasst sich mit dem Thema Pseudonymisierung mit besonderem Fokus auf Big Data. Für sie ist Pseudonymisierung das Verändern personenbezogener Daten durch eine Zuordnungsvorschrift, sodass Einzelangaben oder sachliche Verhältnisse ohne Kenntnis oder Nutzung der Zuordnungsvorschrift nicht mehr einer natürlichen Person zugeordnet werden können. D.h. personenbezogene Daten und Identitätsmerkmal werden getrennt, allerdings besteht immer noch die Möglichkeit der Zuordnung von Daten zu einer Person.
Sie führt hier ein Beispiel aus der medizinischen Forschung an, wo Patientenlistendatenbanken und Forschungsdatenbanken getrennt voneinander geführt werden. Das technische Kernstück der Pseudonymisierung sind zwei getrennte Datenbanken, wobei sich die Daten eines Patienten über einen gemeinsamen Patientenidentifikator (ID) identifizieren. [98]

Das Thema der Pseudonymisierung könnte ggf. auch bei Maßnahmen zur Sicherung von im Vernichtungsprozess befindlichen Behältern mit zu vernichtenden Datenträgen aus Papier zur Anwendung kommen.

Eine bestimmte sichtbare Behälternummer auf einem Sammelbehälter sollte ja für Unbefugte keinen direkten Rückschluss auf die Herkunft der darin befindlichen Datenträger liefern.

Ist ein Behälter von außen einfach bezüglich seiner Herkunft zu identifizieren erhöht dies unter Umständen das Risiko einer unbefugten Aktivität durch Dritte.

[98] *Hödl*, Datenschutzgrundverordnung (2017) Definition und Anwendung der Pseudonymisierung 65ff.

4 Hauptteil

4.1 Beispiel "Datenvernichtung von Ausdrucken mit personenbezogenen Daten"

Um die Komplexität der Definition des Standes der Technik zu beschreiben wähle ich einen Grenzbereich der DSGVO, welcher auf einfachem technischen Niveau zu beschreiben ist:

4.1.1 Sachverhalt

Im Folgenden möchte ich einen wenig beachteten Bereich beleuchten, welcher meiner Auffassung nach Bestandteil der Datenschutzgrundverordnung ist, nämlich *Die Vernichtung von bedrucktem Papier mit personenbezogenen Daten*.

Das spielt insbesondere im DSGVO Art. 17: Recht auf Löschung („Recht auf Vergessen werden“) eine wichtige Rolle aber auch auf die Aspekte Rechtmäßigkeit, Verarbeitung nach Treu und Glaube, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit und Rechenschaftspflicht, eine geeignete Datenvernichtung umfasst auch die Vernichtung von Ausdrucken von personenbezogenen Daten aus umfassten Datenbanken.

An Hand eines fiktiven Sachverhaltes werde ich die Forschungsfragen näher beleuchten:

Ein Unternehmen ist ISO 27001, ONR 192050 und ISO 9001:2015 zertifiziert und möchte die ordnungsgemäße Vernichtung von bedrucktem Papier mit personenbezogenen Daten durch und bei einem externen Dienstleister sicherstellen.

im Folgenden werde ich an Hand dieses Fallbeispiels versuchen die Forschungsfrage(n) zu beantworten:

Wie weit kann das diesbezügliche Sanktionsrisiko für Unternehmen, durch die Nutzung methodischer Herangehensweisen normierter Managementsysteme (ISO 31000, ISO 9001, ISO 27001,...) reduziert werden?
Ergeben sich Vorteile aus der Anwendung dieser Managementsysteme?
Wie kann der Stand der Technik basierend auf Normen ermittelt werden?
Wie kann ich methodisch Sanktionsrisiken prüfen und darauf basierend Maßnahmen zur Risikobewältigung ableiten?

4.1.2 Sicherheitsstufen der Aktenvernichtung

Bei der Verwendung von Aktenvernichtern stellen sich Fragen nach der Vernichtungsklasse des beschafften Gerätes:

Abbildung 7: Beispiele für unterschiedliche Zerkleinerungsformen von Papier Papershred, Gesetze und Normen für die Vernichtung von Daten und Akten (2018)

Dabei ist der Zustand, die Form und die Größe des Aktenvernichtungsendproduktes bestimmend für die Sicherheitsstufe:

- maximale Fläche der Materialteilchen
- maximale Breite des Materialstreifens

Darüber hinaus ist eine bestimmte Toleranz für 10% des Materials zulässig

- maximale Fläche von 10% des verbleibenden Materials

Die Deutsch Firma Documenta garantiert zum Beispiel nach mindestens Schutzklasse 3 und Sicherheitsstufe 4 [99]

Hier muss man die notwendige Sicherheitsstufe definieren, d.h. mit welchem Aufwand soll die Reproduktion von Daten möglich sein:

- Sicherheitsstufe 1: Allgemeine Daten
- Sicherheitsstufe 2: Interne Daten

[99] *PÜG*, Reisswolf DIN 66399 Zertifikat (2016) 1

- Sicherheitsstufe 3: Sensible Daten
- Sicherheitsstufe 4: Besonders sensible Daten
- Sicherheitsstufe 5: Geheim zu haltende Daten
- Sicherheitsstufe 6: Geheime Hochsicherheitsdaten
- Sicherheitsstufe 7: Top Secret Hochsicherheitsdaten [100]

In Abbildung 7 findet sich eine Übersicht über die Sicherheitsstufen der Aktenvernichtung.

documentus®

Tabelle 1 – Informationsdarstellung in Originalgröße

Informationsdarstellung in Originalgröße
z. B. Papier / Film / Druckformen

Sicherheitsstufe	Zustand, Form und Größe nach der Vernichtung	Toleranz für 10 % des Materials
P-1	Fläche der Materialteilchen max. 2000 mm² oder Breite des Streifens max. 12,0 mm Streifenlänge unbegrenzt	Fläche der Materialteilchen max. 3800 mm²
P-2	Fläche der Materialteilchen max. 800 mm² oder Breite des Streifens max. 6,0 mm Streifenlänge unbegrenzt	Fläche der Materialteilchen max. 2000 mm²
P-3	Fläche der Materialteilchen max. 320 mm² oder Breite des Streifens max. 2 mm Streifenlänge unbegrenzt	Fläche der Materialteilchen max. 800 mm²
P-4	Fläche der Materialteilchen max. 160 mm² und für gleichförmige Partikel: Breite des Streifens max. 6 mm	Fläche der Materialteilchen max. 480 mm²
P-5	Fläche der Materialteilchen max. 30 mm² und für gleichförmige Partikel: Breite des Streifens max. 2 mm	Fläche der Materialteilchen max. 90 mm²
P-6	Fläche der Materialteilchen max. 10 mm² und für gleichförmige Partikel: Breite des Streifens max. 1 mm	Fläche der Materialteilchen max. 30 mm²
P-7	Fläche der Materialteilchen max. 5 mm² und für gleichförmige Partikel: Breite des Streifens max. 1 mm	Keine Toleranz zugelassen

Mit freundlicher Genehmigung des Deutschen Instituts für Normung e.V., Oktober 2012

Abbildung 8; Sicherheitsstufen lt. DIN 63399 documentus, Sicherheitsstufen (Stand 16.09.2018, https://din66399.de/tabelle-a-01.html)

[100] *documentus*, Sicherheitsstufen (Stand 16.09.2018, https://din66399.de/tabelle-a-01.html)

4.1.3 Wie kann man den Schutzbedarf / Stand der Technik der Datenträgervernichtung ermitteln?

Der TÜV SÜD beschreibt den richtigen Weg zur Datenvernichtung im Rahmen der DIN 66399 in Form eines einfachen Entscheidungsprozesses:

- Zunächst ist eine Schutzklasse zu definieren, die Schutzklasse 2 ist für personenbezogene Daten heranzuziehen.
- Daraus ergibt sich die mögliche Sicherheitsstufe von 3-5
- Daraus ergeben sich zulässige Verfahren für unterschiedliche Datenträger

Hier wird exemplarisch ausgeführt:
Sicherheitsstufe 3 für Datenträger mit sensiblen und vertraulichen Daten, z.B. Angebote, Bestellungen mit Adressdaten, Sicherheitsstufe 4 für Datenträger mit besonders sensiblen und vertraulichen Daten, z.B. Personaldaten, Arbeitsverträge, Bilanzen, Steuerunterlagen von Personen o.ä., Sicherheitsstufe 5 für Datenträger mit geheim zu haltende Daten, zB. medizinische Berichte, Konstruktionspläne, Strategiepapiere o.ä. [101]

Die Sicherheitsstufen 4 und 5 bzw. P4 und P5 (P steht für Papier), sind hier explizit hier als die geeigneten für *personenbezogene Daten* beschrieben. Sicherheitsstufe P5 erwähnt hier explizit medizinische Berichte, welche in der DSGVO unter *sensible personenbezogene Daten* gemäß 3.9. einzureihen sind. Damit müssen wir auch die Kategorie P6 im Folgenden näher beleuchten.

[101] *TUEVSued*, Schritt für Schritt zur Datenträgervernichtung (Stand: 16.9.2018, https://www.tuev-sued.de/uploads/images/1463469367468222550066/01375-28561-tuev-grafik-din-broschuere.pdf)

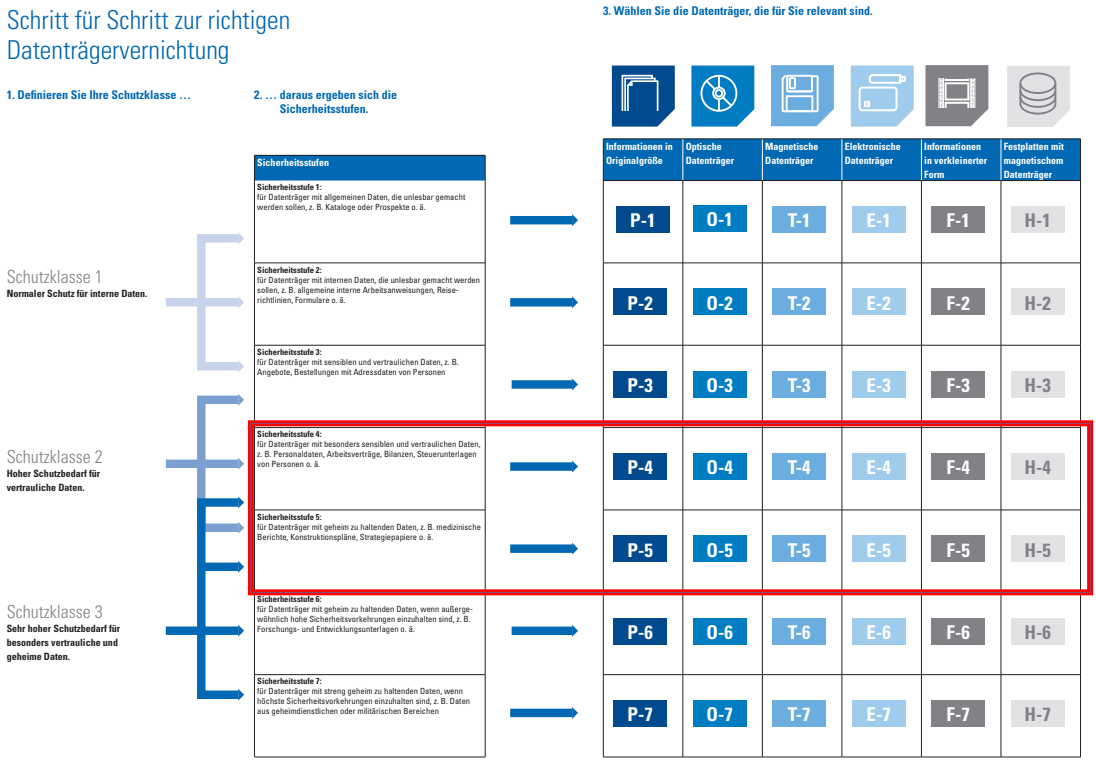


Abbildung 9: Evaluierung der richtigen Datenverarbeitung *TUEVSued*, Schritt für Schritt zur Datenträgervernichtung (Stand: 16.9.2018, https://www.tuev-sued.de/uploads/images/1463469367468222550066/01375-28561-tuev-grafik-din-broschuere.pdf)

Damit schlussfolgere ich, dass personenbezogene Daten gemäß Stand der Technik in der Regel entweder gemäß Sicherheitsstufe 4 oder gemäß Sicherheitsstufe 5 vernichtet werden, im Sinne der Schutzklasse 2.

Gemäß dieser Vorgangsweise könnte es aber in Ausnahmefällen personenbezogener Daten geben, welche unter Umständen gemäß Sicherheitsstufe 6 zu vernichten sind. Sicherheitsstufe 6 ist für Datenträger mit geheim zu haltende Daten anzuwenden, wenn außergewöhnlich hohe Sicherheitsvorkehrungen einzuhalten sind z.B. Forschungs- und Entwicklungsunterlagen o.ä.[102]

[102] *TUEVSued*, Schritt für Schritt zur Datenträgervernichtung (Stand: 16.9.2018, https://www.tuev-sued.de/uploads/images/1463469367468222550066/01375-28561-tuev-grafik-din-broschuere.pdf)

In diese Kategorien könnten unter Umständen gewisse sensible Daten lt. Punkt 3.9.) gehören welche eine der folgenden Informationen einer natürlichen Person enthalten: rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, die zur Identifizierung einer natürlichen Person verarbeitet werden, Gesundheitsdaten und Daten zum Sexualleben oder zur sexuellen Orientierung.

Eine Vernichtung gemäß dieser Sicherheitsstufe ist wirtschaftlich aber nur gerechtfertigt, wenn der Geheimschutz auch in allen anderen Datenverarbeitungsbereichen dieser Daten angewendet wird. Dasselbe gilt für die höchste Sicherheitsstufe 7: Die Sicherheitsstufe 7 ist für Datenträger mit streng geheim zu haltende Daten, wenn höchste Sicherheitsvorkehrungen einzuhalten sind, anzuwenden, z.B. Daten aus geheimdienstlichen oder militärischen Bereichen.

Um die Notwendigkeit der Vernichtung gemäß Sicherheitsstufe 6 oder 7 zu validieren kann in diesem Zusammenhang als Referenz die staatliche Geheimschutzordnung beleuchtet werden:

4.1.4 Informationssicherheitsverordnung

auf Grund der Verordnung der Bundesregierung über die Informationssicherheit (InfoSIV)[103]

§ 3. (1) Klassifizierte Informationen sind zu qualifizieren als

1. *EINGESCHRÄNKT (E), wenn die unbefugte Weitergabe der Informationen den in Art. 20 Abs. 3 B-VG genannten Interessen zuwiderlaufen würde,*
2. *VERTRAULICH (V), wenn die Informationen nach anderen Bundesgesetzen unter strafrechtlichem Geheimhaltungsschutz stehen und ihre Geheimhaltung im öffentlichen Interesse gelegen ist,*
3. *GEHEIM (G), wenn die Informationen vertraulich sind und ihre Preisgabe zudem die Gefahr einer erheblichen Schädigung der in Art. 20 Abs. 3 B-VG genannten Interessen schaffen würde,*

[103] InfoSiV, BGBl II 548/2003 idF 16.9.2018

4. STRENG GEHEIM (SG), wenn die Informationen geheim sind und überdies ihr Bekanntwerden eine sch B-VG genannten Interessen wahrscheinlich machen würde.

(2) Die Klassifizierung, De-Klassifizierung sowie die Herabstufung einer Information erfolgt durch ihren Urheber. Die De-Klassifizierung ist schriftlich festzuhalten. Empfänger einer klassifizierten Information sind von der De-Klassifizierung zu informieren. [104]

Im Info SIV wird die Handhabung solcher Informationen umfassend geregelt, eine entsprechende Klassifizierung ist mit umfassenden Maßnahmen verbunden, welche nur in ihrer Ganzheit einen wirkungsvollen Schutz von Informationen gewährleistet: Insbesondere werden hier Zugang, Unterweisung, Übermittlung, Kennzeichnung, Elektronische Verarbeitung und Übermittlung klassifizierter Informationen, Dienstpflichten, Administrative Behandlung, Registrierung und Verwahrung von klassifizierten Informationen, Kopien und Übersetzungen und Vernichtung sowie die Kontrolle geregelt:[105]

In §15(1) InfoSIV wird hier verordnet:

"(...)Werden Informationen nicht mehr benötigt, sind sie mittels geeigneter Verfahren unter Beachtung internationaler und nationaler Vorgaben zu vernichten(...)"
„(...)Die Vernichtung von Informationen der Klassifizierungsstufe GEHEIM oder höher (STRENG GEHEIM) hat unter Anweisung von Zeugen zu erfolgen, der über eine Sicherheitsüberprüfung oder Verläßlichkeitsprüfung der entsprechenden Klassifizierungsstufe verfügen muss, und ist im Protokoll durch Unterschrift festzuhalten"(Muster: Anlage 5)." [106]

[104] §3 InfoSiV, BGBl II 548/2003 idF 16.9.2018

[105] vgl. InfoSiV, BGBl II 548/2003 idF 16.9.2018

[106] §15 InfoSiV, BGBl II 548/2003 idF 16.9.2018

Anlage 5

Vernichtungsprotokoll

Folgendes klassifiziertes Dokument wurde vernichtet:

Dokumentenname	
Geschäftszahl (Fremdzahl)	
Ausfertigungsnummer	
Datum	
Seitenumfang	
Klassifizierungsstufe	
Urheber	
Eingang	

Art der Vernichtung:

Name des Zeugen in Druckschrift:

Organisationseinheit:

(Datum) (Unterschrift)

Abbildung 10: Vernichtungsprotokoll gemäß InfoSIV InfoSiV, BGBl II 548/2003 idF 16.9.2018 Anlage 5

Die Vernichtung hat nach den von der Informationssicherheitskommission genehmigten Verfahren zu erfolgen. Damit ist bei der Vernichtung sensibler Daten als Auftragsverarbeiter das genehmigte Verfahren der Datensicherheitskommission anzuwenden, dies sollte im Rahmen einer entsprechenden Vereinbarung eindeutig geregelt werden.[107]

Da der Gesetzgeber in der Klassifizierung VERTRAULICH (§3 (1) 2 InfoSIV) von strafrechtlichen Geheimhaltungsschutz spricht, bestätigt dies meinerseits die Annahme dass die Sicherheitsstufen für Aktenvernichtung 4 und 5 gemäß DIB 66399 ausreichend sein sind.

Alle mit Aufgaben der Bundes-, Landes- und Gemeindeverwaltung betrauten Organe sowie die Organe anderer Körperschaften des öffentlichen Rechts sind laut §9 InfoSIG[108], soweit gesetzlich nicht anderes bestimmt ist, zur Verschwiegenheit über alle ihnen ausschließlich aus ihrer amtlichen Tätigkeit bekannt gewordenen Tatsachen verpflichtet, deren Geheimhaltung

- im Interesse der Aufrechterhaltung der öffentlichen Sicherheit,
- der umfassenden Landesverteidigung,
- der auswärtigen Beziehungen,

[107] §15 Zi 2 InfoSiV, BGBl II 548/2003 idF 16.9.2018

[108] §9 InfoSIG BGBl I 23/2002 idF 16.9.2018

durch personenbezogene Daten eine Klassifizierung als **GEHEIM oder STRENG GEHEIM** erfolgen sollte, **sind diese Daten durch das InfoSIV entsprechend geschützt**. In diesem Fall wäre ein entsprechendes Vernichtungsverfahren zu wählen.[109]

Würden als GEHEIM oder STRENG GEHEIM klassifizierte Daten gemäß InfoSIV durch einen privaten Datenverarbeiter vernichtet müssten Verfahren lt. InfoSIV angewendet werden um dem "Stand der Technik" zu entsprechen.

Die Klassifizierung gemäß DIN 66399 ist hier nicht relevant, da die Vernichtung in diesem Fall durch besondere durch die Informationssicherheitskommission genehmigte Verfahren zu erfolgen hat.

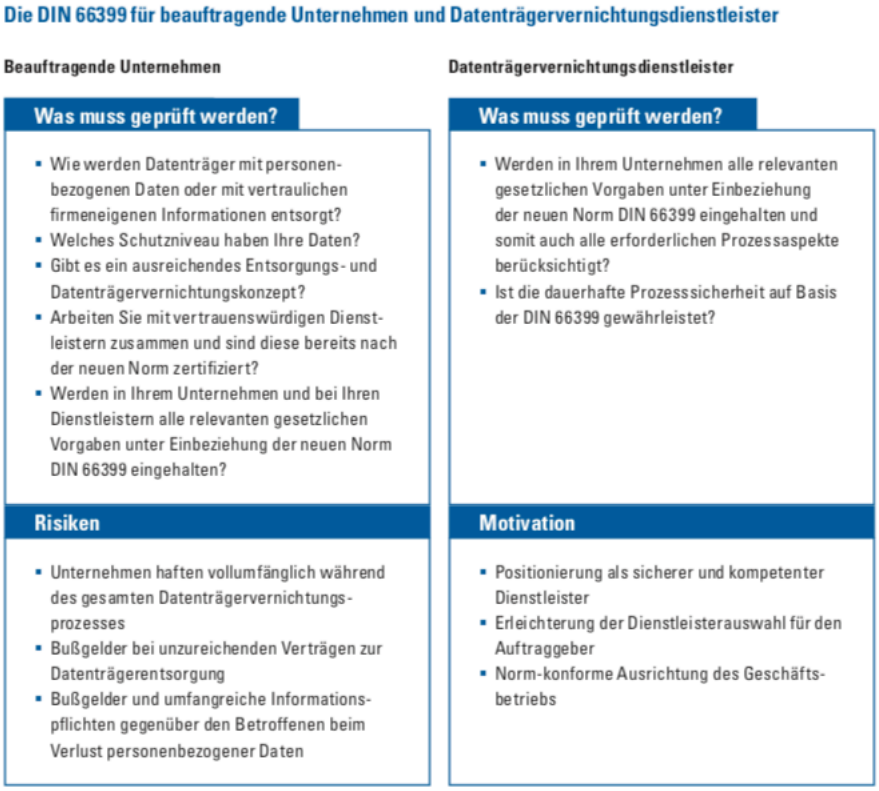
Für die gegenständliche Arbeit gehen ich davon aus dass die zu vernichtenden Daten nicht unter das InfoSIV bzw. InfoSIG fallen.

[109] §15 InfoSIV BGBl I 23/2002 idF 16.9.2018

4.1.5 Wie überprüft man Datenvernichtungsprozesse?

Die DIN 66399 regelt Datenvernichtungsprozesse. In Abbildung 11 beschreibt der TÜV Süd den Prüffokus [110]:

- Wie erfolgt die Entsorgung personenbezogener Daten?
- Welches Schutzniveau haben diese Daten - werden Daten entsprechend klassifiziert?
- Wie ist die Qualität des Entsorgungs- und Vernichtungskonzeptes?
- Wie vertrauenswürdig sind beauftragte Dienstleister?
- Wie ist die Prozesssicherheit gewährleistet?
- Wie werden Haftungen durch Fehler bei Datenträgervernichtungsdienstleister abgesichert?
- Wie werden Fehler im eigenen Haus ausgeschlossen?



[110] TUEVSued, *Zertifizierte Datenträgervernichtung (Stand: 16.9.2018,* https://www.tuev-sued.de/uploads/images/1408537679236711420086/infoblatt-din-66399-datentraegervernichtung.pdf*)*

Abbildung 11: Prüfungsfokus, Risiken und Motivation DIN 66399 TUEVSued, Zertifizierte Datenträgervernichtung (Stand: 16.9.2018, https://www.tuev-sued.de/uploads/images/1408537679236711420086/infoblatt-din-66399-datentraegervernichtung.pdf)

Zahlreiche Datenvernichtungsdienstleister übernehmen mittlerweile Aufgaben der Normkonformen Datenvernichtung:

Das deutsche Unternehmen documentus setzt, wie in Abbildung 12 beschrieben, auf die zentrale Vernichtung von Daten in entsprechenden Vernichtungszentren.[111]

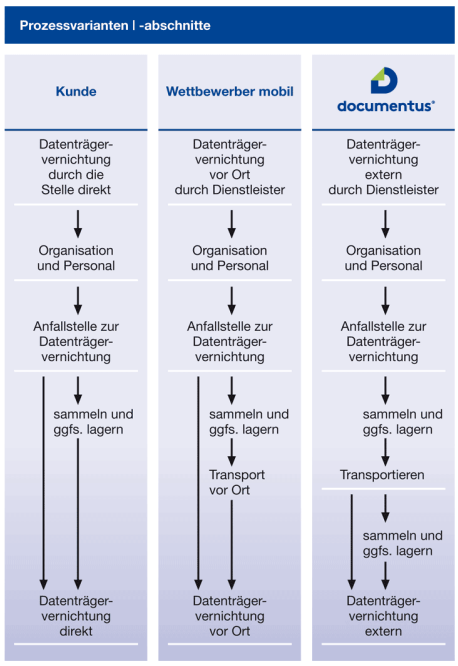


Abbildung 12: Prozessvergleich documentus, NORMteil 66399-3 (Stand: 16.9.2018, https://din66399.de - Auswahl NORMteil 66399-3)

Beleuchtet man nun die einzelnen Schritte dieses Dienstleistungsmodelles ergeben sich zahlreiche Risiken, welche entsprechend zu bewerten sind. Die in Abbildung 12 beleuchteten Aspekte *Organisation und Personal, Anfallstelle zur Datenträgervernichtung, sammeln und ggfs. lagern, Datenträgervernichtung* bergen bei genauerer Betrachtung zahlreiche Risiken.[112]

[111] vgl. documentus, *NORMteil 66399-3 (Stand: 16.9.2018,* https://din66399.de - *Auswahl NORMteil 66399-3*

[112] vgl. documentus, *NORMteil 66399-3 (Stand: 16.9.2018,* https://din66399.de - *Auswahl NORMteil 66399-3*

Für die Leistungserbringung werden seitens documentus versperrbare Behälter benutzt:

Abbildung 13: Sammelbehälter zur Aktenvernichtung documentus, Datenvernichtung (Stand: 16.9.2018, https://documentus.de/datenvernichtung/)

Die Leistungsbeschreibung in Abbildung 14 vermittelt plakativ Sicherheit, die meiner Ansicht nach nicht automatisch gegeben ist. Kurz gesagt – die Abfolge: Vertragsabschluss - Abholung - Vernichtung und darauffolgend ein Vernichtungszertifikat gibt noch nicht automatisch Sicherheit.[113]

Abbildung 14: Erklärung der Leistungen von documentus documentus, Datenvernichtung (Stand: 16.9.2018, https://documentus.de/datenvernichtung/)

[113] *documentus,* Datenvernichtung (Stand: 16.9.2018, https://documentus.de/datenvernichtung/)

Insbesondere möchte ich nun gemäß der von documentus angewendeten die Prozessqualitätszertifizierung nach DIN SPEC 66399-3[114] mit einem alternativen Verfahren auf Verbesserungsmöglichkeiten untersuchen, insbesondere im Kontext der Forschungsfrage bzgl. Sanktionsrisikominimierung im Sinne des VbVG, der DSGVO und des DSG.
Die Ermittlung der Sanktionsrisiken baut auf zu ermittelnden Prozessrisiken auf:

4.1.6 Ermittlung der Prozessrisiken Datenvernichtung

Zunächst muss der Auftrag und die Verpflichtung des Unternehmens gemäß ISO 31000 in Form von **Schutzzielen** (gemäß Definition BMI(DE)) [115] für die Vernichtung personenbezogener Daten für den Prozess der Datenträgervernichtung ermittelt werden.
Dies kann methodisch wie im Folgenden beschrieben erfolgen:

4.1.7 Ermittlung der Schutzziele personenbezogener Daten für den Prozess der Datenträgervernichtung

4.1.7.1 Generelle Schutzziele der DSGVO

Aus der Datenschutzgrundverordnung (Artikel 32 Absatz 1b) lassen sich wie in Abbildung 15 von Stefan Müller visualisiert zunächst **generelle Schutzziele** für Prozesse ableiten:

- **Vertraulichkeit,**
- **Verfügbarkeit,**
- **Integrität**
- **Belastbarkeit der Systeme**

[114] *documentus,* Datenvernichtung (Stand: 16.9.2018, https://documentus.de/datenvernichtung/)

[115] vgl. *BMI (DE),* Basisschutzkonzept 2005 (Stand: 16.9.2018, https://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Basisschutzkonzept_Kritis.pdf?__blob=publicationFile) 20f

Abbildung 15: Generelle Schutzziele und Maßnahmen aus der DSGVO Müller, Schutzziele der DSGVO (Stand: 21.2.2018, https://www.sihk.de/blob/haihk24/servicemarken/ueber_uns/erfa_gruppen/fallback1422607240916/4000890/db3451fc7710362ead9459b22774bab1/ESET-DSGVO-SIHK_Hagen-data.pdf) 11

Die daraus resultierenden **generellen Schutzziele aus der DSGVO** können dem entsprechend auf einzelne Prozessschritte umgelegt werden und daraus Maßnahmen abgeleitet werden.

Im Falle des Schutzes gespeicherter Daten in elektronischer Form bieten sich laut Stefan Müller (siehe Abbildung 15) zum Beispiel folgende Schutzziele an:

- **Gespeicherte Daten in der Organisation schützen** (Daten in Ruhe)
- **Daten bei der Übertragung schützen** (Daten in Bewegung)
- **Die Übermittlung zwischen zwei Speicherorten absichern**
- **Den Zugriff auf bestimmte Daten blockieren**
- **Den sicheren Datenzugriff auf Anfrage / Genehmigung gestatten**
- **Die Zugänge/Logins zu Geräten und Ressourcen abzusichern**
- **Ein angemessenes Schutzniveau zu gewährleisten**[116]

[116]Müller, *Schutzziele der DSGVO (Stand: 21.2.2018,* https://www.sihk.de/blob/haihk24/servicemarken/ueber_uns/erfa_gruppen/fallback1422607240916/4000890/db3451fc7710362ead9459b22774bab1/ESET-DSGVO-SIHK_Hagen-data.pdf) 12

- In Abbildung 16 zeigt er auch mögliche Maßnahmen, welche sich aus den Schutzzielen generisch ableiten lassen: Verschlüsselung, **Remote Management, Regeln/Grundschutz**[117]

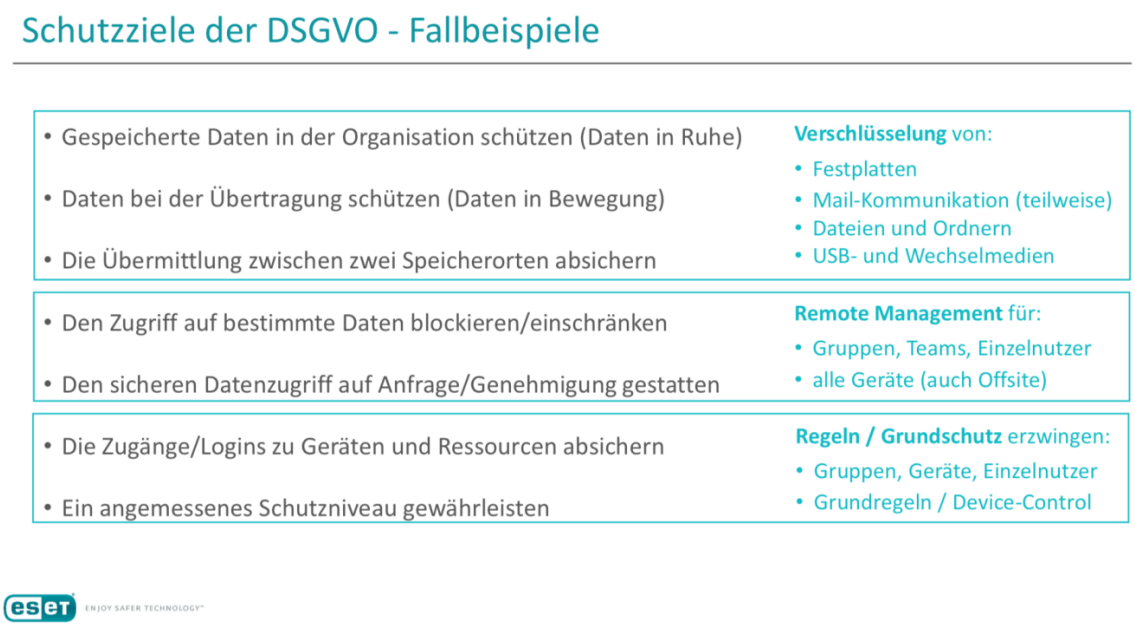


Abbildung 16: Schutzziele der DSGVO - Fallbeispiele Müller, Schutzziele der DSGVO (Stand: 21.2.2018, https://www.sihk.de/blob/haihk24/servicemarken/ueber_uns/erfa_gruppen/fallback1422607240916/4000890/db3451fc7710362ead9459b22774bab1/ESET-DSGVO-SIHK_Hagen-data.pdf*) 12*

Legt man das auf die **Datenvernichtung** um lassen sich für die Datenvernichtung Analogien entwickeln:

4.1.7.2 Besondere Schutzziele bei der Datenvernichtung

Der Verband im Sinne des Verbandsverantwortlichkeitsgesetzes im Folgenden "Organisation", unterscheidet gemäß Punkt 3.1.4 zwischen Entscheidungsträger_innen und Mitarbeiter_innen.

Um die Haftungsfrage im Zusammenhang mit den Schutzzielen bei der Datenvernichtung im Kontext der Datenschutzgrundverordnung zu beleuchten, würde ich die Sicherstellung der

---

[117] Müller, *Schutzziele der DSGVO (Stand: 21.2.2018,* https://www.sihk.de/blob/haihk24/servicemarken/ueber_uns/erfa_gruppen/fallback1422607240916/4000890/db3451fc7710362ead9459b22774bab1/ESET-DSGVO-SIHK_Hagen-data.pdf) 12

folgenden Schutzziele durch geeignete Maßnahmen - am Stand der Technik - **seitens der Entscheidungsträger der Organisation** prüfen:

- **Zu vernichtende Daten der Organisation schützen**
- **Zu vernichtende Daten der Organisation bei der der Aufbewahrung, Sammlung, Transport und Vernichtung schützen**
- **Den Zugriff auf zu vernichtende Daten der Organisation durch Unbefugte innerhalb oder außerhalb der Organisation ausschließen**
- **Den Verlust von Daten während des Prozesses bis zur nachvollziehbaren Vernichtung sicherstellen.**
- **Die nachvollziehbare Vernichtung der Daten in der gewählten Schutzklasse 2 in der Sicherheitsstufe 4-5 gewährleisten**

Damit sind die gesetzlichen Rahmenbedingungen und damit der Auftrag (gemäß 3.3.5) und die Verpflichtung der Organisation in Form von Schutzzielen definiert.

4.1.8 Ermittlung der Prozessrisiken auf Basis der festgelegten Schutzziele

Dafür ist der vom jeweiligen Unternehmen festgelegte Prozess lt. ISO 9001:2015 der Datenvernichtung auf Risiken zu untersuchen:
Dabei ist die **Verarbeitungskomponente** (gemäß 3.8) nicht in Bezug auf ein Datensystem, sondern in Bezug auf ein Vernichtungssystem zu betrachten, die **Inhaltskomponente** (gemäß 3.8) wurde dafür festgelegt, es handelt sich im Fallbeispiel um personenbezogene Daten aus dem die **Identitätskomponente** (gemäß 3.8) einer natürlichen Person hervorgehen könnte.

Exemplarisch stelle ich - mit der **Absicht der Risikoidentifikation** (gemäß 3.3.4) - im Folgenden **Fragen - zum Umfeld**, den **Rahmenbedingungen** (gemäß 3.3.4) zu dem von documentus lt. Abbildung 11 definierten Prozess der Datenvernichtung basierend auf den zuvor definierten Schutzzielen:

4.1.8.1 Datenträgervernichtung extern durch Dienstleister

Die Beauftragung der Datenträgervernichtung durch einen externen Dienstleister bedingt zunächst einmal ein Vertragswerk, welches die Schutzziele gemäß 4.1.7.2 entsprechend berücksichtigt:

Insbesondere ist vertraglich zu regeln:

Welche technischen, organisatorischen und personellen Maßnahmen am Stand der Technik garantiert der Dienstleister zu Erreichung der geforderten Schutzziele?
Wie erfolgt die Überprüfung der Wirksamkeit dieser Maßnahmen?
Wie erkennt der Dienstleister eine Umgehung seiner Maßnahmen?
Welchen Verpflichtungen unterliegt der Dienstleister im Falle eines (vermuteten) Datenverlustes?
An welcher Schnittstelle beginnt und wo endet die Haftung des Dienstleisters?
Welche Prozessdokumentationspflichten gibt es seitens des Dienstleisters?

Damit ist bei nach Normen zertifizierten Prozessen Scope und Systemtiefe allfälliger Zertifizierungen zu prüfen.

4.1.8.2 Organisation und Personal

Organisation und Personal des Auftraggebers und Organisation und Personal des Auftragnehmers aber auch allfällige Dritte sind zu berücksichtigen:

Generelle, organisatorische und personelle Maßnahmen müssen Antworten auf folgende Fragen geben:

Wer hat zu welchem Zeitpunkt Zugriff auf den Behälterinhalt?
Wie wird die Zuverlässigkeit dieser Personen überprüft?
Wie schütze ich diese Behälter vor unbefugten Personen (Drittdienstleister, Besucher, etc.)
Wie sind die Behälter des Dienstleisters verschlossen?
Wie lassen sich diese Schutzvorrichtungen umgehen?
Wie erkennt man die Umgehung dieser Schutzvorrichtungen?
Wer darf kann den Behälter öffnen?
Wie werden Öffnungen des Behälters dokumentiert?
Wird hier ein Internes Kontrollsystem (IKS) angewendet?
Wie werden Mitarbeiter_innen des Auftraggebers und des Dienstleisters unterwiesen und die Einhaltung der Verhaltensrichtlinien überprüft?
Mit welchen Konsequenzen haben Mitarbeiter_innen des Auftraggebers und des Dienstleisters bei Verstößen zu rechnen?
Wie ist das vertraglich / arbeitsrechtlich geregelt?
u.v.a.m.

4.1.8.3 Anfallstelle zur Datenträgervernichtung

Neben den in 4.1.8.1 bis 2 beleuchteten Risiken ist an der Anfallstelle der Datenträgervernichtung einiges in Zusammenhang mit den Schutzzielen zu hinterfragen:

Wie werden zu vernichtende Datenträger am Arbeitsplatz zwischengelagert?
Gibt es eine Clean Desk Policy?
Sind die zu vernichtenden Datenträger versperrt (unter Verschluss)?
Wer bringt die zu vernichtenden Datenträger zur Sammelstelle?
Unterliegen dafür involvierte Personen einer Sicherheitsüberprüfung?
Wie wird die Einlieferung in die Sammelstelle überprüft?

4.1.8.4 Sammeln und ggf. Lagern

Hier stellen sich bezüglich der definierten Schutzzielen vor allem Fragen in Zusammenhang mit den verwendeten Gebinden:

Lassen sich aus dem verschlossenen Behälter wieder Akten entnehmen?
Ist die Einwurfs Öffnung entsprechend gesichert?
Ist der Aufstellort alarmgesichert oder kameraüberwacht ?
Werden die Überwachungsdaten analysiert?
Sind die Behälter besonders gesichert?

4.1.8.5 Transportieren

In Zusammenhang mit dem Transport werfen die definierten Schutzziele besondere Fragen in Bezug auf die Lokalisierung, Überwachung des Verschlusses, Integrität und Verfolgbarkeit auf:

Ist zu jedem Zeitpunkt bekannt, wo sich gerade bestimmte zu vernichtende Daten befinden (Behälterverfolgung, Lokalisierung, Behältertracking)?
Wie wird ein unbefugtes Öffnen der Behälter während des Transports festgestellt bzw. verhindert (Überwachung der Integrität)?
Wie wird verhindert, dass aus Optimierungsgründen Behälterinhalte verschiedener Auftraggeber zusammengemischt werden (um halbvolle Behälter zu füllen)?
Wie wird der Austausch, Transport, der Eingang und die Vernichtung eines bestimmten Behälters dokumentiert?
Welche technischen Systeme werden dafür eingesetzt?
Wie wird die personelle Zuverlässigkeit und Handlungssicherheit der involvierten Mitarbeiter_innen gewährleistet (Fahrer_innen, Beifahrer_innen)?

4.1.8.6 Sammeln und ggf. Lagern

In Zusammenhang mit der zentralen Sammlung und Lagerung beim Dienstleister stellen sich zusätzliche Fragen:

Wie ist die Lagerstätte für diese zu vernichtenden Daten abgesichert (Alarmanlage, Videoüberwachung mit Videoanalyse, Aufschaltung auf eine 24x7 Alarmzentrale, Perimetersicherung, Zutrittskontrolle, Behältereingangs- und Ausgangsdokumentation...)?
Welche technischen, organisatorischen und personellen Maßnahmen sichern die festgelegten Schutzziele ab?
Wie werden diese Maßnahmen und ihre Wirksamkeit überwacht?
Wie wird die Behälterverfolgbarkeit innerhalb der Lagerstätte bis zur Vernichtung sichergestellt?
Wie lange dauert es von der Anlieferung bis zur tatsächlichen Vernichtung?
Werden die zu vollen Behälter im Lager, bis zur tatsächlichen Vernichtung besonders gesichert?
Wie wird verhindert, dass unvollständig entleerte Behälter zu einem anderen Kunden ausgeliefert werden?

Wie wird die Behälterintegrität von entleerten, für die neuerliche Auslieferung bereitgestellten Behältern gewährleistet?
Wie wird die personelle Zuverlässigkeit und Handlungssicherheit der involvierten Mitarbeiter_innen gewährleistet (Lagerarbeiter)?

4.1.8.7 Datenträgervernichtung extern

Bei der effektiven Datenvernichtung ergeben sich aus den Schutzzielen Fragen nach der Integrität des Vernichtungsvorganges:

Wie wird die Öffnung eines bestimmten Kundenbehälters überwacht und dokumentiert?
Wie wird die vollständige Einbringung des Behälterinhaltes in den Shredder sichergestellt und überwacht?
Welche Dokumentation gibt es über diesen Vorgang (Videoarchiv, Kameraposition, Zeitstempel, Behälteridentifikation)?
Wo endet der Vernichtungsprozess derzeit (Datenträger werden zu Recyclingrohstoffen)?
Wie ist ggf. der weitere Vernichtungsvorgang des produzierten Shredderproduktes dokumentiert (Verbrennung, Auflösung im Pulper der Papierfabrik, etc.)?

4.1.9 Risikobewertung von (Prozess)Risiken

Hat sich nun ein Unternehmen zur Einhaltung der Compliance Norm ONR 192050 (gemäß 3.3) , oder ein Risikomanagementsystem nach der Norm ONR 49001 (gemäß 3.3.3) oder ist ein Unternehmen nach ISO 27001 (gemäß 3.3.3) zertifiziert so sind das alles "Selbstverpflichtungen" des Unternehmens ein Risikomanagementsystem zu implementieren und (Prozess)Risiken zu bewerten.

Dasselbe gilt auch für die Neufassung der ISO 9001:2015 (siehe 3.3.2), welche 2018 die alte ISO 9001:2005 Fassung endgültig ablöst.

Aber auch Unternehmen mit besonderen Regulatorischen Auflagen "Verpflichtungen" wie Banken (BASEL IV Richtlinie[118]) oder Versicherung (SOLVENCY II Richtlinie[119]), oder Unternehmen, welche an der Börse notiert sind (SOA/SOX act.[120]) sind zur Risikobewertung verpflichtet.

Im Sinne des Kapitels 3.2.1 muss bei der Risikobewertung die Eintrittswahrscheinlichkeit und die Auswirkung bewertet werden.

4.1.9.1 Skalierung der Risikoauswirkung eines Verstoßes des Verbandes gegen die DSGVO

Da der Gegenstand der Arbeit die Risikominimierung einer strafrechtlichen Verurteilung des Verbandes auf Basis der DSGVO zum Inhalt hat ergeben sich folgende primären Auswirkungen (siehe 3.4.9):

In bestimmten Fällen kann die Datenschutzbehörde an Stelle der Verhängung einer Geldbuße auch eine förmliche Verwarnung aussprechen.

---

[118] vgl. *PwC*, Willkommen in der Welt von Basel IV, (Stand: 16.9.2018, https://www.pwc.at/de/branchen/financial-services/willkommen-in-der-welt-von-basel-iv.html)

[119] vgl. *BaFin;* Solvency II (Stand 16.9.2018, https://www.bafin.de/DE/Aufsicht/VersichererPensionsfonds/Aufsichtsregime/SolvencyII/solvency_II_node.html)

[120] vgl. Sox-Online, (Stand: 16.9.2018, http://www.sox-online.com/compliance-approaches/risks-and-controls/)

Für weniger schwere Verstöße gegen Bestimmungen der DSGVO droht eine Geldstrafe in Höhe bis zu 10 Millionen Euro (keine Mindeststrafe) oder bei Unternehmen bis zu 2 Prozent des weltweiten Jahresumsatzes des letzten Geschäftsjahres. Es gilt der höhere Betrag.

Für schwerwiegende Verstöße gegen Bestimmungen der DSGVO droht eine Geldbuße in Höhe bis zu 20 Millionen Euro (keine Mindeststrafe) oder bei Unternehmen bis zu 4 Prozent des weltweiten Jahresumsatzes des letzten Geschäftsjahres. Es gilt der höhere Betrag.

4.1.9.1.1 Auswirkung "Verwarnung" - **gering** (bis mittel)

Die Verwarnung stellt noch kein unmittelbares finanzielles Risiko für den Verband dar, wobei meines Erachtens Unternehmen mit entsprechenden (Selbst)Verpflichtungen gemäß 4.1.9 neben dem Verurteilungsrisiko auch noch andere Risiken bewerten müssen, d.h. eine förmliche strafrechtliche Verwarnung kann besonders (Selbst)Verpflichtete Unternehmen stärker treffen, da somit evidente Verstöße gegen (Selbst)Verpflichtungen zu weiteren Schäden oder Verurteilungen auf Basis anderer Gesetze führen könnten (siehe 4.1.9 Einleitung) und es damit unter Umständen zu erheblichen Reputationsfolgeschäden führen könnte.
Für das aktuelle Beispiel wähle ich für die "Verwarnung" die Auswirkung "gering".

4.1.9.1.2 Auswirkung "Weniger schwerer Verstoß" - **mittel** (bis schwer)

Das Strafmaß von bis zu 10 Mio. oder 2% des weltweiten Umsatzes kann je nach Finanzsituation (Ertrag, Cash Flow, Eigenkapital- vs. Fremdkapitalanteil, etc.) ein Unternehmen in große Schwierigkeiten bringen (Auswirkung schwer) oder aber nur zu einer massiven Verschlechterung des Jahresergebnisses führen (mittlere Auswirkung).
Dazu kommen indirekte Folgen wie in 4.1.9.1.1 beschrieben.

Für das aktuelle Beispiel wähle ich die Auswirkung "mittel" für einen "weniger schweren Verstoß".

4.1.9.1.3 Auswirkung "Schwerwiegender Verstoß" - (mittel bis) schwer

Das **Strafausmaß bis zu 20 Mio. oder 4% des weltweiten Umsatzes** kann in vielen Fällen als schwere Auswirkung beurteilt werden. Für viele Unternehmensgruppen sind 4% des Umsatzes ein oder mehrere Jahresergebnisse, für viele Unternehmen stellt dies eine schwere Bedrohung dar.
Dazu kommen indirekte Folgen wie in 4.1.9.1.1 beschrieben.

Der "Schwerwiegende Verstoß" wird von mir mit der Auswirkung "schwer" bewertet.

Letztendlich hängt die Bewertung der Auswirkung von folgenden Faktoren ab:

Anzahl der Verstöße
Finanzkraft des betroffenen Unternehmens (Verbandes)
Folgeauswirkungen von Verwarnungen, Geldstrafen oder Geldbußen
Wie schwerwiegend ist das zu Grunde liegende Verbandsversagen gegen die Vorschriften der DSGVO?
usw.

Im aktuellen Beispiel verwende ich exemplarisch fünf Klassifizierungen: sehr gering, gering, mittel, schwer und existenzbedrohend, wobei ich in der gegenständlichen Arbeit davon ausgehe, dass der entsprechende Verband über ausreichend Finanzreserven verfügt um eine Strafe aus der DSGVO zu bezahlen ohne in seiner Existenz bedroht zu sein.

Damit kann man die Skala für die Auswirkung in der Risikomatrix befüllen:

Auswirkung	sehr gering	gering	mittel	schwer	existenzbedrohend

Abbildung 17: Skalierung Risikoauswirkung in der Risikomatrix

4.1.9.2 Skalierung der Risikoeintrittswahrscheinlichkeit eines Verstoßes des Verbandes gegen die DSGVO

Die Eintrittswahrscheinlichkeit sollte an Hand einer geeigneten Häufigkeitswahrscheinlichkeit bewertet werden. Von der Skalierung bietet sich hier ein Prozentschema an:

- sehr wahrscheinlich (X > 75%)
- wahrscheinlich (X > 50%)
- möglich (X > 25%)
- unwahrscheinlich (X > 5%)
- fast unmöglich (X < 5%)

Damit lässt sich die Skala für die Eintrittswahrscheinlichkeit in die Risikomatrix eintragen:

Auswirkung -> Eintrittswahrscheinlichkeit	sehr gering	gering	mittel	schwer	existenzbedrohend
sehr wahrscheinlich					
wahrscheinlich					
möglich					
unwahrscheinlich					
fast unmöglich					

Abbildung 18: Skalierung Eintrittswahrscheinlichkeit in der Risikomatrix

Aufgrund auf dieser Matrix sind dann die möglichen Risiken gemäß 4.1.8 zu bewerten:

4.1.9.3 Risikobewertungsbeispiel eines fiktiven Betriebes

Aufbauend auf Eintrittswahrscheinlichkeit und Auswirkung wird in Folge eine Risikobewertung durchgeführt.
Dafür wurden basierend auf den Schutzzielen Risikoszenarien im Rahmen eines Brainstormings ermittelt und bezüglich Eintrittswahrscheinlichkeit und Auswirkung bewertet.

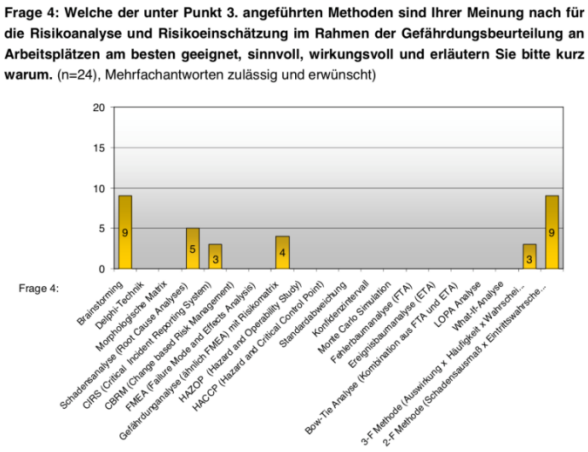


Abbildung 19: Bewertung der Methoden zur Gefährdungsbeurteilung ANDRLIK, Risikoanalyse in der Praxis (2012) 19f

Das **Brainstorming zählt zu einer der höchstbewerteten Methoden der Risikoermittlung** [121]. Im gegenständlichen Fallbeispiel habe ich das Brainstorming alleine durchgeführt. Als Unterstützung wurden von mir anwendbare Fragen des Anhang A der ISO 27001 integriert.[122]

Das gegenständliche Beispiel basiert auf subjektiven Wahrnehmungen des Verfassers, sämtliche **Eintrittswahrscheinlichkeiten und Auswirkungen wurden vom Verfasser auf Basis subjektiver Wahrnehmungen bewertet**:

Risiko Nr.	Vertrag	Eintrittswahrscheinlichkeit	Auswirkung
1	Technische, organisatorische und personelle Maßnahmen des Dienstleisters sind nicht am Stand der Technik, bzw. gewährleisten nicht die Schutzziele gemäß DSGVO/DSG	3 möglich	4 schwer
2	Die Wirksamkeit der Maßnahmen werden nicht überprüft	5 sehr wahrscheinlich	4 schwer
3	Der Dienstleister erkennt keine Umgehungen seiner Maßnahmen	5 sehr wahrscheinlich	4 schwer
4	Der Dienstleister kennt seine Verpflichtungen aus der DSGVO/DSG im Falle des Datenverlustes nicht	2 unwahrscheinlich	4 schwer
5	Die unklaren Schnittstellen der Verantwortung des Dienstleisters ermöglichen dem Dienstleister sich allfälliger Haftungen zu entledigen	2 unwahrscheinlich	3 mittel
6	Der Datenvernichtungsprozess des Dienstleisters ist unzureichend dokumentiert	4 wahrscheinlich	3 mittel
7	Allfällige Zertifizierungen des Dienstleisters berücksichtigen nicht die Schutzziele des Auftraggebers	2 unwahrscheinlich	4 schwer
	Organisation und Personal		
8	Unbefugte erhalten Zugriff auf den Behälterinhalt	2 unwahrscheinlich	4 schwer
9	Prozessinvolvierte Miterbeiter_innen sind unzuverlässig und nicht vertrauenswürdig	2 unwahrscheinlich	3 mittel
10	Drittdienstleister_innen oder Besucher_innen erhalten Zugriff auf Behälterinhalte	2 unwahrscheinlich	4 schwer
11	Behälter können unbemerkt geöffnet werden	2 unwahrscheinlich	4 schwer
12	Schutzvorrichtungen können umgangen werden	3 möglich	4 schwer
13	Der Behälter wird am Weg zur Vernichtung von Personal geöffnet	3 möglich	3 mittel
14	Öffnungen des Behälters werden nicht dokumentiert	3 möglich	3 mittel
15	Es wird im Prozess kein Internes Kontrollsystem IKS angewendet	5 sehr wahrscheinlich	4 schwer
16	Mitarbeiter_innen verfügen nicht über das erforderliche Bewusstsein für die Notwendigkeit von Verhaltenrichtlinien	4 wahrscheinlich	3 mittel
17	Mitarbeiter_innen müssen bei Verstößen mit keinen Konsequenzen rechnen	4 wahrscheinlich	3 mittel
18	Es wurden keine vertraglichen/arbeitsrechtlichen Regelungen bzgl. DSGVO/DSG mit Mitarbeiter_innen getroffen	2 unwahrscheinlich	4 schwer

[121] vgl. ANDRLIK, *Risikoanalyse in der Praxis (2012) 19f*

[122] ONR, ÖNORM 27001:2015 idF 1.3.2018 20ff

	Anfallstelle zur Datenträgervernichtung		
19	Zur Vernichtung bestimmte Datenträger werden frei zugänglich am/beim Schreibtisch gelagert und gesammelt (tagelang)	3 möglich	3 mittel
20	Beim Verlassen des Arbeitsplatzes (tagsüber) bleiben zu vernichtende Datenträger frei zugänglich am Arbeitsplatz liegen	4 wahrscheinlich	3 mittel
21	Unbefugte Mitarbeiter_innen (von Drittfirmen) bringen zu vernichtende Datenträger zur Sammelstelle	4 wahrscheinlich	3 mittel
22	Nicht sicherheitsüberprüfte Mitarbeiter_innen haben Zugriff zu zu vernichtenden Datenträgern	3 möglich	3 mittel
23	Zu vernichtende Datenträger gelangen auf öffentliche Altpapiersammelstellen	3 möglich	4 schwer
	Sammelstelle und Lager beim Auftraggeber		
24	Aus verschlossenen Behältern lassen sich Akten entnehmen	4 wahrscheinlich	3 mittel
25	Die Einwurföffnung ist nicht entsprechend gesichert	4 wahrscheinlich	3 mittel
26	Der Aufstellort ist weder alarmgesichert noch kameraüberwacht	5 sehr wahrscheinlich	2 gering
27	Überwachungsdaten werden nicht analysiert	5 sehr wahrscheinlich	2 gering
28	Behälter sind nicht besonders gesichert und frei zugänglich	2 unwahrscheinlich	4 schwer
	Transport (durch Dienstleister)		
29	Behälter eines Kunden mit zu vernichtende Daten können nicht bis zur Vernichtung nachverfolgt werden	5 sehr wahrscheinlich	3 mittel
30	Unbefugtes Öffnen während des Transports kann nicht festgestellt werden (Integritätsverlust)	5 sehr wahrscheinlich	4 schwer
31	Behälterinhalte verschiedener Kunden werden im LKW vermischt	4 wahrscheinlich	4 schwer
32	Der Austausch, Transport, der Eingang und die Vernichtung des Inhaltes eines bestimmten Behälters kann nicht dokumentiert werden	5 sehr wahrscheinlich	4 schwer
33	Es gibt keine technischen oder organisatorischen Systeme (IKS, Vier Augenprinzip, Siegel) um die Verletzung der Systemintegrität zu prüfen	5 sehr wahrscheinlich	4 schwer
34	Unbefugte erhalten Zugriff auf den Behälterinhalt	3 möglich	4 schwer
35	Prozessinvolvierte Mitarbeiter_innen sind unzuverlässig und nicht vertrauenswürdig	3 möglich	4 schwer
36	Nicht sicherheitsüberprüfte Mitarbeiter_innen haben Zugriff zu zu vernichtenden Datenträgern	3 möglich	4 schwer
37	Es wurden keine vertraglichen/arbeitsrechtlichen Regelungen bzgl. DSGVO/DSG mit Mitarbeiter_innen getroffen	2 unwahrscheinlich	4 schwer
38	Mitarbeiter_innen müssen bei Verstößen mit keinen Konsequenzen rechnen	2 unwahrscheinlich	4 schwer
	Sammelstelle und Lagerung beim Dienstleister		
39	Die Sammelstelle des Dienstleisters verfügt über keine ausreichende Absicherung des Perimeters (Alarmanlage, Videoüberwachung mit Videoanalyse, Aufschaltung auf eine 24x7 Alarmzentrale, Zutrittskontrollsystem, Behältereingangs- und Ausgangsdokumentation	4 wahrscheinlich	4 schwer
40	Die Sammelstelle setzt keine geeigneten Maßnahmen zur Erreichung der festgelegten Schutzziele des Auftraggebers	2 unwahrscheinlich	4 schwer
41	Vereinbarte Maßnahmen werden nicht auf ihre Wirksamkeit überprüft	2 unwahrscheinlich	4 schwer
42	Der Stand der Technik im Bereich Loss Prevention im Handel wird bei der Datenvernichtung nicht angewendet	5 sehr wahrscheinlich	4 schwer
43	Die Behälterverfolgbarkeit innerhalb der Lagerstätte bis zur Vernichtung ist nicht sichergestellt	3 möglich	3 mittel
44	Der Zeitpunkt der Vernichtung eines bestimmten Behälterinhaltes ist nicht klar bestimmbar (Zeitstempel)	4 wahrscheinlich	3 mittel
45	Die zu vernichtenden Behälter werden nicht besonders gesichert	2 unwahrscheinlich	4 schwer
46	Die Vollständigkeit der Entleerung wird nicht geprüft	2 unwahrscheinlich	4 schwer
47	Die Behälterintegrität von ordnungsgemäß entleerten Behältern ist nicht gewährleistet	5 sehr wahrscheinlich	4 schwer
48	Unbefugte erhalten Zugriff auf den Behälterinhalt	3 möglich	4 schwer
49	Prozessinvolvierte Mitarbeiter_innen sind unzuverlässig und nicht vertrauenswürdig	2 unwahrscheinlich	4 schwer
50	Nicht sicherheitsüberprüfte Mitarbeiter_innen haben Zugriff zu zu vernichtenden Datenträgern	3 möglich	4 schwer
51	Es wurden keine vertraglichen / arbeitsrechtlichen Regelungen bzgl. DSGVO/DSG mit Mitarbeiter_innen getroffen	2 unwahrscheinlich	4 schwer
52	Mitarbeiter_innen müssen bei Verstößen mit keinen Konsequenzen rechnen	2 unwahrscheinlich	4 schwer
	Datenträgervernichtung beim Dienstleister		
53	Die Öffnung eines bestimmten Kundenbehältrs wird nicht spezifisch überwacht und dokumentiert	5 sehr wahrscheinlich	4 schwer
54	Die vollständige Einbringung des Behälterinhaltes in den Shredder wird nicht sichergestellt und überwacht	3 möglich	4 schwer
55	Es gibt keine Dokumentation über den effektiven Shredderprozess (Videoarchiv, Kameraposition, Zeitstempel, Behälteidentifikation)	5 sehr wahrscheinlich	4 schwer
56	Das zerkleinerte Shredderprodukt wird frei deponiert	2 unwahrscheinlich	1 sehr gering
57	Die Vernichtung des Shredderproduktes (Verbrennung, Auflösung im Pulper) wird nicht dokumentiert	4 wahrscheinlich	1 sehr gering

Abbildung 20: Risikobewertung eines fiktiven Datenvernichtungsprozesse

Trägt man diese Risikobewertung in die vorbereitete Matrix ein, erkennt man in den roten Bereichen die Risiken mit unmittelbarem Handlungsbedarf, aber auch die Risiken in den orangen Bereichen sind zu überwachen, bzw. zu reduzieren.

Auswirkung -> Eintrittswahrscheinlichkeit	sehr gering	gering	mittel	schwer	existenzbedrohend
sehr wahrscheinlich		26,27,	29,	2,3,15,30, 32,33,42,47, 53, 55	
wahrscheinlich	57		6,16,17,20, 21,22,24,25, 44	31,39,	
möglich			13,14,19,43,	1,12,23,34, 35,36,48,50, 54	
unwahrscheinlich	56		5,9,	4,7,8,10, 11,18,28,37, 38,40,41,45, 46,49,51,52	
fast unmöglich					

Abbildung 21: Risikomatrix mit Risikobewertung ohne geeignete Maßnahmen

Diese **nicht akzeptierbaren Risiken müssen nun durch geeignete Maßnahmen reduziert bzw. bewältigt werden**, oder akzeptiert werden.
Bei der Ergreifung möglicher Maßnahmen habe ich mich auf technisch- und wirtschaftliche sowie am Stand der Technik praktikable Maßnahmen fokussiert.

4.1.10 Risikobewältigung im fiktiven Fallbeispiel

Die Risikobewältigung (Risikominimierung, Risikoreduzierung) erfolgt durch die Festlegung und laufende Überwachung von geeigneten Maßnahmen, wobei die Risikoüberwachung und Risikoüberprüfung (gemäß 3.2.3) integraler Bestandteil eines Risikomanagementsystems sein müssen.

Im Folgenden beschreibe ich geeignete Maßnahmen zur Risikobewältigung an Hand des gegenständlichen fiktiven Fallbeispiels, Die Tabellen sind Ausschnitte der von mir durchgeführten Risikoanalyse an einem fiktiven Fallbeispiel:

4.1.10.1 Vertragsseitige Risikominimierungsmaßnahmen

Vertragsseitige Maßnahmen sind zwischen Dienstleister und Auftraggeber in geeigneter Weise (Auftrag, Bestellung, Besondere Geschäftsbedingungen, etc.) zu vereinbaren und zu überwachen:

Risiko Nr.	Vertrag	Eintritts-wahrscheinlichkeit	Auswirkung	Maßnahme	NEUE Eintritts-wahrscheinlichkeit	Auswirkung
1	Technische, organisatorische und personelle Maßnahmen des Dienstleisters sind nicht am Stand der Technik, bzw. gewährleisten nicht die Schutzziele gemäß DSGVO/DSG	3 möglich	4 schwer	Zwischen Auftraggeber und Auftragnehmer werden Schutzziele und Maßnahmen vertraglich vereinbart	2 unwahrscheinlich	4 schwer
2	Die Wirksamkeit der Maßnahmen werden nicht überprüft	5 sehr wahrscheinlich	4 schwer	Der Dienstleister unterzieht sich regelmäßigen externen Audits und/oder der Prozess wird ISO 9001:2015 bzw. ISO 2700 zertifiziert.	2 unwahrscheinlich	4 schwer
3	Der Dienstleister erkennt keine Umgehungen seiner Maßnahmen	5 sehr wahrscheinlich	4 schwer	Die Behälter werden mechanisch oder elektronisch versiegelt, jede Öffnung des Behälters wird erkannt	2 unwahrscheinlich	4 schwer
6	Der Datenvernichtungsprozess des Dienstleisters ist unzureichend dokumentiert	4 wahrscheinlich	3 mittel	Der Dienstleister dokumentiert jeden Prozessschritt und unterzieht sich regelmäßigen externen Audits und/oder der Prozess wird ISO 9001:2015 bzw. ISO 2700 zertifiziert.	2 unwahrscheinlich	3 mittel

Abbildung 22: Vertragsseitige Risikominimierungsmaßnahmen

Durch die **vertragliche Vereinbarung gemeinsamer Schutzziele und Maßnahmen** wird der Prozess auf Auftraggeberseite - dem Verantwortlichen gemäß DSGVO - und Dienstleisterseite - dem Auftragsverarbeiter gemäß DSGVO - harmonisiert und einheitliche Ziele definiert.

Die **laufenden internen und externen Audits** eines zertifizierten Dienstleistungsunternehmens **reduzieren für den Auftraggeber den Auditierungsbedarf beim Lieferanten** (Risikoüberwachung und Risikoüberprüfung gemäß 3.2.3), dementsprechend einfacher können Vertragsbedingungen vereinbart werden, da Zertifizierungen zum Vertragsbestandteil gemacht werden können.
Erst die Vereinbarung geeigneter **mechanische oder elektronische Versiegelung** ermöglichen dem Verantwortlichen Umgehungen seiner Maßnahmen zu erkennen

Nur die **Sicherstellung eines prozessorientierten dokumentierten Datenvernichtungsprozesses**, welcher im Rahmen von Managementsystemen am aktuellen Stand der Technik abgesichert wird, reduziert Risiken für den Auftraggeber und den Dienstleister.

4.1.10.2 Organisatorische und personelle Maßnahmen des Auftraggebers und Dienstleisters

Einige Maßnahmen können nur unter Beteiligung des Auftraggebers und des Dienstleisters ergriffen werden.

Der Dienstleister sollte zum Beispiel entsprechend **geschlossene Sicherheitssysteme** (Behälter, Dokumentationssystem, Prozessdatenspeicherung, IKS...) **für den Behälterinhalt** bereitstellen, der Auftraggeber sorgt idealerweise für die gesicherten Aufstellflächen der Behälter und entsprechende Sicherheitsmaßnahmen.

Risiko Nr.	Organisation und Personal beim Auftraggeber	Eintritts-wahrscheinlichkeit	Auswirkung	Maßnahme	NEUE Eintritts-wahrscheinlichkeit	Auswirkung
12	Schutzvorrichtungen können umgangen werden	3 möglich	4 schwer	Die Behälter werden mechanisch oder elektronisch versiegelt, jede Öffnung des Behälters wird erkannt. Der Dienstleister dokumentiert jeden Prozessschritt und unterzieht sich regelmäßigen externen Audits und/oder der Prozess wird ISO 9001:2015 bzw. ISO 2700 zertifiziert.	2 unwahrscheinlich	4 schwer
15	Es wird im Prozess kein Internes Kontrollsystem IKS angewendet	5 sehr wahrscheinlich	4 schwer	Der Prozess wird durch 2 Personen im 4 Augen Prinzip durchgeführt oder Einzelpersonen werden elektronisch zusätzlich überwacht.	2 unwahrscheinlich	4 schwer
16	Mitarbeiter_innen verfügen nicht über das erforderliche Bewusstsein für die Notwendigkeit von Verhaltenrichtlinien	4 wahrscheinlich	3 mittel	Prozessbeteiligte Mitarbeiter_innen werden regelmäßig unterwiesen, die Einhaltung der Richtlinien wird regelmäßig überwacht.	2 unwahrscheinlich	3 mittel
17	Mitarbeiter_innen müssen bei Verstößen mit keinen Konsequenzen rechnen	4 wahrscheinlich	3 mittel	Arbeitsverträge werden angepaßt und Konsequenzen in Eskalationsstufen abgebildet, überwacht und umgesetzt. Das Verfahren wird extern auditiert.	2 unwahrscheinlich	3 mittel

Abbildung 23: Organisatorische und personelle Risikominimierungsmaßnahmen

Der Auftraggeber reduziert organisatorische und personelle Risiken durch **kontrollierte Prozessabläufe** im Bereich seiner Mitarbeiter_innen und Besucher um den Gesamtprozess abzusichern.

Entsprechende **Unterweisungen für Mitarbeiter_innen** des Auftraggebers und bei ihm tätigen Drittdienstleistern reduzieren Prozessrisiken auf Seiten des Auftraggebers.

Ein elektronisches oder tatsächliches **4-Augen Prinzip** reduziert Risiko durch menschliches Versagen.

Die konsequente **Verfolgung und Ahndung von Verstößen** gegen Richtlinien sorgt für Bewusstsein und erhöht die Prozesssicherheit.

4.1.10.3 Maßnahmen an der Anfallsstelle zur Datenträgervernichtung beim Auftraggeber

Das **Verhalten von Mitarbeiter_innen des Auftraggebers und Drittdienstleistern** spielt eine entscheidende Rolle beim Schutz von Datenträgern.

Einfache Entscheidungen zur Erhöhung der Prozesssicherheit bedingen oft unumgängliche Verhaltensänderungen von Mitarbeiter_innen: **Clean Desk Richtlinien, Verschluss von zu vernichtenden Datenträgern, persönliche Anlieferung von Datenträgern zum Vernichtungssammelpunkt** und vieles mehr.

Die beste Richtlinie ist nur soviel wert wie der Grad ihrer Befolgung durch die Mitarbeiter_innen!

Vor allem die **Zuverlässigkeit von Mitarbeiter_innen** schaltet wesentliche Prozessrisiken aus. Diese Zuverlässigkeit ist in geeigneter Art und Wiese zu überprüfen.

Risiko Nr.	Anfallstelle zur Datenträgervernichtung beim Auftraggeber	Eintritts-wahrscheinlichkeit	Auswirkung	Maßnahme	NEUE Eintritts-wahrscheinlichkeit	Auswirkung
20	Beim Verlassen des Arbeitsplatzes (tagsüber) bleiben zu vernichtende	4 wahrscheinlich	3 mittel	Eine sog. "Clean Desk Policy" wird beim Auftraggeber	2 unwahrscheinlich	3 mittel
21	Unbefugte Mitarbeiter_innen (von Drittfirmen) bringen zu vernichtende Datenträger zur Sammelstelle	4 wahrscheinlich	3 mittel	Der Transport von zu vernichtenden Datenträger darf nur durch den Besitzer der zu vernichtenden Datenträger erfolgen. Eine entsprechende Regelung wird implementiert und überwacht.	2 unwahrscheinlich	3 mittel
22	Nicht sicherheitsüberprüfte Mitarbeiter_innen haben Zugriff zu zu vernichtenden Datenträgern	4 wahrscheinlich	3 mittel	Personen mit Zugriff auf personenbezogene Daten werden einer jährlichen Sicherheitsüberprüfung unterzogen, Gehaltspfändungen führen ebenso wie Suchtkrankheiten zum Verlust der Zuverlässigkeit. Nicht Sicherheitsüberprüfte MitarbeiterInnen erhalten keinen Zugriff auf personenbezogene Daten.	2 unwahrscheinlich	3 mittel
23	Zu vernichtende Datenträger gelangen auf öffentliche Altpapiersammelstellen	3 möglich	4 schwer	Eine sog. "Clean Desk Policy" wird beim Auftraggeber implementiert und überwacht. Der Transport von zu vernichtenden Datenträger darf nur durch den Besitzer der zu vernichtenden Datenträger erfolgen. Eine entsprechende Regelung wird implementiert und überwacht.	2 unwahrscheinlich	4 schwer

Abbildung 24: Maßnahmen am Anfallort der Datenträger

4.1.10.4 Maßnahmen an der Sammelstelle und Lager beim Auftraggeber

Aber auch die Organisation muss die konsequente Schutzzielerreichung unterstützen:

Bei der Beauftragung sind die kostenintensiveren Sammelbehälter mit **Einwurfklappen**, statt Einwurfschlitzen vorzuschreiben.

Die **Aufstellorte** der Sammelbehälter müssen über grundlegende **physische Absicherungen** verfügen: Alarmanlage und/oder Videoanlage mit Videoanalyse und Aufschaltung auf eine Alarmzentrale.
Alarmvorfälle müssen **lückenlos protokolliert** und die Ursachen ausgewertet werden.

Risiko Nr.	Sammelstelle und Lager beim Auftraggeber	Eintritts-wahrscheinlichkeit	Auswirkung	Maßnahme	NEUE Eintritts-wahrscheinlichkeit	Auswirkung
24	Aus verschlossenen Behältern lassen sich Akten entnehmen	4 wahrscheinlich	3 mittel	Es werden ausschließlich Sammelbehälter mit Einwurfklappen statt Einwurfschlitzen verwendet.	2 unwahrscheinlich	3 mittel
25	Die Einwurföffnung ist nicht entsprechend gesichert	4 wahrscheinlich	3 mittel	Es werden ausschließlich Sammelbehälter mit Einwurfklappen statt Einwurfschlitzen verwendet.	2 unwahrscheinlich	3 mittel
26	Der Aufstellort ist weder alarmgesichert noch kameraüberwacht	5 sehr wahrscheinlich	2 gering	Die Räume in welchen Sammelbehälter aufgestellt sind werden alarmgesichert und ggf. Kameraüberwacht und auf eine Alarmzentrale aufgeschalten.	1 fast unmöglich	2 gering
27	Überwachungsdaten werden nicht analysiert	5 sehr wahrscheinlich	2 gering	Alle Alarme werden protokolliert und ausgewertet	1 fast unmöglich	2 gering

Abbildung 25: Maßnahmen an der Sammelstelle beim Auftraggeber

4.1.10.5 Maßnahmen beim Transport (durch Dienstleister)

Ein wesentliches Risiko ist mit Sicherheit die nur bedingt vorhandene Möglichkeit den **Weg und Zustand der Behälter vom Aufstellort bis zur definitiven Vernichtung** zu dokumentieren.

Dazu kommt die meiner Ansicht nach nur bedingt vorhandene **Möglichkeit unbefugte Behälteröffnungen feststellen zu können**.

Optimiert zum Beispiel eine Fahrer_in aus wirtschaftlichen Gründen den Prozess und leert im LKW Behälterinhalte nur wenig gefüllte Behälter unterschiedlicher Kunden zusammen findet eine Verletzung der Integrität Behälter mit zu vernichtenden Datenträger statt. Der

Auftraggeber/Verantwortliche vertraut schließlich auf den Verschluss des Behälters bis zur Vernichtung.

Aber auch die **Protokollierung der Abholung, Anlieferungen** eines bestimmten Behälters **an der Vernichtungsstelle, die Zwischenlagerung und die endgültige Vernichtung** sollten entsprechend dokumentiert werden.

Die Anwendung eines elektronischen oder tatsächlichen **4 Augenprinzips ist ein Grundprinzip zur Sicherstellung maximaler Systemintegrität im Falle menschlichen Versagens.**

Risiko Nr.	Transport (durch Dienstleister)	Eintritts-wahrscheinlichkeit	Auswirkung	Maßnahme	NEUE Eintritts-wahrscheinlichkeit	Auswirkung
29	Behälter eines Kunden mit zu vernichtende Daten können nicht bis zur Vernichtung nachverfolgt werden	5 sehr wahrscheinlich	3 mittel	Die Behälter werden mechanisch oder elektronisch versiegelt, jede Öffnung des Behälters wird erkannt. Der Dienstleister dokumentiert jeden Prozessschritt und unterzieht sich regelmäßigen externen Audits und/oder der Prozess wird ISO 9001:2015 bzw. ISO 2700 zertifiziert.	1 fast unmöglich	3 mittel
30	Unbefugtes Öffnen während des Transports kann nicht festgestellt werden (Integritätsverlust)	5 sehr wahrscheinlich	4 schwer	Die Behälter werden mechanisch oder elektronisch versiegelt, jede Öffnung des Behälters wird erkannt. Der Dienstleister dokumentiert jeden Prozessschritt und unterzieht sich regelmäßigen externen Audits und/oder der Prozess wird ISO 9001:2015 bzw. ISO 2700 zertifiziert.	1 fast unmöglich	4 schwer
31	Behälterinhalte verschiedener Kunden werden im LKW vermischt	4 wahrscheinlich	4 schwer	Die Behälter werden mechanisch oder elektronisch versiegelt, jede Öffnung des Behälters wird erkannt. Der Dienstleister dokumentiert jeden Prozessschritt und unterzieht sich regelmäßigen externen Audits und/oder der Prozess wird ISO 9001:2015 bzw. ISO 2700 zertifiziert.	1 fast unmöglich	4 schwer

Abbildung 26: Maßnahmen während des Transportes Teil1

Das **Nichterkennen der Behälteröffnung** stellt wie in den anderen Prozessschritten ein potentielles Risikofeld dar.

32	Der Austausch, Transport, der Eingang und die Vernichtung des Inhaltes eines bestimmten Behälters kann nicht dokumentiert werden	5 sehr wahrscheinlich	4 schwer	Die Behälter werden mechanisch oder elektronisch versiegelt, jede Öffnung des Behälters wird erkannt. Der Dienstleister dokumentiert jeden Prozessschritt und unterzieht sich regelmäßigen externen Audits und/oder der Prozess wird ISO 9001:2015 bzw. ISO 2700 zertifiziert.	1 fast unmöglich	4 schwer
33	Es gibt keine technischen oder organisatorischen Systeme (IKS, Vier Augenprinzip, Siegel) um die Verletzung der Systemintegrität zu prüfen	5 sehr wahrscheinlich	4 schwer	Die Behälter werden mechanisch oder elektronisch versiegelt, jede Öffnung des Behälters wird erkannt. Der Dienstleister dokumentiert jeden Prozessschritt und unterzieht sich regelmäßigen externen Audits und/oder der Prozess wird ISO 9001:2015 bzw. ISO 2700 zertifiziert.	1 fast unmöglich	4 schwer
34	Unbefugte erhalten Zugriff auf den Behälterinhalt	3 möglich	4 schwer	Die Behälter werden mechanisch oder elektronisch versiegelt, jede Öffnung des Behälters wird erkannt. Der Dienstleister dokumentiert jeden Prozessschritt und unterzieht sich regelmäßigen externen Audits und/oder der Prozess wird ISO 9001:2015 bzw. ISO 2700 zertifiziert.	2 unwahrscheinlich	4 schwer
35	Prozessinvolvierte Mitarbeiter_innen sind unzuverlässig und nicht vertrauenswürdig	3 möglich	4 schwer	Personen mit möglichem Zugriff auf personenbezogene Daten werden einer jährlichen Sicherheitsüberprüfung unterzogen, Gehaltspfändungen führen ebenso wie Suchtkrankheiten zum Verlust der Zuverlässigkeit. Nicht Sicherheitsüberprüfte MitarbeiterInnen erhalten keinen Zugriff auf personenbezogene Daten.	2 unwahrscheinlich	4 schwer
36	Nicht sicherheitsüberprüfte Mitarbeiter_innen haben Zugriff zu zu vernichtenden Datenträgern	3 möglich	4 schwer	Personen (Transportmitarbeiter_innen) mit möglichem Zugriff auf personenbezogene Daten werden einer jährlichen Sicherheitsüberprüfung unterzogen, Gehaltspfändungen führen ebenso wie Suchtkrankheiten zum Verlust der Zuverlässigkeit. Nicht Sicherheitsüberprüfte MitarbeiterInnen erhalten keinen Möglichkeit zum Zugriff auf personenbezogene Daten.	2 unwahrscheinlich	4 schwer

Abbildung 27: Maßnahmen während des Transportes Teil 2

Die **Prüfung der Zuverlässigkeit von prozessinvolvierten Mitarbeiter_innen** und die **Sicherstellung der Handlungsfähigkeit durch entsprechende Unterweisungen** gehören wie in der Einleitung ausgeführt zu den Grundsätzen von modernen Managementsystemen oder werden in der öffentlichen Verwaltung klar per Verordnung geregelt.

4.1.10.6 Maßnahmen an der Sammelstelle und Lagerung beim Dienstleister

Die Sammelstelle des Dienstleisters und die Lagerreinrichtungen sind in Bezug auf die physische Sicherheit oft ein potentielles Risiko:

Betrachtet man den Behälterinhalt als Altstoff, so gerechtfertigt der Wert des Altstoffes keine wesentlichen Sicherheitsmaßnahmen. Anders verhält sich das aus der Perspektive des durch die DSGVO / DSG verpflichteten Verbandes.

Verschafft sich jemand Zugang zu den in Zwischenlagerung befindlichen Behältern und entwendet die darin befindlichen Datenträger, so handelt es sich um einen schwerwiegenden, zu behördlich sanktionierenden Verstoß gegen die DSGVO / DSG.
Das heißt auch außerhalb der Betriebszeiten ist diese Sammelstelle entsprechend abzusichern.

Unter diesem Perspektivenwechsel ist auch der **Stand der Technik** im Zusammenhang mit ***Retail Loss Prevention*** Lösungen, darunter versteht man im **Einzelhandel** Maßnahmen zur Reduktion der Kosten durch Diebstahl oder andere kriminelle Aktivitäten.[123], zu berücksichtigen.
Die von mir gewählten Maßnahmen finden sich als Stand der Technik in unterschiedlichen Normen und Branchenstandards ob es sich um Loss Prevention Lösungen oder Lösungen der Logistikindustrie entsprechend den TAPA Standards handelt:
Ein Zertifikat nach der ***TAPA*** **-** Norm weist zum Beispiel nach, dass ein Unternehmen gemäß den speziellen Anforderungen des Standards geprüft wurde und diese erfüllt. Die vier TAPA-Standards spezifizieren Mindestsicherheitsanforderungen an die **Transport- und Logistikbranche.** Die vier TAPA-Standards sind FSR (Facility Security Requirements), TSR (Trucking Security Requirements), PSR (Parking Security Requirements) und TACSS (TAPA Air Cargo Security Standards).[124]

---

[123] vgl. *collinsdictionary*, Loss Prevention Definition (Stand: 16.9.2018, https://www.collinsdictionary.com/de/worterbuch/englisch/loss-prevention)

[124] vgl. DNV-GL, TAPA-Zertifizierungen (Stand: 16.9.2018, https://www.dnvgl.de/services/zertifizierung-nach-den-tapa-standards-4345

Der weltweite Marktführer für Sicherheitslösungen im Einzelhandel Tyco setzt laufend Standards in der Warensicherung im Einzelhandel [125]:

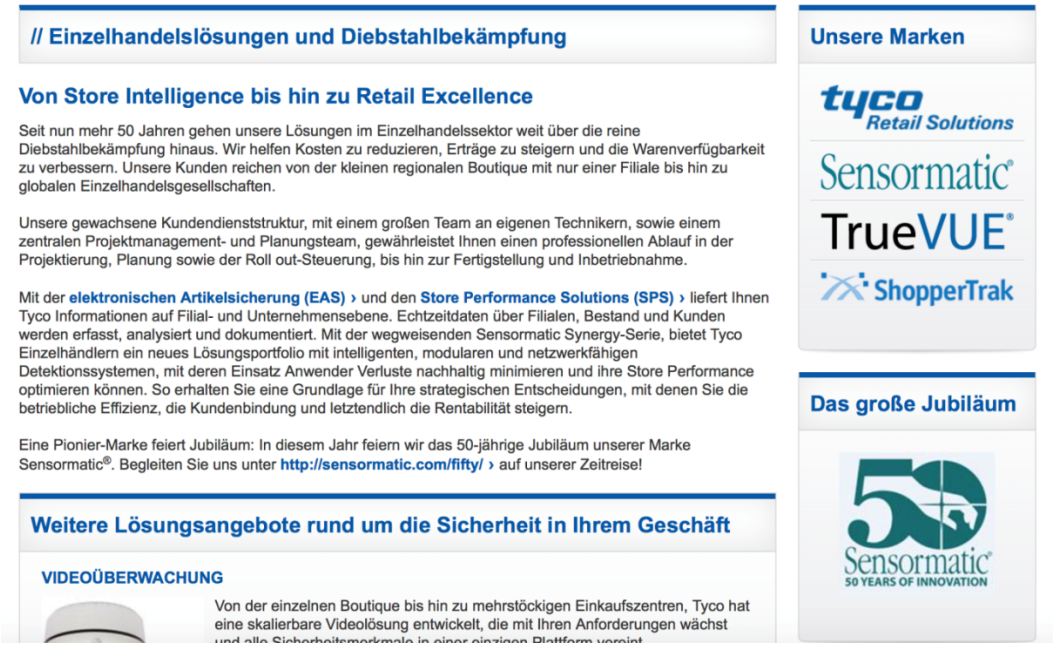


Abbildung 28: Stand der Sicherheitstechnik im Einzelhandel *TYCO*, Einzelhandelslösungen (Stand: 16.9.2018, https://www.tyco.de/loesungen/retail/)

Es ist lediglich eine Frage der Perspektivenverschiebung: Handelt es sich bei den Inhalten der Sammelbehälter vor Vernichtung um Abfall oder um Datenträger?

Bis zur zuverlässigen Vernichtung der Datenträger müssen wir diese als solche (Datenträger) betrachten und behandeln.

[125] vgl. TYCO, Einzelhandelslösungen (Stand: 16.9.2018, https://www.tyco.de/loesungen/retail/)

Risiko Nr.	Sammelstelle und Lagerung beim Dienstleister	Eintritts-wahrscheinlichkeit	Auswirkung	Maßnahme	NEUE Eintritts-wahrscheinlichkeit	Auswirkung
39	Die Sammelstelle des Dienstleisters verfügt über keine ausreichende Absicherung des Perimeters (Alarmanlage, Videoüberwachung mit Videoanalyse, Aufschaltung auf eine 24x7 Alarmzentrale, Zutrittskontrollsystem, Behältereingangs- und Ausgangsdokumentation	4 wahrscheinlich	4 schwer	Alle Sammelstellen des Dienstleisters, an welchen Datenträgern mit personenbezogenen Daten zu Vernichtung übernommen werden müssen über Mindeststandards der physischen Sicherheit verfügen: Alrmanlage, Zutrittskontrolle, Videoüberwachung der Zutrittsbereiche und im Bereich der Behälteröffnung, Entleerung, des Shreddervorganges und des Behälterverschlußes. Darüberhinaus ist der Behälter Ein- und Ausgang zu dokumentieren.	2 unwahrscheinlich	4 schwer
42	Der Stand der Technik im Bereich Loss Prevention im Handel wird bei der Datenvernichtung nicht angewendet	5 sehr wahrscheinlich	4 schwer	Die Sicherung von Behältern mit Datenträgern personenbezogener Daten, erfolgt am gleichen Stand der Technik, wie der Schutz von wertvollen Gütern im Transportgewerbe (Versiegelung, Protokollierung, elektroniche Überwachung, etc.).	2 unwahrscheinlich	4 schwer

Abbildung 29: Maßnahmen an der Sammelstelle und im Lager des Dienstleister Teil 1

Damit ist der Dienstleister die **Behälterintegrität bis zur wirklichen Vernichtung** sicherzustellen und der Verbleib der Datenträger bis dahin auch zu verfolgen.

Die **exakte Vernichtungszeit eines bestimmten Behälterinhaltes** sollte dementsprechend dokumentiert werden.

Aber auch ein **dokumentiert vollständig entleerter Behälter** muss in seiner Integrität bis zur Neuaufstellung überwacht werden. Aus diesem Grund empfehle ich die dokumentierte Versiegelung entleerter Behälter ebenso wie die dokumentierte Öffnung und Vernichtung der Behälterinhalte.
Der Zugriff für Unbefugte muss mit geeigneten Maßnahmen am Stand der Technik verhindert werden, andernfalls wird meiner Meinung nach den Erfordernissen der DSGVO / DSG hier nicht Rechnung getragen.
Damit entsteht sonst für die verpflichteten Unternehmen ein Sanktionsrisiko durch die Behörde.

43	Die Behälterverfolgbarkeit innerhalb der Lagerstätte bis zur Vernichtung ist nicht sichergestellt	3 möglich	3 mittel	Die Sicherung von Behältern mit Datenträgern personenbezogener Daten, erfolgt am gleichen Stand der Technik, wie der Schutz von wertvollen Gütern im Transportgewerbe (Versiegelung, Protokollierung, elektroniche Überwachung, etc.)	2 unwahrscheinlich	3 mittel
44	Der Zeitpunkt der Vernichtung eines bestimmten Behälterinhaltes ist nicht klar bestimmbar (Zeitstempel)	4 wahrscheinlich	3 mittel	Alle Sammelstellen des Dienstleisters, an welchen Datenträgern mit personenbezogenen Daten zu Vernichtung übernommen werden müssen über Mindeststandards der physischen Sicherheit verfügen: Alrmanlage, Zutrittskontrolle, Videoüberwachung der Zutrittsbereiche und im Bereich der Behälteröffnung, Entleerung, des Shreddervorganges und des Behälterverschlußes. Darüberhinaus ist der Behälter Ein- und Ausgang zu dokumentieren.	1 fast unmöglich	3 mittel
47	Die Behälterintegrität von ordnungsgemäß entleerten Behältern ist nicht gewährleistet	5 sehr wahrscheinlich	4 schwer	Die Sicherung von Behältern mit Datenträgern personenbezogener Daten, erfolgt am gleichen Stand der Technik, wie der Schutz von wertvollen Gütern im Transportgewerbe (Versiegelung, Protokollierung, elektroniche Überwachung, etc.)	1 fast unmöglich	4 schwer

Abbildung 30: Maßnahmen an der Sammelstelle und im Lager des Dienstleisters Teil 2

Die **Verhinderung des Unbefugten Zugriffs** auf Datenträgen mit personenbezogenen Daten rechtfertigt Aufwendungen für die Verantwortlichen, da die damit verbundenen Sanktionen massive Auswirkungen auf den Erfolg ihrer Unternehmen haben können.

48	Unbefugte erhalten Zugriff auf den Behälterinhalt	3 möglich	4 schwer	Die Sicherung von Behältern mit Datenträgern personenbezogener Daten, erfolgt am gleichen Stand der Technik, wie der Schutz von wertvollen Gütern im Transportgewerbe (Versiegelung, Protokollierung, elektroniche Überwachung, etc.)	1 fast unmöglich	4 schwer
50	Nicht sicherheitsüberprüfte Mitarbeiter_innen haben Zugriff zu zu vernichtenden Datenträgern	3 möglich	4 schwer	Personen (in der Sammelstelle des Dienstleisters) mit möglichem Zugriff auf personenbezogene Daten werden einer jährlichen Sicherheitsüberprüfung unterzogen, Gehaltspfändungen führen ebenso wie Suchtkrankheiten zum Verlust der Zuverlässigkeit. Nicht Sicherheitsüberprüfte MitarbeiterInnen erhalten keinen Möglichkeit zum Zugriff auf personenbezogene Daten.	1 fast unmöglich	4 schwer

Abbildung 31: Maßnahmen an der Sammelstelle und im Lager des Dienstleisters Teil 3

4.1.10.7 Maßnahmen bei der Datenträgervernichtung (beim Dienstleister)

Risiko Nr.	Datenträgervernichtung beim Dienstleister	Eintritts-wahrscheinlichkeit	Auswirkung	Maßnahme	NEUE Eintritts-wahrscheinlichkeit	Auswirkung
53	Die Öffnung eines bestimmten Kundenbehältrs wird nicht spezifisch überwacht und dokumentiert	5 sehr wahrscheinlich	4 schwer	Alle Sammelstellen des Dienstleisters, an welchen Datenträgern mit personenbezogenen Daten zu Vernichtung übernommen werden müssen über Mindeststandards der physischen Sicherheit verfügen: Alrmanlage, Zutrittskontrolle, Videoüberwachung der Zutrittsbereiche und im Bereich der Behälteröffnung, Entleerung, des Shreddervorganges und des Behälterverschlußes. Darüberhinaus ist der Behälter Ein- und Ausgang zu dokumentieren.	1 fast unmöglich	4 schwer
54	Die vollständige Einbringung des Behälterinhaltes in den Shredder wird nicht sichergestellt und überwacht	3 möglich	4 schwer	Alle Sammelstellen des Dienstleisters, an welchen Datenträgern mit personenbezogenen Daten zu Vernichtung übernommen werden müssen über Mindeststandards der physischen Sicherheit verfügen: Alrmanlage, Zutrittskontrolle, Videoüberwachung der Zutrittsbereiche und im Bereich der Behälteröffnung, Entleerung, des Shreddervorganges und des Behälterverschlußes. Darüberhinaus ist der Behälter Ein- und Ausgang zu dokumentieren.	1 fast unmöglich	4 schwer

Abbildung 32: Maßnahmen bei der Datenträgervernichtung beim Dienstleister Teil1

Bei der effektiven Datenträgervernichtung ist durch **geeignete Maßnahmen die Sicherstellung der Integrität und Nachverfolgbarkeit bis zur tatsächlichen Datenträgervernichtung** zu gewährleisten.

Viele Maßnahmen, welche bereits erwähnt wurden haben Auswirkungen bis zu diesem letzten Vernichtungsschritt und müssen bis zu diesem finalen Prozessschritt beibehalten werden.

55	Es gibt keine Dokumentation über den effektiven Shredderprozess (Videoarchiv, Kameraposition, Zeitstempel, Behälteidentifikation)	5 sehr wahrscheinlich	4 schwer	Alle Sammelstellen des Dienstleisters, an welchen Datenträgern mit personenbezogenen Daten zu Vernichtung übernommen werden müssen über Mindeststandards der physischen Sicherheit verfügen: Alrmanlage, Zutrittskontrolle, Videoüberwachung der Zutrittsbereiche und im Bereich der Behälteröffnung, Entleerung, des Shreddervorganges und des Behälterverschlußes. Darüberhinaus ist der Behälter Ein- und Ausgang zu dokumentieren.	1 fast unmöglich	4 schwer

Abbildung 33: Maßnahmen bei der Datenträgervernichtung beim Dienstleister Teil 2

Damit wurden in allen analysierten Prozessschritten, mit den vorgeschlagenen Maßnahmen am Stand der Technik, für alle nicht akzeptierbaren oder besonders zu überwachenden Restrisiken an der Grenze zu nicht akzeptierbaren Risiken Prozessbewältigungsstrategien/Maßnahmen vorgestellt.

D.h. bei gleichbleibender Auswirkung konnte durch Senkung der Eintrittswahrscheinlichkeit aus nicht akzeptierbaren Risiken, akzeptierbare Risiken gemacht werden.

Aber erst die laufende Überwachung, ggf. Adaptierung und laufende Auditierung dieser Maßnahmen, wie es zum Beispiel die untersuchten normierten Managementsysteme ISO 9001, ISO 310001, ISO 27001 vorsehen, stellen Maßnahmen am Stand der Technik zur Reduzierung des Sanktionsrisikos im strafrechtlichen Sinn dar.

4.1.11 Auswirkungen der Risikobewältigungsmaßnahmen am fiktiven Fallbeispiel

Alle bekannten Risiken wurden durch die diversen im Fallbeispiel ergriffenen Maßnahmen bezüglich Eintrittswahrscheinlichkeit auf ein akzeptierbares Ausmaß reduziert und damit bewältigt.

Auswirkung -> Eintrittswahrscheinlichkeit	sehr gering	gering	mittel	schwer	existenzbedrohend
sehr wahrscheinlich					
wahrscheinlich	57				
möglich			13,14,19,44		
unwahrscheinlich	56		5,9,**6,16,17,20, 21, 22, 24, 25, 43**	4,7,8,10,11,18,28,37, 38,40,41,45,46,49, 51,52,**1,2,3,12,15, 23,34,35,36,39,42, 43**	
fast unmöglich		**26, 27**	**29,44**	**30,31,32,33,47, 48, 50, 53, 54, 55**	

Abbildung 34: Risikomatrix nach entsprechenden Risikominimierungsmaßnahmen

4.2 Schlussfolgerungen aus der Bearbeitung des Fallbeispiels für die Forschungsfrage

4.2.1 Risikoanalyse nach ISO 31000 bzw. ONR 49001

Die systematische Risikoanalyse nach dem normierten Verfahren der ISO 31000 bzw. der ISO 49001 ist ein effektives Instrument zur Ermittlung von Prozessschwachstellen.

Die schrittweise Erarbeitung von Schutzzielen - basierend auf den jeweiligen Sanktionsrisiken bestimmter Gesetze -, die Durchleuchtung vorhandener Prozesse auf Schwachstellen, Ermittlung von Risiken, Bewertung von Risiken und Festlegung von Maßnahmen ist ein gut geeigneter Ansatz zur Analyse von Datenverarbeitungs- (oder Datenvernichtungsprozessen) im Geltungsbereich der DSGVO / DSG.

4.2.2 Integrierte Managementsysteme auf Basis der Logik der ISO 9001:2015

Integrierte Managementsysteme, welche die Risikominimierung für Unternehmen und die Prozessrisikominimierung als gemeinsames Ziel haben ermöglichen den Aufbau einer prozessorientierten Organisation mit dem Vorteil der Sicherstellung von Compliance und Governance-erfordernissen innerhalb eines gemeinsamen Prozesses mit allen anderen Managementrelevanten Systemen und gleichzeitig die Erreichung der Schutzziele der DSGVO / DSG.

Durch den Einsatz solcher normierter Managementsysteme können organisatorische und personelle Maßnahmen zur Risikominimierung in Prozesse integriert und überwacht werden ohne ein paralleles Managementsystem aufbauen zu müssen.

4.2.3 ISO 27001 Informationssicherheitsnorm

Die ISO 27001 bietet mit dem Anhang A ein gutes Instrument zur Prüfung der Informationssicherheit im Sinne DSGVO /DSG im gegenständlichen Fallbeispiel. insbesondere da es bei der Datenvernichtung primär um Informationsschutz und nicht um die Sicherheit von Datenverarbeitungsprozessen geht.

Unternehmen, welche ISO 27001 zertifiziert sind benötigen konsequenterweise ein Datenvernichtungsverfahren, welches den hohen Erfordernissen dieser Norm gerecht wird.

Bei der Ausarbeitung der Prozessrisiken im Fallbeispiel wurde im Rahmen des Brainstormings der Anhang A der ISO 27001 als Checkliste für die Prüfung des Datenvernichtungsprozesses genutzt. Der Einsatz kann wertvolle Anregungen für Risikoszenarien liefern.

4.2.4 DIN 66399 Norm für Datenvernichtungsprozesse

Die DIN 66399 teilt sich in mehrere Unternormen.:

Derzeit haben jedoch nur die DIN 66399-1 "Grundlagen und Begriffe" und die DIN 66399-2 "Anforderung an Maschinen zur Vernichtung von Datenträgern" Normenstatus.[126]

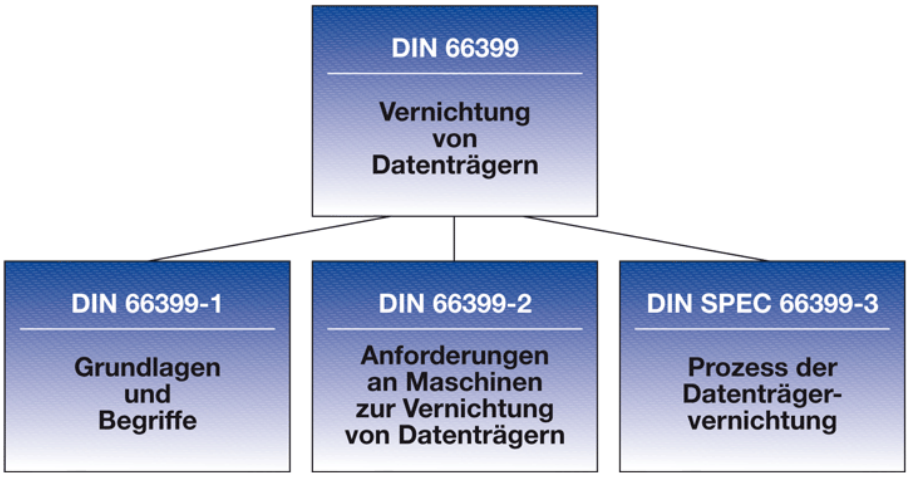


Abbildung 35: Unternormen der DIN 66399 *documentus*, DIN 66399 (Stand: 16.9.2018, https://din66399.de)

[126] *documentus*, DIN 66399 (Stand: 16.9.2018, https://din66399.de)

Die Norm DIN SPEC 66399-3 ist eine Vornorm, welche den Prozess der Datenträgervernichtung spezifiziert. Zahlreiche deutsche Unternehmen verfügen bereits über die Zertifizierung gemäß dieser Vornorm [127]

Die Durchsicht eines mir zugänglichen realen Prüfprotokolls gemäß DIN SPEC 66399-3 **bestätigt meine Risikoanalyse auch bei einem nach dieser Norm zertifizierten Unternehmen**, einige nach den Verfahren 4.2.1 bis 4.2.3 festgestellte Risiken, wurden im Rahmen der DIN SPEC 66399-3 Prüfung eines deutschen Unternehmens nicht ausreichend berücksichtigt[128]:

- Insbesondere erfolgte im gegenständlichen Fall **keine mechanische oder elektronische Versiegelung** der Sammelbehälter
- Das **IKS in Form eines 4 Augenprinzips** (real oder elektronisch) dürfte nicht gewährleistet sein
- Das **Schlüsselmanagement und die Sicherheit des Schlüsselsystems** dürfte nicht spezifisch geprüft worden sein, stellt aber ein relevantes Risiko dar.
- Die **sichtbare Nummerierung** von Behältern sollte bezüglich Pseudonymisierung verändert werden (zusätzlicher Schutzfaktor gegen Behälterzuordnung durch Unbefugte)
- Das physische Sicherheitskonzept konnte auf Basis des Prüfberichtes nicht beurteilt werden.
- Die wesentliche Schwachstelle des Prozesses liegt damit bei Maßnahmen zur Verhinderung menschlichen Versagens auf Mitarbeiter_innen Seite.

Die Qualität der Zertifizierung gemäß DIN SPEC 66399-3 ist abhängig von der Auditqualität und dem Sachverständnis des jeweiligen Auditors bezüglich dem aktuellen Stand der Technik im Bereich Physischer Sicherheit.

Auf Grund meiner bisherigen Erfahrungen gehe ich davon aus, dass das Sicherheitsniveau des geprüften Betriebes, dennoch als überdurchschnittlich zu beurteilen ist!

---

[127] *documentus*, DIN 66399 (Stand: 16.9.2018, https://din66399.de)

[128] BFUB, Prüfbescheinigung Veolia (2017)

4.2.5 ONR 19 20 50 Compliance

Die Zertifizierung der ONR 192050 garantiert seinen Stake Holdern ein erhöhtes Bewusstsein des zertifizierten Unternehmens für Compliance. Damit ist die Bewertung von strafrechtlichen Sanktionsrisiken im zertifizierten Unternehmen von besonderer Bedeutung.

Eine entsprechende Risikoanalyse - mit darauf fokussierten Schutzzielen - gemäß ISO 31000 liefert ein geeignete Bewertung allfälliger Sanktionsrisiken aus der Verletzung von Gesetzen und Selbstverpflichtungen und geeignete Maßnahmen zur Risikominimierung nicht akzeptierbarer Risiken.

5 Zusammenfassung meiner Erkenntnisse

Um **Sanktionsrisiken für den Verband aus der DSGVO / DSG** im Zusammenhang mit Datenträgern in Papierform zu **minimieren** empfehle ich

- Dienstleistern im Datenvernichtungsbereich die **Durchführung geeigneter Risikoanalysen gemäß ISO 31.000 bzw. ONR 49001**
- Lösungen zur Datenvernichtung durch und bei Dienstleistern sollten auch die **Prozesse und Maßnahmen des Kunden zur Erreichung der gemeinsamen Schutzziele unterstützen** um die Total Cost of Compliance auf Auftraggeber- und Dienstleisterseite zu reduzieren. Vertragliche Regelung ist entscheidend!
- Die **Nutzung der ISO 27001 Anhang A** kann bei der Risikobeurteilung in Zusammenhang mit **Informationssicherheitsrisiken** bei der Vernichtung von Datenträgern mit personenbezogenen Daten unterstützen.
- **Integrierte Managementsysteme**, welche durch die **Systematik der ISO 9001:2015** vereint werden, reduzieren durch Prozessklarheit, Überwachung von Prozessrisiken und laufende Entwicklung das Sanktionsrisiko und mittelfristig die Total Cost of Compliance. Alle können sich einer gemeinsamen Risikoanalyse bedienen und die **Umsetzung von Risikominimierungsmaßnahmen gewährleisten**.
- Die Qualität einer Zertifizierung hängt auch von den Kompetenzen der involvierten Prüfer_innen ab. **Die Kompetenz der eingesetzten Prüfer_innen im Bereich intentionaler Risiken ist zu verifizieren**. **Auditberichte stellen eine adäquate Informationsquelle dar.**
- Der **Dienstleistungsprozess** (und die damit verbundenen Zertifizierungen) **der Datenvernichtungsdienstleister** sollte durch Verantwortliche auf Grund der gewonnen Erkenntnisse individuell überprüft werden.

Unternehmen ohne entsprechend zertifizierte Maßnahmen sollten nicht beauftragt werden.

6 Literaturverzeichnis

Andrlik, Die Risikoanalyse und -bewertung in der Praxis der Gefährdungsbeurteilung von Arbeitsplätzen., Bergische Universität Wuppertal (2012)

Austrian Standards, Nutzen von Standards - AUSTRIAN STANDARDS, 15.09.2018 <https://www.austrian-standards.at/ueber-standards/nutzen-von-standards/>, aufgerufen am 15.09.2018

BaFin, Solvency II, 16.09.2018 <https://www.bafin.de/DE/Aufsicht/VersichererPensionsfonds/Aufsichtsregime/SolvencyII/solvency_II_node.html>, aufgerufen am 16.09.2018

Bergauer, Datenschutzgrundverordnung - Das neue Datenschutzrecht in Österreich und der EU, Manz, WIen 2016

——, Das materielle Computerstrafrecht, Jan Sramek Verlag 2016

BFUB, Pruefbescheinigung_Aktenvernichtung_Rostock_DIN_66399.pdf, 05.2017

BMI (DE), Schutz Kritischer Infrastrukturen - Basisschutzkonzept - Empfehlungen für Unternehmen, 2005

Brühwiler, Risikomanagement als Führungsaufgabe - Umsetzung bei strategischen Entscheidungen und operationellen Prozessen[4], Haupt, Zürich 2016

Collinsdictionary, Loss prevention Definition und Bedeutung | Collins Wörterbuch, 16.09.2018 <https://www.collinsdictionary.com/de/worterbuch/englisch/loss-prevention>, aufgerufen am 16.09.2018

DIN, DIN_EN_ISO_22301:2014 idF 12 2014, 12.06.2018

DNVGL, TAPA Zertifizierung für alle 4 TAPA-Standards: FSR, TSR, PSR & TACSS, 16.09.2018 <https://www.dnvgl.de/services/zertifizierung-nach-den-tapa-standards-4345>, aufgerufen am 16.09.2018

documentus, REISSWOLF-DIN66399-Zertifikat-München.pdf, 12.02.2016

——, documentus | Informationsdarstellung der Originalgröße, 16.09.2018 <https://din66399.de/tabelle-a-01.html>, aufgerufen am 16.09.2018

——, DIN 66399 | documentus | Die neue DIN-Norm zur Datenträgervernichtung, 16.09.2018 <https://din66399.de>, aufgerufen am 16.09.2018

——, Datenvernichtung | documentus, 16.09.2018 <https://documentus.de/datenvernichtung/>, aufgerufen am 16.09.2018

EU, MRL Maschninenrichtline, 29.06.2006

——,
RICHTLINIE (EU) 2016/ 680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 27. April 2016 - zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/ 977/ JI des Rates, 28.04.2016

——,
VERORDNUNG (EU) 2016/ 679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES - vom 27. April 2016 - zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/ 46/ EG (Datenschutz-Grundverordnung), 25.05.2018

EUROPOL, SOCTA 2017 - Serious and organised Crime threat Assessment - European Union, 2017

Hirner, Compliance sichert den Wert des Unternehmens" - AUSTRIAN STANDARDS, 2014 <https://www.austrian-standards.at/ueber-standards/nutzen-von-standards/nutzen-in-der-wirtschaft/kaerntner-energiedienstleister-kelag/>, aufgerufen am 13.09.2018

Hödl, Datenschutzgrundverordnung, Manz, Wien 2017

Hotter/Lunzer/Schick/Soyer, Unternehmensstrafrecht - eine Praxisanleitung 12, nwV Verlag, Wien - Graz 2010

Kienapfel/Höpfel/Kert, Strafrecht Allgemeiner Teil[15], MANZ´sche Verlags-und Universitätsbuchandlung, Wien 2016

kiwa, ISO 9001:2015 Die Änderungen im Überblick, 2016 <https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf>, aufgerufen am 13.09.2018

Krystek, Definition: Risikomanagement, 15.09.2018 <https://wirtschaftslexikon.gabler.de/definition/risikomanagement-42454>, aufgerufen am 15.09.2018

Müller, ESET-DSGVO-SIHK_Hagen-data.pdf, 21.02.2018

ONR, ÖNORM ISO 27001:2005 idF 1.3.2008, 01.03.2008

——, ÖNORM S 2403 - Business Continuity and Corporate Security Management — Corporate Security Management, 01.05.2009

——, ONR 49001:2014 Risikomanagement für Organisationen, 2014

——, ÖNORM EN ISO 9001 idF 15.11.2015, 15.11.2015

papershred, Gesetze und Normen für die Vernichtung von Daten und Akten, 15.09.2018 <https://papershred.de/service/gesetze-normen/>, aufgerufen am 15.09.2018

PricewaterhouseCoopers, Willkommen in der Welt von „Basel IV“, 16.09.2018 <https://www.pwc.at/de/branchen/financial-services/willkommen-in-der-welt-von-basel-iv.html>, aufgerufen am 16.09.2018

Rechnungshof, Positionen_2016_03.pdf, 2016

Republik Österreich, Bundesgesetz zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Datenschutzgesetz – DSG) StF: BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.) [CELEX-Nr.: 395L0046], 01.01.2000

——, BGBl. 60/1974 idF BGBl 136/2004, 01.01.2005

——, Bundesgesetz über die Verantwortlichkeit von Verbänden für Straftaten (Verbandsverantwortlichkeitsgesetz – VbVG) StF: BGBl. I Nr. 151/2005 (NR: GP XXII RV 994 AB 1077 S. 122. BR: AB 7387 S. 725.) [CELEX-Nr. 32003L0006], Jänner.2006

——, InfoSIG Informationssicherheitsgesetz - Bundesrecht konsolidiert, Fassung vom 16.09.2018, 25.05.2018

——, InfoSiV BGBl II 548/2003 idF 16.9.2018

Rheinland, Informationssicherheit ISO 27001, 2018 <https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html>, aufgerufen am 13.09.2018

Schmidhuber, ISO 27001 zertfizierte Unternehmen - Österreich - iso-27001.at, ISO 27001 Managment Consulting, 2018

Schmidl, Leitfaden VO (EU) 2016/679 DSGVO, 2017

Schmitt, Integrierte Managementsysteme (IMS): der Geheimtipp zur Verbesserung der Unternehmensperformance, DGQ - Deutsche Gesellschaft für Qualität - Blog, 28.03.2017

Schulthess, Risikomanagement als Führungsaufgabe (Brühwiler, Bruno) - Schulthess Buchhandlungen - Kommentare, Repetitorien, Fachinformationen, 12.09.2018 <https://www.schulthess.com/buchshop/detail/ISBN-9783258079639/Bruehwiler-Bruno/Risikomanagement-als-Fuehrungsaufgabe>, aufgerufen am 12.09.2018

SGSGroup, The ISO Survey of Management System Standard Certifications 2015, 2015 <https://www.sgsgroup.com.hk/en/news/2016/10/2015-iso-survey-results>, aufgerufen am 13.09.2018

SoxOnline, Risks and Controls, Sox-Online, 16.09.2018

Taleb, Der Schwarze Schwan - Die Macht höchst unwahrscheinlicher Ereignisse[1], Knaus, München 2015

TUEVSued, TUEVSued Zertifizierte Datenträgervernichtung, 16.09.2018

——, 01375-28561-tuev-grafik-din-broschuere.pdf, 16.09.2018 <https://www.tuev-sued.de/uploads/images/14634693674682225500 66/01375-28561-tuev-grafik-din-broschuere.pdf>, aufgerufen am 16.09.2018

Tyco, Einzelhandelslösungen | Tyco, 16.09.2018 <https://www.tyco.de/loesungen/retail/>, aufgerufen am 16.09.2018

7 Abbildungsverzeichnis

Abbildung 1: Zusammenfassung der 2015 ISO Befragung OV, The ISO Survey of Management System Standard Certifications 2015, (2015) <https://www.sgsgroup.com.hk/en/news/2016/10/2015-iso-survey-results>, aufgerufen am 13.09.2018 27
Abbildung 2: Abbildung eines Prozessorientierten Qualitätsmanagementsystems *kiwa*, ISO 9001:2015 Die Änderungen im Überblick, 2016 <https://www.kiwa.de/uploadedFiles/Aktuelles/news-Archiv_2016/ISO%209001.pdf>, aufgerufen am 13.09.2018 30
Abbildung 3: IT-Risiken minimieren mit einem ISO 27001 Zertifikat *Rheinland*, Informationssicherheit ISO 27001, (2018) <https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html>, aufgerufen am 13.09.2018 35
Abbildung 4: Kritische Infrastruktur (KRITIS) Vgl. *Rheinland*, Informationssicherheit ISO 27001, (Stand 13.09.2018 https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html) 36
Abbildung 5: Zertifizierungsablauf ISO 27001Vgl. *Rheinland*, Informationssicherheit ISO 27001(Stand 13.09.2018 https://www.tuv.com/germany/de/informationssicherheit-iso-27001.html), ... 37
Abbildung 6: Risikomanagement System mit dem Risikomanagementprozess *ONR,* ONR 49001:2014 Risikomanagement für Organisationen und Systeme (Stand 1.1.2014) 6 39
Abbildung 7: Beispiele für unterschiedliche Zerkleinerungsformen von Papier Pappershred, Gesetze und Normen für die Vernichtung von Daten und Akten (2018) 55
Abbildung 8; Sicherheitsstufen lt. DIN 63399 Documentus,Sicherheitsstufen (Stand 16.09.2018, https://din66399.de/tabelle-a-01.html) 56
Abbildung 9: Evaluierung der richtigen Datenverarbeitung *TUEVSued*, Schritt für Schritt zur Datenträgervernichtung (Stand: 16.9.2018, https://www.tuev-sued.de/uploads/images/1463469367468222550066/01375-28561-tuev-grafik-din-broschuere.pdf) 58

Abbildung 10: Vernichtungsprotokoll gemäß InfoSIV InfoSiV, BGBl II 548/2003 idF 16.9.2018 Anlage 5 61
Abbildung 11: Prüfungsfokus, Risiken und Motivation DIN 66399 TUEVSued, Zertifizierte Datenträgervernichtung (Stand: 16.9.2018, https://www.tuev-sued.de/uploads/images/1408537679236711420086/infoblatt-din-66399-datentraegervernichtung.pdf) 64
Abbildung 12: Prozessvergleich dcumentus documentus, NORMteil 66399-3 (Stand: 16.9.2018, https://din66399.de - Auswahl NORMteil 66399-3 64
Abbildung 13: Sammelbehälter zur Aktenvernichtung documentus, Datenvernichtung (Stand: 16.9.2018, https://documentus.de/datenvernichtung/) 65
Abbildung 14: Erklärung der Leistungen von documentus documentus, Datenvernichtung (Stand: 16.9.2018, https://documentus.de/datenvernichtung/) 65
Abbildung 15: Generelle Schutzziele und Maßnahmen aus der DSGVO Müller, Schutzziele der DSGVO (Stand: 21.2.2018, https://www.sihk.de/blob/haihk24/servicemarken/ueber_uns/erfa_gruppen/fallback1422607240916/4000890/db3451fc7710362ead9459b22774bab1/ESET-DSGVO-SIHK_Hagen-data.pdf) 11 67
Abbildung 16: Schutzziele der DSGVO - Fallbeispiele Müller, Schutzziele der DSGVO (Stand: 21.2.2018, https://www.sihk.de/blob/haihk24/servicemarken/ueber_uns/erfa_gruppen/fallback1422607240916/4000890/db3451fc7710362ead9459b22774bab1/ESET-DSGVO-SIHK_Hagen-data.pdf) 12 68
Abbildung 17: Skalierung Risikoauswirkung in der Risikomatrix 77
Abbildung 18: Skalierung Eintrittswahrscheinlichkeit in der Risikomatrix 78
Abbildung 19: Bewertung der Methoden zur Gefährdungsbeurteilung ANDRLIK, Risikoanalyse in der Praxis (2012) 19f 79
Abbildung 20: Risikobewertung eines fiktiven Datenvernichtungsprozesse 80
Abbildung 21: Risikomatrix mit Risikobewertung ohne geeignete Maßnahmen 81
Abbildung 22: Vertragsseitige Risikominimierungsmaßnahmen 82
Abbildung 23: Organisatorische und personelle Risikominimierungsmaßnahmen 84
Abbildung 24: Maßnahmen am Anfallort der Datenträger 85
Abbildung 25: Maßnahmen an der Sammelstelle beim Auftraggeber 86
Abbildung 26: Maßnahmen während des Transportes Teil1 87

Abbildung 27: Maßnahmen während des Transportes Teil 2 88
Abbildung 28: Stand der Sicherheitstechnik im Einzelhandel *TYCO*, Einzelhandelslösungen (Stand: 16.9.2018, https://www.tyco.de/loesungen/retail/) 90
Abbildung 29: Maßnahmen an der Sammelstelle und im Lager des Dienstleister Teil 1 91
Abbildung 30: Maßnahmen an der Sammelstelle und im Lager des Dienstleisters Teil 2 92
Abbildung 31: Maßnahmen an der Sammelstelle und im Lager des Dienstleisters Teil 3 92
Abbildung 32: Maßnahmen bei der Datenträgervernichtung beim Dienstleister Teil1 93
Abbildung 33: Maßnahmen bei der Datenträgervernichtung beim Dienstleister Teil 2 94
Abbildung 34: Risikomatrix nach entsprechenden Risikominimierungsmaßnahmen 95
Abbildung 35: Unternormen der DIN 66399 *documentus*, DIN 66399 (Stand: 16.9.2018, https://din66399.de) 97