MASTERARBEIT

zur Erlangung des akademischen Grades

Master of Arts in Business

am Masterstudiengang Rechnungswesen & Controlling

der FH CAMPUS 02

Konzeption eines Tools zur Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DSGVO

Betreuer:

DI Dr. Christian Weißensteiner

vorgelegt von:

Susanne Esser, BA (1710532001)

Graz, 26.04.2019

Ehrenwörtliche Erklärung

Ich erkläre ehrenwörtlich, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen nicht benutzt und die den Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe. Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht. Die vorliegende Fassung entspricht der eingereichten elektronischen Version.

Graz, 26.04.2019 Susanne Esser, BA, eh

Kurzfassung

Um den Schutz personenbezogener Daten europaweit sicherzustellen und den EU-Bürgern mehr Kontrolle über diese Daten zu geben, wurde am 25. Mai 2018 die Datenschutz-Grundverordnung (DSGVO) in Kraft gesetzt. Der Kooperationspartner, die Raiffeisen-Landesbank Steiermark AG, ist aufgrund seiner Kerntätigkeit, welche die Verarbeitung von personenbezogenen Daten einschließt, von dieser Verordnung betroffen und zur konformen Umsetzung verpflichtet. Eine wesentliche Neuerung stellt die Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO dar, mit welcher sich die Verfasserin dieser Arbeit näher auseinandersetzt.

Die Arbeit untersucht, wie ein Tool zur Durchführung von DSFAs für den Kooperationspartner konzipiert werden kann, um diesen hinsichtlich DSGVO-Konformität zu unterstützen. Für die Raiffeisen-Landesbank Steiermark AG ist die Klärung der Hauptfrage der Arbeit von großer Bedeutung, da sie aufgrund der DSGVO dazu verpflichtet ist, DSFAs kontinuierlich durchzuführen. Des Weiteren drohen hohe Strafen bei einer nicht ordnungsgemäßen Umsetzung der DSGVO, welche bei der Fälligkeit einen erheblichen Einfluss auf das Jahresergebnis hätten. Außerdem kann die nicht konforme Umsetzung der DSFA einen Reputationsschaden zur Folge haben. Mit Hilfe des Tools kann der Kooperationspartner die DSFAs in Zukunft effizienter durchführen. Dadurch können in weiterer Folge datenschutzrechtliche Sanktionen und damit verbundene Strafzahlungen vermieden werden. Zudem soll die Masterarbeit aufzeigen, welche TOP-5-Risiken in Bezug auf Datenschutz und Datensicherheit beim Kooperationspartner existieren und mit welchen Maßnahmen diese reduziert werden können.

Der Aufbau der Masterarbeit unterteilt sich in einen Theorie- und einen Praxisteil. Im Theorieteil setzt sich die Verfasserin zu Beginn mit der DSGVO auseinander, um ein kohärentes Gesamtverständnis der Arbeit zum Thema DSFA zu ermöglichen. In weiterer Folge wird auf die Vorgehensweise bei der Durchführung von DSFAs eingegangen, um den bestmöglichen Aufbau des Tools sicherstellen zu können. Das nächste Kapitel soll den Datenschutz-Risikomanagementprozess näher beleuchten, da das Hauptaugenmerk der DSFA auf diesen gerichtet ist. Im Praxisteil der Masterarbeit wird zunächst die Vorgehensweise bei der Konzeption des Tools detailliert beschrieben. Danach wird erläutert, wie bei der Durchführung der einzelnen DSFAs in der Raiffeisen-Landesbank Steiermark vorgegangen wurde. Daran anknüpfend erfolgt eine Beschreibung der vorgenommenen Workshops und deren Ergebnisse für die sechs identifizierten Verarbeitungstätigkeiten. Auch der Workshop mit dem IT-Experten der Raiffeisen-Landesbank Steiermark AG findet Erwähnung. Abschließend werden die TOP-5-Risiken der Raiffeisen-Landesbank Steiermark AG aufgezeigt.

Abstract

In order to ensure the protection of personal data throughout Europe and to give EU citizens more control over these data, the General Data Protection Regulation (GDPR) came into force on 25 May 2018. The cooperation partner, Raiffeisen-Landesbank Steiermark AG, is affected by the GDPR and its compliant implementation due to its core activity, which includes the processing of personal data. A major innovation is the Data Protection Impact Assessment (DPIA) according to Art. 35 GDPR, with which the author deals with this work in more detail.

The paper explores how to design a tool to conduct DPIAs for the collaborator to help them with GDPR compliance. For Raiffeisen-Landesbank Steiermark AG, the clarification of the main issue of the work is of great importance, because now there exists a legal obligation to continuously carry out a DPIA. Furthermore, severe penalties in the event of improper implementation of the GDPR, which would have a considerable influence on the annual result at maturity, are threatened. In addition, the non-compliant implementation of DPIAs may result in reputational damage. With the help of the tool, the cooperation partner can carry out the data protection impact assessments more efficiently in the future. As a result, data protection sanctions and related penalties can subsequently be avoided. Furthermore, the Master thesis shows which TOP 5 data protection and data security risks exist at the cooperation partner and how these can be reduced.

The structure of the Master's thesis is divided into a theoretical and a practical part. In the theoretical part, the author starts with the GDPR to enable a coherent overall understanding of the work on the topic of DPIA. Subsequently, the procedure for the implementation of DPIAs will be discussed in order to ensure the best possible structure of the tool. The next chapter is intended to shed more light on the privacy risk management process, as DPIAs main focus is on it. In the practical part of the master thesis, the procedure for the conception of the tool is first described in detail. It then explains how the individual data protection impact assessments were conducted at Raiffeisen-Landesbank Steiermark. Then the workshops and their results for the six identified processing activities are described. The workshop with the IT expert of Raiffeisen-Landesbank Steiermark AG is also mentioned. Finally, the TOP 5 data protection and data security risks of Raiffeisen-Landesbank Steiermark AG are shown.

Inhaltsverzeichnis

Anhangsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BDSG	Bundesdatenschutzgesetz
DSB	Datenschutzbeauftragter
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutzgrundverordnung
FMA	Finanzmarktaufsicht
OeNB	Österreichische-Nationalbank

1. Einleitung

Der Schutz personenbezogener Daten stellt ein grundlegendes Persönlichkeitsrecht dar, welches bereits in Art. 8 Abs. 1 der Charta der Grundrechte der Europäischen Union verankert ist und mit dem Recht auf Achtung des Privatlebens gem. Art. 7 der Charta der Grundrechte der Europäischen Union eng verbunden ist. Um den Schutz personenbezogener Daten europaweit sicherzustellen und den EU-Bürgern mehr Kontrolle über diese Daten zu geben, wurde am 25. Mai 2018 die Datenschutz-Grundverordnung (DSGVO) in Kraft gesetzt. Diese Verordnung stellt das Kooperationsunternehmen, die Raiffeisen-Landesbank Steiermark AG, aufgrund der zahlreichen neuen Vorgaben vor enorme Herausforderungen.

Die vorliegende Masterarbeit befasst sich mit einer wesentlichen Neuerung der DSGVO, der sogenannten Datenschutz-Folgenabschätzung (DSFA) gemäß Art. 35 DSGVO. Diese fordert unter anderem ein Datenschutz-Risikomanagement für die Rechte und Freiheiten von betroffenen Personen basierend auf den Geschäftsprozessen, in denen personenbezogene Daten verarbeitet werden. Der Schwerpunkt dieser Arbeit liegt auf der Konzeptionierung eines Tools zur Durchführung von DSFAs.

1.1. Spezifische Ausgangssituation

Die Raiffeisen-Landesbank Steiermark AG ist das Spitzeninstitut der Raiffeisen-Bankengruppe Steiermark. Gemeinsam mit den 60 selbständigen steirischen Raiffeisenbanken und insgesamt 257 Bankstellen ist sie die führende Bankengruppe in Südösterreich. Als "Bank für Banken" fungiert sie sowohl als Geldausgleichsstelle als auch als Berater der Raiffeisen Bankengruppe.

Täglich werden in der Raiffeisen-Landesbank Steiermark AG im Rahmen von ca. 250 Geschäftsprozessen personenbezogene Daten mit unterschiedlicher Zweckbindung verarbeitet. Bereits im Vorfeld wurden die relevanten Geschäftsprozesse mit den jeweiligen Prozesseignern in Interviews durch den jeweiligen Prozesscoach identifiziert und im Anschluss in einer Prozesslandkarte dargestellt. Die Geschäftsprozesse wurden in Kernprozesse, Unterstützungsprozesse und Managementprozesse untergliedert. Der Kooperationspartner ist aufgrund seiner Kerntätigkeit, welche die Verarbeitung von personenbezogenen Daten einschließt, von der DSGVO und deren konformen Umsetzung betroffen.

Eine wesentliche Neuerung aufgrund der DSGVO stellt die DSFA für die Raiffeisen-Landesbank Steiermark AG dar. Der Schwerpunkt dieser liegt auf dem Datenschutz-Risikomanagement. Bis dato existierte bereits ein Risikobewusstsein, jedoch wurde aufgrund von Ressourcenmangel und Kapazitätsengpässen noch kein systematischer Risikomanagementprozess in der

Abteilung „Datenschutz und Datenmanagement“ umgesetzt. Bis jetzt wurden für jeden Geschäftsprozess im Rahmen von Interviews nur das Risiko einer Kreditschädigung, das Risiko einer betrügerischen Verwendung der Daten, das Risiko einer Diskriminierung und das Risiko aus der Bedrohung der persönlichen Sicherheit ermittelt. Weitere Risiken für die Rechte und Freiheiten der betroffenen Personen, die in der Fachliteratur Erwähnung finden, wurden im Rahmen der Risikoidentifikation bisher nicht berücksichtigt.

Im Rahmen der Risikobeurteilung sind die Kriterien für die Eintrittswahrscheinlichkeit und die Auswirkung noch zu konkretisieren. Im Hinblick auf die Risikosteuerung existiert bereits ein Maßnahmenkatalog, jedoch ist dieser auf Verbesserungsmöglichkeiten zu überprüfen.

1.2. Problemstellung und Forschungsfragen

Aufgrund der rechtlichen Verpflichtung zur Durchführung einer DSFA soll die Masterarbeit untersuchen, wie ein Tool zur Durchführung einer DSFA für den Kooperationspartner konzipiert werden kann, um die Raiffeisen-Landesbank Steiermark AG hinsichtlich DSGVO-Konformität zu unterstützen. Für den Kooperationspartner ist die Klärung der Hauptfrage der Arbeit von großer Bedeutung, da seit 25. Mai die gesetzliche Verpflichtung zur kontinuierlichen Durchführung einer DSFA besteht.

Des Weiteren drohen hohe Strafen bei einer nicht ordnungsgemäßen Umsetzung der DSGVO. Bei einem DSGVO-Verstoß können 4% des globalen Konzernumsatzes bzw. 20 Millionen Euro, wobei der höhere Betrag maßgeblich ist, sanktioniert werden. Ein DSFA-Verstoß hingegen kann Strafen von 2% des globalen Konzernumsatzes bzw. 10 Millionen Euro nach sich ziehen. Die Fälligkeit einer Strafe hätte einen erheblichen Einfluss auf das Jahresergebnis der Raiffeisen-Landesbank Steiermark AG. Darüber hinaus kann die Nichtdurchführung der DSFA bzw. nicht konforme Umsetzung dieser einen Reputationsschaden zur Folge haben. Sowohl ein nicht ausreichender Schutz der Rechte der betroffenen Personen als auch der personenbezogenen Daten der Kunden könnte eine Kundenabwanderung auslösen.

Um dieses Tool DSGVO-konform zu konzipieren und die einzelnen DSFAs ordnungsgemäß durchführen zu können, soll zunächst eruiert werden, welche rechtlichen Aspekte der DSGVO zu beachten sind, und wann eine DSFA vorgenommen werden muss. Anhand dieser Ergebnisse ist jeder Geschäftsprozess zu überprüfen, um herausfinden zu können, für welche konkreten Geschäftsprozesse beim Kooperationspartner eine DSFA in die Praxis umgesetzt werden soll. Zudem ist die Vorgehensweise bei der Durchführung einer DSFA zu eruieren.

Darauf aufbauend soll sich die Masterarbeit intensiv mit dem Risikomanagementprozess befassen, da dieser der Schwerpunkt der DSFA darstellt. Dabei soll das Datenschutz-

Risikomanagement Erwähnung finden und mit dem klassischen Risikomanagement verglichen werden. Zunächst wird auf die Frage eingegangen, wie die Risiken basierend auf den einzelnen Geschäftsprozessen, die eine DSFA notwendig machen, identifiziert und kategorisiert werden können. In weiterer Folge wird ermittelt, wie diese Risiken beurteilt werden können. Hinsichtlich der Beurteilung sind die Kriterien für die Eintrittswahrscheinlichkeit und die Auswirkung explizit festzulegen. Des Weiteren ist eine Risikomatrix zu erstellen, um eine einheitliche Risikoklassifikation in ein geringes, mittleres und hohes Risiko zu gewährleisten. Die Risikobeurteilung ist notwendig, um eine Risiko-Priorisierung zu ermöglichen. Dadurch können schließlich die TOP-5-Datenschutz- und Datensicherheitsrisiken eruiert werden.

Außerdem soll die Arbeit die Risikosteuerung näher betrachten. Dazu soll ein Maßnahmenkatalog optimiert werden, anhand dessen die Risikoeigner der Geschäftsprozesse passende Maßnahmen für die aggregierten TOP-5-Risiken ableiten können. Anschließend befasst sich die Arbeit mit der Berichterstattung und der Überwachung der DSFA.

1.3. Praxisoutput für den Kooperationspartner

Da der Praxisoutput, das Tool, eine unterstützende Maßnahme zur DSGVO-konformen Umsetzung der DSFA darstellt, kann das Risiko, eine substanzielle Strafe zu erhalten, vermindert werden. Die Relevanz des Tools begründet sich auch dadurch, dass der Prozess zur Durchführung einer DSFA keine einmalige Aufgabe ist, sondern einen kontinuierlichen und revolvierenden Prozess darstellt, der laufender Überarbeitung und Überprüfung bedarf. Außerdem kann die einheitliche, gesetzeskonforme und adäquate Umsetzung der DSFA in die Praxis auf steiermärkische Ebene mit dem Tool ermöglicht werden. Des Weiteren kann der Kooperationspartner mit dem Tool die rechtskonforme Umsetzung der DSGVO gegenüber der Datenschutz-Aufsichtsbehörde nachweisen.

Ansonsten sollen, mit Hilfe des Tools, die Risiken für die Rechte und Freiheiten von natürlichen Personen bestmöglich identifiziert, beurteilt, aggregiert, gesteuert, berichtet und überwacht werden können. Nach Fertigstellung des Tools, zur Durchführung der einzelnen DSFAs, kann der weitere Praxisoutput in mehrere Teilergebnisse untergliedert werden. Das erste Teilergebnis der Arbeit soll die Identifikation der Geschäftsprozesse sein, welche die Durchführung einer DSFA notwendig machen. In weiterer Folge sollen die Risiken für diese Prozesse mit Hilfe von Workshops und dem konzipierten Tool mit den jeweiligen Prozesseignern, welche zugleich auch Risikoeigner sind, ermittelt werden.

Ein weiteres Teilergebnis sollen die ermittelten Kriterien zur Risikobeurteilung darstellen, welche in das Tool integriert werden, um die Risiken während des Fachgesprächs bestmöglich beurteilen zu können. Anhand dieser Kriterien werden die Risiken in den einzelnen Workshops

beurteilt, um die Risiken anschließend priorisieren und die TOP-5-Risiken identifizieren zu können. Danach wird ein weiterer Workshop mit den Prozesseignern durchgeführt, um passende Maßnahmen mit Hilfe des optimierten Maßnahmenkatalogs, welcher auch im Tool auffindbar ist, abzuleiten. Die Ergebnisse der Risikoidentifikation, der Risikobeurteilung und der Risikosteuerung sollen im Tool im Rahmen des DSFA-Berichts Erwähnung finden.

Das Tool und die Masterarbeit befassen sich nicht mit allen Neuerungen der DSGVO, sondern nur mit den Neuerungen zum Thema Risikomanagement sowie der DSFA. Der Praxisoutput beinhaltet keine Empfehlungen zu anderen Neuerungen, wie zum Beispiel dem Verzeichnis der Verarbeitungstätigkeiten. Weiters soll das Tool explizit für die Verarbeitungstätigkeiten der Raiffeisen-Landesbank Steiermark AG konzipiert werden, und soll nicht als generelle Empfehlung für andere Unternehmen dienen. Im Rahmen dieser Arbeit werden die Risiken identifiziert und beurteilt, jedoch werden nur für die TOP-5-Risiken passende Maßnahmen abgeleitet, um den Rahmen dieser Arbeit nicht zu sprengen.

1.4. Aufbau der Arbeit und geplante Methoden

Der Aufbau der Masterarbeit gliedert sich in einen Theorie- und einen Praxisteil, welche in sechs Kapitel abgehandelt werden. Was den Theorieteil anbelangt, so ist hervorzuheben, dass im Rahmen der theoretischen Ausführungen stets – in exemplarischer Form – implizite oder explizite Bezugnahmen zur Raiffeisen-Landesbank Steiermark AG vorgenommen werden. Angestrebt wird im theoretischen Teil zunächst eine tiefgreifende Auseinandersetzung mit der DSGVO, das heißt, basale Aspekte und zentrale Termini, die DSGVO betreffend, werden erläutert. Darauf aufbauend, beleuchtet die Arbeit im nächsten Kapitel wesentliche Grundlagen und die Vorgehensweise für die Durchführung einer DSFA, um ein kohärentes Gesamtverständnis der Arbeit zum Thema DSFA zu ermöglichen.

Das darauf folgende Kapitel soll sich insbesondere dem Datenschutz-Risikomanagementprozess widmen, da auf diesen Prozess das Hauptaugenmerk der Masterarbeit gerichtet ist. In diesem Kapitel findet zunächst die Kategorisierung der Risiken Erwähnung. Anschließend werden die Methoden zur Risikoidentifikation aufgezeigt, kritisch beleuchtet und analysiert. Danach wird auf die Risikobewertung und Risikoaggregation näher eingegangen und dargelegt, wie man die Risiken für die Rechte und Freiheiten der betroffenen Personen, hinsichtlich der Eintrittswahrscheinlichkeit und der Auswirkung, bewerten und aggregieren kann. In weiterer Folge setzt sich die Arbeit mit der Risikosteuerung auseinander, um passende Maßnahmen für die einzelnen Risiken treffen zu können. Abschließend finden das Risikoreporting und die Risikoüberwachung Erwähnung.

Im Praxisteil der Masterarbeit wird zunächst die Konzeptionierung des Tools detailliert beschrieben. Danach wird erläutert, wie bei der Durchführung der einzelnen DSFAs in der Raiffeisen-Landesbank Steiermark vorgegangen wurde. Dabei wird eingangs aufgezeigt, wie die Geschäftsprozesse, die die Durchführung einer DSFA notwendig machen, ausgewählt wurden. Als Zweites wird dargestellt, wie die Risiken mit dem Prozesseigner und dem Prozesscoach für die einzelnen Geschäftsprozesse identifiziert und welche Risiken eruiert wurden. Als Drittes wird beschrieben, wie die Risikobeurteilung durchgeführt wurde und welches Ergebnis daraus resultiert. Die Risikobeurteilung soll dazu dienen, die Risiken zu priorisieren, um schlussendlich die TOP-5-Risiken zu eruieren. Als vierter Punkt soll beleuchtet werden, wie passende Maßnahmen für die Risikosteuerung getroffen wurden und welches Ergebnis die Risikosteuerung liefert. Zuletzt findet Erwähnung, wie der DSFA-Report umgesetzt wurde. Eine Zusammenfassung der wesentlichen Ergebnisse der Arbeit, sowie eine kritische Reflexion und ein Ausblick, befinden sich im finalen Teil der Arbeit.

Um die Inhalte der Masterarbeit ausarbeiten zu können, wird vor der Erstellung der Arbeit eine ausführliche Literaturrecherche vorgenommen, um das Tool zur Durchführung der DSFA, insbesondere den Risikomanagementprozess, DSGVO-konform konzipieren zu können. Im Hinblick auf die Risikoidentifikation, der Risikobeurteilung und der Risikosteuerung, so wird hier die Delphi-Methode angewendet. Des Weiteren werden sechs Workshops mit den Prozesseignern für die ausgewählten Geschäftsprozesse und ein Workshop mit dem IT-Experten der Raiffeisen-Landesbank Steiermark AG abgehalten. Im Rahmen dieser Workshops wird zu Beginn ein Brainstorming durchgeführt. Für die Workshops wird im Vorfeld ein Risk-Assessment-Sheet in das Tool integriert, welches einen Risikokatalog zur Risikoidentifikation beinhaltet.

2. Die Datenschutz-Grundverordnung

In diesem Kapitel werden relevante Begriffe und deren Anwendung auf den Kooperationspartner definiert und analysiert. Danach werden die Grundsätze der DSGVO beleuchtet, da diese das Fundament des Datenschutz-Risikomanagements und des zu konzipierenden Praxisoutputs für die Raiffeisen-Landesbank Steiermark AG bilden. Darauf aufbauend wird auf die zu schützenden Betroffenenrechte eingegangen, da im Rahmen des Datenschutz-Risikomanagements die Risiken für die Rechte und Freiheiten der betroffenen Personen zu berücksichtigen sind.

2.1. Definition und Analyse von Kernbegriffen

Am 14. 04. 2016 wurde die DSGVO vom Europäischen Parlament beschlossen[1] und ist seit dem 25. Mai 2018 in der Europäischen Union wirksam. Die Verordnung ersetzt die bisherige Regelung der Datenschutzrichtlinie aus 1995.[2] Das Ziel der DSGVO ist die Verarbeitung der Daten durch Unternehmen in den EU-Mitgliedstaaten zu vereinheitlichen, um das Datenschutzniveau in den verschiedenen Staaten zu harmonisieren.[3] Bis zum 25. Mai 2018, also vor Inkrafttreten der DSGVO, mussten den Aufsichtsbehörden Verarbeitungstätigkeiten hinsichtlich personenbezogener Daten aufgrund des Datenschutzgesetzes 2000 gemeldet werden. Obwohl die Meldepflicht mit hohem bürokratischem und finanziellem Aufwand verbunden ist, konnte dadurch gemäß Erwägungsgrund 89 DSGVO ein ausreichender Schutz personenbezogener Daten nicht erwirkt werden. Dies führte mit Inkrafttreten der DSGVO zur Abschaffung der Meldepflicht. Diese soll durch zeitgemäße Verfahren ersetzt werden, welche durch die Aufsichtsbehörde überprüft werden.[4]

Die DSGVO wirkt unmittelbar und direkt und geht den einzelnen Rechtsvorschriften der einzelnen Mitgliedstaaten vor. Die Verordnung enthält zahlreiche Öffnungsklauseln, die die nationalen Gesetzgeber verpflichten oder berechtigen, bestimmte Bereiche gesetzlich zu regeln. Daher wird es, neben der DSGVO, auch weiterhin ein österreichisches Datenschutzrecht geben.[5] Die Verordnung ist, anders als das Bundesdatenschutzgesetz (BDSG), kein Auffanggesetz, sondern eine Vorrangregelung.[6]

Die Verordnung gilt für alle Unternehmen und deren Niederlassungen in der Union, die personenbezogene Daten verarbeiten. Des Weitern gilt sie für Unternehmen mit Sitz außerhalb der Europäischen Union, sofern die Verarbeitung von personenbezogenen Daten im

[1] Vgl. MÜHLBAUER (2018), S. 3.
[2] Vgl. GRUBER (2017), S. 243.
[3] Vgl. MATTHEWS (2018), S. 12.
[4] Vgl. KNYRIM (2016), S. 217.
[5] Vgl. GRUBER (2017), S. 243.
[6] Vgl. MÜHLBAUER (2018), S. 6.

Zusammenhang mit dem Angebot von Waren oder Dienstleistungen in der Union steht oder das Verhalten von natürlichen Personen in der Union beobachtet wird (z.B. im Internet).[7] Jedes Unternehmen, das personenbezogene Daten verarbeitet (z.B. eine Kundendatei führt, Rechnungen ausstellt, Lieferantendaten speichert), ist prinzipiell betroffen.[8]

Personenbezogene Daten

Gemäß Art. 4 DSGVO werden unter personenbezogenen Daten alle Informationen verstanden, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden: „betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.[9]

Art. 9 Abs. 1 DSGVO untersagt die Verarbeitung personenbezogener Daten der besonderen Kategorie. Darunter versteht man folgende sensible Daten:

- Gesundheitsdaten
- Daten zur rassischen und ethnischen Herkunft
- Daten zu politischen Meinungen
- Daten zu religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten
- Daten zu Sexualleben sowie sexuelle Orientierung

Die Verarbeitung der besonderen Kategorie von personenbezogenen Daten ist gemäß Art. 9 Abs. 2 erlaubt, wenn die Betroffenen der Verarbeitung explizit einwilligen oder eine entsprechende gesetzliche Grundlage[10] besteht.

[7] Vgl. KRANIG/SACHS/GIERSCHANN (2017), S. 21.
[8] Vgl. MÜHLBAUER (2018), S. 3.
[9] Vgl. OCHSENFELD (2017), S. 31.
[10] S. Kapitel 2.1. Definition und Analyse von Kernbegriffen, S. 12.

Um einen Einblick in die verarbeiteten personenbezogenen Daten der Raiffeisen-Landesbank Steiermark zu bekommen, werden in der folgenden Tabelle die Datenkategorien des Kooperationspartners dargestellt.

Datenkategorien in der Raiffeisen-Landesbank Steiermark AG	**Erläuterung, Beispiele**
Persönliche Detailangaben	Name, Titel, Alter, Geschlecht, Geburtsort, Geburtsdatum, Nationalität, interne Identifikationsnummern (z.B. Kundennummer, Vertragspartnernummer)
Haushaltsdaten und familiäre Verhältnisse	Familienstand, Hochzeitsdaten, Scheidungsdaten, Anzahl Kinder, unterhaltsberechtigte Personen und Haushaltsangehörige
Daten zu Identitäts- und Reisedokumenten	Art des Ausweises, Ausstellende Behörde/Organisation, Nummer des Ausweises, Ausstellungsdatum
Kontaktdaten	Aktuelle und frühere Adressen, Telefonnummern, Fax-Nummer, E-Mail-Adressen (jeweils beruflich und privat), Messenger & Social Media Accounts
Lebenslauf u. Mitarbeiterqualifikation	Lebenslauf, frühere Arbeitgeber, Vorerfahrungen bei anderen Arbeitgebern, Name der Einrichtung, Zeugnisse/Diplome, Berufliche Abschlüsse und Ausbildungsdaten, Aus- und Fortbildungen, sonstige Ausbildungen, Kenntnisse, Fähigkeiten (zB Sprachkenntnisse, Erste Hilfe, Führerschein), akademische Titel, Beurteilungen, Einschätzungen i.Z.m. Arbeitsverhältnis
Daten zu Beruf und Arbeitsverhältnis	Arbeitgeber, Funktionstitel, Beschreibung der Funktion, Jobgrade, Einstellungsdatum, Arbeitsort, Mitgliedschaft in innerbetrieblicher Arbeitnehmervertretung, Ersthelfer, Brandschutzbeauftragter, Referenzen, Probezeit, Arbeitsverhältnis, Datum des Ausscheidens, Gründe des Ausscheidens, Daten zur Pension (z.B. Antrittsdatum)
Aufenthaltsstatus	Details zum Aufenthaltstitel, Visum, Arbeitserlaubnis, Wohn- oder Reisebeschränkungen, an das Aufenthaltsrecht gebundene Sonderbedingungen
Lohn- und Gehaltsdaten	Zahlungen, Lohn, Provisionen, Bonus, Zulagen, Spesen, Sachbezüge, Vergünstigungen, Darlehen, Gebühren, Firmen-KfZ, Abzüge (z.B. Steuer, Sozialversicherung)
Arbeitsorganisationsdaten	Personalnummer, Dienstausweis, Zutrittsdaten, Anwesenheiten, gegenwärtige Verantwortungen, Projekte, Arbeitszeiten, geleistete Stunden, Dienstreisen, Urlaubsanspruch, konsumierter Urlaub, Krankenstände, sonstige Abwesenheiten, Arbeitsmittel (z.B. Laptop, Mobiltelefon, Tablet), Berechtigungen, Sicherheitsprotokolle und Authentifizierungsdaten (Zutritt, Zugang, Zugriff, Weitergaben). Ergebnisse von Routinekontrollen, Besucherlisten, Raumbuchungsinformationen
Beteiligungen, Organfunkt., Vertretungsbefugnisse	Detailinformationen zur jeweiligen Rolle (z.B. Art der Vertretungsbefugnis, Stimmrecht, Höhe der Beteiligung)
Lebens- und Konsumgewohnheiten	Lebensstil, Angaben über Aufenthalte und Fahrten, Soziale Kontakte, Hobby, Sport, Mitgliedschaften (andere als berufliche, politische, gewerkschaftliche), andere Interessen
Elektron. Protokoll- u. Identifikationsdaten	IP-Adressen, Cookies, Anschlusszeiten, elektronische Unterschrift, Online-Kennungen, Benutzernamen, Passwörter, Protokollierung von Systemaktivitäten insb. Log-in-Daten
Elektronische Standort- und Bewegungsdaten	GPS-Daten, Mobilfunk-Daten, WLAN-Netzdaten
Bild- und/oder Tonaufzeichnungen	Filme, Fotografien, Videoaufzeichnungen (z.B. Aufzeichnungen von Überwachungskameras, Mitschnitte von Videokonferenzen), digitale Fotos (z. B. Pass- oder Bewerbungsfotos, Firmenausweisfotos), Aufzeichnungen auf Tonbandträgern, Telefonaufzeichnung
Bonitätsdaten	Art (und jeweilige Höhe) der Einkünfte: selbstständige/unselbstständige Tätigkeit, Invaliditäts-/Alterspension, Vermietung/Verpachtung, Einkünfte aus Unternehmens- oder Gesellschaftsbeteiligungen; Vermögen: Konto- oder Sparguthaben, Wertpapierdepots, Liegenschaften, Gesellschaftsbeteiligungen; Unterhaltspflichten (Kinder/Ehegatte),

	wiederkehrende Zahlungsverpflichtungen für Ausbildungskosten/Kinder, Kredittilgungen, Mieten, anhängige Exekutionsverfahren, anhängige/abgeschlossene Insolvenz-, Sanierungs- oder Schuldenregulierungsverfahren, Bilanzdaten.
Finanzidentifikationsdaten	IBAN/BIC, Daten von Kredit-, Debit- oder Prepaidkarten (Kartenart, Inhaber, Aussteller, Gültigkeitsdauer, verfügbarer Rahmen)
Daten zu Kreditgeschäft	Kreditart (Einmal-/revolvierender Kredit), Kreditbetrag, Laufzeit, Verzinsungsart (fix/variabel/antizipativ/dekursiv), Angaben zur Tilgung (Tilgungsstruktur, Tilgungsraten, etc.), (Annuitätentilgung), Angaben zu Kreditsicherheiten (Sicherheitengeber, Art der Sicherheit: Hypothek, Bürgschaft, Garantie, Patronatserklärung, etc.), Basel-II relevante Daten (z.B. Default/Non Default-Status)
Daten zu Einlagengeschäft	Kontoart (Spar-/Girokonto), Kontosalden, Kontoumsätze, Zeichnungs-/Verfügungsberechtigte, Disporahmen, etc.
Daten zu Finanztermin-/Derivatgeschäft	Name/Angaben zur Gegenpartei, eigene/fremde Rechnung, Geschäftsart (FX, IRS, CDS, Put/Call Option), etc.
Kassageschäft, Wertpapierverwahrung u. –verwaltung	Daten zu Devisenkassageschäften und Wertpapiergeschäften, Wertpapierdepotnummer, Wertpapierbestand/-bewegungen, steuerliche Anschaffungsdaten, (Wahl-)Dividenden/Kupons/Kapitalmaßnahmen, Name/Angaben zur Gegenpartei
Versicherungsdaten	Versicherungsart, Details über die gedeckten Risiken, Versicherungssumme, Versicherungsprämie, Deckungszeitraum, Fälligkeitsdatum, ausgeführte oder erhaltene Zahlungen und nicht ausgeführte Zahlungen, sonstige Konditionen
Zahlungsverkehrs- und Clearing-Daten	Angaben über Auftraggeber, Empfänger/Begünstigten, Transaktionsbetrag, Transaktionswährung, IBAN/BIC-Daten von Auftraggeber- und Empfängerkonto, Details über Clearing, sonstige SWIFT-Daten
Daten zu Fuhrparkmanagementgeschäft	KFZ Daten (techn. und preisl. KFZ-Daten i.e.S., Unfälle, Fahrzeugschäden/Reparaturen, Fahr- und Tankverhalten, Service und Wartung, KFZ Versicherung, etc.
Daten zu Bauträgergeschäft	Käuferdaten (nat. und juristische Personen - deren Organe), Kaufobjekt und -preis, allfällige Angaben zu Sicherheiten (Sicherheitengeber, Art der Sicherheit: Hypothek, Bürgschaft, Garantie, Patronatserklärung, etc.), Daten i.Z.m. der Kaufpreisfinanzierung, Sonderausstattungen, Wohnungszweck (Eigennutzung / Vermietung)
Daten zu Vermietungsgeschäft	Mietvertragsart, Miete, Kaution, Laufzeit, Mietobjekt samt Ausstattung, Mietzins und Betriebskosten bzw. sonstige Verpflichtungen des Mieters, Angaben zu Sicherheiten (Sicherheitengeber, Art der Sicherheit: Hypothek, Bürgschaft, Garantie, Patronatserklärung, etc.), Kaufoptionen
AML- (Anti-Money Laundering) und Compliance-Daten	Risikoeinschätzung, PEP, FISA, KYC (incl. Gap-Liste), Suspicious Activity Reports, Fraud checks, FATCA, CRS einschließlich öffentliche Mandate in gesetzgebenden Körperschaften, Mandate oder Mitgliedschaften in Interessensvertretungen, Einordnung als PEP (Politisch exponierte Person), Befugnisse, Ermächtigungen, Bevollmächtigungen
Daten zu Marketing und Vertrieb	Kontakt- und Listendaten, Produktinteressen, Kommunikationshistorie, Geschäftshistorie
Daten zu Safes und Schließfächern	Datum, Zeit, Grund des Zugriffs, Safe-Nummer
Besondere Kategorien personenbezogener Daten	Besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO, insbesondere: rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder weltanschauliche Überzeugungen, biometrische Identifikationsdaten, Gesundheitsdaten, Daten zum/r Sexualleben/-orientierung, körperliche Beschreibungsdaten usw.
strafrechtliche Verurteilungen und Straftaten	inkl. Anschuldigungen, Strafregisterauszug

Tabelle 1: Datenkategorien in der Raiffeisen-Landesbank Steiermark AG, Quelle: eigene Darstellung.

Wesentliche Rollen

Da die betroffenen Personen eine wesentliche Rolle in der DSGVO und auch für die Erstellung des Praxisoutputs darstellen, werden in nachfolgender Tabelle die betroffenen Personen der Raiffeisen-Landesbank Steiermark AG aufgezeigt.

Kategorien betroffener Personen in der Raiffeisen-Landesbank Steiermark AG	Erläuterung
Mitarbeiter	Dienstnehmer des Verantwortlichen, einschließlich ehemalige Mitarbeiter
Angehörige von Mitarbeiter	
Bewerber	Externe und interne Stellenbewerber
Vertragspartner	Lieferanten, Dienstleister, sonstige Vertragspartner, deren Beschäftigten und Vertreter
Von Bildbearbeitung betroffene Personen	
Potenzielle Kunden und Interessenten	
Kunden	Einschließlich Vertreter, Beschäftigte und wirtschaftliche Eigentümer von Kunden sowie auch z.B. Treuhänder und Treugeber, Stifter und Begünstigte von Privatstiftungen
Sicherheitengeber	Einschließlich deren Vertreter und Beschäftigte
Eigentümer des Verantwortlichen	Gesellschafter, Aktionäre oder Genossenschaftsmitglieder
Organe und Funktionäre des Verantwortlichen	Geschäftsführer, Vorstands- und Aufsichtsratsmitglieder
Besucher und sonstige Zutrittsberechtigte	
Organe/Beschäftigte von Konzerngesellschaften	

Tabelle 2: Kategorien der Betroffenen in der Raiffeisen-Landesbank Steiermark AG, Quelle: eigene Darstellung.

Nicht nur betroffene Personen sondern auch der Verantwortliche und der Auftragsverarbeiter stellen Hauptrollen in der DSGVO dar. Als Verantwortlicher bezeichnet man jede natürliche als auch juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Unter einem Auftragsverarbeiter versteht man jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.[11]

[11] Vgl. HOHN (2018), S. 5.

Empfänger

Um einen Einblick zu bekommen, wer Daten von der Raiffeisen-Landesbank Steiermark AG bekommt, sollen in der untenstehenden Tabelle die internen und externen Empfänger des Kooperationsunternehmens verdeutlicht werden.

Interne Empfängerkategorien in der Raiffeisen-Landesbank Steiermark AG	**Abteilung/Detail**
Geschäftsbereich Vertragsverwaltung	Abteilungsleiter/Filialleiter/Gruppenleiter
Aufsichtsrat	Aufsichtsrat
Geschäftsbereich Privat- und Geschäftskunden	Correspondent Banking, ELBA, Filialen, Kundenhandel, Vertriebsunterstützung, Bauträger & Projektgesellschaften, Firmen-/Institutionelle Kunden, Sanierungskunden, Vertriebsunterstützung Firmenkunden
Innenrevision	Innenrevision, IT-Revision
Marketing	Marketing
Personalmanagement	Personalmanagement
Rechnungswesen & Controlling	Rechnungswesen & Controlling
Recht-/Geldwäsche- und Compliance	Recht-/Geldwäsche- und Compliance
Risikomanagement	Risikomanagement
Treasury	Treasury
Vorstand/Geschäftsführung	Vorstand

Tabelle 3: Interne Empfängerkategorien in der Raiffeisen-Landesbank Steiermark AG, Quelle: eigene Darstellung.

Externe Empfängerkategorien in der Raiffeisen-Landesbank Steiermark AG	**Abteilung/Detail**
Kredit- und Finanzinstitute	andere Banken, Kreditkartenunternehmen
Anwälte, Notare	Anwälte, Notare
Verwaltungsbehörden	
Aufsichtsbehörden	FMA, OeNB
Steuerberater und Wirtschaftsprüfer	Externe Prüfer oder Parteienvertreter
Gerichte und Staatsanwaltschaften	Gerichte und Staatsanwaltschaften
IT-Dienstleister	Rechenzentren
Lieferanten	Lieferanten
externe Revision	Revision
Unternehmen des Raiffeisensektors	Raiffeisenbanken, Raiffeisenlandesbanken, RBI, Raiffeisenverband, Lagerhäuser etc.
Versicherungen	sonstige Versicherung (z.B. Sperrscheinersatz)
sonstige Auftragsverarbeiter EU	z.B. Kartenproduzenten, Callcenter
sonstige Auftragsverarbeiter außerhalb EU	
Makler, Vermittler, Finanzdienstleister	
Bonitätsdatenbanken	
Geschäftspartner vermittelter Produkte	Teambank, Bausparkasse, Raiffeisen Leasing, Raiffeisen Versicherung
gesetzlicher Vertreter oder Bevollmächtigter	

Tabelle 4: Externe Empfängerkategorien in der Raiffeisen-Landesbank Steiermark AG, Quelle: eigene Darstellung.

Verarbeitungstätigkeit

Gemäß Art. 4 DSGVO versteht man unter „Verarbeitung“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Unter „Verwenden von Daten“ versteht man somit jede Art der Handhabung von Daten.[12] In der vorliegenden Arbeit wird statt dem Begriff „Verarbeitungstätigkeit“ aufgrund der leichteren Verständlichkeit als Synonym auch „Geschäftsprozess, in dem personenbezogene Daten verarbeitet werden“ verwendet.

Rechtsgrundlage für Verarbeitungstätigkeiten

Gemäß Art. 6 DSGVO dürfen personenbezogene Daten nur in den nachfolgend genannten Fällen verarbeitet werden. Der Verantwortliche hat die Erlaubnis zur Datenverarbeitung, wenn die Daten zur Erfüllung eines Vertrages erforderlich sind.[13] Wenn zum Beispiel die Raiffeisen-Landesbank Steiermark AG einen Vertrag zur Durchführung eines Kreditgeschäftes mit einem Kunden abwickelt, dann dürfen sie auch alle notwendigen Daten verarbeiten.

Des Weiteren dürfen Daten verarbeitet werden, wenn die betroffene Person einwilligt.[14] Dies wäre bei der Raiffeisen-Landesbank Steiermark AG beispielsweise der Fall, wenn sie einen Newsletter an ihre Kunden versenden möchte. Die Versendung eines Newsletters beziehungsweise die Verarbeitung der Daten wäre nur erlaubt, wenn die betroffene Person einwilligt.

Zudem ist die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung, zum Schutz lebenswichtiger Interessen und im öffentlichen Interesse als auch zur Wahrung der berechtigten Interessen des Datenverarbeiters (oder eines Dritten) zulässig, sofern nicht die schutzwürdigen Interessen der betroffenen Person (oder dessen „Grundrechte oder Grundfreiheiten“) überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.[15]

[12] Vgl. MERTINZ (2016), S. 17.
[13] Vgl. GRUBER (2017), S. 243.
[14] Vgl. KÜHLING/KLAR/SACKMANN (2018), S. 196.
[15] Vgl. GRUBER (2017), S. 245.

2.2. Die Grundsätze der Datenschutz-Grundverordnung

Art. 5 Abs. 2 DSGVO legt fest, dass der Verantwortliche für die Einhaltung der Grundsätze der Verarbeitung personenbezogener Daten verantwortlich ist und dies nachweisen können muss („Rechenschaftspflicht“). Sie sind damit zur Einhaltung der folgenden Grundsätze, verpflichtet[16]:

Grundsatz	Interpretation	Erwägungsgrund
Rechtmäßigkeit	Rechtmäßigkeit durch Einwilligung oder eine andere zulässige Rechtsgrundlage der EU oder eines Mitgliedstaates (Rechtspflicht, Vertrag, Vorvertrag) zum Schutz lebenswichtiger Interessen des Betroffenen oder einer anderen natürlichen Person im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt	40, 42, 44, 45, 46, 47
Treu und Glauben	Verlässlichkeit, Redlichkeit, Anstand	Art. 5 Abs. 1 lit. a
Transparenz	Gewährleistung von Nachvollziehbarkeit, Festlegung von Löschfristen oder regelmäßige (definierte Zeiträume) Überprüfung auf Löschbarkeit, Umfangreiche Information des Betroffenen über die Verarbeitung	39, 42, 58, 60, Art. 5 Abs. 2, Art. 12
Zweckbindung	Festgelegte, legitime und eindeutige Zwecke	39
Datenminimierung	Beschränkung der Verarbeitung auf das dem Zweck entsprechende notwendige Maß	39
Richtigkeit	Daten sind aktuell und zutreffend	Art. 5 Abs. 1 lit. d
Speicherbegrenzung	Nach Wegfall des Zwecks Löschung	Art. 5 Abs. 1 lit. d
Integrität und Vertraulichkeit	Schutz vor unbefugter oder unrechtmäßiger Verarbeitung, vor Verlust oder Beschädigung	Art. 5 Abs. 1 lit. f
Nachweisbarkeit der Einhaltung getroffener Datenschutzmaßnahmen	Rechenschaftspflicht über Einhaltung der Datenschutzmaßnahmen	Art. 5 Abs. 2

Tabelle 5: Grundsätze der DSGVO,
Quelle: REIMANN (2018), S. 21.

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten sind gemäß Art. 5 Abs. 1 lit. A DSGVO auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbare Weise zu verarbeiten. Daher kann eine Verarbeitung nur stattfinden, wenn sie von einer gesetzlichen Grundlage oder der Einwilligung der betroffenen Person gedeckt ist. Natürlichen Personen muss es möglich sein zu verstehen, was mit ihren personenbezogenen Daten passiert. Aus diesem Grund sollte für die betroffenen Personen gemäß Erwägungsgrund 39 DSGVO nachvollziehbar sein, dass ihre personenbezogenen Daten gesammelt, verwendet, analysiert

[16] Vgl. KRANIG/SACHS/GIERSCHANN (2017), S. 24.

oder auf andere Weise verarbeitet werden und in welchem Ausmaß diese genutzt werden oder in Zukunft genutzt werden sollen. Der Grundsatz der Transparenz besagt, dass den natürlichen Personen folgende Informationen zur Verfügung gestellt werden sollen:[17]

- Informationen zur Identität des Verantwortlichen
- Informationen zu den Zwecken der Datenverarbeitung
- Weitere relevante Informationen hinsichtlich ihres Rechts, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffenden personenbezogene Daten verarbeitet werden
- Informationen und Aufklärung in Hinblick auf Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten und darüber, wie sie ihre diesbezüglichen Rechte geltend machen können.

Die Rechte auf Information werden durch die Bestimmungen der Art. 13-14 DSGVO darüber hinaus substantiiert. Vor allem sollten die konkreten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der Daten feststehen. Informationen bezüglich der Verarbeitung sollten für die Betroffenen leicht zugänglich und verständlich sein, insbesondere durch die Verwendung einfacher und klarer Sprache.[18]

Zweckbindung

Der Grundsatz der Zweckbindung stellt die zentrale datenschutzrechtliche Anforderung dar. Gemäß Art. 5 Abs. 1 lit. b DSGVO dürfen personenbezogene Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Art. 89 Abs. 1 DSGVO nicht als unvereinbar mit den ursprünglichen Zwecken. Der Grundsatz der Zweckbindung ist jedoch nicht neu, denn dieser ist wortgleich bereits in der zuvor geltenden Datenschutzrichtlinie, die von der DSGVO abgelöst wurde, auffindbar.[19]

Datenminimierung

Es versteht sich von selbst, dass nicht erhobene personenbezogene Daten auch nicht geschützt werden müssen. Wer im Vorfeld zur Datenverarbeitung analysiert, welche personenbezogene Daten wirklich unerlässlich für die Erfüllung einer Arbeitsaufgabe sind, trägt am besten zum Datenschutz bei. Denn oftmals sind die Löschrechte der betroffenen Personen nur eingeschränkt technisch umsetzbar oder bedeuten einen unverhältnismäßig hohen

[17] Vgl. VOIGT/VON DEM BUSSCHE (2018), S. 114.
[18] Vgl. VOIGT/VON DEM BUSSCHE (2018), S. 114.
[19] Vgl. MOOS/SCHEFZIG/ARNING (2018), S. 66.

Aufwand. Daher ist der Grundsatz der Datenvermeidung, Datensparsamkeit und Datenminimierung von praktischer Bedeutung. Die folgende Grafik soll aufzeigen, wie der Grundsatz der Datenminimierung in die Praxis umgesetzt werden kann, wobei die Vermeidung personenbezogener Daten, der Datenminimierung und Pseudonymisierung vorgeht.[20]

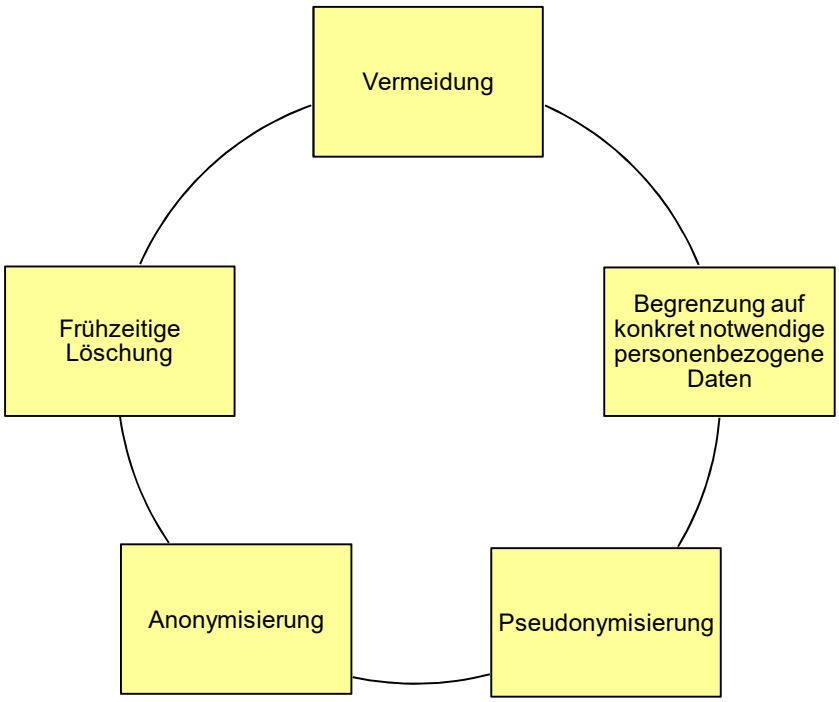


Abbildung 1: Praktische Umsetzung der Datenminimierung,
Quelle: in Anlehnung an REIMANN (2018), S. 22.

Der Grundsatz der Datenminimierung ist schon vor Erhebung der personenbezogenen Daten anzuwenden. Denn, wenn eine Verarbeitungsstruktur einmal vorhanden ist, dann wird diese auch genutzt. Aus diesem Grund ist die Reduktion der Datenquantität als auch der Datenqualität der Schlüssel für einen guten Datenschutz in der Praxis. Der Grundsatz stellt auch einen Appell an die Verantwortlichen für die Verarbeitung personenbezogener Daten dar, solche technischen Systeme beziehungsweise softwaretechnischen Lösungen zu wählen, die mit möglichst wenig personenbezogenen Daten auskommen.[21]

Richtigkeit

Unter dem Grundsatz der Richtigkeit versteht man, dass personenbezogene Daten sachlich richtig und falls dies für den Verarbeitungszweck erforderlich ist, auf dem neuesten Stand sein müssen.[22] Es sind angemessene Maßnahmen zu treffen, damit personenbezogene Daten, die hinsichtlich der Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden. Da aufgrund von Daten die Rekonstruktion einer bestimmten Situation oder der

[20] Vgl. REIMANN (2018), S. 22 ff.
[21] Vgl. FEILER/HORN (2018), S. 11.
[22] Vgl. FEILER/HORN (2018), S. 11.

Merkmale einer Person ermöglicht werden kann, müssen sie sachlich richtig sein, da ihre Verwendung unter Umständen relevante Rechtsfolgen herbeiführen kann. Eine Widerspiegelung der Realität sollte durch die Daten jederzeit gewährleistet sein. Der Grundsatz der Richtigkeit wird auch durch andere Regelungen der DSGVO gestützt, wie beispielsweise durch die Rechte der Betroffenen[23] auf Berichtigung und Löschung ihrer personenbezogenen Daten.[24]

Speicherbegrenzung

Personenbezogene Daten dürfen gemäß Art. 5 Abs. 1 lit. e DSGVO nur so lange gespeichert werden, wie es für die Erreichung des Zwecks der Verarbeitung erforderlich ist. Die Frist der Speicherung ist auf das unbedingt erforderliche Mindestmaß zu begrenzen. Um den Grundsatz in die Praxis umzusetzen, hat der Verantwortliche Fristen für die Löschung oder die kontinuierliche Überprüfung der personenbezogenen Daten zu bestimmen. Diese Regelung wird auch durch die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäß Art. 17 DSGVO substantiiert.[25]

Integrität und Vertraulichkeit

Im Rahmen dieses Grundsatzes sind angemessene technische und organisatorische Maßnahmen zum Schutz der Sicherheit von personenbezogenen Daten zu implementieren, um die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten sicherzustellen.[26] Unter die Verletzung der Integrität würde beispielsweise die unautorisierte Veränderung von personenbezogenen Daten fallen. Wenn Daten für unbefugte zugänglich werden, spricht man von einer Verletzung der Vertraulichkeit. Im Falle einer unautorisierten Löschung würde dies zur Verletzung der Verfügbarkeit führen.[27]

2.3. Die Betroffenenrechte

Betroffenenrechte sind die Rechte der von der Datenanwendung betroffenen Personen wie Kunden und Mitarbeitern gegenüber dem Verantwortlichen (z.B. Raiffeisenbank).[28] Sie sind vor allem im dritten Kapitel der DSGVO, in Art. 12-23 DSGVO, geregelt. Die folgende Tabelle auf der nächsten Seite verschafft einen Überblick über die einzelnen Betroffenenrechte, die in der DSGVO verankert sind:

[23] S. Kapitel 2.3. Die Betroffenenrechte, S. 16.
[24] Vgl. VOIGT/VON DEM BUSSCHE (2018), S. 118.
[25] Vgl. VOIGT/VON DEM BUSSCHE (2018), S. 118.
[26] Vgl. FEILER/HORN (2018), S. 20.
[27] Vgl. FEILER/HORN (2018), S. 69.
[28] Vgl. MATTHEWS (2018), S. 87 ff.

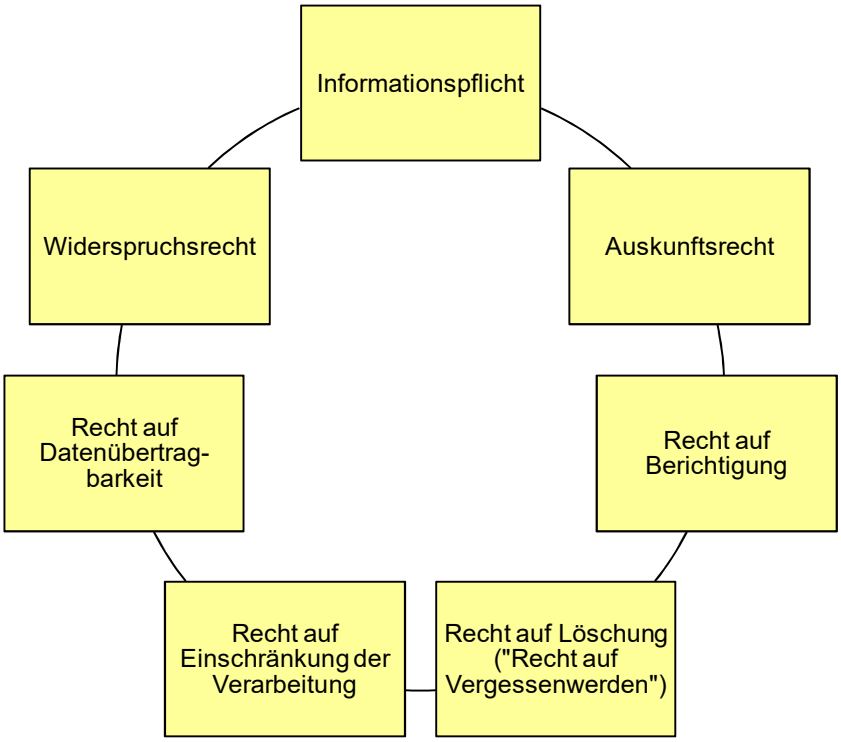


Abbildung 2: Betroffenenrechte,
Quelle: in Anlehnung an MÜHLBAUER (2018), S. 46.

Die Betroffenenrechte erlangen erst bei Geltendmachung durch den Betroffenen an Bedeutung. Eine Ausnahme stellt jedoch die Löschpflicht nach Art. 17 Abs. 1 lit. a, d und f DSGVO dar, welche unabhängig von einer Geltendmachung der betroffenen Person explizite Handlungsverpflichtungen vorsieht.[29]

Informationspflicht

Art. 13 und 14 DSGVO beschreiben die Informationspflichten, nach denen der Verantwortliche verpflichtet ist, die betroffenen Personen proaktiv bei der Erhebung ihrer personenbezogenen Daten über die Datenverarbeitung zu informieren.[30] Der Verantwortliche ist dazu verpflichtet geeignete Maßnahmen zu ergreifen, um den betroffenen Personen alle Informationen und alle Mitteilungen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln. Diese Übermittlung kann schriftlich, elektronisch oder in einer anderen Form erfolgen. Die Informationen können auch auf einer Webseite, wenn sie für die Öffentlichkeit bestimmt ist, zur Verfügung gestellt werden.[31]

[29] Vgl. KNYRIM/TIEN (2017), S. 364.
[30] Vgl. DIHEN (2017), S. 57.
[31] Vgl. MÜHLBAUER (2018), S. 47.

Auskunftsrecht

Art. 15 DSGVO beinhaltet die Regelungen zum Auskunftsrecht der Betroffenen, also dem Recht, von dem Verantwortlichen Auskunft über die Verarbeitung ihrer Daten zu erhalten.[32] Die betroffene Person hat somit das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob ihn betreffende personenbezogene Daten verarbeitet werden. Der Betroffene muss die Identität nachweisen, wenn der Verantwortliche berechtigte Zweifel hat[33]. Die Person hat hinsichtlich ihrer personenbezogenen Daten gemäß Art. 15 DSGVO ein Recht auf Auskunft über:

- Verarbeitungszwecke
- Kategorien der verarbeiteten personenbezogenen Daten
- Empfänger, denen die personenbezogenen Daten offengelegt werden
- Geplante Speicherdauer
- Recht auf Berichtigung, Löschung, Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung
- Beschwerderecht gegenüber einer Aufsichtsbehörde
- Recht auf Informationen über die Herkunft der Daten, sofern die Daten nicht beim Betroffenen direkt erhoben wurden
- Recht auf Informationen über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling[34]

Falls personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt werden, hat der Betroffene das Recht, über die geeigneten Garantien gemäß Art. 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden. Ferner ist der Verantwortliche dazu verpflichtet, eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, dem Betroffenen zu übermitteln, wenn der Betroffene dies verlangt.[35] Dabei ist zu berücksichtigen, dass die erste Kopie kostenlos zur Verfügung gestellt werden muss. Ab der zweiten Kopie dürfen nach Art. 15 Abs. 3 DSGVO die Verwaltungskosten wie zum Beispiel Personal-, Material- und Portokosten in Rechnung gestellt werden. Hinsichtlich des Auskunftsrechts dürfen Interessen Dritter, wie zum Beispiel Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberecht an Software, nicht eingeschränkt werden.[36] Des Weiteren hat der Verantwortliche den Antrag auf Auskunft unverzüglich zu beantworten, in jedem Fall zumindest binnen eines Monats ab Eingang. Falls die Beantwortung

[32] Vgl. KNYRIM/THIEN (2017), S. 365.
[33] Vgl. MÜHLBAUER (2018), S. 47.
[34] S. Kapitel 3.2. Die Notwendigkeitsprüfung in der Vorbereitungsphase, S. 28.
[35] Vgl. DIHEN (2017), S. 60.
[36] Vgl. GOLA/JASPERS/MÜTHLEIN/SCHWARTMANN (2018), S. 64.

des Antrags komplex ist und mehrfache Anträge vorliegen, besteht die Möglichkeit, die Frist um zwei weitere Monate zu verlängern.[37]

Recht auf Berichtigung

In Hinblick auf das Recht auf Berichtigung gemäß Art. 16 DSGVO hat der Betroffene das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten beziehungsweise die Vervollständigung unvollständiger Daten zu verlangen. Die personenbezogenen Daten gelten als unrichtig, wenn sie zum Zeitpunkt der Geltendmachung des Berichtigungsrechts nicht mit der Tatsachenlage übereinstimmen.[38] Unvollständig sind Daten, wenn sie zwar richtig sind, aber im Hinblick auf den Verarbeitungszweck ein unzutreffendes Bild des Betroffenen ergeben. Die Vervollständigung muss also für den mit der Verarbeitung im konkreten Einzelfall verfolgten Zweck relevant sein. Beispielsweise kann die Information, warum ein Kredit von einem Kreditnehmer nicht bedient wurde, die Einschätzung des Kreditausfallrisikos verändern.[39]

Recht auf Löschung („Recht auf Vergessenwerden“)

Das Recht auf Vergessenwerden basiert auf der „Google Spain“-Entscheidung des EuGH im Jahr 2014. Dabei wurde dieses Recht ins Blickfeld der Öffentlichkeit und des Gesetzgebers gerückt und wurde mit der DSGVO verschärft. Der Betroffene hat das Recht, dass, auf Verlangen, sie betreffende personenbezogene Daten unverzüglich gelöscht werden, wenn einer der folgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Verarbeitungszwecke nicht mehr notwendig.
- Der Betroffene widerruft seine Einwilligung, auf die sich die Verarbeitung stützte und daher fehlt die Rechtsgrundlage für die Verarbeitung.
- Der Betroffene legt gemäß Art. 21 Abs. 1 Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor, oder die Person legt gemäß Art. 21 Abs. 2 Widerspruch gegen die Verarbeitung ein.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Recht der EU oder der Mitgliedstaaten erforderlich, dem der Verantwortliche unterliegt.
- Die personenbezogenen Daten wurden mit der Einwilligung eines Kindes hinsichtlich der angebotenen Dienste der Informationsgesellschaft erhoben.[40]

[37] Vgl. MÜHLBAUER (2018), S. 48.
[38] Vgl. MOOS/SCHEFZIG/ARNING (2018), S. 186.
[39] Vgl. MOOS/SCHEFZIG/ARNING (2018), S. 187.
[40] Vgl. VOIGT/VON DEM BUSSCHE (2018), S. 208 ff.

Recht auf Einschränkung der Verarbeitung

Das Ziel des Rechts auf Einschränkung der Verarbeitung gemäß Art. 18 DSGVO ist, einen Interessensausgleich zwischen dem Interesse des Betroffenen an einer Berichtigung oder Löschung seiner personenbezogenen Daten und dem Interesse des Verantwortlichen an der Fortführung der Verarbeitung der betroffenen personenbezogenen Daten herzustellen.[41] Zudem stellt das Recht auf Einschränkung einen Mittelweg zwischen den divergierenden Interessen dar, sofern das Vorliegen von Gründen für die Löschung oder Berichtigung von Daten einer weitergehenden Prüfung bedarf oder zwischen dem Verantwortlichen und der betroffenen Person umstritten ist.[42]

Art. 18 Abs. 1 lit. a-d DSGVO legen vier Gründe, die zu einer Einschränkung der Verarbeitung führen können, fest:

- Die Richtigkeit der personenbezogenen Daten wird vom Betroffenen bestritten und eine Einschränkung der Verarbeitung soll für eine Dauer stattfinden, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen.
- Die Verarbeitung ist unrechtmäßig und der Betroffene lehnt die Löschung der personenbezogenen Daten ab und verlangt stattdessen die Einschränkung der Nutzung dieser Daten. Trotz der Unrechtmäßigkeit der Verarbeitung besteht die Möglichkeit, dass der Betroffene an der Verhinderung der Löschung der betroffenen Daten nach Art. 17 DSGVO interessiert ist, da dieser die Zugriffsmöglichkeit des Verantwortlichen auf die Daten (zu einem späteren Zeitpunkt) beweisen möchte.
- Der Verantwortliche benötigt die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger, aber der Betroffene benötigt sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Die Speicherung der Daten erfolgt somit zu Beweiszwecken.[43]
- Der Betroffene hat Widerspruch gegen die Verarbeitung nach Art. 21 Abs. 1 DSGVO eingelegt und es steht noch nicht fest, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen.

Recht auf Datenübertragbarkeit

Ein neues Betroffenenrecht stellt das Recht auf Datenübertragbarkeit nach Art. 20 DSGVO sowie dem korrespondierenden Erwägungsgrund 68 dar. Die betroffene Person hat, unter bestimmten Voraussetzungen, das Recht, Daten vom Verantwortlichen „ausgehändigt“ zu bekommen beziehungsweise zu verlangen, dass dieser die Daten an einen anderen Verantwortlichen übermittelt, soweit dies technisch machbar ist.[44] Sinn und Zweck dieses

[41] Vgl. MÜTHLEIN (2017), S. 30.
[42] Vgl. VOIGT/VON DEM BUSSCHE (2018), S. 220.
[43] Vgl. VOIGT/VON DEM BUSSCHE (2018), S. 221.
[44] Vgl. MATTHEWS (2018), S. 87 ff.

Betroffenenrechts ist, dass betroffene Personen Daten, die sie beispielsweise einem Sozialen Netzwerk, E-Mail-Providern oder anderen Portalen zur Verfügung gestellt haben, zu einem anderen Netzwerk, E-Mail-Provider oder Portal „mitnehmen“ können. Damit soll die Abhängigkeit der betroffenen Person zu einem Netzwerk, E-Mail-Provider oder Portal verringert werden und der „Umzug“ zu anderen Anbietern erleichtert werden.[45]

Gemäß Art. 20 Abs. 1 DSGVO hat die betroffene Person das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern die Verarbeitung auf einer Einwilligung gemäß Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a oder auf einem Vertrag gemäß Art. 6 Abs. 1 lit. b beruht und die Verarbeitung mithilfe automatisierter Verfahren erfolgt.

Widerspruchsrecht

Die betroffene Person hat gemäß Art. 21 das Recht, Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten zu erheben. Auf das Widerspruchsrecht ist die betroffene Person bei der ersten Kontaktaufnahme explizit in verständlicher Form zu informieren. Darüber hinaus regelt der Erwägungsgrund 70 DSGVO, dass dieses Betroffenenrecht vom Verantwortlichen unentgeltlich zu gewährleisten ist.[46]

[45] Vgl. MOOS/SCHEFZIG/ARNING (2018), S. 280.
[46] Vgl. HOEREN/HOLZNAGL (2018), S. 107.

3. Vorgehensweise bei Datenschutz-Folgenabschätzungen

Neben der Erläuterung grundlegender Aspekte der DSGVO, setzt sich dieses Kapitel näher mit einer wesentlichen Neuerung der DSGVO, und zwar der sogenannten DSFA auseinander. Die Umsetzung der DSFA ist von großer Bedeutung, da die DSGVO bei Nichteinhaltung der DSFA-Anforderungen ein Bußgeld von bis zu 10 Mio. EUR bzw. bis zu 2 % des jährlichen weltweiten Konzernumsatzes verhängt, wobei der höhere der beiden Beträge maßgeblich ist.[47]

Zu Beginn dieses Kapitels werden die wesentlichen Grundlagen der DSFA dargestellt. In weiterer Folge werden die Phasen der DSFA beschrieben. Der Schwerpunkt der Phasen liegt auf der ersten Phase, der sogenannten Vorbereitungsphase. Im Rahmen dieser Phase setzt sich die Verfasserin unter anderem mit der Fragestellung auseinander, wann eine DSFA durchzuführen ist. Dabei werden zahlreiche Beispiele anhand der Raiffeisen-Landesbank Steiermark AG aufgezeigt. Die weiteren Phasen, die Bewertungsphase, die Maßnahmenphase und die Berichtsphase werden zwar beschrieben, jedoch detailliert erst im nächsten Hauptkapitel „Datenschutz-Risikomanagement“ betrachtet.

3.1. Wesentliche Grundlagen der Datenschutz-Folgenabschätzung

Die DSFA wird in der Literatur auch als „privacy impact assements (PIA)“ oder in der englischen Übersetzung der DSGVO auch als „Data Protection Impact Assessment“ bezeichnet.[48] FEILER und HORN beschreiben die DSFA als eine Dokumentation eines Prozesses, der darin besteht, die Verarbeitungstätigkeit zu beschreiben, die Rechtmäßigkeit zu prüfen, die Risiken für die Betroffenen zu identifizieren und zu bewerten, die Risiken zu mindern und das verbleibende Restrisiko zu bewerten.[49] HANSEN definiert die DSFA als ein Instrument, um die Risiken für die betroffenen Personen zu identifizieren und zu bewerten, die durch den Einsatz einer bestimmten Technologie und eines Systems entstehen.[50] FRIEDEWALD beschreibt die DSFA als eine systematische Untersuchung eines Datenverarbeitungsverfahrens im Hinblick darauf, welche Risiken für den Datenschutz durch Organisationen (z.B. Unternehmen oder Behörden) aus der Perspektive der betroffenen Personen in verschiedenen Rollen und Kontexten (z.B. Bürger, Kunden, etc.) entstehen.[51] Hinsichtlich der Funktionen der DSFA, soll diese einerseits die Einhaltung der DSGVO überprüfen und dokumentieren und andererseits feststellen, ob eine Konsultation mit der Datenschutzbehörde erforderlich ist.[52]

[47] Vgl. WICHTERMANN (2016), S. 798.
[48] Vgl. WICHTERMANN (2016), S. 797.
[49] Vgl. FEILER/HORN (2018), S. 61.
[50] Vgl. HANSEN (2016), S. 587.
[51] Vgl. FRIEDEWALD (2017), S. 67.
[52] Vgl. FEILER/HORN (2018), S. 61.

Für HANSEN ist das Ziel der DSFA die Beherrschbarkeit der Datenverarbeitung und auch der damit verbundenen Risiken, indem passende technische und organisatorische – und möglicherweise auch juristische – Gegenmaßnahmen ausgewählt und umgesetzt werden.[53] Für FRIEDEWALD ist das Ziel der DSFA, dass die Datenflüsse und Folgen der Datenverarbeitung so komplett wie möglich erfasst, sowie objektiv nach einheitlichen Kriterien bewertet werden, um typischen Risikoquellen mit adäquaten technischen und organisatorischen Gegenmaßnahmen zu begegnen und das Risiko für die Rechte der Betroffenen zu verringern.

Neben diesem Kernzweck werden weitere Nebenziele verfolgt. Ein Nebenziel stellt dabei die Erkennung von Datenschutzrisiken dar, um diese zu vermeiden. Des Weiteren soll ein Nebenziel die Herstellung von Transparenz gegenüber der Öffentlichkeit sein.[54] Laut WICHTERMANN verfolgt die DSFA drei Ziele. Als erstes Ziel legt er fest, dass eine frühzeitig durchgeführte DSFA dabei helfen kann, die Anforderungen aus Art. 25 DSGVO des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) zu erfüllen. Außerdem können durch die rechtzeitige Einbindung des Datenschutzbeauftragten (DSB) und die Durchführung einer DSFA hohe Folgekosten für Verfahrens- bzw. Produktanpassungen verhindert werden. Die DSFA kann auch als ein Teil einer internen Datenschutzstrategie und -maßnahme verstanden werden, welche als Nachweis für die Einhaltung der DSGVO dienen soll. Das zweite Ziel stellt die Analyse der Risiken dar, durch die entsprechende Sicherheitsvorkehrungen und Maßnahmen, insbesondere technische und organisatorische Lösungen, abgeleitet und nachgewiesen werden können. Beim dritten Ziel von WICHTERMANN gibt es eine Übereinstimmung mit dem Nebenziel von FRIEDEWALD, denn auch für ihn stellt ein Ziel die Schaffung von Transparenz über die Verarbeitung dar. Externen soll es dabei möglich sein, die Rechtmäßigkeit und die Risiken zu bewerten, einzuschätzen und Schwächen beim Datenschutz und -sicherheit zu erkennen.[55]

In weiterer Folge wird in diesem Kapitel die Vorgehensweise bei der Durchführung einer DSFA näher beleuchtet. Der dargestellte Prozess orientiert sich an den Anforderungen des Art. 35 DSGVO und basiert auf einer ausführlichen Analyse der Datenschutzgruppe nach Art. 29. Mit diesem Prozess können in der Praxis die bestmöglichen Resultate erzielt werden. Durch einen standardisierten Prozess wird die Reproduzierbarkeit und Überprüfbarkeit der Ergebnisse gewährleistet. Dies ermöglicht die Kontrolle, ob rechtliche Vorschriften eingehalten werden.

[53] Vgl. HANSEN (2016), S. 587.
[54] Vgl. FRIEDEWALD (2017), S. 67.
[55] Vgl. WICHTERMANN (2016), S. 798.

Außerdem ermöglicht der Prozess für die Betroffenen einen Vergleich der Datenschutzfolgen verschiedener technischer Systeme.[56]

Wie man der Abbildung auf der folgenden Seite entnehmen kann, wird der Prozess der DSFA in vier Phasen untergliedert. Als Erstes ist in der Vorbereitungsphase das geplante Verfahren zur Datenverarbeitung zu erläutern. Als Zweites werden die identifizierten Risiken aus der Perspektive der betroffenen Personen in der Bewertungsphase beurteilt. Als Drittes erfolgt in der Maßnahmenphase das Treffen von Vorkehrungen, um die Risiken einzudämmen. Als Viertes werden in der Berichtsphase die Ergebnisse des DSFA-Verfahrens dokumentiert. Die anlassbezogen und kontinuierlich erforderliche Fortschreibung der DSFA wird durch die Einbindung in das Datenschutz-Management gewährleistet.[57]

[56] Vgl. FRIEDEWALD (2017), S. 68.
[57] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 132.

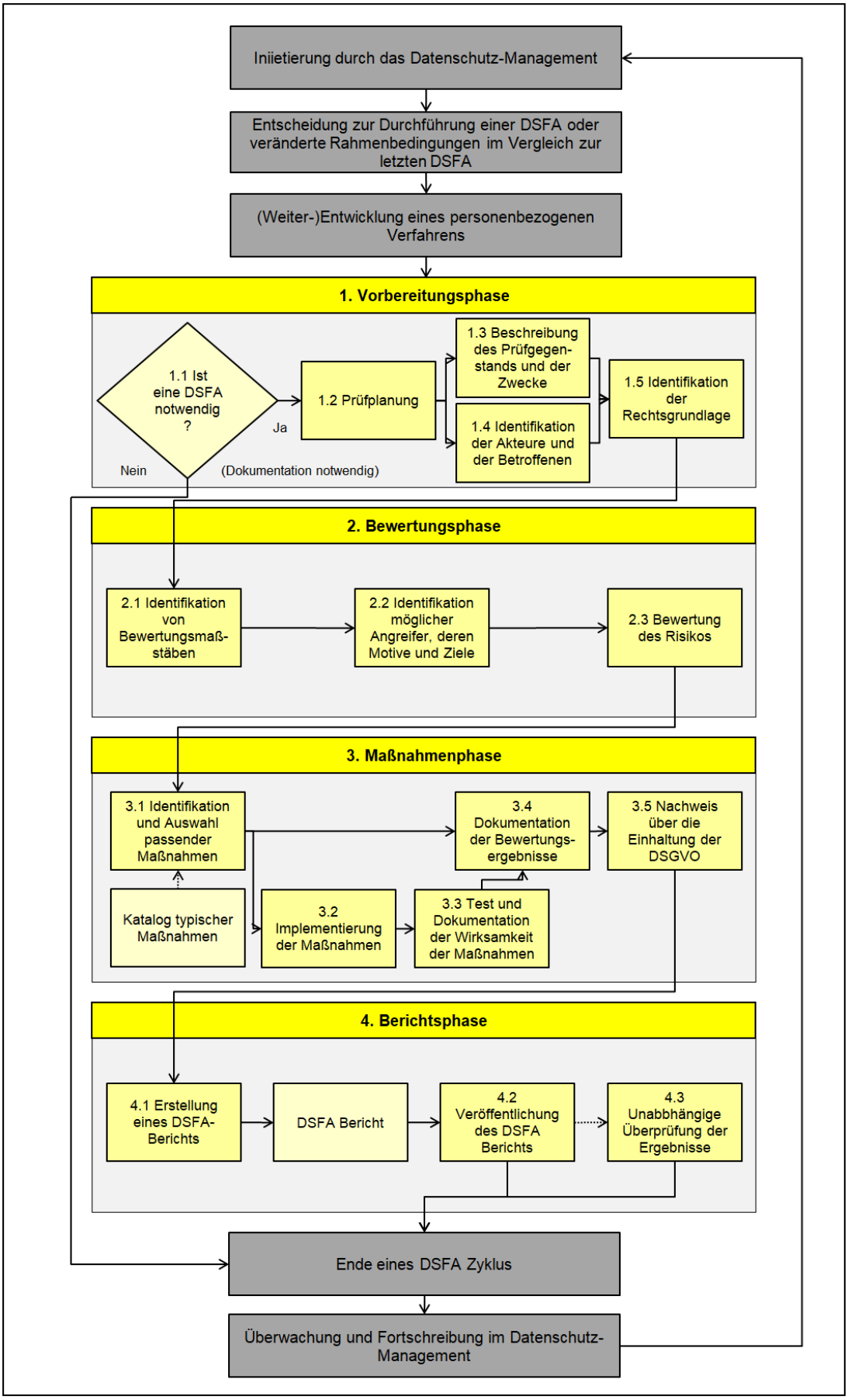


Abbildung 3: Vorgehensweise bei der Datenschutz-Folgenabschätzung,
Quelle: in Anlehnung an LEPPERHOF/MÜTHLEIN (2018), S. 133.

3.2. Die Notwendigkeitsprüfung in der Vorbereitungsphase

Wie bereits in der Abbildung 3 ersichtlich, setzt sich dieses Kapitel mit dem Prüfschema für die Notwendigkeit einer DSFA auseinander. Danach finden die Prüfplanung, die Beschreibung des Prüfgegenstandes und die Zwecke der Verarbeitung Erwähnung. In weiterer Folge beschäftigt sich dieses Kapitel mit der Identifikation der Akteure und der betroffenen Personen, der Identifikation der Rechtsgrundlagen sowie der Dokumentation der Ergebnisse der Vorbereitungsphase.

Prüfschema für die Notwendigkeit einer DSFA

Zu Beginn hat der Verantwortliche zu überprüfen, ob im konkreten Fall eine DSFA notwendig ist. In der folgenden Grafik wird veranschaulicht, wie bei dieser Prüfung vorzugehen ist.

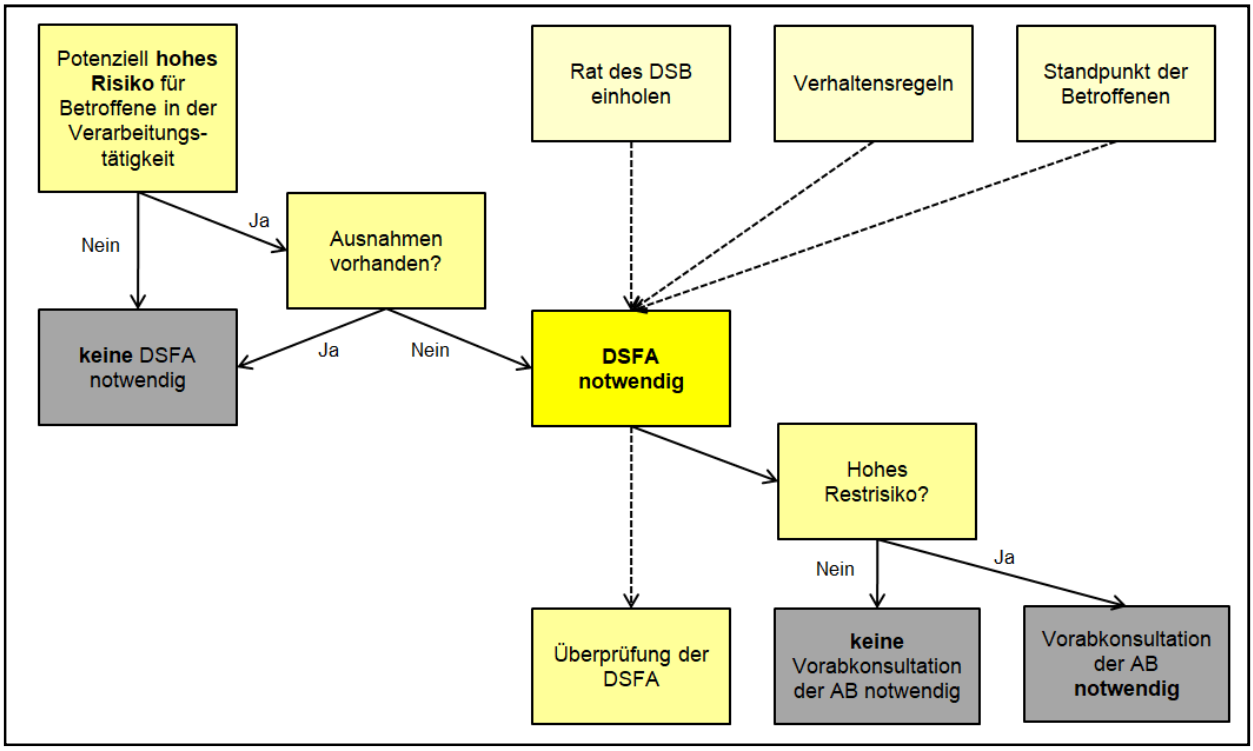


Abbildung 4: Prüfschema für die Notwendigkeit einer Datenschutz-Folgenabschätzung, Quelle: eigene Darstellung.

Schritt 1: Überprüfung des hohen Risikos

Art. 35 Abs. 1 legt fest, dass eine DSFA durchzuführen ist, wenn „insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten“ der betroffenen Personen besteht.

Gemäß Art. 35 Abs. 3 ist eine DSFA in nachfolgenden Fällen verpflichtend durchzuführen:[58]

- Die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen.
- Die umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 oder von Personen über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10.
- Die systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Für die Untersuchung von mehreren ähnlichen Verarbeitungsvorgängen mit ähnlich hohen Risiken kann eine einzige DSFA vorgenommen werden. Dies kann der Fall sein, wenn zur Erfassung derselben Art von Daten zum gleichen Zweck eine ähnliche Technologie zum Einsatz kommt. Es muss jedoch eine Begründung vorgelegt werden, warum eine einzige DSFA ausreichend ist.[59]

Beispiel:
Zusätzlich zu einer bereits bestehenden Videoüberwachungsanlage wird eine neue (ähnliche) Videoüberwachungsanlage eingerichtet. Es kann eine einzige DSFA durchgeführt werden, mit der die Verarbeitung durch die Verantwortlichen abgedeckt ist.

Des Weiteren ist zu erwähnen, dass die Erwägungsgründe 75 und 76 Hilfestellungen liefern, jedoch existiert aufgrund der Verwendung von unbestimmten Begriffen („voraussichtlich … hohes Risiko“) und nicht abschließenden Aufzählungen ein erheblicher Interpretationsspielraum. Daher hat die Datenschutzgruppe nach Art. 29 neun Kriterien erarbeitet, nach denen sich eine Verarbeitung mit hohem Risiko bestimmen lässt.[60] Da diese Kriterien vage formuliert wurden[61], existiert erhebliche Unsicherheit, in welchen Fällen in der Praxis tatsächlich eine DSFA durchzuführen ist.[62]
Gemäß der Datenschutzgruppe nach Art. 29 liegt auf jeden Fall ein hohes Risiko vor, wenn mindestens zwei der folgenden Kriterien zutreffen:[63]

[58] Vgl. BAUER/EICKMEIER/ECKARD (2018), S.152.
[59] Vgl. CALDER (2017), S. 55.
[60] Vgl. FEILER/HORN (2018), S. 62.
[61] Vgl. FEILER/HORN (2018), S. 65.
[62] Vgl. FRIEDEWALD (2017), S. 68.
[63] Vgl. FEILER/HORN (2018), S. 65.

- **Profiling/Scoring natürlicher Personen**

  Es werden Profile und Prognosen erstellt, insbesondere auf der Grundlage von „Aspekten, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel der Person betreffen“ (Erwägungsgrund 71 und 91).

  Beispiel für die Raiffeisen-Landesbank Steiermark AG:
  Einer Datenbank werden personenbezogene Daten, wie z.B. Lohn- und Gehaltsdaten, Bonitätsdaten, Lebens- und Konsumgewohnheiten, automatisiert verarbeitet und somit persönliche Aspekte bewertet. Die Datenbank vergibt schließlich ein Rating, ob der Kunde kreditwürdig ist oder nicht.

- **Vollständig automatisierte Entscheidungen**

  Verarbeitungen, auf deren Grundlage für Betroffene Entscheidungen getroffen werden sollen, „die Rechtswirkung gegenüber natürlichen Personen entfalten“ oder diese „in ähnlich erheblicher Weise beeinträchtigen“. Die Verarbeitung kann zum Ausschluss oder zur Benachteiligung von Personen führen.

  Verarbeitungsvorgänge, die keine oder wenige Auswirkungen auf Personen haben, erfüllen nicht dieses spezielle Kriterium.

- **Systematische Überwachung**

  Verarbeitungsvorgänge, die die Beobachtung, Überwachung oder Kontrolle von Betroffenen zum Ziel haben und auf beispielsweise über Netzwerke erfasste Daten oder auf „eine systematische [...] Überwachung öffentlich zugänglicher Bereiche“ (Art.35 Abs. 3 lit. c) zurückgreifen.

  Die systematische Überwachung stellt ein Kriterium dar, weil die personenbezogenen Daten möglicherweise in Situationen erfasst werden, in denen die Betroffenen unter Umständen nicht wissen, wer ihre Daten erfasst und wie die Daten verwendet werden. Darüber hinaus kann es vorkommen, dass die Betroffenen keine Möglichkeit haben, eine solche Verarbeitung ihrer in der Öffentlichkeit (oder in öffentlich zugänglichen Bereichen) erfassten Daten zu verhindern.

  Beispiel für die Raiffeisen-Landesbank Steiermark AG:
  Ein Bankomat betreibt ständige Videoüberwachung durch seine Kamera, um die überwachten Objekte bzw. Personen zu schützen. Alles was vor dem Bankomat passiert, wird rund um die Uhr aufgezeichnet.

- **Vertrauliche Daten oder höchst persönliche Daten (Sensible Daten)**

  Hierzu zählen besondere Kategorien personenbezogener Daten im Sinne von Art. 9 (z. B. Informationen über die politischen Meinungen von Einzelpersonen) sowie personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten im Sinne von Art. 10. Diese Daten gelten als vertraulich, da sie sich auf die Ausübung der Grundrechte auswirken oder die Verletzung mit ernsthaften Konsequenzen für den Alltag des Betroffenen einhergeht.

  Beispiel für die Raiffeisen-Landesbank Steiermark AG:
  Um das Rechenzentrum betreten zu können, werden biometrische Daten wie zum Beispiel das Gewicht des Mitarbeiters abgefragt.

- **Datenverarbeitung in großem Umfang**

  „In großem Umfang“ ist in der DSGVO nicht definiert, aber Erwägungsgrund 91 liefert einige Hinweise. In jedem Fall empfiehlt die Datenschutzgruppe nach Art. 29 die Berücksichtigung speziell folgender Faktoren, wenn ermittelt werden soll, ob die fragliche Verarbeitung in großem Umfang durchgeführt wird:

  - Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe
  - verarbeitete Datenmenge bzw. Bandbreite der unterschiedlichen verarbeiteten Datenelemente
  - Dauer oder Dauerhaftigkeit der Datenverarbeitung
  - geografisches Ausmaß der Datenverarbeitung

- **Abgleichen oder Zusammenführen von Datensätzen**

  z.B. solcher Datensätze, die aus zwei oder mehreren Datenverarbeitungsvorgängen stammen, die zu unterschiedlichen Zwecken und/oder von verschiedenen für die Datenverarbeitung Verantwortlichen durchgeführt wurden und zwar in einer Weise, die über die vernünftigen Erwartungen der Betroffenen hinausgeht.

Beispiel für die Raiffeisen-Landesbank Steiermark AG:
Es werden personenbezogene Daten wie z.B. persönliche Detailangaben, Haushaltsdaten und familiäre Verhältnisse, Daten zu Identitäts- und Reisedokumenten, Kontaktdaten, Daten zu Beruf und Arbeitsverhältnis, Aufenthaltsstatus, Steuerliche Daten und Sozialversicherungsdaten, Arbeitsorganisationsdaten, Beteiligungen, Zahlungsverkehrs- und Clearing-Daten, Anti-Money Laundering und Compliance-Daten für die Verarbeitungstätigkeit „Konto eröffnen" verarbeitet, um den Zahlungsverkehr durchführen zu können. Die Daten werden schließlich auch für Einlagengeschäfte, Finanzierungen, Wertpapiergeschäfte, Treasury-Geschäfte und Vermittlungsgeschäfte verwendet.

- **Daten schutzbedürftiger/besonders verwundbarer natürlicher Personen**
  Die Verarbeitung dieser Art von Daten stellt ein Kriterium dar, weil zwischen den Betroffenen und dem für die Datenverarbeitung Verantwortlichen ein größeres Machtungleichgewicht vorliegt; d. h. den Personen ist es unter Umständen nicht ohne weiteres möglich, der Verarbeitung ihrer Daten zuzustimmen bzw. dieser zu widersprechen oder ihre Rechte auszuüben.

  Als schutzbedürftige Betroffene gelten beispielsweise folgende Bevölkerungsgruppen: Kinder (bei ihnen kann nicht davon ausgegangen werden, dass sie in der Lage sind, der Verarbeitung ihrer Daten wissentlich und überlegt zuzustimmen bzw. zu widersprechen), Arbeitnehmer, Teile der Bevölkerung mit besonderem Schutzbedarf (psychisch Kranke, Asylbewerber, Senioren, Kunden usw.) und Betroffene in Situationen, in denen ein ungleiches Verhältnis zwischen der Stellung des Betroffenen und der des für die Verarbeitung Verantwortlichen vorliegt. Ein Arbeitnehmer gilt nicht als „besonders verwundbar", wenn ein Betriebsrat eingerichtet wurde.[64]

Beispiel für die Raiffeisen-Landesbank Steiermark AG:
Bei dem Verarbeitungsprozess „Kundenabwanderungen vorbeugen und bearbeiten" gibt es ein Machtungleichgewicht zwischen dem Verantwortlichen und den Kunden, da dieser Prozess nur auf der Rechtsgrundlage „berechtigtes Interesse" basiert und der Kunde nicht die Möglichkeit hat der Verarbeitung ihrer Daten zuzustimmen.
Wenn ein Verarbeitungsprozess auf der Rechtsgrundlage „Gesetzeserfüllung, Vertragserfüllung oder Einwilligung" basiert, trifft dieses Kriterium nicht zu, da der Kunde die Möglichkeit einer Zustimmung bzw. der Ausübung ihrer Rechte hat.

[64] Vgl. FEILER/HORN (2018), S. 66.

- **Neue Technologien oder neuartiger Einsatz von Technologien**

  Beispiel für die Raiffeisen-Landesbank Steiermark AG:
  Falls eine Fingerabdruck- und Gesichtserkennung zum Zwecke einer verbesserten Zugangskontrolle für jeden Mitarbeiter neu eingesetzt wird.

- **Datenverarbeitungen, die Betroffene an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern (Art. 22 und Erwägungsgrund 91)**

  Hierzu zählen Verarbeitungsvorgänge, mit deren Hilfe Betroffenen der Zugriff auf eine Dienstleistung oder der Abschluss eines Vertrags gestattet, geändert oder verwehrt werden soll.

  Beispiel für die Raiffeisen-Landesbank Steiermark AG:
  Eine Bank, die eine von Kreditauskunfteien betriebene Datenbank nach ihren Kunden durchsucht, um über Kreditvergaben zu entscheiden.

Für den Fall, dass unklar ist, ob eine DSFA erforderlich ist, empfiehlt die Datenschutzgruppe nach Art. 29 dennoch die Durchführung einer DSFA, weil den für die Verarbeitung Verantwortlichen damit ein hilfreiches Instrument für die Einhaltung der Datenschutzgesetze zur Verfügung steht. In einigen Fällen kann es vorkommen, dass ein für die Datenverarbeitung Verantwortlicher von der Notwendigkeit einer DSFA ausgehen muss, obwohl der fragliche Verarbeitungsvorgang nur eines dieser Kriterien erfüllt.
Folgendes Beispiel soll veranschaulichen, wie bei der Prüfung, ob eine DSFA wahrscheinlich notwendig ist, vorzugehen ist:

In der Raiffeisenlandesbank Steiermark AG werden personenbezogene Daten in dem Verarbeitungsprozess „Neufinanzierung durchführen“ verarbeitet.

- Liegt Profiling vor? **Ja**, da persönliche Aspekte (persönliche Daten wie zum Beispiel Daten zu Beruf und Arbeitsverhältnis, Lohn- und Gehaltsdaten, Lebens- und Konsumgewohnheiten und Bonitätsdaten) automatisiert verarbeitet werden.
- Liegt eine automatisierte Entscheidung mit Rechtswirkung vor? **Ja**, es wird eine automatisierte Entscheidung getroffen. Das Programm vergibt ein Rating und entscheidet über die Neufinanzierung.
- Liegt eine systematische Überwachung vor? **Nein**, da keine öffentlich zugänglichen Bereiche überwacht werden.
- Werden sensible Daten verarbeitet? **Nein**, es werden keine Daten der besonderen Kategorie personenbezogener Daten verarbeitet.

- Werden Daten in großem Umfang verarbeitet? **Ja**, da 26 unterschiedliche Datenkategorien verarbeitet werden und diese Anzahl einen großen Umfang in Bezug auf die maximal möglichen Datenkategorien von 33 darstellt. (Ja, da mehr als 17 Datenkategorien verarbeitet werden.)
- Werden Daten abgeglichen oder zusammengeführt? **Nein**, da die personenbezogenen Daten nicht in mehreren Verarbeitungstätigkeiten und zu unterschiedlichen Zwecken verarbeitet werden.
- Handelt es sich um Daten schutzbedürftiger Personen und gibt es ein Machtungleichgewicht? **Nein**, da zwar personenbezogen Daten von Kunden verarbeitet werden, aber der Kunde aufgrund eines Vertrages die Möglichkeit einer Zustimmung hat.
- Handelt es sich um eine neue Technologie? **Nein**.
- Werden Betroffene an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert? **Ja**, da die Kunden aufgrund eines schlechten Ratings daran gehindert werden einen Vertrag abzuschließen.

Notwendigkeit einer DSFA wahrscheinlich? **Ja**, da mindestens zwei Kriterien zutreffen!

Es kann vorkommen, dass ein für die Verarbeitung Verantwortlicher einen Verarbeitungsvorgang, der den vorgenannten Fällen entspricht, nicht als Vorgang bewertet, der „wahrscheinlich ein hohes Risiko mit sich bringt“. In einem solchen Fall muss der für die Verarbeitung Verantwortliche begründen und dokumentieren, warum er keine DSFA durchführt, und den Standpunkt des Datenschutzbeauftragten mit einbeziehen bzw. festhalten.

Schritt 2: Überprüfung der Ausnahmen

Aufsichtsbehörden dürfen weitere Datenverarbeitungen definieren und veröffentlichen in denen verpflichtend eine DSFA vorzunehmen ist („Blacklist“). Gemäß Art.35 Abs. 5 dürfen Aufsichtsbehörden Fälle definieren und veröffentlichen in denen eine DSFA explizit nicht notwendig ist („Whitelist“). Beide Listen wurden bereits veröffentlicht. [6566]

Wenn einer der nachfolgenden Punkte zutrifft, muss gemäß der Datenschutzgruppe nach Art. 29 ebenso keine DSFA durchgeführt werden:[67]

- wenn die Verarbeitung „wahrscheinlich [kein] hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt“ (Art. 35 Abs.1);
- wenn sich die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung von denen einer anderen Verarbeitung, für die bereits eine DSFA durchgeführt wurde, nur in geringem

65 Vgl. FEILER/HORN (2018), S. 62.
66 Vgl. ROßNAGEL (2017), S.115.
67 Vgl. Datenschutzgruppe nach Art. 29 (2017), S. 15.

Maße unterscheiden. In diesen Fällen können die DSFA-Ergebnisse einer solchen ähnlichen Verarbeitung verwendet werden (Art. 35 Abs. 119);

- wenn die Verarbeitungsvorgänge vor Mai 2018 von einer Aufsichtsbehörde unter bestimmten Bedingungen geprüft worden sind, die sich nicht geändert haben;
- falls ein Verarbeitungsvorgang gemäß Art. 6 Abs. 1 lit. c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht der Mitgliedstaaten beruht und diese Rechtsvorschrift den konkreten Verarbeitungsvorgang regelt und falls bereits im Rahmen der Schaffung dieser Rechtsgrundlage eine DSFA erfolgte (Art. 35 Abs. 10), es sei denn, ein Mitgliedstaat erklärt, dass es notwendig ist, vor den fraglichen Verarbeitungstätigkeiten eine DSFA durchzuführen;
- falls der Verarbeitungsvorgang auf einer (von der Aufsichtsbehörde erstellten) optionalen Liste der Verarbeitungsvorgänge aufgeführt ist, für die keine DSFA erforderlich ist (Art. 35 Abs. 5). Eine solche Liste kann Verarbeitungstätigkeiten enthalten, die die Voraussetzungen dieser Behörde erfüllen, die sie insbesondere in Form von Leitlinien, besonderen Beschlüssen oder Genehmigungen, Konformitätsvorschriften usw. festgelegt haben (z. B. in Frankreich, Genehmigungen, Befreiungen, vereinfachte Vorschriften, Konformitätspakete etc.). In solchen Fällen, die einer Überprüfung durch die zuständige Aufsichtsbehörde unterliegen, ist nur dann keine DSFA erforderlich, wenn die Verarbeitung genau einem Geltungsbereich des jeweils in der Liste aufgeführten Verfahrens entspricht und weiterhin ausnahmslos alle zutreffenden Voraussetzungen der DSGVO erfüllt.

Schritt 3: Durchführung einer DSFA

Nachdem überprüft wurde, ob ein potenziell hohes Risiko für die betroffene Person in einer Verarbeitungstätigkeit existiert und die Ausnahmen kritisch examiniert wurden, kommt man zum Ergebnis, ob die Durchführung einer DSFA notwendig ist. Wenn die Überprüfung ergibt, dass ein hohes Risiko besteht und keine Ausnahmen zutreffen, ist eine DSFA verpflichtend durchzuführen.

Im Hinblick auf den Zeitpunkt der Durchführung einer DSFA ist zu berücksichtigen, dass eine DSFA nach Art. 35 Abs. 1, Art. 35 Abs. 10 und nach den Erwägungsgründen 90 und 93 „vor den betreffenden Verarbeitungsvorgängen“ durchzuführen ist.[68] Des Weiteren muss eine DSFA für bereits laufende Verarbeitungsvorgänge, also für alte Verarbeitungstätigkeiten, die es bereits vor dem Geltungsbereich der DSGVO gab, durchgeführt werden, wenn nach erster Betrachtung ein hohes Risiko vorliegt.

Als einzige Ausnahme gilt, wenn die Verarbeitungstätigkeit:[69]

[68] Vgl. SCHWICHTENBERG (2018), S. 147.
[69] Vgl. FEILER/HORN (2018), S. 66.

- nach alter Rechtslage an die Datenschutzbehörde gemeldet wurde und im Rahmen der sogenannten Vorabkontrolle (§18 Abs. 2 DSG 2000) von der Datenschutzbehörde positiv geprüft und im Datenverarbeitungsregister geprüft wurde und
- die Verarbeitungstätigkeit seit der Registrierung nicht verändert wurde.

Die soeben erwähnten Ausnahmen können überprüft werden, indem man im Online-Datenverarbeitungsregister der Datenschutzbehörde die „Detailansicht" einer Datenanwendung aufruft und im Feld „Angaben zur Vorabkontrolle" nachsieht. Falls dort steht „Vorliegen keiner der Voraussetzungen", bedeutet dies, dass keine Prüfung durch die Datenschutzbehörde vorgenommen wurde. Wenn das Feld „Angaben zur Vorabkontrolle" aber einen der folgenden Inhalte aufweist, bedeutet dies, dass bereits eine positive Prüfung der Datenschutzbehörde durchgeführt wurde und aus diesem Grund keine DSFA erforderlich ist:[70]

- Verwendung von sensiblen Daten,
- Verwendung von strafrechtlich relevanten Daten,
- Vorliegen eines Kreditinformationssystems oder
- Videoüberwachung (gemäß § 50c DSG 2000).

Ansonsten muss die DSFA bereits in der Entwicklungsphase der Verarbeitungstätigkeit zum frühestmöglichen Zeitpunkt begonnen werden, auch wenn einige Verarbeitungsvorgänge noch nicht bekannt sind. Aus dem Erwägungsgrund 89 geht jedoch hervor, dass für bereits bestehende Verarbeitungstätigkeiten eine DSFA notwendig werden kann und diese somit ebenso zu überprüfen sind. Hier sei hervorgehoben, dass die Durchführung einer DSFA keine einmalige Aufgabe, sondern einen kontinuierlichen Prozess darstellt.[71]

Am Rande sei auch erwähnt, dass der für die Verarbeitung Verantwortliche in Kooperation mit dem Datenschutzbeauftragten und den Auftragsverarbeitern eine DSFA durchzuführen haben. Gemäß Art. 35 Abs. 2 hat der für die Verarbeitung Verantwortliche dafür zu sorgen, dass die DSFA durchgeführt wird.[72] Die eigentliche Durchführung einer DSFA kann durch eine andere Person erfolgen, im Falle der Raiffeisen-Landesbank Steiermark AG entweder durch eine Person ihrerseits oder durch eine ausgelagerte Person. Zur letztlich zur Rechenschaft gezogene, stellt aber der für die Verarbeitung Verantwortliche dar.

Bei der Durchführung einer DSFA kann gemäß Art. 35 Abs. 2 der für die Verarbeitung Verantwortliche den Rat des Datenschutzbeauftragten einholen.[73] Dabei sind der Rat und auch die Entscheidungen, die für die Verarbeitung Verantwortlichen getroffen werden, explizit zu

[70] Vgl. FEILER/HORN (2018), S. 67.
[71] Vgl. Datenschutzgruppe nach Art. 29 (2017), S. 17 ff.
[72] Vgl. FEILER/HORN (2018), S. 61.
[73] Vgl. SCHMIDT/SCHWEIßGUTH/HOFFMANN/HUMMEL (2018), S. 43.

dokumentieren. Falls die Verarbeitung vollständig oder nur teilweise durch einen Auftragsverarbeiter erfolgt, muss dieser den für die Verarbeitung Verantwortlichen bei der Durchführung der DSFA unterstützen und notwendige Informationen zur Verfügung stellen.
An dieser Stelle ist auch anzumerken, dass der Verantwortliche nach Art. 35 Abs. 9 „gegebenenfalls“ den Standpunkt der betroffenen Personen oder ihrer Vertreter einzuholen hat. Die Datenschutzgruppe nach Art. 29 ist der Auffassung, dass:[74]

- die Einholung des Standpunktes auf verschiedensten Wegen erfolgen kann – und zwar je nach dem welcher Kontext vorliegt (z.B. eine generische Studie zu Zweck und Mitteln der Verarbeitung, eine Frage an die Arbeitnehmervertreter oder gewöhnliche Umfragen, die an die potenziellen Kunden des für die Datenverarbeitung Verantwortlichen gesendet werden) und ob sich der Verantwortliche auf eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten im Rahmen einer solchen Kommunikation stützen kann. Die Einholung des Standpunktes stellt jedoch keine Zustimmung zur Verarbeitung dar.
- sofern die endgültige Entscheidung des für die Datenverarbeitung Verantwortlichen vom Standpunkt der Betroffenen abweichen sollte, die Gründe für das weitere Fortfahren dokumentiert werden müssen.
- der für die Verarbeitung Verantwortliche zudem seine Begründung für den Verzicht auf die Einholung des Standpunktes der Betroffenen dokumentieren muss, nämlich wenn er eine solche Einholung für nicht angemessen hält, weil sie z. B. eine Verletzung der Geheimhaltungspflichten bezüglich der Geschäftspläne des Unternehmens darstellen würde oder unverhältnismäßig bzw. impraktikable wäre.

Laut FRIEDEWALD stellt die Mitwirkung der Betroffenen eine besondere Herausforderung an Zeitpunkt und Umstände dar und er steht – wie in de nachfolgenden Ausführungen ersichtlich – der Einholung des Standpunktes daher eher kritisch gegenüber. Erstens ist er der Meinung, dass bei einer DSFA, die vor der Markteinführung bzw. parallel zum Entwicklungsprozess durchgeführt wird, die Einbeziehung von externen – unter Umständen kritisch eingestellten – Personengruppen unpassend sind, da Betriebs- und Geschäftsgeheimnisse betroffen sind und auch aus Imagegründen keine unausgereiften Lösungen offen gelegt werden sollen. Zweitens kann die Einholung des Standpunktes der Betroffenen ein Problem darstellen, da eine sorgfältige und systematische Bewertung häufig Fachwissen erfordert, das bei technischen Laien nicht als gegeben angenommen werden kann. Hiermit muss man sich mit der Frage auseinandersetzen, wie sich dieses Fachwissen vermitteln lässt, um eine Diskussion „auf Augenhöhe“ zwischen Laien und Experten zu ermöglichen. Drittens hat das für das Bewertungsverfahren verwendete Sprachgut Folgen für die Intensität und Qualität der Einbeziehung unterschiedlicher Akteursgruppen. Daher dürften manche Formulierungsweisen

[74] Vgl. Datenschutzgruppe nach Art. 29 (2017), S. 18.

vor allem technophilen Akteuren oder solchen mit Rechtskenntnissen besonders entgegenkommen. Hierbei ist zu klären, wie sich Übersetzungsprozesse zwischen den beteiligten Gruppen erfolgreich arrangieren lassen. Außerdem werden detaillierte partizipative DSFAs unter Einholung des Standpunktes von Externen eher die Ausnahme bleiben, da dieser Prozess zeitaufwendiger ist und es bei bestimmten Akteursgruppen rapid zu einer „Konsultationsmüdigkeit“ kommen kann.[75]

Auch darf nicht unerwähnt bleiben, dass bei der Durchführung einer DSFA gemäß Art. 40 Verhaltensregeln zu berücksichtigen sind. Auch sollten nach Art. 42 Zertifizierungen, Siegel und Prüfzeichen Berücksichtigung finden, die dem Nachweis darüber dienen, dass die DSGVO bei Verarbeitungsvorgängen von Verantwortlichen oder Auftragsverarbeitern ebenso eingehalten wird, wie verbindliche interne Datenschutzvorschriften. Darüber hinaus hat der Verantwortliche gemäß Art. 35 Abs. 11 zu überprüfen, ob die Verarbeitung bei Änderung des Risikos bei einem Verarbeitungsvorgang gemäß der DSFA durchgeführt wird.

[75] Vgl. FRIEDEWALD (2017), S. 71.

Um einen Überblick darüber zu bekommen, wie eine DSFA durchgeführt wird, wird nachfolgend das generische Iterationsverfahren für die Durchführung dieser veranschaulicht.

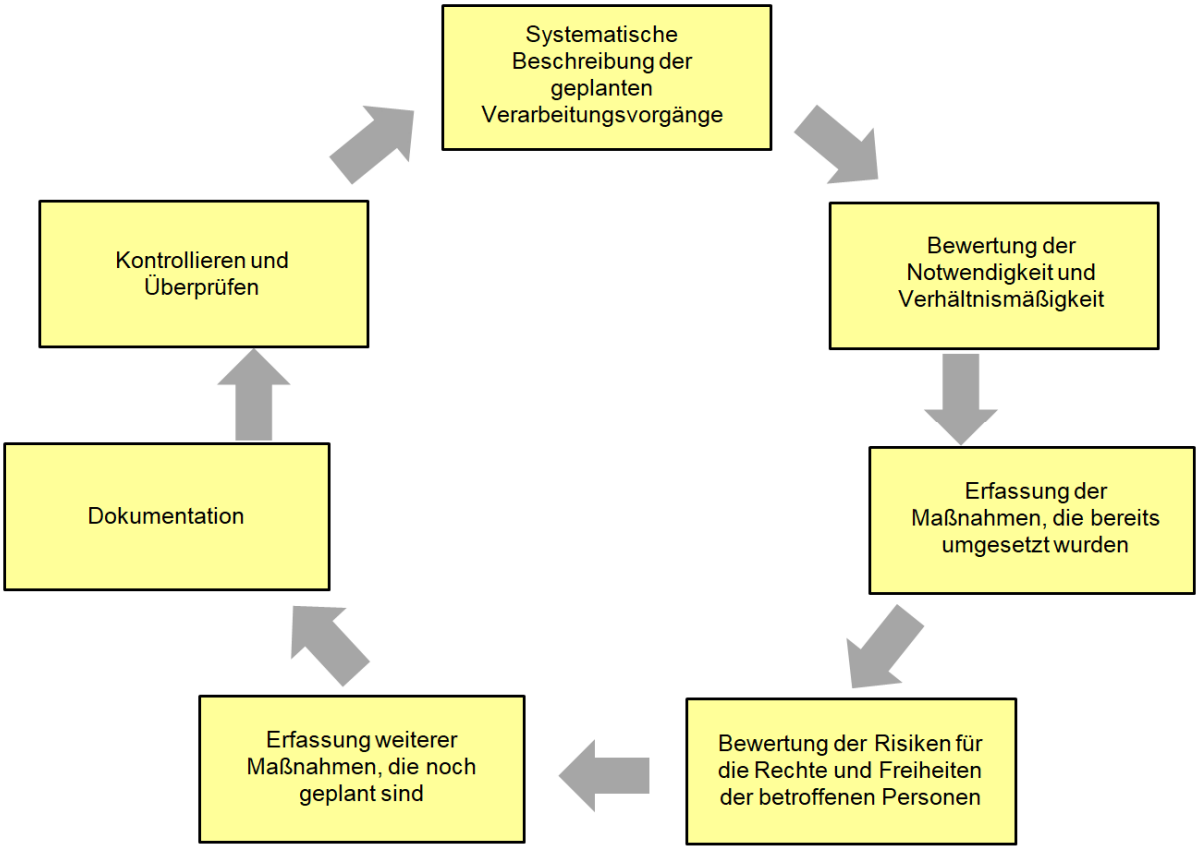


Abbildung 5: Datenschutz-Folgenabschätzungs-Prozess,
Quelle: in Anlehnung an Datenschutzgruppe nach Art. 29 (2017), S. 20.

Schritt 4: Konsultation der Aufsichtsbehörde

In Fällen, in denen der für die Datenverarbeitung Verantwortliche keine hinreichenden Maßnahmen bestimmen kann, mit denen sich die Risiken auf ein vertretbares Maß reduzieren lassen (d. h. es bestehen weiterhin hohe Restrisiken), ist eine Konsultation der Aufsichtsbehörde erforderlich.[76]

Prüfplanung

Wenn nun eine DSFA durchzuführen ist, müssen als nächstes Ziele und Rahmenbedingungen festgelegt werden und ein eigenes Team zusammengestellt werden. Das Team muss definieren, welchen Charakter die DSFA besitzen soll. Dies muss später bei der Veröffentlichung der Ergebnisse kommuniziert werden.[77]

[76] Vgl. GEIST (2017), S. 19.
[77] Vgl. FRIEDEWALD (2018), S. 70.

Des Weiteren ist zwischen folgenden drei Typen von DSFAs zu unterscheiden:

- Marketing-DSFA
- Standard-DSFA (DSFA im engeren Sinne)
- wissenschaftliche DSFA (DSFA im weiteren Sinne)

Die Standard-DSFA ist die einzige Methode, die am ehesten den Vorstellungen des europäischen Gesetzgebers entspricht. Das Ziel der DSFA im engeren Sinne ist, einen Nachweis zu liefern, dass ein Datenverarbeitungssystem konform mit den datenschutzrechtlichen Anforderungen ist. Auch Schutzmaßnahmen sollen für dieses System identifiziert werden. Die Ergebnisse werden dokumentiert und veröffentlicht.[78][79]

Beschreibung des Prüfgegenstandes und der Zwecke der Verarbeitung

Um beurteilen zu können, ob wahrscheinlich ein hohes Risiko existiert, muss der Verantwortliche einen Überblick über die Datenverarbeitung haben. Daher fordert Art. 35 Abs. 7 lit. a DSGVO eine systematische Beschreibung der Verarbeitungstätigkeiten und ihrer Zwecke.[80] Es ist auch zu begründen, warum die Datenverarbeitung für die verfolgten Zwecke notwendig und verhältnismäßig ist.[81]

Identifikation der Akteure und der betroffenen Personen

Ein weiterer wesentlicher Punkt der Vorbereitungsphase stellt die Identifikation der Akteure und der betroffenen Personen dar. Zu identifizieren sind insbesondere

- der Hersteller des Prüfgegenstandes;
- der Betreiber des Prüfgegenstandes, etwa als Dienstleister im Rahmen einer Auftragsverarbeitung;
- Mitarbeiter der für den Einsatz des Prüfgegenstandes verantwortlichen Organisation;
- und Dritte, die im Zuge des Einsatzes des Prüfgegenstandes Kenntnis von personenbezogenen Daten nehmen, entweder zufällig oder absichtlich.

Die betroffenen Personen nach Art. 35 Abs. 9 DSGVO in ihren Rollen als Bürger, Kunde, Arbeitnehmer etc.[82]

Identifikation der relevanten Rechtsgrundlagen

Wie bereits in Kapitel 1 erwähnt, müssen für jede Verarbeitungstätigkeit die Rechtsgrundlagen bestimmt werden.[83]

[78] Vgl. Datenschutzgruppe nach Art. 29 (2017), S. 21.
[79] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 135.
[80] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 135.
[81] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 136.
[82] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 136.
[83] Vgl. FRIEDEWALD (2017), S. 69.

Dokumentation der Ergebnisse

Die Ergebnisse der Vorbereitungsphase sind zu dokumentieren.[84]

3.3. Grundlagen der Bewertungsphase

In der Bewertungsphase werden zunächst die Schutzziele definiert. Anschließend werden mögliche Angreifer, deren Motive und Ziele bestimmt. Näheres über die Bewertungsphase wird im nächsten Hauptkapitel „Datenschutz-Risikomanagement“ untersucht.

Identifikation der Bewertungsmaßstäbe mit Hilfe der Schutzziele

Unter Schutzziele versteht man die Anforderungen des Datenschutzes, die gesetzlich normiert sind und zwar die bereits erwähnten Grundsätze der DSGVO[85].[86] Die Schutzziele thematisieren wesentliche datenschutzrechtliche Risiken. Des Weiteren gelten im Bereich des Datenschutzes folgende klassische Schutzziele als etabliert:[87]

- Vertraulichkeit: Darunter versteht man, dass personenbezogene Daten vor unbefugter und unbeabsichtigter Preisgabe geschützt werden müssen. Dabei sind die Daten vor externen wie internen Angreifern (z.B. Cyberkriminelle, Hacker, frustrierte oder neugierige Mitarbeiter etc.) sowie fahrlässigen oder strukturellen Gefährdungen (z.B. ungeschulte Mitarbeiter, mangelhafte Rollen/Rechtekonzepte, Mängel in der Datenschutzorganisation etc.) zu bewahren.
- Integrität: Dieses Schutzziel bedeutet, dass die Bereitstellung personenbezogener Daten richtig und vollständig erfolgen muss. Unzulässige Änderungen an Daten sollten erkannt werden und Verfahren zur Berichtigung sind vorzuhalten.
- Verfügbarkeit: Wenn personenbezogene Daten benötigt werden, dann müssen diese auch zur Verfügung stehen. Es ist zu berücksichtigen, dass eine Wiederherstellung der Daten bei Verlust oder Vernichtung möglich sein muss.

Identifikation möglicher Angreifer, Angriffsmotive und Angriffsziele

Laut LEPPERHOF und MÜTHLEIN können Angriffe nicht nur durch Dritte, sondern auch durch interne Anwender der Organisation erfolgen. Die Autoren definieren staatliche Stellen, wie Sicherheitsbehörden oder die Leistungsverwaltung, und Unternehmen, wie IT-Dienstanbieter, Banken, oder Interessensvereinigungen sowie Gesundheitsdienstleister oder Forschungsstellen als potenzielle Angreifer, die auf ihre Motive und Ziele zu analysieren sind.[88]

---

84 Vgl. HANSEN (2016), S. 587.
85 S. Kapitel 2.2. Die Grundsätze der Datenschutz-Grundverordnung, S. 13 ff.
86 Vgl. SOWA (2017), S. 26.
87 Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 139.
88 Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 139.

Bewertung des Risikos

Das Hauptaugenmerk der DSFA liegt auf der Risikobewertung. Art. 35 Abs. 7 regelt das Erfordernis der Bewertung der Risiken für die Rechte der Betroffenen. Nach Erwägungsgrund 90 DSGVO ist für jedes Risiko die Eintrittswahrscheinlichkeit und die Schwere zu bestimmen.[89] Da der Kern der DSFA die Risikobewertung ist, wird sich das nächste Kapitel „Datenschutz-Risikomanagement" ausführlicher damit befassen.[90]

3.4. Die Eckpfeiler der Maßnahmenphase

In der Maßnahmenphase erfolgt die Umsetzung der Risikobewertung und passende Schutzmaßnahmen werden identifiziert. Zudem fordert Art. 35 Abs. 7 lit. d DSGVO, dass im Rahmen der DSFA Maßnahmen getroffen werden, die die ermittelten Risiken bewältigen und es muss der Nachweis erbracht werden, dass DSGVO-konform gehandelt wird. Dabei sind die Rechte und berechtigten Interessen der betroffenen Personen zu beachten.

Identifikation und Auswahl passender Schutzmaßnahmen

In der Maßnahmenphase müssen passende Schutzmaßnahmen identifiziert werden. Es ist ein Katalog typischer Schutzmaßnahmen zu erstellen.[91]

Implementierung der Maßnahmen

Nachdem geeignete Maßnahmen ausgewählt wurden, müssen diese auch umgesetzt werden.[92] Die Umsetzung betrifft technisch-organisatorische Maßnahmen, wie zum Beispiel hardware- oder softwarebasierte Funktionalität für einen besseren Schutz personenbezogener Daten, Konfigurationsanpassungen oder Konzepte mit Festlegungen der Rollen und Rechte.[93] Im Hinblick auf die Identifikation und der Implementierung der Maßnahmen wird im nächsten Kapitel „Datenschutz-Risikomanagement" näher eingegangen.[94]

Test und Dokumentation der Wirksamkeit

Die alleinige Implementierung der Maßnahmen ist nicht ausreichend. Die Wirksamkeit der Maßnahmen ist auch zu testen und zu dokumentieren. Des Weiteren sind die Durchführungen der Tests als auch die Testergebnisse festzuhalten.[95]

Dokumentation der Bewertungsergebnisse

Anschließend sind die Bewertungsergebnisse zu dokumentieren. Dabei sind nicht nur die erfolgreich eindämmbaren Risiken zu belegen, sondern auch die Risiken, die nicht durch

[89] Vgl. BOZKURT (2018), S. 62.
[90] S. Kapitel 4.2.2. Die Risikobewertung als Vorstufe zur Risikosteuerung, S. 57.
[91] Vgl. SCHWARTMANN/JASPERS/THÜSING/KUGELMANN (2018), S. 140.
[92] Vgl. VOIGT/VON DEM BUSSCHE (2018), S. 51.
[93] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 144.
[94] S. Kapitel 4.2.3. Mögliche Strategien zur Steuerung der Risiken, S. 61.
[95] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 144.

entsprechende Maßnahmen beseitigt werden können. Dadurch entstehen Restrisiken, welche gerechtfertigt werden müssen. Falls es sich bei solch einem Restrisiko um ein hohes Risiko handelt, darf das untersuchte System nicht freigegeben werden und auch nicht zum Einsatz kommen. In solch einem Fall wären die Anforderungen der DSGVO nicht erfüllt. [96] Gemäß Art. 36 DSGVO ist der Verantwortliche vor der Verarbeitung dazu verpflichtet, die Aufsichtsbehörde zu kontaktieren („vorherige Konsultation"), welche dann die DSFA überprüfen und Empfehlungen diesbezüglich abgeben.[97]

Nachweis über die Einhaltung der Datenschutz-Grundverordnung

Eine Dokumentation der Verarbeitungstätigkeiten, der Risiken und der Maßnahmen ist notwendig. Diese Dokumentation dient schließlich als Grundlage für den DSFA-Bericht.[98]

3.5. Die Erstellung eines Berichts im Rahmen der Berichtsphase

Im Rahmen der Berichtsphase ist ein DSFA-Bericht zu erstellen, welcher veröffentlicht werden kann. Außerdem muss eine unabhängige Überprüfung der Ergebnisse durchgeführt werden.

Erstellung eines DSFA-Berichts

Gemäß Art. 35 Abs. 7 muss die DSFA folgende Punkte enthalten:[99]

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und Zweck der Verarbeitung (gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten Interessen)
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen
- die zur Bewältigung der Risiken geplanten Maßnahmen (einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird, und die Festlegung eines Beteiligten, der für die Maßnahmen zuständig ist)

Veröffentlichung des DSFA-Berichts

Eine Kurzversion des DSFA-Berichts sollte im Sinne der Transparenz veröffentlicht werden. Dabei ist zu berücksichtigen, dass Geschäftsgeheimnisse sowie die Restrisikoanalyse, die sonst als Angriffsvorlage missbraucht werden könnte, geschützt und nicht in der Öffentlichkeit verbreitet werden. Es sollten die wesentlichen Informationen dargelegt werden und keine

[96] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 144.
[97] Vgl. VON WALTER (2018), S. 349.
[98] Vgl. VON WALTER (2018), S. 349.
[99] Vgl. REINIS (2017), S.85.

(negativen) Ergebnisse verschwiegen werden. Besonders hervorzuheben ist, dass nach der DSGVO die Veröffentlichung des Berichts nicht erforderlich ist.[100]

Unabhängige Überprüfung der DSFA-Ergebnisse

Der DSFA Bericht sollte von einem unabhängigen Dritten, beispielsweise der zuständigen Aufsichtsbehörde, überprüft werden, um sicherzustellen, dass der DSFA Bericht angemessen durchgeführt wurde. Des Weiteren kann eine unabhängige Überprüfung der DSFA Glaubwürdigkeit verleihen, die Transparenz verbessern, aus Erfahrung lernen lassen und die Qualität der DSFA verbessern.[101]

Überwachung und Fortschreibung im Datenschutz-Management

Besonders zu erwähnen ist, dass die DSFA keinen strikt linearen und abgeschlossenen Prozess darstellt, sondern diese muss über den gesamten Lebenszyklus des Projekts fortlaufend überwacht werden. Zudem regelt Art. 35 Abs. 11 DSGVO, dass die DSFA zumindest dann zu wiederholen ist, wenn sich das mit der Verarbeitung einhergehende Risiko verändert. Zu solch einer Änderung kann es durch Veränderung der organisatorischen oder rechtlichen Rahmenbedingungen oder der Risiken kommen. Die Anpassung der Maßnahmen ist stets zu gewährleisten. Damit auf Veränderungen der Rahmenbedingungen effizient reagiert werden kann, sollte das Datenschutz-Management eingebunden werden.[102]

[100] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 145.
[101] Vgl. REINIS (2017), S. 57.
[102] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 146.

4. Datenschutz-Risikomanagement

Da der Schwerpunkt der DSFA auf dem Risikomanagement liegt, wird sich dieses Kapitel näher mit dem spezifischen Datenschutz-Risikomanagement befassen. Dabei wird zuerst auf wesentliche Grundlagen des klassischen Risikomanagement und des Datenschutz-Risikomanagements eingegangen. Danach findet der gesamte Risikomanagementprozess Erwähnung. Zudem wird zunächst die Risikoidentifikation beleuchtet. Es wird aufgezeigt, wie die Risiken in der Bank kategorisiert werden können. Auch mögliche Risikoquellen, Datenschutz-und Datensicherheitsrisiken sowie potenzielle Folgen der Risiken werden betrachtet. In weiterer Folge werden die Methoden zur Risikoidentifikation kritisch dargestellt. Das nächste Unterkapitel beschäftigt sich mit dem zweiten Schritt des Risikomanagementprozesses, der Risikobewertung. Die Verfasserin setzt sich dabei mit den Anforderungen der Bewertung und den möglichen Bewertungskategorien auseinander. Anschließend wird auf die Risikomatrix eingegangen. Im Rahmen des dritten Schrittes des Risikomanagementprozesses, der Risikosteuerung, werden die einzelnen Risikostrategien beschrieben. Abschließend wird der vierte Schritt des Risikomanagementprozesses, die Risikoüberwachung und das Risikoreporting, näher erläutert.

4.1. Grundlagen des Datenschutz-Risikomanagements

Um die DSGVO Vorgaben einzuhalten, ist eine adäquate Berücksichtigung der Risiken von wesentlicher Bedeutung. Der Risikobegriff wird an verschiedenen Stellen in der DSGVO erwähnt (beispielsweise in Art. 35, 36: DSFA und Art. 33 und 34: Datenschutzverletzungen) und ist einheitlich zu interpretieren und anzuwenden. Besonders hervorzuheben ist, dass der Risikobegriff in der DSGVO nicht definiert wird, auch wenn im Erwägungsgrund 75 Beispiele für Risiken genannt werden. KRANIG, SACHS und GIESCHMANN empfehlen, sich bei der Umsetzung der DSGVO Vorgaben der DSFA, an bereits existierenden Ansätzen des Risikomanagements zu orientieren. Ebenso soll das Datenschutz-Risikomanagement als Teil des unternehmensweiten Risikomanagements gesehen werden.[103]

Definition des Risikobegriffs

Nach den bereits existierenden Ansätzen des Risikomanagements definieren DENK, EXNER-MERKELT und RUTHNER den Begriff „Risiko“ als die Gefahr einer negativen Abweichung von den Unternehmenszielen.[104] Daher könnte man im Rahmen des Datenschutz-Risikomanagements den Begriff „Risiko“ als die Gefahr einer negativen Abweichung von den

[103] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 78.
[104] Vgl. DENK/EXNER-MERKELT/RUTHNER (2008), S. 29.

Schutzzielen betrachten.[105] In der ISO 31000, welches einen internationalen Standard für das Risikomanagement darstellt, wird Risiko als „Auswirkung von Unsicherheit auf Ziele“ bezeichnet.[106]

Definition des Risikomanagementbegriffs

Aufbauend auf den Risikobegriff kann Risikomanagement als systematisches Denken und Handeln im Umgang mit Chancen und Gefahren (Risiken) definiert werden. Die Risikoanalyse, Risikoaggregation, Risikoüberwachung, Risikobewältigung und die Nutzung von Risikoinformationen bei unternehmerischen Entscheidungen stellen eine Teilaufgabe des Risikomanagements dar. Dabei betont GLEIßNER, dass das Risikomanagement nicht darauf abzielt, die Risiken im Unternehmen möglichst klein zu halten oder sogar vollständig zu eliminieren, denn unternehmerisches Handeln ist ohne das Eingehen von Risiken nicht vorstellbar.[107]

Ziele des Risikomanagements

In der ISO 31000 werden die Ziele klassifiziert nach Ziele betreffend die Führung, die Risikobeurteilung und die Ergebnisse des Risikomanagements.
Ziele betreffend die Führung sind:[108]

- eine proaktive Führung anstelle von reaktiver Führung fördern
- die Führung der Organisation verbessern
- die Steuerungs- und Kontrollmechanismen verbessern
- eine zuverlässige Grundlage für die Entscheidung und Planung aufbauen
- das Lernen der Organisation verbessern
- das Vertrauen der Stakeholder verbessern

Ziele betreffend die Risikobeurteilung sind:[109]

- die Risikoidentifikation und die Risikobewältigung durch die Organisation hindurch bewusst machen
- die Erkennung von Chancen und Gefahren bzw. Bedrohungen verbessern
- die Ressourcen für die Bewältigung wirksam zuteilen und nutzen
- mit relevanten gesetzlichen und regulatorischen Anforderungen sowie mit internationalen Normen überein stimmen
- das finanzielle Reporting verbessern

[105] Vgl. KÖNIGS (2013), S. 40.
[106] Vgl. BRÜHWILER/ROMEIKE (2010), S. 88.
[107] Vgl. GLEIßNER (2017), S. 21.
[108] Vgl. BRÜHWILER/ROMEIKE (2010), S. 92.
[109] Vgl. BRÜHWILER/ROMEIKE (2010), S. 93.

Ziele betreffend die Ergebnisse des Risikomanagements sind:[110]

- die operationelle Leistungsfähigkeit und Wirksamkeit verbessern
- die Widerstandsfähigkeit der Organisation erhöhen
- die Gesundheit und Sicherheit erhöhen
- das Management von Vorkommnissen, die Schadensverhütung verbessern
- Schadenfälle minimieren

Grundsätze des Risikomanagements

Gemäß ISO 31000 gelten folgende Risikomanagementgrundsätze als etabliert:[111][112]

- schafft Werte
- ist integraler Bestandteil aller Geschäftsprozesse (prozessbezogen)
- ist Teil der Entscheidungsfindung (entscheidungsbezogen)
- adressiert gezielt die Unsicherheiten (wahrscheinlichkeitsbezogen)
- ist systematisch, strukturiert und zeitgerecht (ergebnisbezogen)
- basiert auf den bestverfügbarsten Informationen (informationsbezogen)
- ist maßgeschneidert (situationsbezogen)
- berücksichtigt soziale und kulturelle Faktoren (kulturbezogen)
- ist transparent und integrativ (bedeutungsbezogen)
- ist dynamisch, iterativ und reagiert gezielt auf Veränderungsprozesse (änderungsbezogen)
- erleichtert kontinuierliche Verbesserung (zukunftsbezogen)

Risikomanagementsystem

Das Risikomanagementsystem umfasst verschiedene Elemente, welche die Grundlage für die organisatorische Gestaltung zur Entwicklung, Einführung, Überwachung, Überprüfung und kontinuierlichen Verbesserung des Risikomanagements innerhalb der Organisation bilden. Das Risikomanagementsystem gemäß ISO 31000 setzt sich aus fünf Elementen zusammen:[113]

- Auftrag und Selbstverpflichtung
- Entwicklung eines Systems für das Managen von Risiken (PLAN)
- Einführung des Risikomanagements (DO)
- Überwachung und Überprüfung des Systems (CHECK)
- Kontinuierliche Verbesserung des Systems (ACT)

[110] Vgl. BRÜHWILER/ROMEIKE (2010), S. 93.
[111] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 90 ff.
[112] Vgl. BRÜHWILER (2016), S. 58 ff.
[113] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 91.

In der nachfolgenden Abbildung wird das Risikomanagementsystem veranschaulicht:

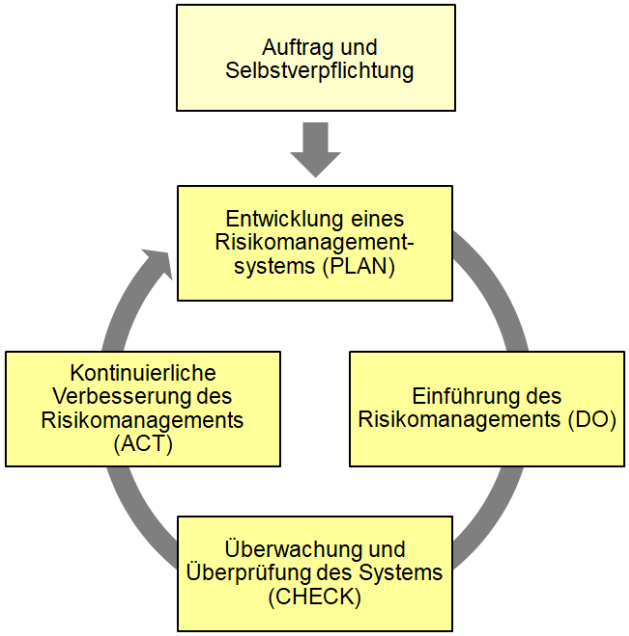


Abbildung 6: Elemente des Risikomanagementsystems,
Quelle: in Anlehnung an KRANIG/SACHS/GIERSCHMANN (2017), S. 91.

4.2. Der revolvierende Risikomanagementprozess

Nachdem die wesentlichen Grundlagen des Risikomanagements aufbereitet wurden, kann in weiterer Folge auf den sequenziellen Risikomanagementprozess näher eingegangen werden. In der folgenden Abbildung auf der nächsten Seite wird der Prozess gemäß ISO 31000, welcher aus fünf Schritten besteht, dargestellt. Zu Beginn ist der Kontext festzulegen. Dabei werden externe als auch interne Parameter festgelegt, die beim Risikomanagement zu berücksichtigen sind. Der zweite Schritt stellt die Risikobeurteilung dar, wobei gemäß ISO 31000 eine weitere Gliederung in den Prozess der Risikoidentifikation, der Risikoanalyse und der Risikobewertung erfolgt. Im Rahmen des dritten Schrittes wird die Risikobehandlung durchgeführt. Danach werden die Risiken überwacht und überprüft. Im Wesentlichen werden die Risiken in diesem weiteren Schritt fortlaufend gesteuert und die Durchführung der Risikomaßnahmen, des Risikomanagementprozesses, sowie das Risikomanagement werden auf Angemessenheit und Wirksamkeit kontrolliert. Im Rahmen des letzten Schrittes erfolgt die Risikokommunikation und -konsultation, welcher einen kontinuierlichen und iterativen Prozess darstellt, um Informationen zu erheben, zu teilen und, um die Stakeholder am Dialog bezüglich des Managements von Risiken zu beteiligen.[114][115]

[114] Vgl. KÖNIGS (213), S. 64 ff.
[115] Vgl. GLEIßNER (2017), S. 81.

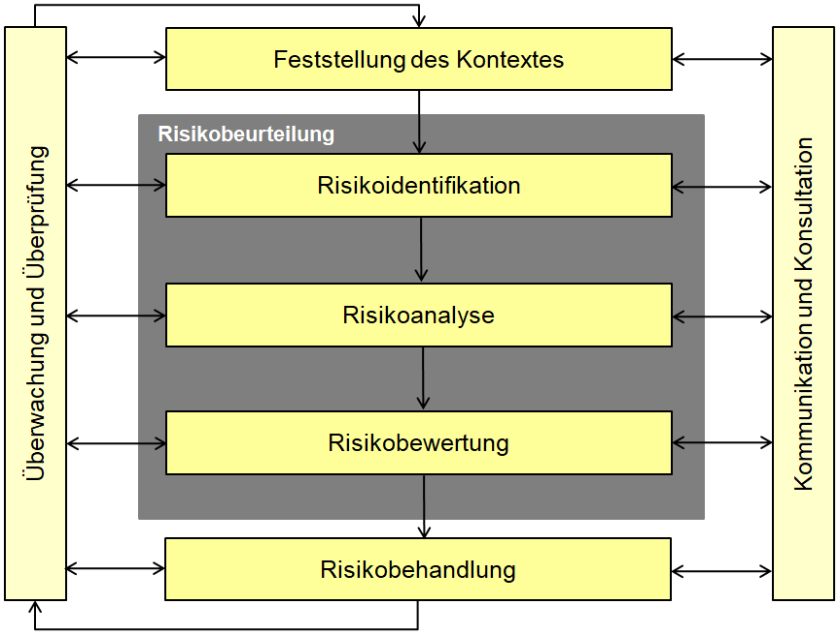


Abbildung 7: Risikomanagementprozess nach ISO 31000,
Quelle: KÖNIGS (2013), S. 64.

Die Autoren ROMEIKE und HAGER klassifizieren den Risikomanagementprozess in vier Phasen, wobei die einzelnen Schritte anders benannt werden.

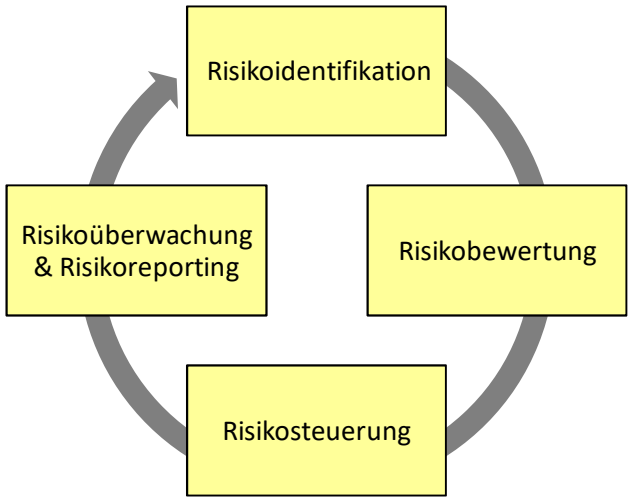


Abbildung 8: Der strategische und operative Risikomanagementprozess,
Quelle: in Anlehnung an ROMEIKE/HAGER (2009), S. 121.

Da der 4-Schritte-Prozess in der Literatur als etabliert gilt, finden in weiterer Folge die vier Schritte Risikoidentifikation, Risikobewertung, Risikosteuerung, Risikoüberwachung inklusive Risikoberichterstattung Erwähnung.

4.2.1. Die Risikoidentifikation als Schlüsselphase

Die Risikoidentifikation stellt die Schlüsselphase im Risikomanagementprozess dar und bestimmt dessen Effektivität und Effizienz. Ziel dieser ersten Phase ist die aktuelle, systematische, vollständige und wirtschaftliche Erfassung aller Gefahrenquellen, Schadensursachen, Störpotenziale und Chancen sowie deren Abhängigkeiten und wechselseitigen Beziehungen.[116] Es sind nicht nur bereits bestehende Risiken, sondern auch zukünftige mögliche Risiken zu erfassen. Dabei spielt die Informationsbeschaffung eine wesentliche Rolle.[117] Zu den Aufgaben der Risikoidentifikation zählen nicht nur die systematische und strukturierte Erhebung aller relevanten Risiken, sondern auch die Kategorisierung und Gruppierung der Risiken.[118] Außerdem ist die Risikoidentifikation laufend durchzuführen, da Unternehmen und deren Umfeld einem ständigen Wandel ausgesetzt sind.[119] Besonders zu betonen ist, dass die umfassende Identifikation der Risiken von zentraler Bedeutung ist, da ein nicht erfasstes Risiko im Risikomanagementprozess nicht bewertet und gesteuert werden kann.[120]

In Bezug auf das Datenschutz-Risikomanagement werden im Rahmen der Risikoidentifikation mögliche Risikoszenarien und jene daraus resultierenden potenziellen Folgen identifiziert. Dabei sind mögliche Risikoquellen[121] (interne und externe Personen, nicht-menschliche Quellen), die sich auf Schwachstellen im Zusammenhang mit der Verarbeitung von personenbezogenen Daten beziehen, zu berücksichtigen. Des Weiteren sind für die identifizierten Bedrohungen die möglichen Ereignisse (Folgen) zu analysieren. Danach sind diese Ergebnisse zu dokumentieren. Auch im Datenschutz-Risikomanagement besteht die Schwierigkeit darin, alle relevanten Szenarien zu berücksichtigen. Deshalb ist es wichtig, dass man die richtigen Personen mit der erforderlichen Qualifikation und Erfahrung für die Risikoidentifikation auswählt.[122]

Als Nächstes wird auf eine mögliche Kategorisierung der Risiken eingegangen, um im Praxisoutput die Risiken bestmöglich klassifizieren zu können.

[116] Vgl. GLEIßNER/KLEIN (2017), S. 69.
[117] Vgl. BRÜHWILER/ROMEIKE (2010), S. 149.
[118] Vgl. DENK/EXNER-MERKELT/RUTHNER (2008), S. 83.
[119] Vgl. VANINI (2012), S. 68.
[120] Vgl. ROMEIKE (2018), S. 36.
[121] S. Kapitel 4.2.1. Die Risikoidentifikation als Schlüsselphase, S. 53.
[122] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 103.

Kategorisierung der Risiken

In der nachfolgenden Grafik wird eine beispielhafte Risikokategorisierung, speziell auf einen Finanzdienstleister bezogen, dargestellt:

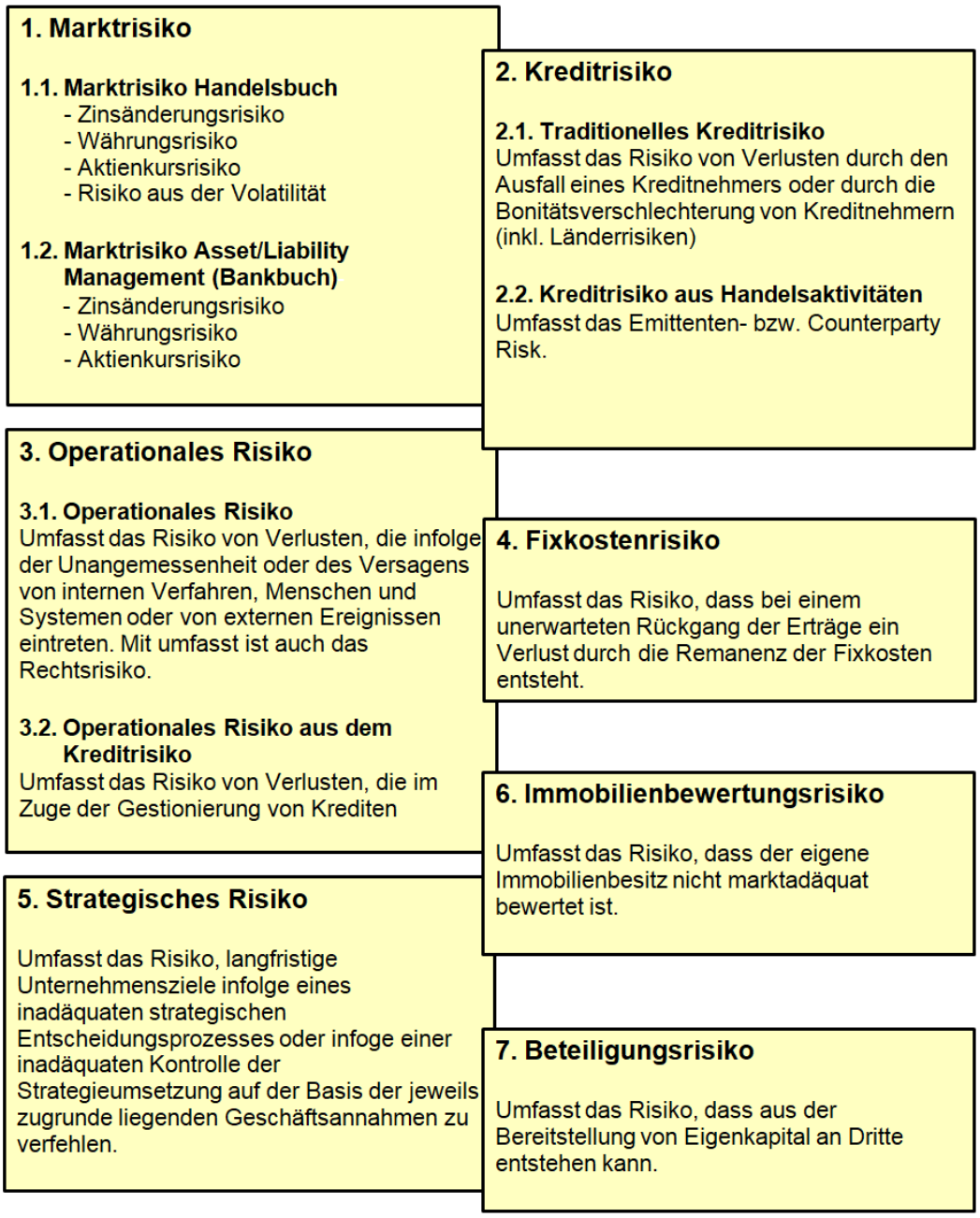


Abbildung 9: Risikokategorisierung eines Finanzdienstleisters,
Quelle: in Anlehnung an DENK/EXNER-MERKELT/RUTHNER (2008), S. 88 ff.

Die nächste Grafik zeigt, wie das Risikofeld „operationelle Risiken“ weiter untergliedert werden kann. Wie die Grafik zeigt, kann man bei operationellen Risiken zwischen „IT-Risiken“ und „sonstige operationelle Risiken“ unterscheiden. Unter einem IT-Risiko versteht man die Gefahr der Realisierung von Verlusten, die infolge der Verletzung eines oder mehrerer der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Rechtmäßigkeit aufgrund eines durchgeführten Angriffs unter Ausnutzung von Schwachstellen eintreten.[123]

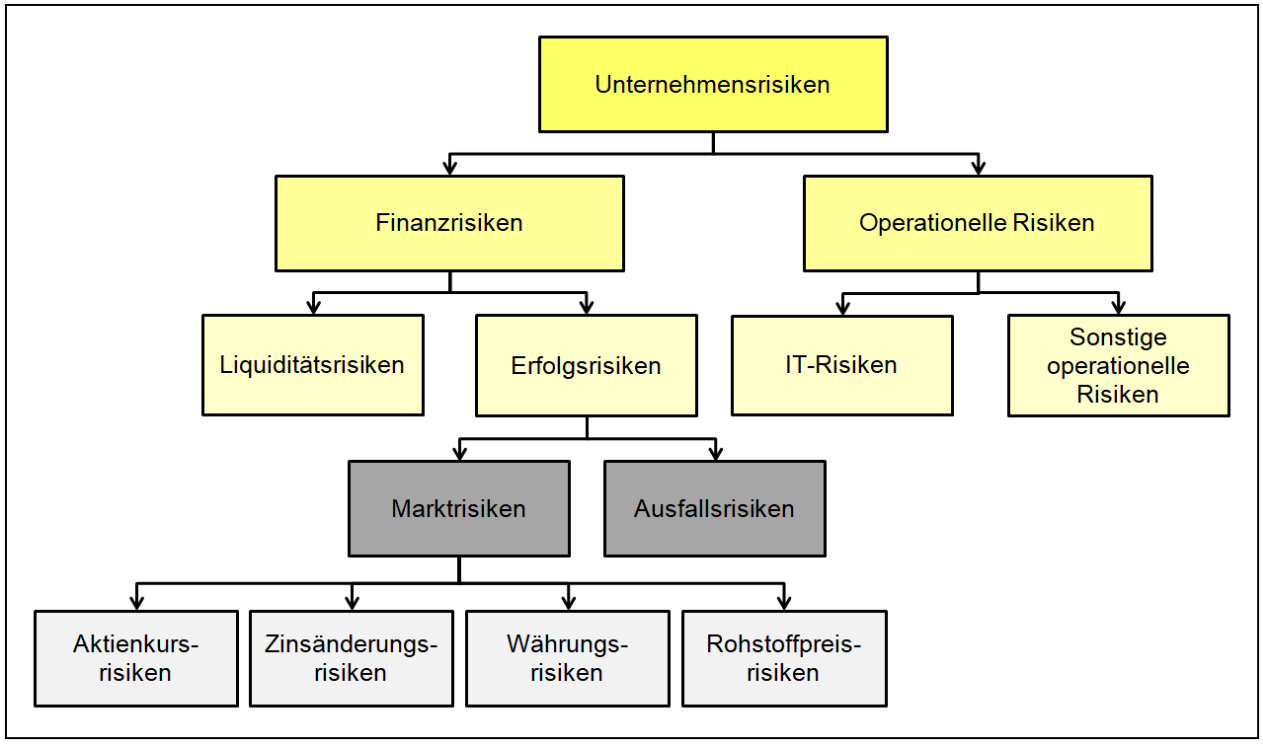


Abbildung 10: Unternehmensrisiken,
Quelle: in Anlehnung an PROKEIN (2008), S. 10.

Im Hinblick auf die Kategorisierung der IT-Risiken empfiehlt die Literatur die Gliederung in Risikogruppen wie Risiken aus der Verletzung der Schutzziele Integrität, Verfügbarkeit, Vertraulichkeit und Rechtmäßigkeit.[124] In weiterer Folge wird diese Arbeit näher auf die Einzelrisiken „Datenschutz- und die Datensicherheitsrisiken“ eingehen.

[123] Vgl. KÖNIGS (2013), S. 162.
[124] Vgl. FEILER/HORN (2018), S. 69; HECHENBLAIKNER (2006), S. 23; KÖNIGS (2013), S. 40; PROKEIN (2008), S. 11; ROMEIKE/HAGER (2009), S. 374.

Datenschutz- und Datensicherheitsrisiken

Die Literatur und die ISO/IEC 29134 nennen folgende Beispiele für Datenschutzrisiken:

Beispiele für Datenschutzrisiken
Nicht autorisierter Zugang zu personenbezogenen Daten (Verlust der Vertraulichkeit)
Nicht autorisierte Veränderung von personenbezogenen Daten (Verlust der Integrität)
(Total)Verlust, Diebstahl oder nicht autorisiertes Entfernen personenbezogener Daten (Verlust der Verfügbarkeit)
Ausufernde Erhebung personenbezogener Daten (Verlust der betrieblichen Steuerungsfähigkeit)
Nicht autorisierte oder unangemessene Verknüpfung von personenbezogenen Daten
Unzureichende Information über den Zweck der Verarbeitung personenbezogener Daten (Mangel an Transparenz)
Versäumnis bei der Beachtung von Betroffenenrechten
Verarbeitung personenbezogener Daten ohne das Wissen oder die Einwilligung des Betroffenen (außer solch eine Verarbeitung ist in den relevanten Gesetzen oder Verordnungen Sorge getroffen)
Das Teilen von, oder die Zweckänderung an, personenbezogenen Daten mit dritten Parteien ohne die Einwilligung des Betroffenen
Unnötig verlängerte Aufbewahrung personenbezogener Daten

Tabelle 6: Beispiele für Datenschutzrisiken,
Quelle: REINIS (2017), S.68.

Des Weiteren beleuchtet die Literatur als auch Erwägungsgrund 83 DSGVO folgende Datensicherheitsrisiken:

Beispiele für Datensicherheitsrisiken
Vernichtung von personenbezogenen Daten
Verlust von personenbezogenen Daten
Veränderung von personenbezogenen Daten
Unbefugte Offenlegung von personenbezogenen Daten
Unbefugter Zugang zu personenbezogenen Daten

Tabelle 7: Weitere Beispiele für Datensicherheitsrisiken,
Quelle: KRANIG/SACHS/GIERSCHMANN (2017), S. 140 ff.; LEPPERHOFF/MÜTHLEIN (2018), S. 141.; WYBITUL (2017), S. 20.

Vernichtung von personenbezogenen Daten

Unter einer unbeabsichtigten oder unrechtmäßigen Vernichtung wird das Nicht mehr Vorhandensein von personenbezogenen Daten beim Verantwortlichen verstanden.[125] Beim Eintritt dieses Risikos wäre das Schutzziel der Verfügbarkeit betroffen. Zudem sind fahrlässige Bedrohungen (z.B. kein Backup-Konzept) als auch Organisationsmängel (z.B. Löschung, obwohl gesetzliche Aufbewahrungspflichten bestehen) zu beachten.[126]

[125] Vgl. KÜHLING/KLAR/SACKMANN (2018), S. 163.
[126] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 140 ff.

Verlust von personenbezogenen Daten

Unter einem unbeabsichtigten oder unrechtmäßigen Verlust wird das Nicht mehr Vorhandensein von personenbezogenen Daten eventuell beim Verantwortlichen verstanden, wobei diese Daten möglicherweise von Dritten zur Kenntnis genommen werden können. Unter dieses Risiko fallen beispielsweise alle verlorengegangene Datenträger (z.B. USB-Sticks) oder mobile Endgeräte (Smartphones, Notebooks etc.) aber auch Papierakten (die z.B. in einem Mülleimer entsorgt und von Passanten „gefunden" werden). Bei diesem Risiko sind die Schutzziele der Vertraulichkeit, gegebenenfalls auch der Verfügbarkeit, betroffen.[127]

Unbefugte Offenlegung von personenbezogenen Daten

Falls personenbezogene Daten an Stellen oder Personen übermittelt werden, die keinen Einblick in diese haben dürften, ist das Schutzziel der Vertraulichkeit betroffen. Eine Offenlegung von Daten setzt dabei eine Aktion des Verantwortlichen oder eines Mitarbeiters bzw. eines Systems desselben voraus. Es ist irrelevant, ob diese fahrlässig oder absichtlich erfolgte, da der primär zu bewertende Faktor die Verletzung der Vertraulichkeit ist. Als Beispiel ist der Fehlversand (z.B. per E-Mail oder Post) oder das Posten von internen personenbezogenen Daten in einem sozialen Netzwerk zu nennen.[128]

Unbefugter Zugang zu personenbezogenen Daten

Es kann auch passieren, dass Verantwortliche Opfer von Cyberkriminellen oder Hackern werden. Dann haben sich diese unbefugten Zugang zu den Systemen und Diensten einschließlich der Daten beschafft. Dabei wird das Schutzziel der Vertraulichkeit, Integrität und der Verfügbarkeit verletzt. Des Weiteren fallen unter diese Kategorie Aktionen von Innentätern, die sich zum Beispiel personenbezogene Daten eines fremden Aufgabengebietes auf einen USB-Stick kopieren, was aufgrund von Mängeln am Rechte- und Rollenkonzept möglich sein kann. Die Voraussetzung für einen unbefugten Zugang ist somit eine kriminelle Tätigkeit einer Organisation oder Person, die sich Mängel an technischen und organisatorischen Maßnahmen zu eigen macht. Nicht alle Verarbeitungstätigkeiten werden automatisiert innerhalb von IT-Systemen durchgeführt. Daher haben oftmals Mitarbeiter des Verantwortlichen Zugriff auf diese Daten. Diese Tätigkeiten sind zwar rechtmäßig, jedoch sollten „Schritte" ergriffen werden, damit die legitime Datenverarbeitung nicht auf Bereiche ausgeweitet wird, die nicht zur üblichen Tätigkeit eines Mitarbeiters gehört.[129]

Des Weiteren sind im Rahmen der Risikoidentifikation auch Risiken zu ermitteln, die möglicherweise dazu führen, dass bestimmte Vorgaben der DSGVO nicht erfüllt werden.[130]

[127] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 140 ff.
[128] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 140 ff.
[129] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 141.; WYBITUL (2017), S. 20.
[130] Vgl. FEILER/HORN (2018), S. 68.

Dabei können Risiken, beispielsweise die Nichteinhaltung der Betroffenenrechte[131] oder der DSGVO-Grundsätze[132], eintreten.

Nachfolgend werden relevante Risikoquellen im Datenschutz-Risikomanagement angeführt:

<table>
<tr><th colspan="3">Risikoquellen (Art)</th><th>Relevante Risikoquellen</th></tr>
<tr><td rowspan="4">Menschlich</td><td rowspan="2">intern</td><td>unbeabsichtigt</td><td rowspan="2">Mitarbeiter
Vorgesetzte</td></tr>
<tr><td>vorsätzlich</td></tr>
<tr><td rowspan="2">extern</td><td>unbeabsichtigt</td><td rowspan="2">Wartungspersonal
Mitbewerber
Hacker</td></tr>
<tr><td>vorsätzlich</td></tr>
<tr><td rowspan="2">Nichtmenschlich</td><td colspan="2">intern</td><td>Wasserschaden durch
Rohrbruch
Feuer</td></tr>
<tr><td colspan="2">extern</td><td>Stromausfall
Ausfall der Internet Leitung</td></tr>
</table>

Tabelle 8: Relevante Risikoquellen,
Quelle: bitkom Leitfaden (2017), S. 27.; KRANIG/SACHS/GIERSCHMANN (2017), S. 103.

Potenzielle Folgen von Datenschutz- und Datensicherheitsrisiken

In weiterer Folge werden mögliche Folgen von Datenschutz- und Datensicherheitsrisiken, welche unter anderem auch in Erwägungsgrund 83 DSGVO erwähnt werden, dargestellt:[133]

- Diskriminierung
- Identitätsdiebstahl
- Betrügerische Verwendung
- Finanzieller Verlust
- Rufschädigung
- Verlust der Vertraulichkeit
- Unbefugte Aufhebung der Pseudonymisierung
- Andere erhebliche wirtschaftliche Nachteile
- Gesellschaftliche Nachteile
- Kreditschädigung[134]
- Verlust der Kontrolle
- Einschränkung der Rechte[135]

[131] S. Kapitel 2.3. Die Betroffenenrechte, S. 16 ff.
[132] S. Kapitel 2.2. Die Grundsätze der Datenschutz-Grundverordnung, S. 13 ff.
[133] Vgl. GOLA/JASPERS/MÜTHLEIN/SCHWARTMANN (2018), S. 66.
[134] Vgl. WEICHERT (2015), S.16.

- Verletzung der Privatsphäre[136]
- Erpressung[137]

Methoden zur Risikoidentifikation

Des Weiteren wird auf die Methoden zur Risikoidentifikation eingegangen, da die richtige Methode von wesentlicher Bedeutung ist. Wenn bei der Risikoidentifikation zum Beispiel aufgrund einer schwachen methodischen Fundierung, zu oberflächlicher Betrachtung oder anderen Gründen Fehler gemacht werden, wirken sich diese Fehler auf die Priorisierung von Risiken und die Risikosteuerung aus. Risiken, die nicht erkannt werden, können zu gravierenden Konsequenzen führen.[138]

Daher werden in der nachfolgenden Grafik mögliche Methoden zur Risikoidentifikation dargestellt. Anschließend wird auf die in der Praxis am häufigsten angewendeten Methoden eingegangen.

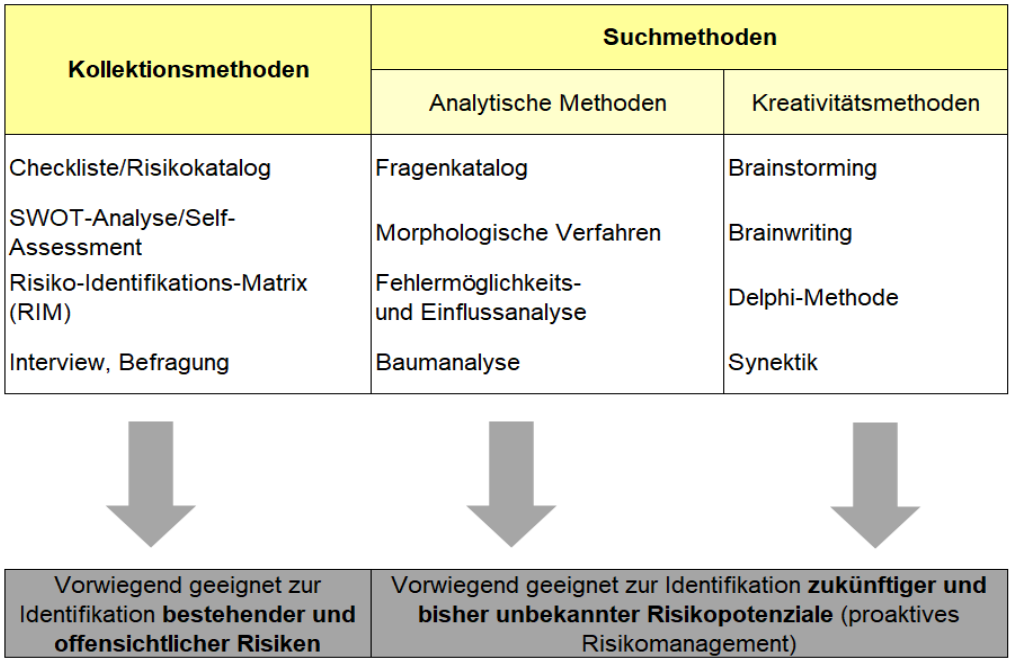


Abbildung 11: Methoden zur Risikoidentifikation,
Quelle: ROMEIKE/FINKE (2003), S. 174 (leicht modifiziert).

Im Hinblick auf die Kollektionsmethoden sind Checklisten/Risikokataloge die in der Praxis am häufigsten angewendeten Instrumente. In Bezug auf die Suchmethoden gilt das Brainstorming als das am häufigsten angewendete Instrument zur Ideenfindung. Dabei werden diese Methoden in der Praxis kombiniert verwendet.[139]

---

[135] Vgl. SCHWARTMANN/JASPERS (2018), S. 153.
[136] Vgl. REINIS (2017), S. 67.
[137] Vgl. KUGLER/ANRICH (2018), S. 86.
[138] Vgl. ROMEIKE (2018), S. 55.
[139] Vgl. ROMEIKE/HAGER (2009), S. 125 ff.

Bezüglich der Risikoidentifikation wurde in der Praxis eine PwC-Benchmarkingstudie zum Risikomanagement durchgeführt. Das Ergebnis der Studie zeigt, dass vor allem Risikokataloge, Erhebungsbögen und IT-Eingabetools zur Risikoidentifikation eingesetzt werden. Interviews und Workshops werden von ca. 30% bzw. 20% der Unternehmen zur Risikoidentifikation angewendet. GLEIßNER und KLEIN erwähnen ausdrücklich, dass die Voraussetzung für eine erfolgreiche Risikoidentifikation die Existenz eines Risikokatalogs ist, welcher die möglichen Risikofelder und Risikokategorien systematisch abbildet.[140]

Risikokatalog als Methode zur Risikoidentifikation

Checklisten bzw. Risikokataloge sind standardisierte Fragebögen, welche der Identifikation von Risikoquellen durch ein strukturiertes Erfassungsraster dienen. Zu den Vorteilen zählen die einfache Handhabung, die individuellen Gestaltungsmöglichkeiten, die Ermöglichung einer systematischen Vorgehensweise und eine vergleichsweise homogene Datenbasis.[141] Außerdem ermöglichen Checklisten eine eindeutige Aufgabenzuordnung an Risikoverantwortliche, die Gestaltung eines standardisierten Berichtssystems speziell für Risiken als auch eine Einbindung des Risikomanagements in existierende Planungs- und Berichtssysteme. Ein weiterer Vorteil standardisierter Fragenkataloge stellt die universelle Anwendbarkeit dar. Ein Nachteil dieses Instruments ist, dass bei einem starren Raster ein Vollständigkeitsproblem auftreten kann. Ein starres Raster kann dazu führen, dass neue und essentielle Risikoquellen übersehen werden.[142] Eine andere Schwäche besteht in der Vergangenheitsorientierung. Daher sollten regelmäßige Anpassungen und Aktualisierungen vorgenommen werden.[143]

Risk-Assessment-Sheet

Auch Risk-Assessment-Sheets gehören wie Checklisten zu den standardisierten Befragungen. Ein Vorteil dieser besteht in der strukturierten Vorgehensweise. Checklisten bieten eine abgeschlossene Auswahl an Lösungsmöglichkeiten, wobei Risk-Assessment-Sheets eine Kombination von offenen als auch geschlossenen Fragen darstellen. Im Vergleich zu anderen „reinen“ Instrumenten zur Risikoidentifikation werden bei Risk-Assessment-Sheets die Elemente der Risikobewertung, wie zum Beispiel die Grobscheinschätzung von Schadensausmaß und Eintrittswahrscheinlichkeit, sowie Risikomanagementmaßnahmen mit berücksichtigt. Diese Risk-Assessment-Sheets werden entweder in Einzelbefragungen oder in Risikomanagement-Workshops, wenn für die Bearbeitung das Fach-Know-how mehrerer Personen erforderlich ist, ausgearbeitet. Ein großer Vorteil dieses Instruments ist, dass eine gewisse Mindeststruktur zur näheren Beschreibung des Risikos gegeben ist und die zu

[140] Vgl. GLEIßNER/KLEIN (2017), S. 69 ff.
[141] Vgl. BURGER/BUCHHART (2002), S. 88.
[142] Vgl. ROMEIKE/FINKE (2003), S. 175.
[143] Vgl. BURGER/BUCHHART (2002), S. 88 ff.

befragenden Personen nicht in der Nennung von Risiken eingeschränkt sind. Eine Herausforderung von standardisierten Befragungen ist, dass man aktuelle als auch potenzielle Risiken unter die bestehenden Risikoarten subsumiert.[144]

Brainstorming-Methode

Die Qualität des Ergebnisses der Brainstorming-Methode beruht darauf, dass[145]

- zur Lösung eines Problems das Wissen mehrerer Personen genutzt wird,
- denkpsychologische Verfahren eliminiert werden,
- die Lösungsvielfalt erweitert wird,
- das Kommunikationsverhalten der beteiligten Personen gestrafft und „demokratisiert" wird sowie
- unnötige Diskussionen unterlassen werden.

Brainstorming-Begründer Alex Faickney Osborn entwickelte bereits Anfang des 20. Jahrhunderts basierend auf folgenden vier Regeln das Verfahren:[146]

- Übe keine Kritik!
- Je mehr Ideen, desto besser!
- Ergänze und verbessere bereits vorhandene Ideen!
- Je ungewöhnlicher die Idee, desto besser!

Durch eine ungezwungene Atmosphäre wird die Kreativität der Beteiligten gefördert. Für die Ideenfindung ist die richtige Auswahl der Teilnehmer für den Erfolg ausschlaggebend.[147] GLEIßNER empfiehlt diese Methode mit anderen zu kombinieren, um nicht überbordende und unstrukturierte Risikolisten zu erhalten oder bedeutende Risiken zu übersehen.[148]

4.2.2. Die Risikobewertung als Vorstufe zur Risikosteuerung

Das Hauptaugenmerk der DSFA liegt auch auf der Risikobewertung. Nach Art. 35 Abs. 7 DSGVO sind die Risiken für die Rechte der betroffenen Personen zu bewerten. Die Phase der Risikobewertung beruht auf den Ergebnissen der Risikoidentifikation und umfasst eine möglichst vollständige und kontinuierliche Bewertung. Wenn eine Quantifizierung nicht möglich ist, sollte eine qualitative Beurteilung aller identifizierten Risiken durchgeführt werden. Durch die

[144] Vgl. DENK/EXNER-MERKELT/RUTHNER (2008), S. 91 ff.
[145] Vgl. ROMEIKE/HAGER (2009), S. 129.
[146] Vgl. ROMEIKE/HAGER (2009), S. 129.
[147] Vgl. DENK/EXNER-MERKELT/RUTHNER (2008), S. 90.
[148] Vgl. GLEIßNER (2017), S. 123.

Beurteilung kann eine Rangordnung erstellt werden. Mit Hilfe der Priorisierung der Risiken können schließlich passende Maßnahmen abgeleitet werden.[149]

Des Weiteren ist bei der Risikobewertung zwischen der Bruttobewertung und der Nettobewertung zu unterscheiden. Unter der Bruttobewertung versteht man die Bewertung der Risiken, ohne risikosteuernde Maßnahmen zu berücksichtigen, also ohne Beachtung bereits eingeleiteter Maßnahmen zur Risikobewältigung (Bruttorisiko). Im Gegensatz zur Bruttobewertung werden bei der Nettobewertung die Risikosteuerungsmaßnahmen einbezogen und es wird das verbleibende Restrisiko (Nettorisiko) beurteilt.[150]

Die Bewertung der Risiken sollte folgende Anforderungen erfüllen:[151]

- Objektivität: Wo möglich, sollte ein Marktbezug hergestellt werden; bei unternehmensinternen Risiken sind mehr oder weniger subjektive Schätzungen notwendig.
- Vergleichbarkeit: Die Bewertung der Risiken hat zu vergleichbaren Ergebnissen zu führen. Dies kann durch die Verwendung einheitlicher, standardisierter Methoden und Daten gewährleistet werden.
- Quantifizierung: Durch die Quantifizierung ist es möglich, dass Bestandsgefährdung bzw. wesentliche Abweichungen von Zielgrößen erkannt werden können. Außerdem ermöglicht die Quantifizierung die Aggregation von Einzelrisiken. Daher sind Risiken – wo möglich – quantitativ zu bewerten.
- Berücksichtigung von Interdependenzen: Bei aggregierter Bewertung von Risiken sind Kompensationseffekte und Interdependenzen zwischen Risiken zu berücksichtigen.

Darüber hinaus sind gemäß Erwägungsgrund 90 DSGVO für jedes identifizierte Risiko die spezifische Eintrittswahrscheinlichkeit und die Schwere zu berücksichtigen.[152] In der Unternehmenspraxis ist der Erwartungswert zu ermitteln, indem die Eintrittswahrscheinlichkeit mit dem Schadensausmaß multipliziert wird.[153] Nach LEPPERHOFF und MÜTHLEIN ist das Schadensausmaß aus Sicht der Organisation häufig zumindest grob kalkulierbar, da finanzielle Auswirkungen abgeschätzt werden können. Ein Risiko für die Rechte der Betroffenen kann jedoch kaum beziffert werden und ist nur in Ausnahmefällen seriös in einer Einheit wie Euro ausdrückbar. Daher ist auf Pseudo-Berechnungen in der DSFA zu verzichten.[154] Auch KRANIG, SACHS und GIERSCHMANN empfehlen eine qualitative und keine quantitative

[149] Vgl. DENK/EXNER-MERKELT/RUTHNER (2008), S. 102.
[150] Vgl. DIEDERICHS (2017), S. 139.
[151] Vgl. DENK/EXNER-MERKELT/RUTHNER (2008), S. 103.
[152] Vgl. LEPPERHOF/MÜTHLEIN (2018), S. 141.
[153] Vgl. AHRENDTS/MARTON (2008), S. 23.
[154] Vgl. LEPPERHOFF/MÜTHLEIN (2018), S. 141.

Risikobewertung.[155] Zudem wird hinsichtlich des Schadensausmaßes in der DSGVO angeführt, dass aus der Verarbeitung personenbezogener Daten physische, materielle oder immaterielle Schäden resultieren können.[156] Die Autoren FEILER und HORN sind jedoch der Auffassung, dass das Schadensausmaß in materielle oder immaterielle Schäden einzugliedern ist.[157]

Im Hinblick auf die Anzahl der Kategorien empfiehlt die ISO 29134 vier Kategorien für die Zuordnung des Risikos in Bezug auf die Schwere und die Eintrittswahrscheinlichkeit. Mehr als vier Kategorien erweisen sich auch nicht als praktikabel. Was die Kategorien anbelangt, so werden von der DSGVO keine bestimmten Kriterien vorgegeben. Die einzige Vorgabe ist, dass eine Einteilung in Risiko und hohes Risiko möglich sein soll.

Die Schwere des Risikos kann in folgende vier Kategorien untergliedert werden:[158]

Bereich	Auswirkung auf Betroffenen	Folgen überwinden können	Beispiele
Vernachlässigbar	Nicht betroffen oder nur kleine Unannehmlichkeiten	Unannehmlichkeiten sollten sich problemlos beheben lassen	Zeitverlust durch erneute Eingabe von Informationen, Ärgernisse, Irritationen, etc.
Begrenzt	Wesentliche Unannehmlichkeiten	Wesentliche Unannehmlichkeiten sollten sich – trotz gewisser Schwierigkeiten – überwinden lassen	Zusätzliche Kosten, Verweigerung des Zugangs zu Geschäftsdiensten, Angst, Mangel an Verständnis, Stress, leicht körperliche Beschwerden, etc.
Wesentlich	Wesentliche Folgen	Wesentliche Folgen sollten sich – trotz gewisser Schwierigkeiten – überwinden lassen	Missbrauch von Geldern, Blacklisting von Banken, Sachschäden, Arbeitslosigkeit, Vorladung, Verschlechterung des Gesundheitszustandes usw.
Maximal	Wesentliche und/oder irreversible Folgen	Irreversible Folgen kaum bzw. nicht überwindbar	Finanzielle Not wie Schulden oder Arbeitsunfähigkeit, langfristige psychische oder körperliche Beschwerden, Tod usw.

Tabelle 9: Kategorien für die Schwere des Risikos,
Quelle: KRANIG/SACHS/GIERSCHMANN (2017), S. 104.

Wie man aus der Tabelle auf der nächsten Seite erkennen kann, definiert der Autor REINIS das Schadensausmaß auf ähnliche Art und Weise als die Autoren KRANIG, SACHS und GIERSCHMANN.

[155] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 103.
[156] Vgl. LEPPERHOFF/MÜTHLEIN (2018), S. 141.
[157] Vgl. FEILER/HORN (2018), S. 68.
[158] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 104.

Bereich	Auswirkung auf Betroffenen	Beispiele
Unbedeutend	Betroffene werden nicht belangt oder könnten auf ein paar Unannehmlichkeiten treffen, welche sie problemlos bewältigen können	Zeitbedarf zur Wiedereingabe von Informationen, Verärgerung, Irritationen usw.
Eingeschränkt	Betroffene könnten bedeutende Unbequemlichkeiten erfahren, welche sie trotz einiger weniger Schwierigkeiten bewältigen können	Zusätzliche Kosten, Ablehnung beim Zugang zu kommerziellen Diensten, Angst, mangelndes Verständnis, Stress, kleine körperliche Gebrechen usw.
Signifikant	Betroffene könnten bedeutende Konsequenzen erfahren, welche sie trotz ernsthafter Schwierigkeiten zu bewältigen in der Lage sein sollten	Fehlgeleitete Zahlungsmittel, Verlust der Kreditwürdigkeit, Eigentumsschaden, Arbeitsplatzverlust, Vorladung, Verschlechterung des Gesundheitszustandes usw.
Maximal	Betroffene könnten erhebliche oder sogar unumkehrbare Konsequenzen erfahren, welche sie nicht bewältigen könnten	Finanzielle Notlage, uneinbringbare Schulden oder Arbeitsunfähigkeit, langfristige psychologische oder physische Gebrechen, Tod usw.

Tabelle 10: Kategorien für die Schwere des Risikos,
Quelle: REINIS (2018), S. 71 ff.

Für die Eintrittswahrscheinlichkeit empfehlen die Autoren KRANIG, SACHS und GIERSCHMANN die folgenden vier Kategorien:

Bereich	Realisierbarkeit der Bedrohung durch die Risikoquelle auf einen Vermögenswert	Beispiele
Vernachlässig-bar	Scheinbar unmöglich	Diebstahl von Papierdokumenten, die in einem von einem Ausweisleser und einem Zugangscode geschützten Raum gelagert sind
Begrenzt	Schwierig (machbar mit gewissem Aufwand)	Diebstahl von Papierdokumenten, die in einem durch ein Ausweislesegerät geschützten Raum aufbewahrt werden
Wesentlich	Möglich (machbar auch mit geringem Aufwand)	Diebstahl von Papierdokumenten, die in Büros gelagert sind, die durch Personenkontrollen geschützt sind
Maximal	Einfach	Diebstahl von Papierdokumenten, die in einer Lobby lagen

Tabelle 11: Kategorien für die Eintrittswahrscheinlichkeit des Risikos,
Quelle: KRANIG/SACHS/GIERSCHMANN (2017), S. 104

Die folgende Tabelle zeigt, dass der Autor REINIS die Kriterien der Eintrittswahrscheinlichkeit ähnlich als die Autoren KRANIG, SACHS und GIERSCHMANN festlegt.

Bereich	Realisierbarkeit der Bedrohung durch die Risikoquelle auf einen Vermögenswert	Beispiele
Unbedeutend	Die Ausführung einer Bedrohung durch ausnutzen der Eigenschaften der unterstützenden Vermögensgüter erscheint für die ausgewählten Risikoquellen nicht möglich	Diebstahl von Papierdokumenten, die in einem Raum aufbewahrt wurden, der durch Ausweislesegerät und Zugangscode geschützt ist
Eingeschränkt	Die Ausführung einer Bedrohung durch ausnutzen der Eigenschaften der unterstützenden Vermögensgüter erscheint schwierig für die ausgewählten Risikoquellen	Diebstahl von Papierdokumenten, die in einem Raum aufbewahrt wurden, der durch ein Ausweislesegerät geschützt ist
Signifikant	Die Ausführung einer Bedrohung durch ausnutzen der Eigenschaften der unterstützenden Vermögensgüter erscheint möglich für die ausgewählten Risikoquellen	Diebstahl von Papierdokumenten, die in Geschäftsräumen aufbewahrt wurden, in die man nicht gelangt ohne sich zuerst am Empfang anzumelden
Maximal	Die Ausführung einer Bedrohung durch ausnutzen der Eigenschaften der unterstützenden Vermögensgüter erscheint äußerst einfach für die ausgewählten Risikoquellen	Diebstahl von im Vorraum aufbewahrten Papierdokumenten

Tabelle 12: Kategorien für die Eintrittswahrscheinlichkeit des Risikos, Quelle: REINIS (2018), S. 71 ff.

Nach der Beurteilung der einzelnen Risiken lassen sich diese in einer Risikomatrix, auch Risk Map genannt, darstellen. Wie man aus der folgenden Grafik auf der nächsten Seite erkennen kann, gehören die einzelnen Felder zu einem bestimmten Risikobereich. Diese Risikobereiche lassen sich in ein geringes (Grafik: graue Farbe), mittleres (Grafik: hellgelbe Farbe) und hohes Risiko (Grafik: gelbe Farbe) klassifizieren[159]. Nachdem die Risikobereiche bestimmt wurden, lassen sich unterschiedliche Handlungsstrategien und Prioritäten für die Risikobehandlung zuordnen.[160]

[159] Vgl. FEILER/HORN (2018), S. 68.
[160] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 105.

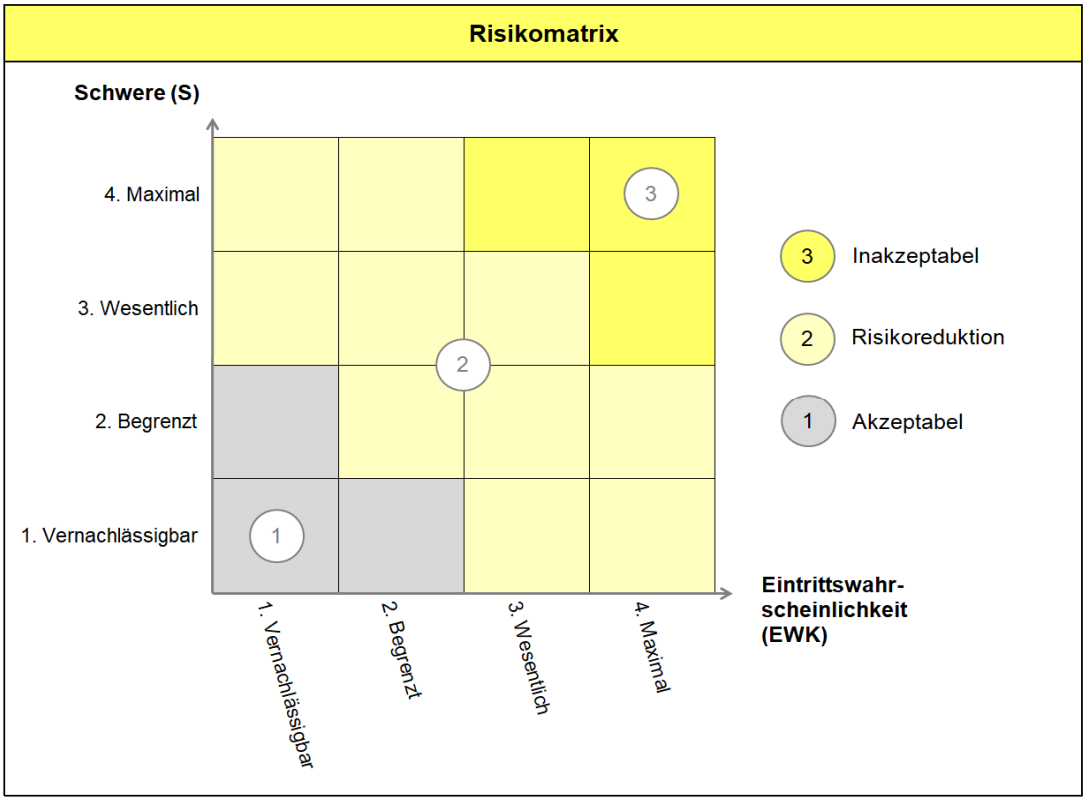


Abbildung 12: Risikomatrix,
Quelle: KRANIG/SACHS/GIERSCHMANN (2017), S. 105 (leicht modifiziert).

4.2.3. Mögliche Strategien zur Steuerung der Risiken

Nach der Risikoidentifikation und der Risikobewertung folgt die Steuerung der ermittelten Risiken. Ohne Risikosteuerung macht Risikomanagement keinen Sinn, denn es geht darum, dass geeignete Maßnahmen für die Risiken getroffen und überwacht werden. Gemäß ISO 31000 umfasst die Risikobewältigung die Auswahl und Umsetzung einer oder mehrerer Möglichkeiten, um den Risiken zu begegnen.[161] Ziel der Risikobewältigung ist, durch passende Maßnahmen eine optimale Risikoposition zu erreichen und eine vorgegebene Obergrenze für den Gesamtrisikoumfang nicht zu überschreiten.[162]

Im Umgang mit Risiken gibt es im klassischen Risikomanagement mehrere grundlegende Strategien, insbesondere die Risikovermeidung, die Risikoverminderung, die Risikoüberwälzung und „Risiko selbst tragen“. In der nachfolgenden Grafik auf der nächsten Seite wird der Prozess der Risikosteuerung illustriert:

[161] Vgl. BRÜHWILER (2016), S. 59.
[162] Vgl. GLEIßNER (2017), S. 287.

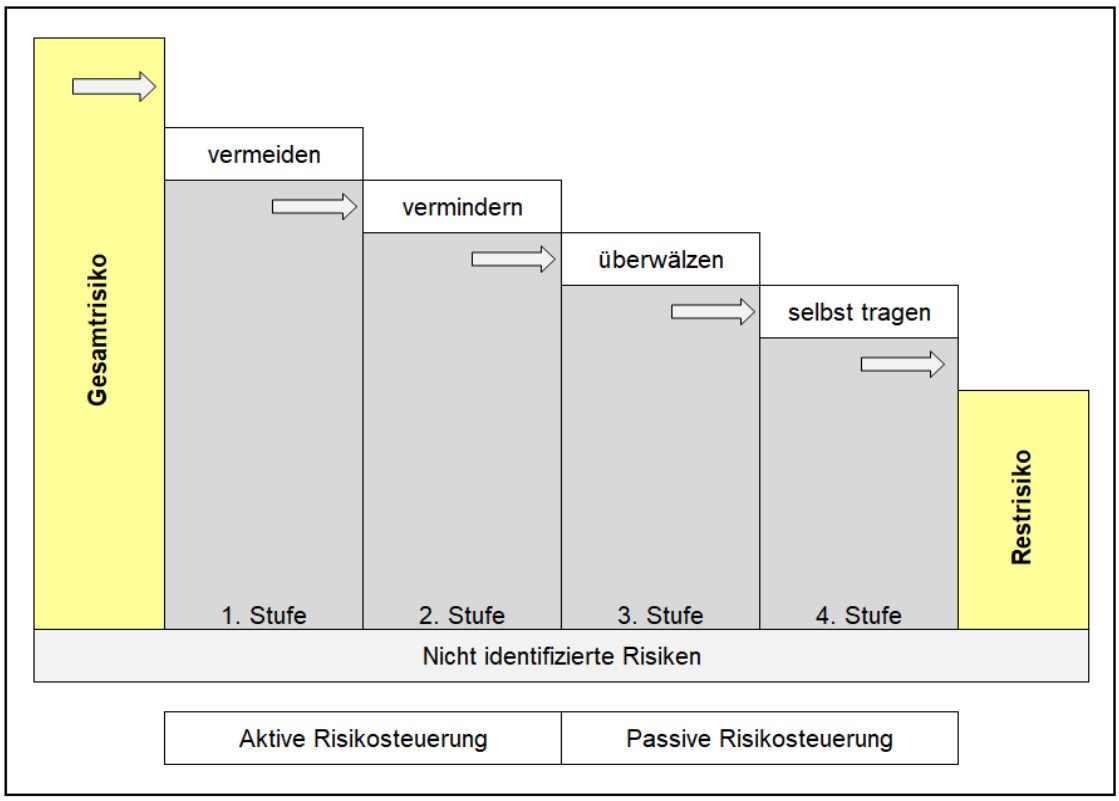


Abbildung 13: Risikobewältigungsstrategien,
Quelle: in Anlehnung an DENK/EXNER-MERKELT/RUTHNER (2008), S. 130; GLEIßNER (2017), S. 288; GLEIßNER/ROMEIKE (2005), S. 36.; ROMEIKE/HAGER (2009), S. 161.

Wie aus der Grafik ersichtlich ist, unterscheidet man zwischen aktiven (präventiven) und passiven (korrektiven) Maßnahmen der Risikobeeinflussung. Das Ziel der aktiven Maßnahmen ist, die Eintrittswahrscheinlichkeit und/oder das Schadensausmaß einzelner Risiken tatsächlich zu reduzieren. Als Synonym wird auch der Begriff „ursachenbezogene Maßnahmen“ benutzt. Im Gegensatz dazu lassen passive Risikobewältigungsmaßnahmen die Risikostrukturen unverändert und beeinflussen die Eintrittswahrscheinlichkeit und das Schadensausmaß nicht. Das Ziel dieser Maßnahmen ist, dass finanzielle Auswirkungen auf das Unternehmen nach einem Risikoeintritt, beispielsweise durch eine vertragliche Haftungsverlagerung auf einen Vertragspartner oder einen Risikotransfer durch eine Versicherung reduziert werden. Als Synonym wird auch der Begriff „wirkungsbezogene Maßnahmen“ verwendet.[163]

Des Weiteren geht aus der Grafik hervor, dass sich auf der ersten Stufe der Risikobewältigungsstrategien die Risikovermeidung befindet. Von Risikovermeidung spricht man, wenn sich ein Unternehmen auf Grund bestehender, nicht reduzierbarer Gefahren sich für den Verzicht auf bestimmte Aktivitäten entscheidet. Diese Strategie ist sinnvoll, wenn Risiken aufgrund hoher Eintrittswahrscheinlichkeiten und/oder großer Schadenshöhe ein existenzbedrohendes Ausmaß aufweisen, das nicht auf ein akzeptables Ausmaß vermindert

[163] Vgl. DENK/EXNER-MERKELT/RUTHNER (2008), S. 128.

werden kann.[164] Ein Beispiel für die Risikovermeidung wäre der Ausstieg aus einem Geschäftsfeld.[165]

In der zweiten Stufe werden die Risiken reduziert. Hinsichtlich der Risikoverminderung unterscheidet man zwischen einer ursachenorientierten und einer wirkungsorientierten Minderung. Bei der ursachenorientierten Minderung wird die Eintrittswahrscheinlichkeit reduziert, wobei man bei der ursachenorientierten Minderung die Schadenshöhe schmälert. Unter die ursachenorientierte Minderung fällt beispielsweise die verstärkte Wartung wichtiger IT-Systeme zur Vermeidung von Ausfällen. Die wirkungsorientierte Minderung könnte beispielsweise die Reduzierung des Anteils fixer Kosten („Outsourcing“) bedeuten, um die Folgewirkungen eines unerwarteten Umsatzrückgangs einzuschränken.[166] Außerdem können die Risiken durch personelle Maßnahmen (zum Beispiel durch Mitarbeiterschulung), durch technische Maßnahmen (zum Beispiel eine Firewall im Bereich der Informationstechnologie) oder durch organisatorische Maßnahmen (zum Beispiel durch eine Prozessoptimierung) reduziert werden.[167]

In der dritten Stufe widmet man sich der Risikoüberwälzung (Risikotransfer). Die Risiken können einerseits durch Versicherungen überwälzt werden, andererseits können auch Instrumente des Finanzmarkts (zum Beispiel die Absicherung von Zinsänderungen mit Derivaten) angewendet werden.[168] Die Vertragsgestaltung mit Kunden und Lieferanten stellt ebenso eine Möglichkeit für einen Risikotransfer dar. Nach der Risikoüberwälzung lassen sich die Risiken nicht mehr sinnvoll eliminieren.

Einige Risiken müssen als letzte Möglichkeit in der vierten Stufe selbst getragen werden. Dies gilt vor allem für die „Kernrisiken“ eines Unternehmens, also die Risiken, die in direktem Zusammenhang mit dem Aufbau und der Nutzung seiner Erfolgspotenziale stehen. Einerseits macht es häufig nicht nur keinen Sinn, diese Risiken auf Dritte zu übertragen, es ist meist gar nicht möglich.[169]

In der DSGVO ist immer nur die Rede von einer Risikobewältigungsstrategie und zwar die Risikoverminderung. Die Autoren REINIS, KRANIG, SACHS und GIERSCHMANN sind jedoch der Auffassung, dass auch im Datenschutz-Risikomanagement vier Risikobewältigungsstrategien zur Verfügung stehen. Er nennt diese Optionen Risikovermeidung, Risikominderung, Risikoübertragung und Risikobehandlung. Wird ein ermitteltes Risiko als zu hoch betrachtet und es gibt keine passenden Maßnahmen zur

[164] Vgl. DENK/EXNER-MERKELT/RUTHNER (2008), S. 129.
[165] Vgl. GLEIßNER (2017), S. 288.
[166] Vgl. GLEIßNER/ROMEIKE (2005), S. 37.
[167] Vgl. ROMEIKE/HAGER (2009), S. 162.
[168] Vgl. GLEIßNER/ROMEIKE (2005), S. 37.
[169] Vgl. GLEIßNER (2017), S. 288 ff.

Risikominderung oder dies nicht in einem angemessen Verhältnis steht (beispielsweise aufgrund von sehr hohen Implementierungskosten)[170], kann die Organisation sich dafür entscheiden das Risiko zu vermeiden. Dabei kann das Risiko durch das Einstellen eines Verfahrens oder das Zurückziehen eines bestehenden Verfahrens vermieden werden. Außerdem können die Bedingungen verändert werden, unter denen das Vorhaben betrieben wird. Die Autoren FEILER und HORN sind der Auffassung, dass das Risiko eliminiert werden kann, indem fragliche Daten gar nicht erhoben werden.[171]

Risikominderung bedeutet, dass die Folgen bei Eintritt des Risikos durch das Auswählen passender Maßnahmen verringert, jedoch nicht vollständig abgewendet werden kann. Daher ist es erforderlich, dass das verbleibende Restrisiko unter der Annahme der Wirksamkeit aller geplanten Steuerungsmaßnahmen bewertet wird. Prinzipiell ist es erforderlich, solange Maßnahmen zu treffen oder zusätzliche Risikobewältigungsstrategien festzulegen, bis ein akzeptables Restrisiko erreicht werden kann.[172]

Im Hinblick auf die Risikoübertragung erwähnt der Autor REINIS, dass bestimmte Risiken auch mit externen Partnern geteilt werden können (beispielsweise durch Outsourcing[173]). Einerseits kann die Übertragung als eine Versicherung erfolgen, die die Konsequenzen aus dem Eintritt des Risikos auffängt. Andererseits kann ein Partner mit der Überwachung des Informationssystems und dem Ergreifen unmittelbarer Maßnahmen, zum Stoppen eines Angriffes bevor ein kritischer Schadensumfang erreicht wird, beauftragt werden. Bei der Strategie der Risikoübertragung ist jedoch besonders hervorzuheben, dass die teilweise oder vollständige Verlagerung von Risiken auf den Betroffenen, beispielsweise bei Betrug nach dem Verlust von personenbezogenen Daten, keine legitime Option darstellt. Des Weiteren kann die Übertragung von Risiken neue Risiken entstehen lassen oder existierende, ermittelte Risiken verändern. Aus diesem Grund kann eine zusätzliche Risikobehandlung notwendig werden. Außerdem kann im Rahmen der Übertragung der Risiken die operative Verantwortung zur Behandlung eines Risikos übertragen werden. Anzumerken ist jedoch, dass sich die Verantwortung für eine Folgewirkung nicht übertragen lässt. Die betroffenen Personen würden die negativen Folgen bei Eintritt des Risikos als Verschulden der Organisation ansehen.[174]

Eine weitere Möglichkeit zur Risikosteuerung besteht in der Risikobehandlung. Darunter versteht man, dass das jeweilige Risiko akzeptiert wird und kein Bedarf zur Einführung einer

[170] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 106.
[171] Vgl. FEILER/HORN (2018), S. 69.
[172] Vgl. REINIS (2018), S. 76 ff.
[173] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 106.
[174] Vgl. REINIS (2018), S. 76 ff.

Maßnahme besteht. Das Risiko wird schließlich mit den bereits vorhandenen Maßnahmen behandelt.[175]

Nachdem geeignete Risikobewältigungsstrategien ausgewählt wurden, empfehlen die Autoren KRANIG, SACHS und GIERSCHMANN angemessene Maßnahmen zur Risikoreduktion und anschließend einen Plan zur Risikobewältigung festzulegen. Mögliche Risikominderungsmaßnahmen (Sicherheitsmaßnahmen) – das heißt Maßnahmen zum Schutz der Vertraulichkeit, der Integrität oder Verfügbarkeit der Daten – lassen sich klassifizieren nach[176]

- ihrer Art: technische, organisatorische und physische Sicherheitsmaßnahmen und
- ihrer Wirkungsweise: präventive, detektive, reaktive und abschreckende Maßnahmen

Nach Art. 42 Abs. 1 DSGVO hat der Verantwortliche geeignete technische und organisatorische Maßnahmen umzusetzen, die sicherstellen und den Nachweis erbringen, dass die Datenverarbeitung gemäß der Verordnung erfolgt. Diese Maßnahmen sind erforderlichenfalls zu überprüfen und zu aktualisieren. Welche Maßnahmen geeignet sind, wird nach der Art, dem Umfang, den Umständen und Zwecken der Verarbeitung sowie der Schwere und Eintrittswahrscheinlichkeit der Risiken für die betroffenen Personen festgelegt.[177] Technische Maßnahmen sind Sicherheitsmaßnahmen, die in Form von Computer-Hardware oder Software implementiert werden, beispielsweise eine Firewall oder eine Anti-Viren-Software. Unter organisatorische Maßnahmen versteht man Sicherheitsmaßnahmen, die in Form von Organisationsstrukturen oder Unternehmensabläufen implementiert werden, beispielsweise das Vier-Augen-Prinzip für spezifische Tätigkeiten. Physische Maßnahmen hingegen sind Sicherheitsmaßnahmen, die den physischen Zugang zu Daten sichern, beispielsweise ein Wachhund oder ein simples Vorhängeschloss.[178]

Des Weiteren sollen präventive Maßnahmen die Verwirklichung von Risiken vermeiden. Es wird somit der Erfolg eines Angriffes verhindert, beispielsweise eine Firewall oder die Entscheidung, bestimmte Datenkategorien gar nicht zu erheben. Detektive Maßnahmen ermöglichen das Erkennen von Angriffen, beispielsweise ein System zur Erkennung von Serverausfällen. Reaktive Maßnahmen haben zur Folge, dass im Falle eines erkannten erfolgreichen Angriffs Gegenmaßnahmen eingeleitet werden, welche die Auswirkungen des Angriffs mindern, beispielsweise eine Incident Response Policy oder ein Prozess zur Datensicherung und -wiederherstellung. Durch abschreckende Maßnahmen soll bewirkt werden, dass den Angreifern die Motivation genommen wird, den Angriff überhaupt auszuführen, beispielsweise durch eine

[175] Vgl. REINIS (2018), S. 76 ff.
[176] Vgl. FEILER/HORN (2018), S. 75 ff.
[177] Vgl. KRANIG/SACHS/GIERSCHMANN (2017), S. 41.
[178] Vgl. FEILER/HORN (2018), S. 75 ff.

Disziplinarrichtlinie für Mitarbeiter. Die Autoren FEILER und HORN sind der Auffassung, dass präventive Maßnahmen niemals zu 100% effektiv sein werden, daher kommt den detektiven und reaktiven Maßnahmen eine besondere Bedeutung zu.[179]

Auch zum Schutz der Rechtmäßigkeit der Datenverarbeitung existieren Risikominderungsmaßnahmen. Diese Maßnahmen lassen sich in folgende Kategorien klassifizieren:[180]

Einschränkung der Arten der erhobenen Daten
Beispielsweise ist bei einer Videoüberwachungsanlage sicherzustellen, dass der Pausenraum der Mitarbeiter nicht im Blickfeld der Kameras liegt oder die Verarbeitung auf pseudonyme Daten beschränkt wird, statt reguläre personenbezogene Daten zu verarbeiten.

Einschränkung des Datenumfangs
Beispielsweise durch die Reduktion der Frequenz der Datenerhebung (Protokollierung der Standortdaten nur ein Mal pro Stunde statt alle 30 Sekunden).

Einschränkung der Kategorien von Betroffenen
Beispielsweise bei einer Whistleblowing-Hotline nur Meldungen über Entscheidungsträger zuzulassen.

Einschränkung der Anzahl von Betroffenen
Beispielsweise für eine statistische Untersuchung ein kleines statistisches Sample zu wählen.

Einschränkung der Verarbeitungszwecke
Beispielsweise die Daten einer Videoüberwachung nur im Fall eines begründeten Verdachts einer gerichtlich strafbaren Handlung auszuwerten.

Einschränkung des Kreises der Zugangsberechtigten
Beispielsweise eine Auswertung der der Videoüberwachungsdaten nur durch Mitarbeiter der Sicherheitsabteilung zu erlauben oder eine Datenauswertung im Rahmen einer internen Compliance-Untersuchung nur durch Personen zu gestatten, die spezifisch geschult wurden.

Einschränkung der Übermittlungsempfänger
Beispielsweise die Kundendaten nur mit einer statt mit allen Konzerngesellschaften zu teilen.

Einschränkung der Speicherdauer
Beispielsweise Beschränkung der Datenspeicherung einer Videoüberwachung auf 72 Stunden.

[179] Vgl. FEILER/HORN (2018), S. 163 ff.
[180] Vgl. FEILER/HORN (2018), S. 76.

Maßnahmen zur Sicherstellung der Richtigkeit der Daten

Beispielsweise bei einer Whistleblowing-Hotline anonyme Meldungen entweder zu untersagen oder zumindest nicht zu fördern, um die Wahrscheinlichkeit von Falschmeldungen zu mindern.

4.2.4. Risikoüberwachung und Risikoreporting

Der letzte Schritt des Risikomanagementprozesses nach der Risikosteuerung ist die Risikoüberwachung einschließlich der Risikoberichterstattung. Im klassischen Risikomanagement werden laufend neue Rahmenbedingungen und die Veränderung der Risikolage berücksichtigt. Es werden laufend Veränderungen ermittelt und auf diese reagiert. Es wird überwacht und überprüft, welche internen und externen Ereignisse eintreten könnten, ob neue Risiken auftreten, sich verändert haben oder nicht mehr existieren. Die Risikoüberwachung befasst sich primär mit der Beobachtung von Restrisiken. Zu diesen Risiken gehören nicht nur die Risiken, die nach Umsetzung der jeweiligen Maßnahmen verbleiben, sondern auch solche, die vorhanden sind, aber noch nicht identifiziert und deshalb noch nicht gesteuert wurden. Das Restrisiko umfasst auch Risiken, die bewusst eingegangen wurden.[181]

Eine wesentliche Aufgabe der Risikoüberwachung ist die Untersuchung, wie sich Risiken im Zeitablauf verhalten. Hinsichtlich der Risiken können sich die Eintrittswahrscheinlichkeit, das Schadensausmaß oder auch beide Faktoren verändern. Die Entwicklungstrends müssen kontinuierlich verfolgt werden.[182] Eine weitere Aufgabe der Überwachung stellt die Früherkennung von Risiken, auch die Verstärkung oder Abschwächung von Früherkennungs-Indikatoren, dar. Neue Risiken entstehen oft durch die Veränderung von internen und externen Rahmenbedingungen, insbesondere von eigenen Zielen, Tätigkeiten und externen Anforderungen an die Organisation. Im Rahmen der Risikoüberprüfung wird die Umsetzung der Risikobewältigungsmaßnahmen kontrolliert. Es wird regelmäßig festgestellt, ob die Maßnahmen umgesetzt werden und die Risikobehandlung wirksam ist. Der Begriff Risikoüberprüfung wird als Synonym für den Begriff Risikocontrolling verwendet.[183]

Im Zuge der Risikoberichterstattung ist, über die identifizierten und bewerteten sowie über die eingeleiteten Maßnahmen zur Risikobewältigung regelmäßig zu berichten. Die Aufgabe des Risikoreporting ist, den systematischen Fluss relevanter Risikoinformationen an alle wesentlichen Stellen und Ressourcen zu gewährleisten. Der Inhalt dieser Ergebnisse soll die Risikoidentifikation, -analyse und -bewertung, den Status der Planung, Steuerung und Umsetzung der Maßnahmen zur Risikobewältigung als auch Informationen aus der

[181] Vgl. GLEIßNER (2017), S. 426.
[182] Vgl. GLEIßNER (2017), S. 426.
[183] Vgl. BRÜHWILER (2016), S. 175.

Risikoüberwachung und -überprüfung sein. Dabei ist zu betonen, dass das Risikoreporting mit dem bestehenden Berichtssystem abzustimmen ist und nicht als isolierter Prozess anzusehen ist.[184] Des Weiteren ist zwischen der internen und externen Berichterstattung zu unterscheiden.[185] Die interne Berichterstattung richtet sich beispielsweise an Bereichsleiter, Corporate Risk Management bzw. zentrales Risikomanagement, Risk Committee, Vorstand und Aufsichtsrat. Im Gegensatz dazu baut die externe Berichterstattung auf die interne Berichterstattung auf und richtet sich vor allem an Wirtschaftsprüfer, Shareholder, Debtholder, Analysten und Rating-Agenturen.[186]

Auch im Rahmen der DSFA, also im Datenschutz-Risikomanagement, sind die Risiken kontinuierlich zu überwachen.[187] Der Autor FRIEDEWALD empfiehlt jedoch, dass die DSFA zumindest alle drei Jahre überprüft werden sollte, ob die Ergebnisse der DSFA noch zutreffend sind. Zudem hat der Verantwortliche kontinuierlich zu überwachen, ob sich die Rahmenbedingungen des Einsatzes in technischen, organisatorischen oder rechtlichen Weisen ändern und ob neue Datenschutzrisiken entstehen könnten. Außerdem hat er zu überprüfen, ob die ausgewählten Schutzmaßnahmen den erwarteten Nutzen haben. Dabei muss sichergestellt werden, dass die Maßnahmen an Veränderungen angepasst werden. Um eine effiziente Reaktion auf veränderte Rahmenbedingungen zu ermöglichen, ist eine Einbindung in das allgemeine Risiko- und/oder Datenschutz-Management zu empfehlen.[188]

Im Hinblick auf die Berichtslegung sind zwei Funktionen zu erfüllen. Die erste Funktion soll eine Bestandsaufnahme sein, in der die betroffenen Daten, die betroffene Umwelt und die Datenschutzrisiken über den Lebenszyklus der betroffenen Daten identifiziert werden, und mit der die entsprechenden Anspruchsgruppen informiert werden können. Die zweite Funktion dient zur Nachverfolgung der Maßnahmen und der nachträglichen Verbesserung der Risiken. Die Organisation kann den Empfängerkreis, die Inhalte des Berichtes und den Grad der Vertraulichkeit selbst bestimmen. Dabei kann der Bericht, der vertraulich einem unabhängigen Auditor oder einer AB vorgelegt wird, mehr Details enthalten, als einer, der den Anspruchsgruppen oder der Öffentlichkeit vorgelegt wird.[189] Art. 35 Abs. 7 DSGVO legt die Mindestinhalte eines DSFA-Berichts fest, welche im vorigen Kapitel bereits erwähnt wurden.[190]

Im Rahmen des nächsten Kapitels wird näher auf die praktische Umsetzung der DSFAs eingegangen und aufgezeigt, wie das Tool zur Durchführung dieser konzipiert wurde.

---

[184] Vgl. DENK/EXNER-MERKELT/RUTHNER (2008), S. 134.
[185] Vgl. VANINI (2012), S. 210.
[186] Vgl. DENK/EXNER-MERKELT/RUTHNER (2008), S. 134 ff.
[187] Vgl. BIEKER/BREMERT/HANSEN (2018), S. 494.
[188] Vgl. FRIEDEWALD (2017), S. 70.
[189] Vgl. REINIS (2017), S. 85.
[190] S. Kapitel 3.5. Die Erstellung eines Berichts im Rahmen der Berichtsphase, S. 41.

5. Datenschutz-Folgenabschätzungen beim Kooperationspartner

Da im Rahmen dieser Arbeit ein Tool zur Durchführung von DSFAs zu konzipieren ist, wird dieses in diesem Kapitel ausführlich beschrieben. Dabei wird näher auf die einzelnen Arbeitsblätter des Tools eingegangen. Zuerst wird das Navigationsfeld des Tools aufgezeigt. Anschließend widmet sich das erste Unterkapitel der Beschreibung des Arbeitsblattes zur Überprüfung der Notwendigkeit einer DSFA. Danach befasst sich das erste Unterkapitel mit einem Arbeitsblatt, in dem grundsätzliche Fragen zur DSFA aufgelistet sind. Der Fokus liegt jedoch auf dem Risk-Assessment-Sheet, welches in das Tool integriert wurde. Dabei wird gezeigt, wie der Risikomanagementprozess im Tool umgesetzt werden kann.

Das zweite Unterkapitel setzt sich mit der Durchführung der einzelnen DSFAs in der Raiffeisen-Landesbank Steiermark AG auseinander. Zudem werden die vorgenommen Workshops und deren Ergebnisse für die sechs identifizierten Prozesse beschrieben. Auch der Workshop mit dem IT-Experten der Raiffeisen-Landesbank Steiermark AG findet Erwähnung. Die TOP-5-Brutto- und Nettorisiken beschließen dieses Kapitel.

5.1. Das Tool zur Durchführung von Datenschutz-Folgenabschätzungen

In diesem Unterkapitel wird das konzipierte Tool beschrieben und näher erklärt. Wie man aus der Abbildung 14 auf der nächsten Seite erkennen kann, wird beim Öffnen des Tools ein Navigationsfeld angezeigt, welches in fünf Bereiche gegliedert ist.

Im ersten Teil des Tools findet man ein Prüfschema, mit dem die einzelnen Prozesse, in denen personenbezogene Daten verarbeitet werden, der Raiffeisen-Landesbank geprüft werden können, ob eine DSFA durchzuführen ist. Der zweite Teil des Tools befasst sich mit grundsätzlichen Fragen zur DSFA. Der dritte Teil des Tools stellt den Schwerpunkt dar, da es sich dabei um das Risk-Assessment-Sheet handelt. Dieses Sheet dient zur Umsetzung des Risikomanagementprozesses. Im Rahmen des vierten Bereiches des Tools werden in jeweils eigenen Arbeitsblättern die Bruttorisiken, die TOP-5-Bruttorisiken, die Nettorisiken sowie die TOP-5-Nettorisiken dargestellt. Der letzte Bereich des Tools dient zur Erstellung eines DSFA-Berichts. In den folgenden Unterkapiteln wird auf die einzelnen Bereiche des Tools detailliert eingegangen.

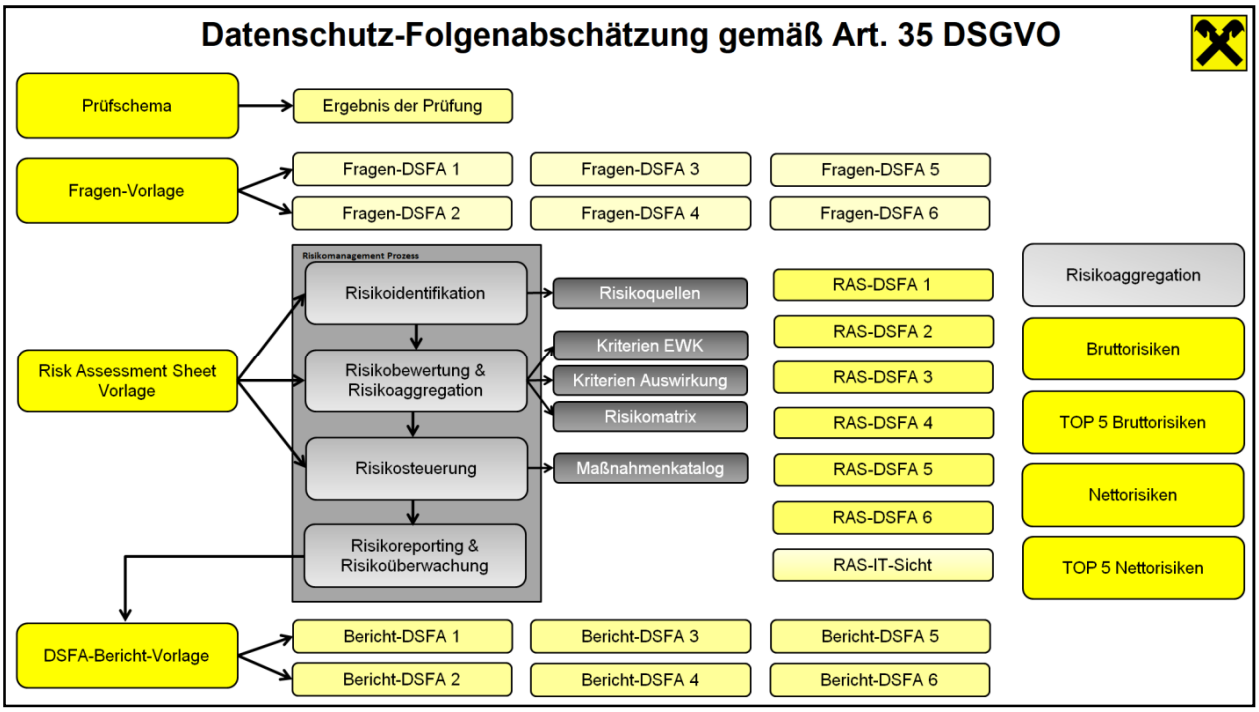


Abbildung 14: Aufbau des Tools,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

5.1.1. Die Notwendigkeitsprüfung einer Datenschutz-Folgenabschätzung im Tool

Um eine DSFA durchführen zu können, hat der Anwender des Tools zu Beginn auf den Button „Prüfschema“ zu klicken. Dadurch öffnet sich ein Tabellenblatt, in dem alle Geschäftsprozesse der Raiffeisen-Landesbank Steiermark AG, in denen personenbezogene Daten verarbeitet werden, aufgelistet sind. Des Weiteren befinden sich in diesem Tabellenblatt alle Kriterien zur Überprüfung, ob die Durchführung einer DSFA notwendig ist und somit wahrscheinlich ein hohes Risiko vorliegt. Diese ausgewählten Kriterien richten sich nach den einzelnen Kriterien[191], die bereits im dritten Kapitel ausgearbeitet wurden. Beginnt man mit der Prüfung, ob die Durchführung einer DSFA notwendig ist, hat man in dem Tabellenblatt zunächst die drei Kriterien zur verpflichtenden Durchführung zu überprüfen. Die folgende Abbildung zeigt einen Auszug aus dem Tool.

[191] S. Kapitel 3.2. Die Notwendigkeitsprüfung in der Vorbereitungsphase, S. 27 ff.

Startseite	Prüfschema	Zum Ergebnis der Prüfung

Prozess	Überprüfung der Kriterien zur verpflichtenden Durchführung		
	Profiling (automatisierte Entscheidung)	umfangreiche Verarbeitung besondere Kategorie pb Daten/Daten über strafrechtliche Verurteilungen	system. weitr. Überwachung öff. zug. Bereiche
K01.01.01 Veranlagungs-Beratung durchführen 3.00	-	-	-
K01.01.02 Kunden anlegen 4.00	-	-	-
K01.01.06 Kundenabwanderungen vorbeugen und bearbeiten 1.00	-	-	-
K01.99.01 Ausweise scannen oder kopieren 3.00	-	-	-
K02.01.01 Konto eröffnen PK und FK 7.00	-	-	-
K02.01.02 Kontoänderungen vornehmen PK und FK 4.00	-	-	-
K02.01.03 Zeichnungsberechtigung ändern PK und FK 4.00	-	-	-

Tabelle 13: Kriterien zur verpflichtenden Durchführung,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

Der Anwender des Tools hat zunächst zu hinterfragen, ob bei dem jeweiligen Geschäftsprozess „Profiling“ vorliegt. Um die Kriterien besser verstehen zu können, sind diese mit Kommentaren, in denen die Kriterien näher erklärt werden, versehen. Hinsichtlich des Kriteriums „Profiling“ findet man daher in den Kommentaren nähere Fragestellungen, um beantworten zu können, ob „Profiling“ in dem jeweiligen Prozess vorliegt oder auch nicht. Beispielsweise wird bei diesem Kriterium gefragt, ob eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen durchgeführt wird, die als Grundlage für Entscheidungen dienen, die für natürliche Personen Rechtswirkung entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen könnte. Das zweite Kriterium zur verpflichtenden Durchführung einer DSFA stellt die „Umfangreiche Verarbeitung der besonderen Kategorie personenbezogener Daten bzw. Daten über strafrechtliche Verurteilungen“ dar. Hierbei hat der Anwender zu evaluieren, ob sensible Daten, welche im zweiten Kapitel näher beschrieben wurden[192], und Daten über strafrechtliche Verurteilungen umfangreich verarbeitet werden. Im Rahmen des nächsten Schrittes hat der Anwender herauszufinden, ob eine systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche, beispielsweise über Videoüberwachungen, durchgeführt wird. Anschließend sind die neun Kriterien gemäß der Datenschutzgruppe nach Art. 29 zu überprüfen. Wenn zumindest zwei Kriterien zutreffen, liegt ein hohes Risiko vor und

[192] S. Kapitel 2.1. Definition und Analyse von Kernbegriffen, S. 7.

eine DSFA ist durchzuführen.[193] Diese neun Kriterien wurden folgendermaßen in das Tool eingepflegt:

Überprüfung 9 Kriterien der Art-29-Gruppe								
Profiling/ Segmentierung	Automatisierte Entscheidung mit Rechtswirkung oder ähnlicher Wirkung	Systematische Überwachung	Sensible Daten	DV in großem Umfang	in mehrere VT/untersch. Zweck verarbeitet	Daten schutzbedürftiger Personen	Neue Technologie/ neuartiger Einsatz	Betroffene werden an Ausübung eines Rechts/Nutzung einer DL/ Durchführung Vertrag gehindert
-	-	-	-	-	-	-	-	-
Ja	-	-	-	Ja	-	-	-	-
Ja	-	-	-	-	-	Ja	-	-
-	-	-	-	-	-	-	-	-
Ja	-	-	-	-	-	-	-	-

Tabelle 14: Neun Kriterien gemäß Datenschutzgruppe Art. 29,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

Auf diese neun Kriterien wird im Rahmen dieses Kapitels nicht näher eingegangen, da sich die Verfasserin dieser Arbeit bereits im dritten Kapitel mit diesen Kriterien tiefgreifend auseinandergesetzt hat. Der Anwender hat zudem zu prüfen, ob sich der jeweilige Geschäftsprozess auf der Blacklist oder auf der Whitelist befindet oder ob andere Ausnahmen zutreffen. Das Tool beinhaltet alle Ausnahmen, welche bereits im dritten Kapitel[194] näher beschrieben wurden. Diese Ausnahmen wurden im Tool wie folgt berücksichtigt:

Blacklist	Whitelist	Ausnahmen			
VT befindet sich auf Blacklist	VT befindet sich auf Whitelist	wsl kein hohes Risiko	für ähnliche VT bereits DSFA durchgeführt	VT wurde bereits von Aufsichtsbehörde geprüft	VT beruht auf Rechtsgrunlage im Unionsrecht/ Recht Mitgliedstaat
-	-	Ja	-	-	-
-	-	Nein	-	-	-
-	-	Nein	-	-	-
-	-	Ja	-	-	-
-	-	Ja	-	-	-

Tabelle 15: Kriterien zur Überprüfung der Ausnahmen,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

[193] S. Kapitel 3.2. Die Notwendigkeitsprüfung in der Vorbereitungsphase, S. 27 ff.
[194] S. Kapitel 3.2. Die Notwendigkeitsprüfung in der Vorbereitungsphase, S. 32 ff.

Wenn alle bereits erwähnten Kriterien überprüft wurden, kann festgestellt werden, ob die Durchführung einer DSFA notwendig ist. Hierbei ist im Tool für jeden Geschäftsprozess zu dokumentieren, ob eine DSFA durchzuführen ist oder nicht. Außerdem ist zu begründen, warum eine DSFA vorzunehmen ist. Als Nächstes kann man in dem Sheet „Prüfschema“ oder über die Startseite mit Hilfe eines Buttons zu den Ergebnissen der Prüfung springen. Wie aus Tabelle 16 ersichtlich wird, werden die relevanten Geschäftsprozesse in ihre Kernzwecke untergliedert. Für die Prozesse, die gelb markiert sind, ist eine DSFA durchzuführen. Für die grau hinterlegten Prozesse muss keine DSFA vorgenommen werden, da diese von der Whitelist ausgeschlossen wurden.

Startseite	Ergebnis der Prüfung			Zurück
Kunden gewinnen und betreuen	**Finanzierungen durchführen**	**Vermittlungsgeschäfte durchführen**	**Revision durchführen**	**Personalmanagement durchführen**
K01.01.06 Kundenabwanderungen vorbeugen und bearbeiten 1.00	K04.01.01 PzStr1 StandardPz PK_Standard-/Internrahmen 2.00	K07.09.01 Maklergeschäft durchführen	U03.01.02 Prüfung durchführen 2.00	U06.02.03 Personal rekrutieren 2.00
K01.01.09 Lebenspuzzle-Beratung durchführen 1.00	K04.01.02 PzStr1 StandardPz Finanzierung blanko 4.00		U03.01.03 Sonderauftrag durchführen 2.00	U06.02.02 Mitarbeiter einführen 2.00
K01.01.02 Kunden anlegen 4.00	K04.01.03 PzStr1 StandardPz Finanzierung besichert 7.00		U03.01.04 Bericht an Vorstand durchführen 2.00	U06.04.01 Personal-/Organisationsentwicklung betreiben 1.00
	K04.02.01 PzStr2_Neufinanzierung durchführen 9.00		U03.01.05 Quartalsreporting (Bericht § 42 Abs. 3 BWG) durchführen 2.00	
	K04.05.01 Prolongation Betriebsmittelkredit 3.00		U03.01.06 Ad hoc-Reporting durchführen 2.00	**Rechtsberatung bereitstellen**
	K04.05.02 Kreditüberwachung incl. EWS durchführen 5.00		U03.01.07 Erledigung überwachen 2.00	U08.01.01 Rechtsberatung (Standard) durchführen 2.00
	K04.05.03 Rating_tourlich aktualisieren 4.00			
	K04.05.07 Intensivbetreuung gestionieren 1.00			**Kommunikation u. Marketing betreiben**
	K04.07.03 ADB bearbeiten 4.00			U10.02.02 Veranstaltungen organisieren 1.00
	K04.99.02 Eskalation durchführen 1.00			
	K04.99.10 Organgeschäft §28(1) BWG 2.00			**Rechenzentrum**
	K04.99.15 Bestandsdaten evaluieren 1.00			Verwaltung physischer Sicherheitssysteme
	K04.07.04 Sanierungskredit gestionieren 3.00			
	K04.99.18 Konsortialfinanzierung abstimmen 2.00			

Tabelle 16: Ergebnis der Prüfung,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

Wenn die einzelnen Geschäftsprozesse, für welche die Durchführung einer DSFA notwendig sind, identifiziert wurden, können die einzelnen DSFAs vorgenommen werden. Um diese DSGVO-konform zu erstellen, wurde in das Tool ein eigenes Arbeitsblatt mit Fragen zur DSFA integriert. Das nächste Unterkapitel beschreibt dieses Arbeitsblatt näher.

5.1.2. Fragen zur Datenschutz-Folgenabschätzung im Tool

Nachdem die DSFA relevanten Geschäftsprozesse identifiziert wurden, kann für jeden einzelnen Prozess das Arbeitsblatt „Fragen“ ausgefüllt werden. Im Tool wurde eine Vorlage erstellt, welche für weitere Prozesse kopiert werden kann. Auch kann über die Startseite mit Hilfe des Buttons „Fragen“ dorthin navigiert werden. Zuerst hat der Anwender die Verarbeitungstätigkeit, die befragten Personen und das Datum zu nennen. Danach ist die Verarbeitung von personenbezogenen Daten und deren Zweck in der jeweiligen Verarbeitungstätigkeit systematisch zu beschreiben, da dies, wie bereits im dritten Kapitel erwähnt[195] wurde, verpflichtend durchzuführen ist. Ferner hat gemäß Art. 35 Abs. 7 lit. b. eine Bewertung der Notwendigkeit und Verhältnismäßigkeit in Bezug auf den Zweck zu erfolgen. Daher lautet die dritte Frage im Arbeitsblatt, wie notwendig und verhältnismäßig man den Verarbeitungsvorgang in Bezug auf den Zweck einschätzt. Wie man in der nächsten Abbildung erkennen kann, wurde dafür eine vierstufige Skala konzipiert, um eine klare Tendenz zwischen „notwendig und verhältnismäßig“ und „nicht notwendig und verhältnismäßig“ erkennen zu können.

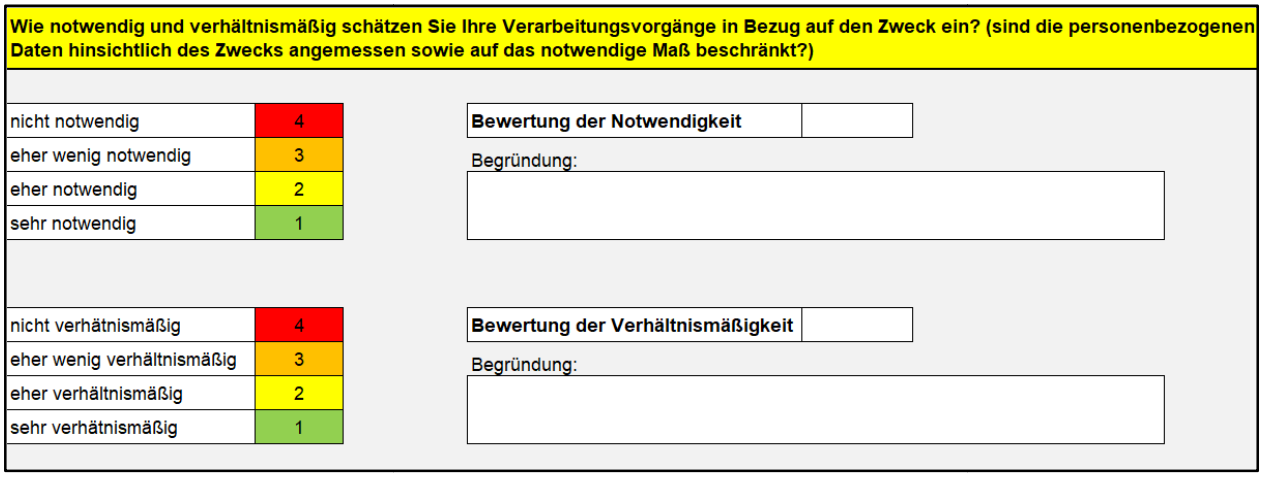


Abbildung 15: Bewertung der Notwendigkeit und Verhältnismäßigkeit,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

Da der nächste Schritt im DSFA-Prozess die Identifikation der Akteure und der betroffenen Personen darstellt[196], sind darauf folgend die involvierten Parteien, der Verantwortliche und der Auftragsverarbeiter anzuführen. Es können auch die Kategorien betroffener Personen als auch interne und externe Empfänger[197] der personenbezogenen Daten ausgewählt werden. Um auch einen Überblick über die verarbeiteten Datenarten zu erlangen, kann auch diesbezüglich eine Auswahl getroffen werden. Aufgrund der Verpflichtung zur Bestimmung der Rechtsgrundlage[198],

[195] S. Kapitel 3.2. Die Notwendigkeitsprüfung in der Vorbereitungsphase, S. 38.
[196] S. Kapitel 3.2. Die Notwendigkeitsprüfung in der Vorbereitungsphase, S. 38.
[197] S. Kapitel 2.1. Definition und Analyse von Kernbegriffen, S. 11.
[198] S. Kapitel 2.1. Definition und Analyse von Kernbegriffen, S. 12; S. Kapitel 3.2. Die Notwendigkeitsprüfung in der Vorbereitungsphase, S. 38.

können diese selektiert werden. Anschließend folgt die Frage, ob es in der jeweiligen Verarbeitungstätigkeit bereits eine bekannte Datenschutzverletzung gab, um mit Hilfe dieser Frage auf erste Risiken aufmerksam werden zu können. Abschließend lautet die letzte Frage, welche Risiken bezogen auf die verarbeiteten Daten für die Rechte und Freiheiten der betroffenen Personen existieren könnten. Im Rahmen dieser Frage ist zu erwähnen, dass dafür die Brainstorming-Methode, welche im vorigen Kapitel näher beschrieben wurde[199], angewendet werden soll. Diese letzte Frage dient bereits zur Identifikation potenzieller Risiken.[200] Das nächste Unterkapitel befasst sich damit, wie weitere Risiken im Tool identifiziert, beurteilt und gesteuert werden können.

5.1.3. Das Risk-Assessment-Sheet im Tool

Nachdem alle Fragen in dem Arbeitsblatt „Fragen“ beantwortet wurden hat man von der Startseite aus zum Risk-Assessment-Sheet weiter zu navigieren. Für dieses Arbeitsblatt wurde zur Risikoidentifikation ein Risikokatalog mit einigen möglichen Risiken[201] erstellt, auf welche bereits im Kapitel Datenschutz-Risikomanagement eingegangen wurde. Ebenso wurde dabei eine Kategorisierung der Risiken vorgenommen. Wie aus der folgenden Tabelle auf der nächsten Seite ersichtlich wird, gliedert sich der Katalog in Risikogruppen, Einzelrisiken, Unterkategorien der Einzelrisiken und in eine Beschreibung bzw. ein Beispiel zu dem jeweiligen Risiko. Die Risikogruppen stellen die Schutzziele wie Verfügbarkeit, Vertraulichkeit, Rechtmäßigkeit, und Integrität dar, da einige Autoren wie beispielsweise KÖNIGS, PROKEIN, ROMEIKE und HAGER diese Kategorisierung empfehlen[202]. Hinsichtlich des Schutzziels Rechtmäßigkeit wurde eine Gruppierung in die DSGVO-Grundsätze, wie Transparenz, Zweckbindung, Treu und Glauben, Datenminimierung, Speicherbegrenzung und Richtigkeit, vorgenommen, da auch diese für eine DSGVO-konforme Umsetzung der DSFA zu berücksichtigen sind[203].

Welche Einzelrisiken, Unterkategorien der Einzelrisiken, Beschreibungen bzw. Beispiele verwendet wurden, können der nachfolgenden Tabelle entnommen werden. Bezüglich der Einzelrisiken sei hervorgehoben, dass diese im Großen und Ganzen auf einer Literaturrecherche basieren, jedoch auch in den einzelnen, durchgeführten Workshops ergänzt wurden. Beispielsweise wurde das Risiko „Vernichtung von personenbezogenen Daten“ aufgrund des Vorschlages des IT-Experten im Rahmen eines Workshops in das Risiko der physischen Vernichtung und das Risiko der elektronischen Vernichtung von personenbezogenen Daten gruppiert. Ansonsten wurde das Risiko „Missbräuchliche

[199] S. Kapitel 4.2.1. Die Risikoidentifikation als Schlüsselphase, S. 56.
[200] S. Kapitel Anhang, S. 118 ff.
[201] S. Kapitel 4.2.1. Die Risikoidentifikation als Schlüsselphase, S. 51 ff.
[202] S. Kapitel 4.2.1. Die Risikoidentifikation als Schlüsselphase, S. 50.
[203] S. Kapitel 2.2. Die Grundsätze der Datenschutz-Grundverordnung, S. 13 ff.

Verwendung von Kundendaten durch Mitarbeiter“, aufgrund der mehrmaligen Nennung dieses Risikos in den Workshops, in den Risikokatalog aufgenommen.

Risikokatalog				
Risikogruppe (Schutzziel)	**Einzelrisiko**	**Unterkategorie**	**Beschreibung/Beispiel**	**Existiert dieses Risiko? (Ja/Nein)**
Beispiel	Verlust von pb Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können	-	Verlorengegangener USB-Stick	Ja
Verfügbarkeit	**Vernichtung von personenbezogenen Daten**	Vernichtung von physischen pb Daten	Vernichtung von physischen Dokumenten mit pb Daten	
		Vernichtung von elektronischen pb Daten	Vernichtung von beispielsweise gescannten Dokumenten mit pb Daten	
	Verlust von pb Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können		verlorengegangene Datenträger z.B. USB-Sticks verlorengegangene mobile Endgeräte z.B. Smartphones, Notebooks verlorengegangene Papierakten, die z.B. in einem Mülleimer entsorgt und von Passanten "gefunden" wurden	
Vertraulichkeit	**Unbefugte Offenlegung von personenbezogenen Daten**		z.B. Fehlversand per E-Mail oder per Post Posting von internen personenbezogenen Daten in einem sozialen Netzwerk	
	Unbefugter Zugang zu personenbezogenen Daten	Unbefugter Zutritt zu Datenverarbeitungsanlagen	z.B. Unbefugter Zutritt zu sensiblen Daten	
		Unbefugte Systembenutzung	z.B. Hacker verschaffen sich Zugang zum System (Kundenkonten)	
	Nichteinhaltung eines Betroffenenrechts	Nichteinhaltung des Rechts auf Auskunft	z.B. Kunde erhält keine vollständige Auskunft, zu viel Auskunft, über Daten von Dritten Auskunft	
		Nichteinhaltung des Rechts auf Information	z.B. Kunde erhält keine Information	
		Nichteinhaltung des Rechts auf Widerspruch	z.B. Kundendaten werden trotz Verweigerung verarbeitet	
		Nichteinhaltung des Rechts auf Berichtigung	z.B. Berichtigung ist aufgrund von anderen Systemabhängigkeiten nicht möglich	
		Nichteinhaltung des Rechts auf Löschung	z.B. Keine Löschung personenbezogener Daten trotz Aufforderung des Kunden	
		Nichteinhaltung des Rechts auf Übertragbarkeit	z.B. Personenbezogene Daten werden trotz Aufforderung nicht übertragen	
		Nichteinhaltung des Rechts auf Einschränkung der Verarbeitung	z.B. Newsletter Aktion	
Rechtmäßigkeit	**Risiko der unrechtmäßigen Verarbeitung**	Verarbeitung von personenbezogenen Daten ohne gültiger Rechtsgrundlage und ohne dem Wissen der betroffenen Person	z.B. die Verarbeitung personenbezogener Daten zur Überwachung ohne das Wissen der Mitarbeiter	
		Unbefugte Aufhebung der Pseudonymisierung	falls z.B. in Excel ein weiteres, ggf. sogar verborgenes, Tabellenblatt mit den dazugehörigen personenbezogenen Daten zum Pseudonym existiert und dadurch die Pseudonymisierung unbefugt aufgehoben werden kann	
		Das Teilen von pb Daten mit dritten Parteien ohne gültige Rechtsgrundlage	z.B der Arbeitgeber gibt sensible Daten von Kunden/Mitarbeitern weiter (z.B biometrische Daten, Gesundheitsdaten, Finanzdaten, etc.)	
Rechtmäßigkeit (Transparenz)	**Unzureichende Information über Zweck der Verarbeitung (Mangel an Transparenz)**		z.B. Einschränkung der Rechte des Kunden aufgrund der unzureichenden Information über den Zweck der Verarbeitung	
	Unnötig verlängerte Aufbewahrung von personenbezogenen Daten		Aufbewahrungsfristen werden ignoriert	
Rechtmäßigkeit (Zweckbindung)	**Risiko der Nichtbeachtung der Zweckbindung**		z.B. nicht legitime Zweckänderung von pb Daten für andere Verarbeitungstätigkeiten	
Rechtmäßigkeit (Treu und Glauben)	**Missbräuchliche Verwendung von Kundendaten durch Mitarbeiter**		z.B. Bankdaten werden für einen Zahlungsbetrug missbraucht	
Rechtmäßigkeit (Datenminimierung)	**Risiko der Nichteinhaltung der Datenminimierung**		Ausufernde Erhebung personenbezogener Daten, unnotwendige Daten werden verarbeitet, die Verarbeitung wird nicht auf das dem Zweck notwendige Maß beschränkt	
Rechtmäßigkeit (Speicherbegrenzung)	**Risiko der Nichteinhaltung der Speicherbegrenzung**		Nach Wegfall des Zwecks der Verarbeitungstätigkeit wird keine Löschung durchgeführt	
Rechtmäßigkeit (Richtigkeit)	**Risiko der Nichteinhaltung der Datenrichtigkeit**		z.B. Gewünschte Datenänderung des Kunden wird nicht im System umgesetzt und sind daher nicht auf aktuellem Stand	
Integrität	**Veränderung von personenbezogenen Daten**		z.B. Fehlerhafte Software ändert Rating bei einem Kredit wodurch es zur Ablehnung eines Kredites kommt	

Tabelle 17: Risikokatalog,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

Wenn Einzelrisiken im Risk-Assessment-Sheet ausgewählt wurden, besteht danach die Möglichkeit Szenarien zu kreieren. Dabei kann zunächst die Art der Risikoquellen ausgesucht werden. Mit Hilfe des Buttons „Risikoquellen“ kann man in ein eigenes Arbeitsblatt springen, um sich dort eine Übersicht über verschiedene Risikoquellen verschaffen zu können. Diese Risikoquellen basieren auf einer Literaturrecherche und wurden bereits im Kapitel Datenschutz-Risikomanagement beleuchtet[204]. Im Risk-Assessment-Sheet kann schließlich ausgewählt werden, ob das jeweilige Risiko menschlich oder nichtmenschlich, intern oder extern, unbeabsichtigt oder vorsätzlich eintreten kann und was bzw. wer der Auslöser des Risikos sein kann. Dafür wurde ein Drop-Down-Feld geschaffen, bei dem man auswählen kann, ob der Auslöser ein Mitarbeiter, ein Vorgesetzter, das Wartungspersonal, der Mitbewerber, ein Hacker, ein Wasserschaden durch Rohrbruch, ein Feuer, ein Stromausfall, ein Ausfall der Internet-Leitung oder ein sonstiger Auslöser sein kann.

Außerdem besteht die Option, eine Auswahl möglicher Folgen für das Risiko mit Hilfe eines Drop-Down-Feldes treffen zu können. Als potenzielle Folgen kann man den Verlust der Kontrolle, die Einschränkung der Rechte, die Diskriminierung, den Identitätsdiebstahl, den finanziellen Verlust, die unbefugte Aufhebung der Pseudonymisierung, die Rufschädigung, den Verlust der Vertraulichkeit, den wirtschaftlichen Nachteil, den gesellschaftlichen Nachteil, die Kreditschädigung, die Erpressung, die Verletzung der Privatsphäre oder die betrügerische Verwendung auswählen. Diese Folgen wurden auf Grundlage der Literaturrecherche in das Risk-Assessment-Sheet eingearbeitet und wurden bereits im Kapitel-Datenschutz-Risikomanagement[205] angeführt. Danach kann der Anwender den Risikoverantwortlichen angeben.

Wenn die einzelnen Risiken identifiziert wurden und Szenarien ausgearbeitet wurden, kann in Folge dessen mit der Risikobeurteilung beginnen. Hierbei kann man die Risiken vor etwaigen Maßnahmen als auch nach definierten Maßnahmen beurteilen. Hinsichtlich der Risiken vor Maßnahmen ist zuerst die Eintrittswahrscheinlichkeit festzulegen. Dafür gibt es wieder ein Drop-Down-Feld mit einer fünfstufigen Skala. Um zu mehr Informationen hinsichtlich dieser Skala zu gelangen, kann man mittels dem Button „Kriterien EWK“ zu einem eigenen Arbeitsblatt springen, in dem die Kriterien in Bezug auf die Eintrittswahrscheinlichkeit nachgelesen werden können. Diese Kriterien beruhen auf einer Literaturrecherche. Die Autoren KRANIG, SACHS, GIERSCHMANN und REINIS empfehlen eine ähnliche vierstufige Skala, welche im Kapitel Datenschutz-Risikomanagement[206] erwähnt wurde. Die Verfasserin dieser Arbeit wollte diese vierstufige Skala für die Raiffeisen-Landesbank Steiermark AG umsetzen, jedoch stellte sich nach Absprache mit dem Datenschutzbeauftragten heraus, dass diese Möglichkeit nicht

[204] S. Kapitel 4.2.1. Die Risikoidentifikation als Schlüsselphase, S. 53.
[205] S. Kapitel 4.2.1. Die Risikoidentifikation als Schlüsselphase, S. 53 ff.
[206] S. Kapitel 4.2.2. Die Risikobewertung als Vorstufe zur Risikosteuerung, S. 58 ff.

bestand, da das Computersystem die Änderung auf eine vierstufige Skala nicht zuließ. An dieser Stelle muss betont werden, dass eine vierstufige Skala mehr Vorteile gehabt hätte, denn bei einer fünfstufigen Skala wird der Risikoeigner eher dazu tendieren, die Auswahl in der Mitte zu treffen. Eine vierstufige Skala hingegen zwingt den Risikoeigner zu einer präziseren Entscheidung. In der folgenden Abbildung sieht man, wie die Kriterien in Bezug auf die Eintrittswahrscheinlichkeit im Tool für die Raiffeisen-Landesbank Steiermark AG umgesetzt wurden.

Kriterien in Bezug auf die Eintrittswahrscheinlichkeit			
Bereich	Auswirkung auf Betroffene	Kriterien	Beispiele
5	Sehr wahrscheinlich	Für die ausgewählte Risikoquelle scheint es sehr wahrscheinlich zu sein, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen	Diebstahl von Dokumenten/USB-Sticks mit Kundendaten aus einer öffentlich zugänglichen Lobby der Bank in der kein Personal anwesend ist
4	Wahrscheinlich	Für die ausgewählte Risikoquelle scheint es wahrscheinlich zu sein, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen	Diebstahl von Dokumenten/USB-Sticks mit Kundendaten aus einer öffentlich zugänglichen Lobby der Bank in der Personal anwesend ist
3	Möglich	Für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen	Diebstahl von Dokumenten/USB-Sticks mit Kundendaten aus einem Büro in der Bank, welches nur zugänglich ist, nachdem man den Empfang passiert hat
2	Unwahrscheinlich	Für die ausgewählte Risikoquelle scheint es unwahrscheinlich zu sein, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen	Diebstahl von Dokumenten/USB-Sticks mit Kundendaten aus einem Raum in der Bank, der durch ein Ausweislesegerät gesichert ist
1	Sehr unwahrscheinlich	Für die ausgewählte Risikoquelle scheint es sehr unwahrscheinlich zu sein, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen	Diebstahl von Dokumenten/USB-Sticks mit Kundendaten aus einem Raum in der Bank, der durch ein Ausweislesegerät und einen Zugangscode gesichert ist

Tabelle 18: Kriterien in Bezug auf die Eintrittswahrscheinlichkeit,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

Wie aus der oberen Tabelle ersichtlich ist, kann man bei der Auswahl der Eintrittswahrscheinlichkeit auf einer fünfstufigen Skala zwischen sehr unwahrscheinlich und sehr wahrscheinlich wählen. Trifft man die Entscheidung, „sehr unwahrscheinlich“ zu wählen, bedeutet dies, dass es für die ausgewählte Risikoquelle sehr unwahrscheinlich scheint, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen. Dies ist beispielsweise der Fall, wenn ein Diebstahl von Dokumenten oder USB-Sticks mit Kundendaten aus einem Raum in der Bank, der durch ein Ausweislesegerät und einen Zugangscode gesichert ist, möglich ist. Beurteilt der Risikoeigner ein Risiko als „unwahrscheinlich“, heißt das, dass für die ausgewählte Risikoquelle es unwahrscheinlich scheint, eine Schwachstelle ausnutzen zu können, um eine Bedrohung eintreten zu lassen. Als Beispiel sei der Diebstahl von Dokumenten oder USB-Sticks mit Kundendaten aus einem Raum in der Bank, der nun nur durch ein Ausweislesegerät gesichert ist, erwähnt. Wird auf der fünfstufigen Skala für die Risikobeurteilung „möglich“ ausgewählt, bedeutet dies, dass es möglich ist, eine Schwachstelle auszunutzen, um eine Bedrohung eintreten zu lassen. Dies ist der Fall, wenn ein Diebstahl von Dokumenten bzw. USB-Sticks mit Kundendaten aus einem Büro in der Bank möglich ist, welches nur zugänglich ist, nachdem man den Empfang passiert hat. Gilt ein Risiko als

„wahrscheinlich“, besagt dies, dass es wahrscheinlich ist, dass eine Schachstelle ausgenutzt werden kann, um eine Bedrohung eintreten zu lassen. Ein Risiko ist als wahrscheinlich einzustufen, wenn ein Diebstahl aus einer öffentlich zugänglichen Lobby, in der Personal anwesend ist, möglich ist. Die Stufe „sehr wahrscheinlich“ bedeutet hingegen, dass es sehr wahrscheinlich ist, dass eine Schwachstelle ausgenutzt werden kann, um eine Bedrohung eintreten zu lassen. Als sehr wahrscheinlich gilt ein Risiko, bei dem beispielsweise ein Diebstahl aus einer öffentlich zugänglichen Lobby, in der kein Personal anwesend ist, möglich ist.
Des Weiteren ist im Risk-Assessment-Sheet zu begründen, warum die jeweilige Eintrittswahrscheinlichkeit ausgewählt wurde. Infolgedessen ist die Auswirkung des Risikos zu beurteilen. Dabei hat der Risikoeigner zwischen der materiellen und der immateriellen Auswirkung zu unterscheiden, welche von den Autoren FEILER und HORN empfohlen werden[207]. Hinsichtlich der Auswirkung wurde ebenso eine fünfstufige Skala erstellt, da nur diese vom Computersystem akzeptiert wird. Mit Hilfe des Buttons „Kriterien Auswirkung“ kann man zu der Übersicht dieser Kriterien springen. Ansonsten wurde die bereits beschriebene vierstufige Skala[208] auf eine fünfstufige Skala transformiert.

Hinsichtlich der Auswirkung kann sich der Risikoeigner zwischen einer sehr geringen und einer sehr hohen Auswirkung entscheiden. Als „sehr gering“ kann die Auswirkung beurteilt werden, wenn die Betroffenen eventuell unbedenkliche Unannehmlichkeiten erleiden, welche sie aber mit wenigen Problemen überwinden können. Als Beispiel für eine materielle Auswirkung gilt der Erhalt von unerwünschtem Werbematerial, der Zeitverlust bei der Wiederholung von Formalitäten, die Wiederverwendung von bekanntgegebenen Daten, ein gesperrtes Bankkonto, der Empfang unerwünschter E-Mails und die telefonische Kontaktierung des Betroffenen. Beispiele für eine immaterielle Auswirkung sind die Entwicklung leichter psychologischer Leiden, eine leichte Verärgerung durch eine unerwünschte erfragte Information, Angst durch Kontrollverlust persönlicher Daten, das Gefühl der Verletzung der Privatsphäre ohne Grund.

Die Auswirkung eines Risikos kann als gering eingestuft werden, wenn die Betroffenen eventuell minimale Unannehmlichkeiten erleiden, welche sie aber mit einigen Problemen überwinden können. Beispiele für eine materielle Auswirkung wären unbestellte E-Mails mit rufschädigender Wirkung, veraltete Daten ohne Update, die Verarbeitung unrichtiger Daten oder eine gezielte Werbung gerichtet auf persönliche Informationen, die die betroffene Person geheim halten wollte. Als Beispiele für eine immaterielle Auswirkung gelten die Entwicklung heilbarer psychologischer Leiden, die Einschüchterung in sozialen Netzwerken oder die Verletzung der Privatsphäre ohne nachhaltige Effekte.

[207] S. Kapitel 4.2.2. Die Risikobewertung als Vorstufe zur Risikosteuerung, S. 58 ff.
[208] S. Kapitel 4.2.2. Die Risikobewertung als Vorstufe zur Risikosteuerung, S. 58 ff.

Wenn die Auswirkung als Mittel einzustufen ist, lässt das darauf schließen, dass die Betroffenen eventuell signifikante Unannehmlichkeiten erleiden, welche sie aber mit einigen Schwierigkeiten überwinden können. Als materielle Auswirkung gelten beispielsweise permanente finanzielle Schwierigkeiten, das Verbot der Führung von Bankkonten, eine Kontensperrung im Ausland oder eine Beschädigung von Eigentum. Beispiele für eine immaterielle Auswirkung wäre die Entwicklung leichter, bleibender psychologischer Leiden, das Gefühl der Verletzung von Grundrechten (Diskriminierung), Erpressung, Cybermobbing, Belästigung oder das Gefühl der Verletzung der Privatsphäre mit nachhaltigen Effekten.

Eine Beurteilung als hohe Auswirkung ist dann vorzunehmen, wenn die Betroffenen eventuell signifikante Konsequenzen erleiden, welche sie nur mit ernsthaften Schwierigkeiten überwinden können. Hierfür sei als Beispiel für eine materielle Auswirkung der finanzielle Verlust infolge eines Betruges, die Verweigerung von Vertragsabschlüssen, der Entgang nicht wiederkehrender Kreditangebote oder der Verlust des Arbeitsplatzes zu erwähnen. Beispiele für eine immaterielle Auswirkung wären die Entwicklung bleibender, schwerer psychologischer Leiden oder eine Entführung.

Als sehr hoch wird die Auswirkung betrachtet, wenn die Betroffenen eventuell signifikante oder sogar unumkehrbare Konsequenzen erleiden, die sie nicht überwinden können. Als Beispiel für eine materielle Auswirkung sei eine finanzielle Not oder der Verlust einer Wohnung genannt. Beispiele für eine immaterielle Auswirkung wäre ein Personenschaden mit Todesfolge oder eine schwerste Invalidität. Nachdem die Auswirkung beurteilt wurde hat im Risk-Assessment-Sheet wieder eine Begründung der jeweiligen Auswahl der Auswirkung zu erfolgen. Die nachfolgende Tabelle auf der nächsten Seite zeigt die Kriterien in Bezug auf die Auswirkung für die Raiffeisen-Landesbank Steiermark AG:

Kriterien in Bezug auf die Auswirkung				
Bereich	Auswirkung auf Betroffene	Kriterien	Beispiele Materielle Auswirkung	Beispiele Immaterielle Auswirkung
5	Sehr hoch	Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können	- Finanzielle Not - Verlust der Wohnung	- Personenschaden mit Todesfolge - Schwerste Invalidität (Einbruch)
4	Hoch	Betroffene erleiden eventuell signifikante Konsequenzen, welche sie nur mit ernsthaften Schwierigkeiten überwinden können	- Finanzieller Verlust infolge eines Betruges - Verweigerung von Vertragsabschlüssen - Entgang nicht wiederkehrender Kreditangebote - Verlust des Arbeitsplatzes	- Entwicklung schwerer, bleibender psychologischer Leiden (starke Verminderung der Lebensqualität z.B. Depression) - Entführung
3	Mittel	Betroffene erleiden eventuell signifikante Unannehmlichkeiten, welche sie aber mit einigen Schwierigkeiten überwinden können	- Permanente finanzielle Schwierigkeiten - Verbot der Führung von Bankkonten - Kontosperrung im Ausland - Beschädigung von Eigentum	- Entwicklung leichter, bleibender psychologischer Leiden (Beeinflussung der Lebensqualität) - Gefühl der Verletzung von Grundrechten (Diskriminierung) - Erpressung - Cyber Mobbing - Belästigung - Gefühl der Verletzung der Privatsphäre mit nachhaltigen Effekten
2	Gering	Betroffene erleiden eventuell minimale Unannehmlichkeiten, welche sie aber mit einigen Problemen überwinden können	- Unvorhergesehene Zahlungsverpflichtungen - Zusätzliche Kosten (Prozesskosten) - Kostenerhöhungen (Erhöhte Prämien) - Unbestellte Mails die rufschädigende Wirkung entfalten - Veraltete Daten ohne Update - Verarbeitung unrichtiger Daten - Gezielte Werbung gerichtet auf persönliche Informationen, welche die betroffene Person geheim halten wollte	- Entwicklung heilbarer psychologischer Leiden (Rufschädigung) - Einschüchterung in sozialen Netzwerken - Verletzung der Privatsphäre ohne nachhaltige Effekte
1	Sehr gering	Betroffene erleiden eventuell unbedenkliche Unannehmlichkeiten, welche sie aber mit wenigen Problemen überwinden können	- Erhalt von unerwünschtem Werbematerial - Zeitverlust bei der Wiederholung von Formalitäten oder Warten - Wiederverwendung von bekanntgegebenen Daten - Gesperrtes Bankkonto - Gezielte Werbung für Finanzprodukte - Empfang unerwünschter E-Mails (Spam) - telefonische Kontaktierung des Betroffenen	- Entwicklung leichter psychologischer Leiden - Leichte Verärgerung (durch erhaltene/erfragte Informationen) - Angst (Kontrollverlust hinsichtlich persönlicher Daten) - Gefühl der Verletzung der Privatsphäre (ohne Grund)

Tabelle 19: Kriterien in Bezug auf die Auswirkung,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

Nachdem die Auswirkung und die Eintrittswahrscheinlichkeit mittels Drop-Down-Feld bestimmt wurden, berechnet sich im Risk-Assessment-Sheet der Erwartungswert. Zudem wird die Risikoklasse automatisiert angezeigt. Je nach Erwartungswert ergibt sich entweder ein geringes, mittleres oder hohes Risiko. Dadurch weiß der Anwender des Tools mit welchen Maßnahmen das jeweilige Risiko gesteuert werden kann. Wenn man darüber Bescheid wissen möchte, ab welchem Erwartungswert ein geringes, mittleres oder hohes Risiko vorliegt, kann man mit Hilfe des Buttons „Risikomatrix“ in ein weiteres Arbeitsblatt springen, um dies zu begutachten. Wie aus der nachfolgenden Abbildung ersichtlich ist, gilt ein Erwartungswert zwischen eins bis vier als ein geringes Risiko und damit als ein akzeptables Risiko. Berechnet das Tool einen Erwartungswert zwischen fünf und zwölf liegt ein mittleres Risiko vor, welches nur bedingt akzeptiert werden kann und für welches Maßnahmen zur Risikoreduktion zu definieren sind. Bei einem Erwartungswert zwischen fünfzehn und fünfundzwanzig resultiert ein hohes und inakzeptables Risiko, für welches Maßnahmen zur Risikovermeidung zu treffen sind.

Risikomatrix							
Risikomatrix			Schadensausmaß [materiell/immateriell]				
			1	2	3	4	5
			Sehr gering	Gering	Mittel	Hoch	Sehr hoch
Eintrittswahrscheinlichkei	5	Sehr wahrscheinlich	5	10	15	20	25
	4	Wahrscheinlich	4	8	12	16	20
	3	Möglich	3	6	9	12	15
	2	Unwahrscheinlich	2	4	6	8	10
	1	Sehr unwahrscheinlich	1	2	3	4	5

Tabelle 20: Risikomatrix,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

In weiterer Folge sind nach der Risikobeurteilung im Risk-Assessment-Sheet bereits umgesetzte (IST-Maßnahmen), sowie weitere geeignete Maßnahmen zu treffen. Dafür kann man sich für jedes Einzelrisiko mittels Drop-Down-Feld für eine passende Maßnahme entscheiden. Mit Hilfe des Buttons „Maßnahmenkatalog“ kann man sich einen Überblick über alle möglichen Maßnahmen verschaffen. Stellt man nach der Risikobeurteilung fest, dass ein hohes Risiko existiert, kann man sich beispielsweise dafür entscheiden, die personenbezogenen Daten nicht zu erheben oder die Verarbeitungstätigkeit einzustellen. Kristallisiert sich heraus, dass ein mittleres Risiko besteht, können die Maßnahmen, welche in der nächsten Tabelle aufzufinden sind, optiert werden.

Hinsichtlich dieses Maßnahmenkataloges wurde untersucht, wie dieser optimiert werden kann. Nach der Durchführung der Literaturrecherche wurde festgestellt, dass in Bezug auf die Sicherstellung der Vertraulichkeit, der Integrität, der Verfügbarkeit und Belastbarkeit und der Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung kein Verbesserungspotenzial besteht. Allerdings kam man zum Ergebnis, dass auch Maßnahmen zur Sicherstellung der Rechtmäßigkeit zu treffen sind[209]. Wie bereits im Kapitel Datenschutz-Risikomanagement erwähnt wurde, können zur Gewährleistung der Rechtmäßigkeit Maßnahmen wie die Einschränkung der Datenkategorien, Einschränkung des Datenumfangs, Einschränkung der Kategorien von Betroffenen, Einschränkung der Anzahl von Betroffenen, Einschränkung der Verarbeitungszwecke, Einschränkung des Kreises der Zugangsberechtigten, Einschränkung des Kreises der Übermittlungsempfänger, Einschränkung der Speicherdauer, Maßnahmen zur Sicherstellung der Richtigkeit und Durchführung von Audits getroffen werden. Des Weiteren wurden auch die Maßnahmen zur Risikovermeidung basierend auf der Literaturrecherche im Maßnahmenkatalog ergänzt.

[209] S. Kapitel 4.2.3. Mögliche Strategien zur Steuerung der Risiken, S. 66 ff.

Maßnahmen zur Risikominderung - Technische, organisatorische und physische Maßnahmen für mittlere Risiken		
Art	**Maßnahme**	**Beschreibung**
Vertraulichkeit (Art 32 Abs 1 lit b DSGVO)	**Zutrittskontrolle**	Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, z.B.: Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Sicherheitspersonal, Portier, Alarmanlagen, Videoanlagen;
	Zugangskontrolle	Schutz vor unbefugter Systembenutzung, z.B.: (sichere) Kennwörter (einschließlich entsprechender Policy), automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern;
	Zugriffskontrolle	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems, z.B.: Standard-Berechtigungsprofile auf „need to know-Basis", Standardprozess für Berechtigungsvergabe, Protokollierung von Zugriffen, periodische Überprüfung der vergebenen Berechtigungen, insb. von administrativen Benutzerkonten;
	Trennungskontrolle	Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;
	Pseudonymisierung	Sofern für die jeweilige Datenverarbeitung zweckmäßig, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt, sodass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer konkreten betroffenen Person zugeordnet werden können, und diese zusätzlichen Informationen werden gesondert aufbewahrt und unterliegen entsprechenden technischen und organisatorischen Maßnahmen;
	Klassifikationsschema für Daten	Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich);
	Technische Löschkonzept-Einstellungen	Sowohl für Daten selbst als auch Metadaten wie Logfiles, udgl.;
Integrität (Art 32 Abs 1 lit b DSGVO)	**Weitergabekontrolle**	Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;
	Eingabekontrolle	Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;
Verfügbarkeit und Belastbarkeit (Art 32 Abs 1 lit b,c DSGVO)	**Verfügbarkeitskontrolle**	Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV, Dieselaggregat), Virenschutz, Firewall, Meldewege und Notfallpläne; Security Checks auf Infrastruktur- und Applikationsebene, mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern;
	Rasche Wiederherstellbarkeit	Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Es besteht eine Sicherung der Daten, Die IT-Administration ist in der Lage, die Sicherung zeitnahe einzuspielen)
Rechtmäßigkeit	**Einschränkung der Datenkategorien**	
	Einschränkung des Datenumfangs	
	Einschränkung der Kategorien von Betroffenen	
	Einschränkung der Anzahl von Betroffenen	
	Einschränkung der Verarbeitungszwecke	
	Einschränkung des Kreises der Zugangsberechtigten	Nur spezifisch geschulte Mitarbeiter bekommen Zugang zu Datenverarbeitungsanlagen
	Einschränkung der Übermittlungsempfänger	Teilen der Daten nur mit Konzerngesellschaften, die für die Zweckerreichung notwendig sind
	Einschränkung der Speicherdauer	Löschung der Daten nach der Zweckerreichung und nach Ablauf der gesetzlichen Aufbewahrungspflicht
	Maßnahmen zur Sicherstellung der Richtigkeit	Keine Datenänderung bei anonymen Meldungen
	Durchführung von Audits	Um die Einhaltung aller datenschutzrechtlicher Vorgaben sicherzustellen
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art 32 Abs 1 lit d DSGVO; Art 25 Abs 1 DSGVO)	**Auftragskontrolle**	Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen
	Incident-Response-Management	
	Datenschutzfreundliche Voreinstellungen	
	Datenschutz-Management; einschließlich regelmäßiger Mitarbeiter-Schulung	

Tabelle 21: Optimierte Maßnahmen zur Risikominderung,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

In weiterer Folge kann im Risk-Assessment-Sheet unter dem Punkt „Risikosteuerung" die zuständige Person für die Umsetzung der jeweiligen Maßnahme und die Deadline für die Umsetzung festgelegt werden, um später bei der Risikoüberwachung kontrollieren zu können, ob diese Person die Maßnahme im geplanten Zeitraum tatsächlich umgesetzt hat.

Wenn passende Maßnahmen für die Einzelrisiken getroffen wurden, sind in weiterer Folge die Risiken nach Umsetzung der Maßnahmen zu beurteilen. Diese zweite Beurteilung ist von

großer Bedeutung, da man am Ende des DSFA-Prozesses darüber informiert sein will, ob ein hohes Restrisiko vorliegt oder auch nicht. Denn bei einem hohen Restrisiko, wäre die Aufsichtsbehörde verpflichtend zu konsultieren[210]. Um diesbezüglich einen Fehler zu vermeiden, erscheint am Ende des Risk-Assessment-Sheets und somit auch am Ende des DSFA-Zykluses bei einem geringen und mittleren Risiko die automatisierte Meldung, dass die Konsultation der Aufsichtsbehörde nicht notwendig ist. Ergibt sich jedoch ein hohes Restrisiko, erscheint die Meldung, dass die Maßnahmen abermals zu überarbeiten sind, da ansonsten die Aufsichtsbehörde zu konsultieren ist. Im Hinblick auf die Überwachung des DSFA-Prozesses kommt am Ende auch die Meldung „Bitte zumindest in 3 Jahren wieder überprüfen, ob sämtliche DSFA Ergebnisse noch zutreffen“ automatisch zum Vorschein. Im nächsten Unterkapitel wird erläutert, wie der DSFA-Bericht in das Tool integriert wurde.

5.1.4. Der Datenschutz-Folgenabschätzungs-Bericht im Tool

Da im Rahmen der Berichtsphase auch ein DSFA-Bericht zu erstellen ist, wurde im Tool eine Vorlage für diesen Bericht erarbeitet. Der konzipierte Bericht enthält dabei alle Mindestanforderungen, die im Rahmen der DSGVO zu erfüllen sind.[211] Dieser Bericht kann im Falle einer Prüfung der Aufsichtsbehörde vorgelegt werden, jedoch kann dieser auch für die interne Berichterstattung an den Datenschutzbeauftragten verwendet werden. Zu Beginn des Berichts erfolgt eine systematische Beschreibung der Verarbeitungstätigkeit. Diese Beschreibung wurde bereits im Arbeitsblatt „Fragen zur DSFA“ vorgenommen und somit nur noch im Arbeitsblatt „DSFA-Bericht“ verlinkt. In weiterer Folge werden die involvierten Parteien, wie der Verantwortliche, der Auftragsverarbeiter und die Kontaktdaten des Datenschutzbeauftragten im Bericht dargelegt. Danach wird auf den Zweck der jeweiligen Verarbeitung eingegangen, welcher ebenfalls automatisch erscheint, da der Zweck mit dem Arbeitsblatt „Fragen zur DSFA“ verlinkt wurde. Da die DSGVO auch eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck fordert, ist auch dies im Bericht enthalten. Die Bewertung wurde ebenfalls im Arbeitsblatt „Fragen zur DSFA“ durchgeführt, daher wurde auch hier nur noch eine Verlinkung zum Arbeitsblatt „Bericht“ vorgenommen.

Der Schwerpunkt des Berichts liegt auf der Darlegung der identifizierten Risiken, sowie deren Beurteilung und Steuerungsmaßnahmen. Die nachfolgende Abbildung zeigt einen Ausschnitt aus dem konzipierten Bericht anhand des Beispiels der Verarbeitungstätigkeit „Finanzierung durchführen“, welcher die Einzelrisiken, deren Folgen, die Beurteilung vor etwaigen Maßnahmen inklusive dem Erwartungswert und der Risikoklasse beinhaltet. Auch hier wurde wieder eine Verlinkung mit dem Risk-Assessment-Sheet vorgenommen, um das Tool

[210] S. Kapitel 3.2. Die Notwendigkeitsprüfung in der Vorbereitungsphase, S. 37.
[211] S. Kapitel 3.5. Die Erstellung eines Berichts im Rahmen der Berichtsphase, S. 41.

benutzerfreundlicher zu gestalten. Zudem wurde im Bericht eine Risikomatrix erarbeitet, um die Risiken zu visualisieren. Die Risikomatrix soll auch zur Erkennung von Kernrisiken in der jeweiligen Verarbeitungstätigkeit dienen.

Datenschutz-Folgenabschätzung Report für die Verarbeitungstätigkeit "Finanzierung durchführen"

1) Systematische Beschreibung der Verarbeitungstätigkeit

Siehe Tool "DSFA5_Bericht"

2) Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck

nicht notwendig	4
eher wenig notwendig	3
eher notwendig	2
sehr notwendig	1

Bewertung der Notwendigkeit 1

Begründung:
Ist notwendig zur Durchführung des Geschäfts.

nicht verhätnismäßig	4
eher wenig verhältnismäßig	3
eher verhältnismäßig	2
sehr verhätnismäßig	1

Bewertung der Verhältnismäßigkeit 1

Begründung:
Um der gesetzlichen Verpflichtung (Meldewesen) nachzukommen.

3) Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Person

Risiko Nr.	Risiko	Folge	EWK vor Maßnahmen	Auswirkung vor Maßnahmen	Erwartungswert	Risikoklasse
1	Verlust von pb Daten, die möglicherweise von Dritten zur Kenntnis genommen werden	Verlust der Vertraulichkeit	1	1	1	Gering
2	Unbefugte Offenlegung von personenbezogenen Daten	Verlust der Vertraulichkeit	3	1	3	Gering
3	Missbräuchliche Verwendung von Kundendaten durch Mitarbeiter	Rufschädigung	1	3	3	Gering
4	Veröffentlichung von pb Daten	Rufschädigung	1	3	3	Gering
5	Veröffentlichung von pb Daten	Kreditschädigung	1	3	3	Gering

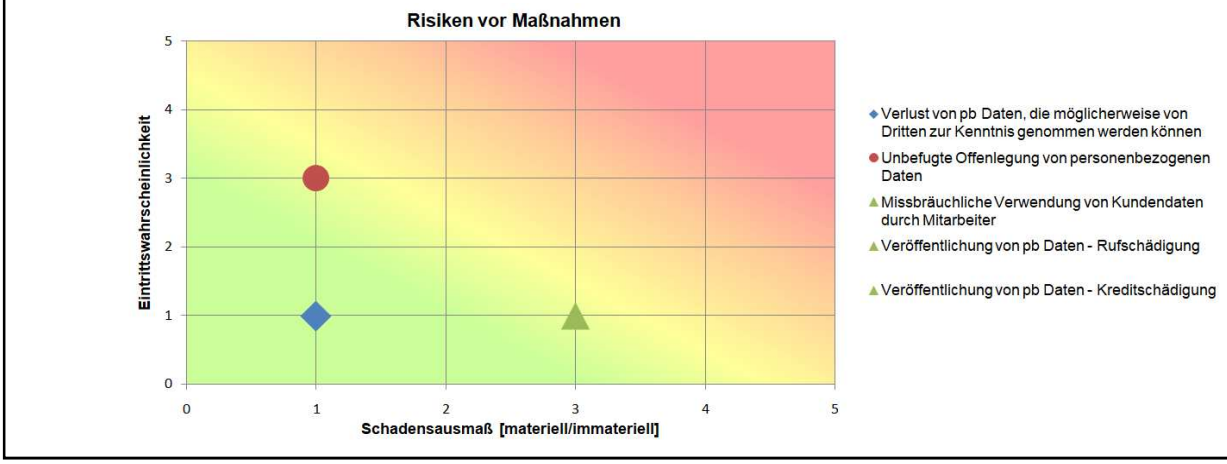
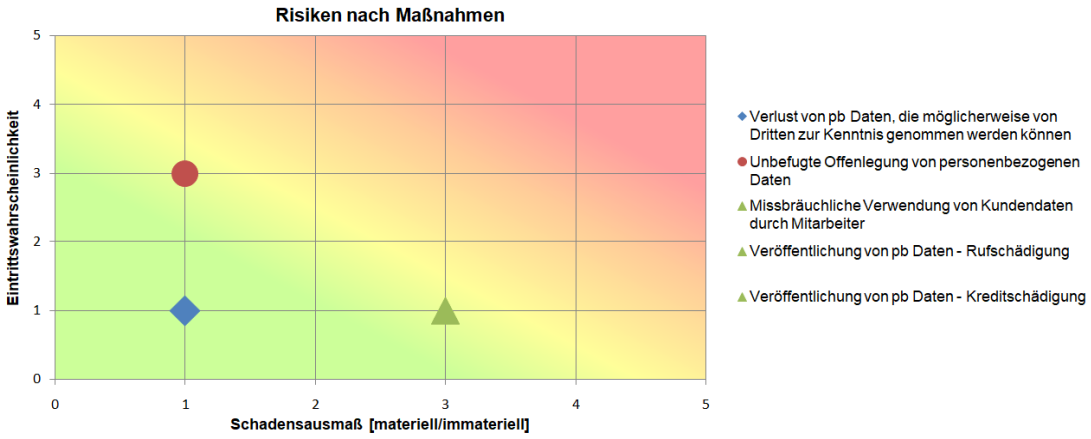


Abbildung 16: Beispiel Datenschutz-Folgenabschätzungs-Bericht Teil 1,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

In weiterer Folge zeigt der Bericht, wie in der Abbildung 12 ersichtlich wird, die Beurteilung der Risiken nach definierten Maßnahmen, deren Erwartungswert und die dazugehörige Risikoklasse. Als Ergebnis erscheint im Bericht, ob die Aufsichtsbehörde konsultiert werden muss. Danach werden die Risiken nach Maßnahmen in einer Risikomatrix veranschaulicht. Der letzte Bereich des Berichts stellt die Erläuterung der geplanten Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt wird.

Datenschutz-Folgenabschätzung Report für die Verarbeitungstätigkeit "Finanzierung durchführen"

Risiko Nr.	Risiko	Ergebnis	EWK nach Maßnahmen	Auswirkung nach Maßnahmen	Erwartungswert	Risikoklasse
1	Verlust von pb Daten, die möglicherweise von Dritten zur Kenntnis genommen werden	Aufsichtsbehörde muss nicht konsultiert werden	1	1	1	Gering
2	Unbefugte Offenlegung von personenbezogenen Daten	Aufsichtsbehörde muss nicht konsultiert werden	3	1	3	Gering
3	Missbräuchliche Verwendung von Kundendaten durch Mitarbeiter	Aufsichtsbehörde muss nicht konsultiert werden	1	3	3	Gering
4	Veröffentlichung von pb Daten	Aufsichtsbehörde muss nicht konsultiert werden	1	3	3	Gering
5	Veröffentlichung von pb Daten	Aufsichtsbehörde muss nicht konsultiert werden	1	3	3	Gering



4) Geplante Abhilfemaßnahmen, einschließlich Garantien, Sicherhietsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird

Risiko Nr.	Maßnahmen
1	Ein geringes Risiko kann akzeptiert werden, daher sind keine Maßnahmen notwendig.
2	Ein geringes Risiko kann akzeptiert werden, daher sind keine Maßnahmen notwendig.
3	Ein geringes Risiko kann akzeptiert werden, daher sind keine Maßnahmen notwendig.
4	Ein geringes Risiko kann akzeptiert werden, daher sind keine Maßnahmen notwendig.
5	Ein geringes Risiko kann akzeptiert werden, daher sind keine Maßnahmen notwendig.

Abbildung 17: Beispiel Datenschutz-Folgenabschätzungs-Bericht Teil 2,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

5.1.5. Die Risikoaggregation und Ermittlung der TOP-5-Risiken im Tool

In Bezug auf die Risikoaggregation besteht im Tool die Möglichkeit von der Startseite mit Hilfe des Buttons „Bruttorisiken“ zu einer Übersicht über alle identifizierten Risiken in den einzelnen Verarbeitungstätigkeiten, für welche eine DSFA notwendig ist, zu gelangen. Dieses Arbeitsblatt soll vor allem dem Datenschutzbeauftragten zur schnellen Informationsbeschaffung dienen. Denn dieser kann sich dadurch einen Überblick verschaffen, welche Einzelrisiken in den jeweiligen Verarbeitungstätigkeiten existieren und welche Folgen der Eintritt des Risikos mit sich bringen könnte. Außerdem sieht man mit welcher Eintrittswahrscheinlichkeit und Auswirkung das Risiko beurteilt wurde, welcher Erwartungswert vorliegt und in welche Risikoklasse das Risiko eingegliedert wird. Die folgende Tabelle zeigt einen Ausschnitt aus dem Arbeitsblatt „Bruttorisiken“.

Bruttorisiken (Risiken vor Maßnahmen)							
Verarbeitungstätigkeit	Risikokategorie	Unterkategorie	Folgen des Risikos	EWK	Auswirkung	Erwartungs-wert	Risikoklasse
Lebenspuzzle durchführen	**Missbräuchliche Verwendung von Kundendaten durch Mitarbeiter**	-	Rufschädigung Verlust der Vertraulichkeit alle Folgen	1	2	2	Gering
Kundenabwanderung vorbeugen und bearbeiten	**Unbefugte Aufhebung der Pseudonymisierung**	-		3	1	3	Gering
	Rufschädigung	-		1	3	3	Gering
	Gesellschaftlicher Nachteil	-		1	1	1	Gering
	Verletzung der Privatsphäre	-		1	1	1	Gering
Revision durchführen	**Verlust von pb Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können**	-	Kreditschädigung Veröffentlichung in Medien	1	3	3	Gering
	Unbefugte Offenlegung von personenbezogenen Daten	-	Verlust der Vertraulichkeit	1	1	1	Gering
Verwaltung physischer Sicherheitssysteme	**Unbefugte Offenlegung von personenbezogenen Daten**	-	Rufschädigung	1	1	1	Gering
	Missbräuchliche Speicherung von Kundendaten	-	Rufschädigung	1	1	1	Gering
Finanzierung durchführen	**Verlust von pb Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können**	-	Verlust der Vertraulichkeit Veröffentlichung von pb Daten	1	1	1	Gering
	Unbefugte Offenlegung von personenbezogenen Daten	-	Verlust der Vertraulichkeit	3	1	3	Gering
	Missbräuchliche Verwendung von Kundendaten durch Mitarbeiter	-	Rufschädigung	1	3	3	Gering
	Bekanntgabe von pb Daten	-	Rufschädigung	1	3	3	Gering
	Bekanntgabe von pb Daten	-	Kreditschädigung	1	3	3	Gering
IT-Experte	**Vernichtung von personenbezogenen Daten**	Vernichtung von physischen pb Daten	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	4	3	12	Mittel
	Vernichtung von personenbezogenen Daten	Vernichtung von elektronischen pb Daten	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	4	3	12	Mittel
	Verlust von pb Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können	-	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	4	3	12	Mittel
	Unbefugte Offenlegung von personenbezogenen Daten	-	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	3	4	12	Mittel
	Unbefugter Zugang zu personenbezogenen Daten	Unbefugter Zutritt	Identitätsdiebstahl Verletzung der Privatsphäre Kreditschädigung betrügerische Verwendung	2	3	6	Mittel
	Unbefugter Zugang zu personenbezogenen Daten	Unbefugte Systembenutzung	Identitätsdiebstahl Verletzung der Privatsphäre Kreditschädigung betrügerische Verwendung	2	3	6	Mittel
	Veränderung von personenbezogenen Daten	-	Verlust der Vertraulichkeit	2	5	10	Mittel

Tabelle 22: Bruttorisiken,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

Da das Ziel der Masterarbeit auch die Identifikation der TOP-5-Risiken ist, kann man mit dem Button „Weiter“ zum Arbeitsblatt „TOP-5-Bruttorisiken“ navigieren. Im Hinblick auf alle ermittelten Bruttorisiken wurde eine Priorisierung vorgenommen, um zu den TOP-5-Risiken zu gelangen. Dafür wurden die 5 Risiken mit dem höchsten Erwartungswert ausgewählt.

Des Weiteren wurde im Tool ein eigenes Arbeitsblatt für die Nettorisiken erarbeitet, zu dem man auf dem Arbeitsblatt „TOP-5-Bruttorisiken“ mit dem Button “Weiter“ springen kann. Die folgende Abbildung auf der nächsten Seite zeigt einen Ausschnitt dieses Arbeitsblattes.

Nettorisiken (Risiken nach Maßnahmen)							
Verarbeitungstätigkeit	Risikokategorie	Unterkategorie	Folgen des Risikos	EWK	Auswirkung	Erwartungs-wert	Risikoklasse
Lebenspuzzle durchführen	**Missbräuchliche Verwendung von Kundendaten durch Mitarbeiter**	-	Rufschädigung Verlust der Vertraulichkeit alle Folgen	1	2	2	Gering
Kundenabwanderung vorbeugen und bearbeiten	**Unbefugte Aufhebung der Pseudonymisierung**	-		3	1	3	Gering
	Rufschädigung	-		1	3	3	Gering
	Gesellschaftlicher Nachteil	-		1	1	1	Gering
	Verletzung der Privatsphäre	-		1	1	1	Gering
Revision durchführen	**Verlust von pb Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können**	-	Kreditschädigung Veröffentlichung in Medien	1	3	3	Gering
	Unbefugte Offenlegung von personenbezogenen Daten	-	Verlust der Vertraulichkeit	1	1	1	Gering
Verwaltung physischer Sicherheitssysteme	**Unbefugte Offenlegung von personenbezogenen Daten**	-	Rufschädigung	1	1	1	Gering
	Missbräuchliche Speicherung von Kundendaten	-	Rufschädigung	1	1	1	Gering
Finanzierung durchführen	**Verlust von pb Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können**	-	Verlust der Vertraulichkeit Veröffentlichung von pb Daten	1	1	1	Gering
	Unbefugte Offenlegung von personenbezogenen Daten	-	Verlust der Vertraulichkeit	3	1	3	Gering
	Missbräuchliche Verwendung von Kundendaten durch Mitarbeiter	-	Rufschädigung	1	3	3	Gering
	Bekanntgabe von pb Daten	-	Rufschädigung	1	3	3	Gering
	Bekanntgabe von pb Daten	-	Kreditschädigung	1	3	3	Gering
IT-Experte	**Vernichtung von personenbezogenen Daten**	Vernichtung von physischen pb Daten	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	2	3	6	Mittel
	Vernichtung von personenbezogenen Daten	Vernichtung von elektronischen pb Daten	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	2	3	6	Mittel
	Verlust von pb Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können	-	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	2	3	6	Mittel
	Unbefugte Offenlegung von personenbezogenen Daten	-	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	2	4	8	Mittel
	Unbefugter Zugang zu personenbezogenen Daten	Unbefugter Zutritt	Identitätsdiebstahl Verletzung der Privatsphäre Kreditschädigung betrügerische Verwendung	1	3	3	Gering
	Unbefugter Zugang zu personenbezogenen Daten	Unbefugte Systembenutzung	Identitätsdiebstahl Verletzung der Privatsphäre Kreditschädigung betrügerische Verwendung	1	3	3	Gering
	Veränderung von personenbezogenen Daten	-	Verlust der Vertraulichkeit	2	4	8	Mittel

Tabelle 23: Nettorisiken,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

Der Button „Weiter“, welcher sich auf dem Arbeitsblatt „Nettorisiken“ befindet, führt den Anwender danach zum Arbeitsblatt „TOP-5-Nettorisiken“, damit der Anwender auch über die höchsten Restrisiken informiert ist.

5.2. Ergebnisse der durchgeführten Datenschutz-Folgenabschätzungen

Nach der Erstellung des Tools und der Prüfung der einzelnen Geschäftsprozesse für welche eine DSFA durchzuführen ist, konnte man mit den Workshops beginnen. Für folgende Verarbeitungstätigkeiten wurde ein Workshop durchgeführt, da man durch die Prüfung der einzelnen Kriterien zum Ergebnis kam, dass für diese sechs Verarbeitungstätigkeiten eine DSFA durchzuführen ist, da im Wesentlichen das Kriterium „umfangreiche Verarbeitung der besonderen Kategorie personenbezogener Daten“ erfüllt ist:

- Lebenspuzzle durchführen
- Kundenabwanderung vorbeugen und bearbeiten
- Revision durchführen
- Verwaltung physischer Sicherheitssysteme
- Finanzierung durchführen
- Maklergeschäft durchführen

Überdies wurde ein Workshop mit dem IT-Experten durchgeführt, da die Risikoeigner nicht alle Risiken wie zum Beispiel das Risiko eines unbefugten Zugangs zu personenbezogenen Daten beurteilen konnten. Die Workshops wurden gemeinsam mit dem Risikoeigner, welcher zugleich der Prozesseigner ist, dem Prozesscoach und einem Mitarbeiter der Abteilung „Datenmanagement“, der zukünftig das Tool zu bedienen hat, abgehalten.

Zu Beginn der einzelnen Workshops wurden den Beteiligten die wesentlichen Grundlagen der DSFA mitgeteilt. Das Hauptziel dieser Workshops lag in der Vervollständigung des Tools und somit in der Durchführung des gesamten DSFA-Prozesses. In weiterer Folge wird auf die einzelnen Workshops und deren Ergebnisse näher eingegangen.

5.2.1. Workshop für den Prozess „Lebenspuzzle durchführen“

Der erste Schritt im Workshop für den Prozess „Lebenspuzzle durchführen“ bestand in der Beantwortung der einzelnen Fragen des Arbeitsblattes „Fragen_DSFA1“. Dabei war zunächst die Verarbeitungstätigkeit systematisch zu beschreiben. Im Rahmen des Workshops kam man zum Ergebnis, dass zu Beginn der Verarbeitungstätigkeit von der Abteilung „Vertriebsmanagement“ eine Kundenselektion für das Rechenzentrum durchgeführt wird. Die Abteilung „IT-Service & Quality“ übermittelt danach die Einladungen an die Kunden. Wenn der

Kunde die Einladung annimmt, wird vom Kundenbetreuer das Lebenspuzzle-Gespräch durchgeführt. Wird das Lebenspuzzle vom Kunden abgelehnt, wird die Wartung der Ablehnung durchgeführt und es erfolgt kein Lebenspuzzle mehr. Wird das Lebenspuzzle jedoch nicht abgelehnt, werden die Informationen des Gesprächs, vor allem die Kundenziele samt Ablaufdatum, gespeichert. Im Anschluss erfolgt durch das „Vertriebsmanagement“ eine Auswertung über die Ziele und Interessen der Kunden. Diese Auswertungen werden den Privat- und Geschäftskunden Filialen weitergeleitet, welche schließlich die Daten verarbeiten. Nach dieser Verarbeitung entscheiden die Privat- und Geschäftskunden Filialen dann über die Vertriebsaktivität. Danach setzt das „Vertriebsmanagement“ die Vertriebsaktivität auf und es wird ein Reminder festgesetzt, um eine Termineinladung durch die Abteilung „IT-Service & Quality“ oder den Kundenbetreuer vornehmen zu können. Der Termin wird schließlich vom Kunden bestätigt oder abgelehnt. Wird der Termin abgelehnt, wird der Lebenspuzzle Kontakt beendet. Falls der Termin angenommen wird, erfolgt wieder ein Lebenspuzzle-Gespräch.

Hinsichtlich des Zwecks der Verarbeitungstätigkeit zeigt die Befragung im Workshop, dass der Zweck in der Betreuung des Kunden liegt und dass die Beratung auf die Wünsche, Bedürfnisse und Ziele des Kunden abgestimmt werden soll. Der Verarbeitungsvorgang wurde in Bezug auf den Zweck als sehr notwendig und verhältnismäßig eingestuft, da durch diese Verarbeitungstätigkeit ein persönliches Lebenspuzzle für jeden Kunden gestaltet werden kann. Des Weiteren ist zu erwähnen, dass je genauer die Wünsche, Bedürfnisse und Ziele des Kunden bekannt gegeben werden, desto besser, zielorientierter und maßgeschneiderter kann die Beratung erfolgen. Außerdem können die Kunden frei entscheiden, ob sie die personenbezogenen Daten bekannt geben wollen.

Als Verantwortlicher im Sinne der DSGVO gelten die Raiffeisen-Landesbank Steiermark AG und die Landes-Hypothekenbank Steiermark AG. Das Rechenzentrum stellt den Auftragsverarbeiter dar. In weiterer Folge wurden als betroffene Personen potenzielle Kunden und Interessenten, Kunden als auch Mitarbeiter sowie nahe Angehörige bestimmt. Zu den internen Empfängerkategorien zählen der Geschäftsbereich „Vertragsverwaltung“, der Geschäftsbereich „Privat- und Geschäftskunden“ und die „Innenrevision“. Als externe Empfängerkategorien wurden IT-Dienstleister, Kartenproduzenten als auch Callcenter eruiert.

Im Hinblick auf die personenbezogenen Datenarten kam man zum Ergebnis, dass im Rahmen der Verarbeitungstätigkeit persönliche Detailangaben, Haushaltsdaten bzw. Daten zu familiären Verhältnissen, Kontaktdaten, Lebenslauf und Mitarbeiterqualifikation, Daten zu Beruf und Arbeitsverhältnis, Aufenthaltsstatus, Lohn- und Gehaltsdaten, Daten zu Beteiligungen, Lebens- und Konsumgewohnheiten, elektronische Protokoll- und Identifikationsdaten, Bild- und oder Tonaufzeichnungen, Bonitätsdaten, Finanzidentifikationsdaten, Daten zu Kreditgeschäft, Daten zu Einlagengeschäft, Daten zu Finanztermin -/Derivatgeschäft, Kassageschäft,

Wertpapierverwahrung und -verwaltung, Versicherungsdaten, Zahlungsverkehrs- und Clearing-Daten, Daten zu Fuhrparkmanagementgeschäft, Daten zu Bauträgergeschäft, Vermittlungsgeschäft, Vermietungsgeschäft, Anti-Money Laundering und Compliance-Daten, Marketing/Vertrieb, Safes und Schließfächern und die besondere Kategorie von personenbezogenen Daten verarbeitet werden.

Die Verarbeitung der personenbezogenen Daten basiert auf dem berechtigten Interesse. Auch hat es bis dato noch keine Datenschutzverletzungen gegeben. Im Rahmen des Brainstormings konnte das Risiko einer missbräuchlichen Verwendung von Kundendaten durch einen Mitarbeiter identifiziert werden. Im Risk-Assessment-Sheet wurde im Rahmen dieses Risikos die Risikoquellenart als menschlich, intern und vorsätzlich beschrieben und als tatsächliche Risikoquelle der Mitarbeiter genannt. Als Folge des Risikos wurde Rufschädigung und Verlust der Vertraulichkeit ausgewählt. Außerdem wurde das Risiko durch den Risikoeigner/Prozesseigner als sehr unwahrscheinlich eingeschätzt, da der Eintritt dieses Risikos die Kündigung des jeweiligen Mitarbeiters zur Folge hätte. Hinsichtlich der Auswirkung wurde eine immaterielle Auswirkung bestimmt, welche gering eingestuft wurde, da das Risiko mindere psychologische Leiden zur Folge hätte. Somit resultiert ein geringes Risiko, welches akzeptiert werden kann und für welches keine weiteren Maßnahmen zu treffen sind.

5.2.2. Workshop für den Prozess „Kundenabwanderung vorbeugen und bearbeiten“

Im Rahmen des Workshops für den Prozess „Kundenabwanderung vorbeugen und bearbeiten“ wurde zunächst der Prozess an sich näher systematisch beschrieben. Dabei kam man zum Ergebnis, dass das „Vertriebsmanagement“ verantwortlich für das Vorbeugen der Kundenabwanderungen ist und das Churn Management durchführt. Mit Hilfe des Churn Managements werden abwanderungsgefährdete Kunden rechtzeitig angesprochen und vom Bleiben überzeugt. Dabei spielen wichtige Parameter beispielsweise "häufiger Beraterwechsel", "Anzahl der Produkte" oder "Unbetreuter Kunde" eine Rolle. Des Weiteren wird ein externer Datenanalyst beauftragt, um die Wahrscheinlichkeit zu berechnen, ob ein Kunde abwanderungsgefährdet ist.

Danach beauftragt das „Vertriebsmanagement“ den Kundenberater mit der Herstellung des Kundenkontakts. Der Betreuer dokumentiert das Gespräch mit dem Kunden und leitet die Informationen dem „Vertriebsmanagement“ weiter. Diese sind dann zuständig für die Durchführung des Kontakt- und Ergebnismonitorings. Danach erfolgt die Analyse der Zusammenfassung und der Bereichsleiter trifft geeignete Maßnahmen.

Des Weiteren wird diese Verarbeitungstätigkeit durchgeführt, wenn der Kundenbetreuer ein Konto löscht und die Kontolöschungs-Checkliste befüllt. Diese Liste wird der „ Zahlungsverkehr

& Marktservice (ZMS)“ weitergeleitet, die in weiterer Folge postalisch oder persönlich den Kundenbetreuer über die Kontolöschungsgründe informieren. Die Abteilung „ZMS“ füllen die Checkliste aus und fasst die Kontolöschungsgründe vierteljährlich zusammen. Danach erfolgt wieder eine Analyse der Zusammenfassung und Maßnahmen werden abgeleitet. Ansonsten besteht die Möglichkeit, dass bei der Abteilung „ZMS“ eine postalische Kontolöschung eingeht. Dann wird das „IT-Service & Quality“ des Rechenzentrums mit der Durchführung der Kundentelefonate beauftragt. Wenn der Kunde innerhalb von drei Telefonversuchen erreichbar ist, erfolgt eine Rückmeldung des Kunden. Schließlich informiert das „IT-Service & Quality“ das „ZMS“ über die Kontolöschungsgründe.

Die Befragung im Workshop hat gezeigt, dass der Zweck dieser Verarbeitungstätigkeit in der Erkennung von abwanderungsgefährdeten Kunden liegt. Der Verarbeitungsvorgang wurde in Bezug auf den Zweck als sehr notwendig und verhältnismäßig eingestuft, da abwanderungsgefährdete Kunden sonst nicht erkannt werden können und der Kunde schließlich frei entscheiden kann, ob er seine Daten bekannt geben will. Als Verantwortlicher gilt die Raiffeisen Landesbank Steiermark AG. Das Rechenzentrum und ein externer Datenanalyst werden als Auftragsverarbeiter betrachtet.

Des Weiteren klärte der Workshop darüber auf, dass nur Kunden von der Verarbeitungstätigkeit betroffen sind. Zu den internen Empfängern zählen der Geschäftsbereich „Privat- und Geschäftskunden“ und das „Marketing“. Außerdem kam man zum Ergebnis, dass hinsichtlich der personenbezogenen Datenarten persönliche Detailangaben, Kontaktdaten, Daten zu Kreditgeschäft, Einlagengeschäft, Kassageschäft, Wertpapierverwahrung, Wertpapierverwaltung, Zahlungsverkehrs- und Clearing-Daten als auch Daten zu Marketing und Vertrieb verarbeitet werden.

Es soll auch nicht unerwähnt bleiben, dass die Verarbeitung von personenbezogenen Daten auf der Rechtsgrundlage „berechtigtes Interesse“ basiert. Im Rahmen des Brainstormings wurden keine Risiken eruiert. Mit Hilfe des Risikokatalogs im Risk-Assessment-Sheet konnte man vier Risiken wie das Risiko einer unbefugten Aufhebung der Pseudonymisierung, das Risiko einer Rufschädigung, das Risiko eines gesellschaftlichen Nachteils und das Risiko einer Verletzung der Privatsphäre identifizieren. Als Risikoquelle wurde für alle vier Risiken der Mitarbeiter genannt. Hinsichtlich der Risikoquellenart wurde somit menschlich, intern und vorsätzlich ausgewählt. Die Eintrittswahrscheinlichkeit des Risikos der unbefugten Aufhebung der Pseudonymisierung wurde als möglich und die Auswirkung als „sehr gering“ geschätzt, da dieses Risiko eine leichte Verärgerung zur Folge haben könnte. Das Risiko einer Rufschädigung wurde als „sehr unwahrscheinlich“ und die Auswirkung als „mittel“ klassifiziert. Das Risiko „Gesellschaftlicher Nachteil“ und „Verletzung der Privatsphäre“ wurden als „sehr unwahrscheinlich“ und die Auswirkung als „sehr gering“ beurteilt. Daher ergeben sich im

Rahmen dieser Verarbeitungstätigkeit nur geringe Risiken, die akzeptiert werden können und für welche keine weiteren Maßnahmen zu treffen sind.

5.2.3. Workshop für den Prozess „Revision durchführen“

Im Workshop „Revision durchführen“ wurden zunächst die Unterprozesse, für die eine DSFA bestimmt wurde systematisch beschreiben.

- Verarbeitungstätigkeit „Sonderauftrag durchführen“:

Zu Beginn erteilt der Vorstand einen Sonderauftrag bei der IRV-Leitung (Interne Revision & Konzernrevision). Anschließend beauftragt die Leitung den IRV-Prüfer, welcher in weiterer Folge Planungsüberlegungen durchführt. Er holt Informationen ein und stellt sie dem Revisionspartner zur Verfügung. Danach wird die Prüfung durchgeführt und nachvollziehbar dokumentiert. Der Prüfer, die IRV-Assistenz und die IRV-Leitung bearbeiten den Prüfungsbericht. Die IRV-Leitung erstellt im Anschluss den Prüfungsbericht. Zum Schluss wird der Prüfungsbericht von der IRV-Assistenz an den Vorstand übermittelt.

- Verarbeitungstätigkeit „Bericht an Vorstand durchführen“:

Bei dieser Verarbeitungstätigkeit startet die IRV-Leitung mit der Durchführung des Berichts an den Vorstand. Die IRV-Assistenz erstellt die benötigten Unterlagen und versendet diese an die IRV-Leitung. Nachfolgend erfolgt bei einer Besprechung die Durchführung des Berichts an den Vorstand.

- Verarbeitungstätigkeit „Quartalsreporting durchführen“ (Bericht § 42 Abs. 3 BWG):

Auch hier startet die IRV-Leitung den Prozess. Die IRV Assistenz erstellt und versendet den Quartalsbericht nach §42 Abs. 3 BWG an den Prüfungsausschuss, den Aufsichtsrat, das Vorstand- und Verbund-Head Office (VHO) der RLB und an das Vorstandsbüro der HYPO.
In weiterer Folge wird das Reporting schriftlich bzw. mündlich durchgeführt.

- Verarbeitungstätigkeit „Ad-hoc-Reporting durchführen“:

Die IRV-Leitung startet den Ad-hoc-Reporting-Prozess und führt das Reporting an den Vorstand durch.

- Verarbeitungstätigkeit „Erledigung überwachen“:

Dieser Prozess startet durch die IRV-Assistenz. Es wird eine Stellungnahme beim Revisionspartner eingeholt, der die Stellungnahme dem Prüfer weiterleitet. Der Prüfer bearbeitet diese und sendet sie an die IRV-Assistenz. In weiterer Folge führt die IRV-Assistenz eine Auswertung durch, während die IRV-Leitung die Stellungnahme überprüft.

Der Zweck der einzelnen Verarbeitungstätigkeiten ist die Durchführung der Revision. Die Verarbeitungsvorgänge wurden in Bezug auf den Zweck als sehr notwendig und verhältnismäßig eingestuft, da die Verarbeitung auf einer gesetzlichen Grundlage (BWG) durchgeführt werden muss. Als Verantwortlicher gelten die Raiffeisen-Landesbank Steiermark AG und die Landes-Hypothekenbank Steiermark AG. Hinsichtlich der betroffenen Personen kam man zum Ergebnis, dass Mitarbeiter, Angehörige von Mitarbeiter, Bewerber, Vertragspartner, von Bildbearbeitung betroffene Personen, potenzielle Kunden und Interessenten, Kunden, Sicherheitengeber, Eigentümer des Verantwortlichen, Organe und Funktionäre des Verantwortlichen, Besucher und sonstige Zutrittsberechtigte, Organe/Beschäftigte von Konzerngesellschaften betroffen sind. Zu den internen Empfängern zählen der Geschäftsbereich „Vertragsverwaltung“, der „Aufsichtsrat“, der Geschäftsbereich „Privat- und Geschäftskunden“, die „Innenrevision“, das „Personlmanagement“, das „Rechnungswesen & Controlling“, „Recht-/Geldwäsche- und Compliance“, „Risikomanagement“, „Treasury“ und der „Vorstand/Geschäftsführung“. Zu den externen Empfängern gehören die „Aufsichtsbehörden“, „IT-Dienstleister“, „externe Revision“, „Unternehmen des Raiffeisensektors“ und „Geschäftspartner vermittelter Produkte“.

Bezüglich der Datenarten werden alle möglichen Datenarten[212] der Raiffeisen-Landesbank Steiermark AG mit Ausnahme von elektronischen Standort- und Bewegungsdaten verarbeitet, welche auf der Rechtsgrundlage „Gesetzliche Verpflichtung“ basieren. Im Zuge des Brainstormings kam man zum Ergebnis, dass die größte Gefahr im Versenden eines E-Mails an einen falschen Empfänger besteht. Diese Gefahr wurde schließlich im Risikokatalog als das Risiko einer unbefugten Offenlegung von personenbezogenen Daten ausgewählt. Hierfür wurde der Mitarbeiter als Auslöser des Risikos bestimmt. Die Risikoquellenart wurde als menschlich, intern und unbeabsichtigt klassifiziert. Des Weiteren zeigte der Workshop, dass dieses Risiko einen Verlust der Vertraulichkeit zur Folge haben könnte, jedoch existiert für dieses Risiko nur ein geringes Risiko, da der Risikoeigner die Eintrittswahrscheinlichkeit als „sehr unwahrscheinlich“ und die Auswirkung als „sehr gering“ einstufte.

Das zweite Risiko, welches in dieser Verarbeitungstätigkeit identifiziert wurde, war das Risiko eines Verlustes von personenbezogenen Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können. Auch hier ist der Mitarbeiter der Hauptauslöser des Risikos, wodurch die Risikoquellenart als menschlich, intern und unbeabsichtigt eingeordnet wurde. Wesentliche Folgen des Risikos stellen die Kreditschädigung und die Veröffentlichung in Medien dar. Insgesamt wurde dieses Risiko als gering eingestuft, da die Eintrittswahrscheinlichkeit als „sehr unwahrscheinlich“ und die Auswirkung als „mittel“ beurteilt wurde.

[212] S. Kapitel 2.1. Definition und Analyse von Kernbegriffen, S. 8 ff.

5.2.4. Workshop für den Prozess „Verwaltung physischer Sicherheitssysteme“

Bei dem Prozess „Verwaltung physischer Sicherheitssysteme“ besteht zu Beginn dieser Verarbeitungstätigkeit ein Bedarf nach einer Zutrittsberechtigung aufgrund der Einstellung eines neuen Mitarbeiters. Deshalb muss zunächst eine Zutrittsberechtigung angefordert werden. In weiterer Folge wird die Handgeometrie des Mitarbeiters in ein Lesegerät eingelernt und in einer Datenbank gespeichert. Danach erfolgt die Erteilung der Berechtigung für den Zutritt. Nach der Freigabe der Berechtigung muss der Mitarbeiter bei jedem Zutritt einen PIN-Code eingeben und seine Hand auf das Lesegerät legen, um sich Zutritt zu den Gebäuden aller Standorte der RLB/HYPO Steiermark verschaffen zu können. Die Hand wird im System mit der gespeicherten Hand in der Datenbank abgeglichen. Der Zutritt wird nur dann gewährt, wenn die Hand mit der gespeicherten Hand ident ist.

Der Hauptzweck der Verarbeitungstätigkeit liegt in der Ermöglichung eines berechtigten Zutritts. Der weitere Zweck soll der Schutz von Daten, die Garantie der Verfügbarkeit, die Schaffung von Sicherheit sowie das Nachkommen gesetzlicher Verpflichtungen sein. Des Weiteren wird der Verarbeitungsvorgang in Bezug auf den Zweck als sehr notwendig und verhältnismäßig eingestuft, da dadurch Sicherheit geschaffen werden kann und somit nachvollzogen bzw. kontrolliert werden kann, wer die Räume betritt. Als Verantwortlicher gelten die Raiffeisen-Landesbank Steiermark AG und die Landes-Hypothekenbank Steiermark AG. In die Rolle des Auftragsverarbeiters tritt das Rechenzentrum.

Von der Verarbeitung der personenbezogenen Daten betroffen sind nur Mitarbeiter. Zu den personenbezogenen Datenarten zählen persönliche Detailangaben, Kontaktdaten und die besondere Kategorie von personenbezogenen Daten, da es sich in dieser Verarbeitungstätigkeit um biometrische Daten handelt. Die Verarbeitung der Daten erfolgt auf Basis der Rechtsgrundlage „berechtigtes Interesse“. Im Zuge des gemeinsamen Brainstormings stellte sich heraus, dass ein Risiko in der missbräuchlichen Speicherung von personenbezogenen Daten durch den Servicetechniker besteht. Für dieses Risiko wurde die Risikoquellenart als menschlich, extern und vorsätzlich eingeordnet. Als Auslöser des Risikos wurde der Servicetechniker bestimmt. Als Folge dieses Risikos wurde Rufschädigung und die Veröffentlichung von personenbezogenen Daten gewählt, wobei das Risiko nur als gering eingestuft wurde, das die Eintrittswahrscheinlichkeit „sehr unwahrscheinlich“ und die immaterielle Auswirkung „sehr gering“ beurteilt wurde. Dieses Risiko gilt als „sehr unwahrscheinlich“, da die Vertragsverhältnisse genau geklärt wurden, es eine Aufsichtsperson gibt und der Servicetechniker überwacht wird.

Die Folge „Veröffentlichung von personenbezogenen Daten“ des Risikos „Missbräuchliche Speicherung von personenbezogenen Daten durch den Servicetechniker“ steht in direktem

Zusammenhang mit dem nächsten identifizierten Risiko. Denn, wenn personenbezogene Daten missbräuchlich gespeichert werden, existiert auch das Risiko, dass personenbezogene Daten unbefugt offengelegt werden. Der Hauptauslöser dieses Risikos könnte wieder der Servicetechniker sein, daher wurde die Risikoquellenart als menschlich, extern und vorsätzlich eingestuft. Als Folge der unbefugten Offenlegung wurde Rufschädigung genannt. Im Großen und Ganzen besteht auch hierbei nur ein geringes Risiko, da die Eintrittswahrscheinlichkeit als „sehr unwahrscheinlich“ und die immaterielle Auswirkung als „sehr gering“ klassifiziert wurde.

5.2.5. Workshop für den Prozess „Finanzierung durchführen“

Da die systematische Beschreibung der Verarbeitungstätigkeiten für den Prozess „Finanzierung durchführen“ sehr umfangreich sind, kann diese aus dem Anhang entnommen werden. Der Zweck der Verarbeitungstätigkeiten liegt in der Erfüllung eines Vertrages, wobei diese auch aufgrund einer gesetzlichen Verpflichtung (BWG) durchgeführt werden muss. Der Verarbeitungsvorgang wurde in Bezug auf den Zweck als sehr notwendig und verhältnismäßig eingestuft, da die Verarbeitung der personenbezogenen Daten zur Durchführung des Geschäfts notwendig ist und somit der gesetzlichen Verpflichtung nachgekommen werden kann. Als Verantwortlicher im Sinne der DSGVO gilt die Raiffeisen-Landesbank Steiermark AG. Von den einzelnen Verarbeitungstätigkeiten betroffen sind Personen wie Vertragspartner, potenzielle Kunden und Interessenten, Kunden, Sicherheitengeber, Eigentümer des Verantwortlichen, Organe und Funktionäre des Verantwortlichen sowie Organe und Beschäftigte von Konzerngesellschaften.

Zu den internen Empfängern gehören der Geschäftsbereich „Vertragsverwaltung“, der „Aufsichtsrat“, der Geschäftsbereich „Privat- und Geschäftskunden“, „Recht-/Geldwäsche und Compliance“, „Risikomanagement“, „Treasury“ sowie „Vorstand/Geschäftsführung“. Ansonsten werden die Daten an externe Empfänger wie „Kredit- und Finanzinstitute“, „Anwälte“, „Notare“, „Gerichte“, „Staatsanwaltschaften“, „IT-Dienstleister“, „Unternehmen des Raiffeisensektors“, „Versicherungen“, „Bonitätsdatenbanken“, „Geschäftspartner vermittelter Produkte“, „gesetzliche Vertreter oder Bevollmächtigte oder Begünstigten aus Garantien“ übermittelt. Zudem wurden alle möglichen personenbezogenen Datenarten[213] ausgewählt mit Ausnahme von Daten zu Lebenslauf und Mitarbeiterqualifikation, Arbeitsorganisationsdaten, elektronische Standort und Bewegungsdaten, Daten zu Fuhrparkmanagementgeschäft, die besondere Kategorie von personenbezogenen Daten sowie strafrechtliche Verurteilungen und Straftaten. Des Weiteren beruht die Verarbeitung auf Basis der Rechtsgrundlage „Vertragserfüllung“, „Gesetzliche Verpflichtung“ als auch „berechtigtes Interesse“.

[213] S. Kapitel 2.1. Definition und Analyse von Kernbegriffen, S. 8 ff.

Im Rahmen des Brainstormings kam man zum Ergebnis, dass Risiken wie Kreditschädigung, Diskriminierung oder Rufschädigung existieren. Nach der kritischen Betrachtung des Risikokatalogs stellten sich vier Risiken heraus. Das erste Risiko besteht im Verlust von personenbezogenen Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können. Der Mitarbeiter wird dabei als Auslöser des Risikos betrachtet. Die Risikoquellenart wird daher als menschlich, intern, unbeabsichtigt oder vorsätzlich eingestuft. Eine Folge im Verlorengehen von personenbezogenen Daten liegt im Verlust der Vertraulichkeit und in der Veröffentlichung der Daten. Insgesamt ergibt sich ein geringes Risiko, da die Eintrittswahrscheinlichkeit „sehr unwahrscheinlich“ und die immaterielle Auswirkung „sehr gering“ beträgt. Der Grund für diese Beurteilung liegt darin, dass dem Risikoeigner kein entsprechender Fall bekannt war und Vorsorge durch entsprechende Dienstanweisungen und der Sorgfaltspflicht getroffen wird.

Als zweites Risiko wurde die unbefugte Offenlegung von personenbezogenen Daten identifiziert, welches unmittelbar mit dem ersten Risiko zusammenhängt. Auch hierfür gilt der Mitarbeiter als Auslöser des Risikos und die Risikoquellenart wurde als menschlich, intern, und unbeabsichtigt klassifiziert. Als Folge wurde wieder der Verlust der Vertraulichkeit bekannt gegeben. Hinsichtlich der Risikobeurteilung stellte sich heraus, dass das Risiko in die geringe Risikoklasse einzustufen ist, da die Eintrittswahrscheinlichkeit zwar als „möglich“, jedoch die immaterielle Auswirkung als „sehr gering“ geschätzt wurde. Der Grund für die mögliche Einstufung liegt darin, dass das Risiko aufgrund von Unachtsamkeit eintreten kann. Als Begründung für die geringe Auswirkung wurde genannt, dass kritische Daten beispielsweise nicht per E-Mail versendet werden und sorgfältig behandelt werden. Außerdem werden keine Daten der besonderen Kategorie von personenbezogenen Daten verarbeitet, wodurch es bei einer Offenlegung der Daten nur zu einer geringen Auswirkung kommen könnte.

Das dritte ermittelte Risiko besteht in der missbräuchlichen Verwendung von Kundendaten durch den Mitarbeiter. Daher wurde auch die Risikoquellenart als menschlich, intern und vorsätzlich eingeordnet. Bei Eintritt dieses Risikos könnte dies eine Rufschädigung oder Diskriminierung zur Folge haben. Im Ganzen besteht nur ein geringes Risiko aufgrund der Beurteilung des Risikos als „sehr unwahrscheinlich“ und „mittel“. Der Eintritt wird als sehr unwahrscheinlich betrachtet, da die Mitarbeiter grundsätzlich den Verhaltenskodex einhalten.

Das vierte Risiko existiert in der Veröffentlichung von personenbezogenen Daten, welches durch den Mitarbeiter vorsätzlich ausgelöst werden könnte. Dieses Risiko könnte einerseits Eine Rufschädigung, eine Diskriminierung oder eine Kreditschädigung mit sich bringen. Bei diesem Risiko kam man zum Ergebnis, dass es in die geringe Risikoklasse einzustufen ist, da der Eintritt „sehr unwahrscheinlich“ und die immaterielle sowie materielle Auswirkung als „mittel“ zu klassifizieren ist.

5.2.6. Workshop für den Prozess „Maklergeschäft durchführen“

Die Verarbeitungstätigkeit „Maklergeschäft durchführen“ beginnt mit dem Versicherungsbedarf (Sachversicherung) des Kunden. Aus diesem Grund wird ein Termin zwischen der Raiffeisenbank und dem Kunden koordiniert. In weiterer Folge führt der Regionalbetreuer ein Beratungsgespräch mit dem Kunden durch. Es wird der Versicherungsbedarf näher spezifiziert und Anbote bei der Abteilung „Versicherung & Bausparen“ angefordert. Diese Abteilung kontaktiert die Versicherung, um ein Angebot zu erlangen. Die Abteilung „Versicherung & Bausparen“ speichert die Angebote und leitet diese an den Regionalbetreuer weiter, welcher schließlich ein Bestangebot für den Kunden ermittelt und an diesen weiterleitet. Das Angebot wird schließlich vom Kunden angenommen, wenn es für diesen in Ordnung ist und übermittelt es an die Abteilung „Versicherung & Bausparen“. Wenn das Anbot per Mail einlangt, wird der RVS-Maklerei-Briefkasten bearbeitet. Falls das Anbot papierhaft übermittelt wird, wird der Antrag gescannt. In weiterer Folge erfolgt eine Prüfung des Antrags. Falls es einen Fehler gibt, wird der Antrag zurückgesendet und eine Korrektur angefordert. Ansonsten wird der Antrag erfasst, der Briefkasten auf erledigt gesetzt, der gescannte Antrag gelöscht, der Antrag polizziert und an die Abteilung „Versicherung & Bausparen“ gesendet. Dort wird der Antrag erfasst, geprüft und an den Kunden gesendet.

Der Zweck dieser Verarbeitungstätigkeit liegt in der Anbahnung und der Vermittlung eines Versicherungsgeschäftes. Der Verarbeitungsvorgang wurde in Bezug auf den Zweck als sehr notwendig und verhältnismäßig eingestuft. Als Verantwortlicher gelten wieder die Raiffeisen-Landesbank Steiermark AG sowie die Landes-Hypothekenbank Steiermark AG. Zudem tritt die Versicherung als Auftragsverarbeiter auf. Von der Verarbeitung der personenbezogenen Daten betroffen sind Mitarbeiter, Angehörige von Mitarbeitern, Vertragspartner, von der Bildverarbeitung betroffene Personen, potenzielle Kunden und Interessenten, Kunden, Eigentümer des Verantwortlichen, Organe und Funktionäre des Verantwortlichen sowie Organe und Beschäftigte von Konzerngesellschaften. Des Weiteren werden die Daten an interne Empfänger wie dem „Personalmanagement“, „Rechnungswesen & Controlling“ und dem „Vorstand/Geschäftsführung“ übermittelt. Ansonsten erfolgt eine Weitergabe der Daten an „IT-Dienstleister“, „Unternehmen des Raiffeisensektors“, „Versicherungen und Geschäftspartner vermittelter Produkte“.

Hinsichtlich der Datenarten werden im Rahmen der Verarbeitungstätigkeit persönliche Detailangaben, Daten zu Identitäts- und Reisedokumenten, Kontaktdaten, Daten zu Beruf und Arbeitsverhältnis, Lohn- und Gehaltsdaten, steuerliche Daten und Sozialversicherungsdaten, Arbeitsorganisationsdaten, Beteiligungen, Vertretungsbefugnisse, Lebens- und Konsumgewohnheiten, Bild-/ und oder Tonaufzeichnungen, Bonitätsdaten, Finanzidentifikationsdaten, Daten zu Kreditgeschäft, Versicherungsdaten, Zahlungsverkehrs-

und Clearing-Daten, Daten zu Fuhrparkmanagementgeschäft, Bauträgergeschäft, Vermittlungsgeschäft, Marketing und Vertrieb, Safes und Schließfächern und die besondere Kategorie von personenbezogenen Daten wie die Sozialversicherungsnummer verarbeitet.

Die Verarbeitung basiert auf der Grundlage der gesetzlichen Verpflichtung und der Vertragserfüllung. Im Zuge des gemeinsamen Brainstormings konnten keine Risiken festgestellt werden. Erst durch die Begutachtung des Risikokatalogs konnte das Risiko einer missbräuchlichen Verwendung von Kundendaten eruiert werden. Wie es bei den meisten Risiken bisher der Fall ist, gilt auch hier der Mitarbeiter als Hauptauslöser des Risikos, wobei es sich hierbei um eine vorsätzliche Tat handeln würde. Als Folge wurde der Verlust der Vertraulichkeit im Tool erfasst. Zudem handelt es sich um ein geringes Risiko mit einer Eintrittswahrscheinlichkeit von „sehr unwahrscheinlich“ und einer immateriellen Auswirkung von „gering“.

5.2.7. Workshop mit dem IT-Experten der Raiffeisen-Landesbank Steiermark AG

Da die Risikoeigner der einzelnen Verarbeitungstätigkeiten gewisse Risiken wie beispielsweise das Risiko eines unbefugten Zutritts zu personenbezogenen Daten durch einen Hacker oder die Möglichkeit des Risikos der Veränderung von personenbezogenen Daten im System nicht beurteilen konnten, wurde ein eigener Workshop mit dem IT-Experten der Raiffeisen-Landesbank Steiermark AG durchgeführt. Mit Hilfe des Risk-Assessment-Sheets wurden wesentliche Risiken identifiziert, beurteilt und gesteuert. In weiterer Folge wird auf diese Risiken näher eingegangen.

Als Erstes wurde die Vernichtung von physischen und elektronischen Daten als Risiko, welches durch den Mitarbeiter oder einen Hacker vorsätzlich ausgelöst werden kann, genannt. Als mögliche Folgen wurden Diskriminierung, Identitätsdiebstahl, Rufschädigung und Verletzung der Privatsphäre angeführt. Beurteilt wurde dieses Risiko insgesamt als „mittel“, da der Eintritt „wahrscheinlich“ und die immaterielle sowie materielle Auswirkung als „mittel“ geschätzt wurde.

Als zweites Risiko wurde der Verlust von personenbezogenen Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können, ausgewählt. Die Risikoquelle und die Folgen wurden gleich wie beim vorigen Risiko angegeben. Die Risikobeurteilung vor Maßnahmen ergibt ein mittleres Risiko mit einer Eintrittswahrscheinlichkeit von „wahrscheinlich“ und einer immateriellen sowie materiellen Auswirkung von „mittel“.

Als drittes Risiko wurde die unbefugte Offenlegung von personenbezogenen Daten als Risiko vermerkt, welches durch den Mitarbeiter vorsätzlich verursacht werden kann. Als mögliche Folgen wurden die gleichen wie bei den bisher erwähnten Risiken eruiert. An dieser Stelle ist anzumerken, dass es sich ebenso um ein mittleres Risiko handelt.

Außerdem wurde der unbefugte Zugang zu personenbezogenen Daten als Risiko bestimmt. Als Auslöser des Risikos wird entweder intern, daher der Mitarbeiter, oder extern, der Hacker, mit einer vorsätzlichen Tat betrachtet. Folglich könnte dieses Risiko einen Identitätsdiebstahl, die Verletzung der Privatsphäre, eine Kreditschädigung oder eine sonstige betrügerische Verwendung mit sich bringen. Insgesamt besteht diesbezüglich ein mittleres Risiko.

Zuallerletzt stellt auch die Veränderung von personenbezogenen Daten ein Risiko dar, welches wieder durch den internen Mitarbeiter vorsätzlich bewirkt werden könnte. Der Eintritt dieses Risikos könnte den Verlust der Vertraulichkeit herbeiführen. Eingestuft wird dieses Risiko in der Risikoklasse „mittel“.

5.3. TOP-5-Risiken in der Raiffeisen-Landesbank Steiermark AG

Die nachfolgende Abbildung zeigt eine Übersicht über die TOP 5 Bruttorisiken, welche in den Workshops identifiziert wurden und auf den Risiken mit dem höchsten Erwartungswert basieren. Wie die Risikomatrix zeigt, zählen die Risiken „Vernichtung von personenbezogenen Daten“, der „Verlust von personenbezogenen Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können“, die „unbefugte Offenlegung von personenbezogenen Daten“, der „unbefugte Zugang zu personenbezogenen Daten“ sowie die „Veränderung von personenbezogenen Daten“ zu den TOP-5-Risiken.

Top 5 Bruttorisiken (Risiken vor Maßnahmen)					
Nummer	Risiko	Folge	Eintrittswahrscheinlichkeit	Auswirkung	Erwartungswert
1	**Vernichtung von personenbezogenen Daten**	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	4	3	12
2	**Verlust von personenbezogenen Daten**	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	4	3	12
3	**Unbefugte Offenlegung von personenbezogenen Daten**	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	3	4	12
4	**Unbefugter Zugang zu personenbezogenen Daten**	Identitätsdiebstahl Verletzung der Privatsphäre Kreditschädigung betrügerische Verwendung	2	3	6
5	**Veränderung von personenbezogenen Daten**	Verlust der Vertraulichkeit	2	5	10

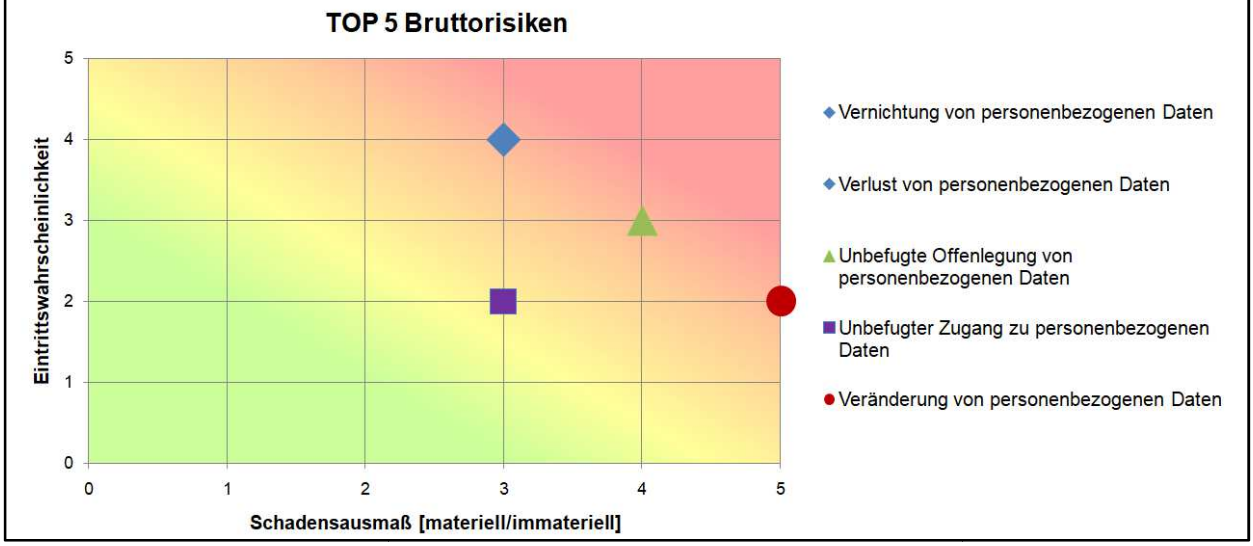


Abbildung 18: TOP-5-Bruttorisiken,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

Die nächste Abbildung zeigt die TOP-5-Nettorisiken, welche die Risiken nach den Maßnahmen darstellen. Um den Risiken der Vernichtung und dem Verlust von personenbezogenen Daten entgegenzuwirken soll in Zukunft verstärkt darauf geachtet werden, dass Verfügbarkeitskontrollen durchgeführt werden. Dabei schützt man sich gegen eine zufällige oder mutwillige Zerstörung bzw. dem Verlust. Beispiele dafür wären eine Backup-Strategie, eine unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, Meldewege und Notfallpläne, ein mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei einem Wechsel oder Ausscheiden von Mitarbeitern. Auch auf eine rasche Wiederherstellbarkeit soll geachtet werden. Dadurch ist gewährleistet, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Im Hinblick auf die Risiken der Offenlegung und dem unbefugten Zugang zu personenbezogenen Daten sollen in Zukunft Zutritts-, Zugangs-, und Zugriffskontrollen beachtet werden. Zutrittskontrollen dienen zum Schutz vor einem unbefugten Zutritt zu Datenverarbeitungsanlagen. Beispiele für diese Maßnahme wären Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Alarmanlagen und Videoanlagen. Zugangskontrollen sollen vor einer unbefugten Systembenutzung schützen, beispielsweise durch sichere Kennwörter, automatische Sperrmechanismen und der Verschlüsselung von Datenträgern. Zugriffskontrollen hingegen ermöglichen kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb eines Systems, beispielsweise durch einen Standardprozess für eine Berechtigungsvergabe, Protokollierung von Zugriffen, eine periodische Überprüfung der vergebenen Berechtigungen.

Das Risiko der Veränderung von personenbezogenen Daten soll mit Weitergabe-, und Eingabekontrollen reduziert werden. Bei Weitergabekontrollen wird kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport ermöglicht. Beispiele dafür wären eine Verschlüsselung, die Verwendung von Virtual Private Networks (VPN) oder eine elektronische Signatur. Mit Hilfe von Eingabekontrollen, kann festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, beispielsweise durch Protokollierung und dem Dokumentenmanagement. Des Weiteren dienen für alle TOP-5-Risiken die Einschränkung der Datenkategorien als auch regelmäßige Mitarbeiterschulungen als weitere Maßnahmen zur Risikoreduktion. In der nachfolgenden Abbildung auf der nächsten Seite werden die TOP-5-Nettorisiken dargestellt.

Top 5 Nettorisiken (Risiken nach Maßnahmen)					
Nummer	Risiko	Folge	Eintrittswahrscheinlichkeit	Auswirkung	Erwartungswert
1	**Vernichtung von personenbezogenen Daten**	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	2	3	6
2	**Verlust von personenbezogenen Daten**	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	2	3	6
3	**Unbefugte Offenlegung von personenbezogenen Daten**	Diskriminierung Identitätsdiebstahl Rufschädigung Verletzung der Privatsphäre	2	4	8
4	**Unbefugter Zugang zu personenbezogenen Daten**	Identitätsdiebstahl Verletzung der Privatsphäre Kreditschädigung betrügerische Verwendung	1	3	3
5	**Veränderung von personenbezogenen Daten**	Verlust der Vertraulichkeit	2	4	8

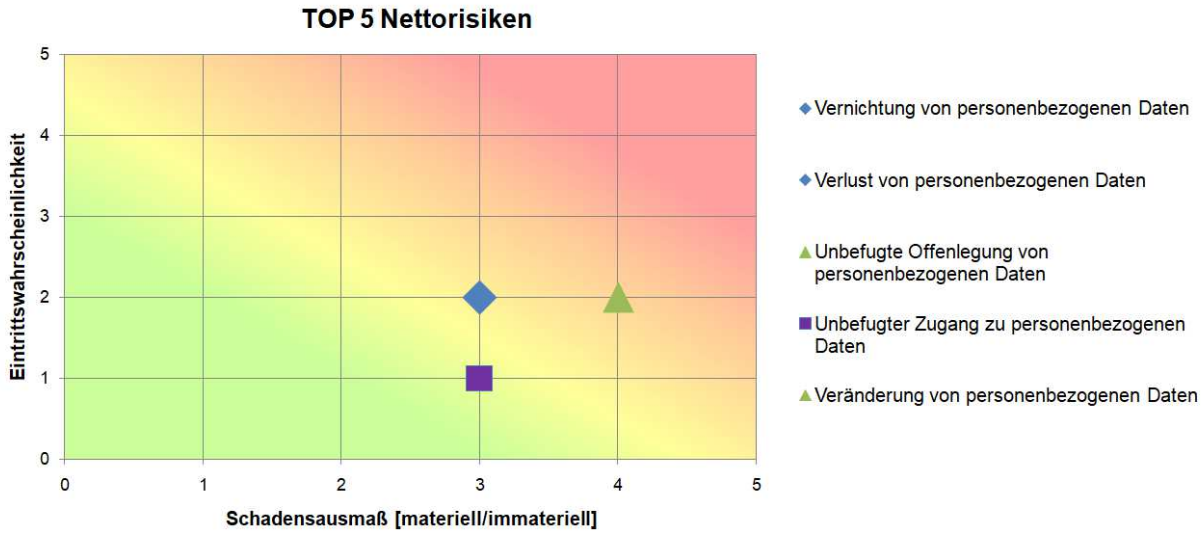


Abbildung 19: TOP-5-Nettorisiken,
Quelle: eigene Darstellung, Excel-Datei DSFA_RLB_Stmk_04_2019.xlsx.

6. Resümee

Das letzte Kapitel der vorliegenden Arbeit gliedert sich in zwei Unterkapitel. Im ersten Unterkapitel erfolgt eine fundierte Zusammenfassung der wesentlichen Ergebnisse dieser Arbeit. Des Weiteren werden die zu Beginn der Arbeit aufgeworfenen Forschungsfragen beantwortet. Das zweite Unterkapitel befasst sich schließlich mit einem Ausblick und einer kritischen Reflexion der Ergebnisse.

6.1. Zusammenfassung

Das Ziel der Arbeit war, ein Tool zur Durchführung einer DSFA für die Raiffeisen-Landesbank Steiermark AG zu konzipieren, um diese Bank hinsichtlich DSGVO-Konformität zu unterstützen. Ein weiteres Ziel bestand auch in der Durchführung der einzelnen DSFAs und der Identifikation der TOP-5-Datenschutz- und Datensicherheitsrisiken.

Um diese Ziele der Arbeit erreichen zu können, befasste sich die Verfasserin im Rahmen des zweiten Kapitels näher mit der DSGVO, da aufgrund dieser eine DSFA durchzuführen war. Im Rahmen dieses Kapitels wurden relevante Begriffe und deren Anwendung auf den Kooperationspartner definiert und analysiert. Auch die Grundsätze der DSGVO fanden Erwähnung, da diese das Fundament des Datenschutz-Risikomanagements und des zu konzipierenden Tools für die Raiffeisen-Landesbank Steiermark AG bilden. Darüber hinaus wurden die zu schützenden Betroffenenrechte betrachtet, da es im Zuge des Datenschutz-Risikomanagements die Risiken für die Rechte und Freiheiten der betroffenen Personen zu berücksichtigen galt.

Das zweite Kapitel beschäftigte sich mit der Vorgehensweise bei DSFAs. Dabei kam man zum Ergebnis, dass sich die Vorgehensweise in vier Phasen untergliedern lässt. Die erste Phase wird in der Literatur als Vorbereitungsphase bezeichnet. In dieser Phase erfolgt hauptsächlich die Prüfung der Notwendigkeit einer DSFA. Die zweite Phase stellt die Bewertungsphase dar. In dieser Phase werden eine Risikoidentifikation und eine Risikobewertung vorgenommen. Im Rahmen der dritten Phase werden passende Maßnahmen identifiziert. Der Fokus der letzten Phase, der sogenannten Berichtsphase, liegt auf der Erstellung eines DSFA-Berichts.

Das dritte Kapitel befasste sich mit dem Schwerpunkt der DSFA, dem Datenschutz-Risikomanagement. Dabei wurde näher auf den Risikomanagementprozess eingegangen, welcher aus den vier Schritten Risikoidentifikation, Risikobewertung, Risikosteuerung, Risikoüberwachung inklusive Risikoberichterstattung besteht. Es wurde aufgezeigt, wie die Risiken in einer Bank kategorisiert werden können. Zudem wurde auf mögliche Risikoquellen, Datenschutz- und Datensicherheitsrisiken und potenzielle Folgen der Risiken eingegangen. Im

Rahmen der Risikobewertung setzte sich die Verfasserin mit den Anforderungen der Bewertung, den möglichen Bewertungskategorien und der Risikomatrix auseinander. In weiterer Folge wurden im Zuge der Risikosteuerung mögliche Risikostrategien beschrieben. Am Ende des Kapitels wurden die Risikoüberwachung und das Risikoreporting näher erläutert.

Das vierte Kapitel beschrieb, wie das Tool zur Durchführung von DSFAs konzipiert wurde. Hierbei ist zu erwähnen, dass sich das Tool in fünf Bereiche gliedern lässt. Im ersten Teil des Tools findet man ein Prüfschema, mit dem die einzelnen Prozesse der Raiffeisen-Landesbank geprüft werden können, ob eine DSFA durchzuführen ist. Die Literaturrecherche ergab, dass es drei verpflichtende Kriterien gibt, bei denen eine DSFA durchzuführen ist. Zum einen ist dies dann der Fall, wenn eine systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen durchgeführt wird, die als Grundlage für Entscheidungen dienen. Auch ist eine DSFA verpflichtend vorzunehmen, wenn personenbezogene Daten der besonderen Kategorie oder Daten zu strafrechtlichen Verurteilungen umfangreich verarbeitet werden. Zum dritten Kriterium zählt die systematische, umfangreiche Überwachung öffentlich zugänglicher Bereiche. Es gibt ebenso noch 9 andere Kriterien, bei denen zumindest zwei Kriterien zutreffen müssen, damit eine DSFA durchgeführt werden muss. Außerdem gibt es eine Blacklist und eine Whitelist. Die Blacklist bestimmt Verarbeitungstätigkeiten für die zwingend eine DSFA durchzuführen ist, wobei die Whitelist Verarbeitungstätigkeit von der Durchführung einer DSFA befreit. In der Arbeit wurden jedoch noch andere Ausnahmen beschrieben.

Der zweite Teil des Tools befasst sich mit grundsätzlichen Fragen zur DSFA, die vom Anwender des Tools zu beantworten sind. Der dritte Teil des Tools beschäftigt sich mit dem Schwerpunkt der DSFA, deshalb wurde ein Risk-Assessment-Sheet in das Tool integriert. Dieses Sheet dient zur Umsetzung des Risikomanagementprozesses und beinhaltet einen Risikokatalog. Dabei erfolgt eine Kategorisierung der Einzelrisiken nach DSGVO-Grundsätzen, welche als Schutzziel ins Tool integriert wurden. Die Risikogruppen werden dabei in das Schutzziel Verfügbarkeit, Vertraulichkeit, Rechtmäßigkeit und Integrität untergliedert.
Im Rahmen des vierten Bereiches des Tools werden in jeweils eigenen Arbeitsblättern die Bruttorisiken, die TOP-5-Bruttorisiken, die Nettorisiken sowie die TOP-5-Nettorisiken dargestellt. Der letzte Bereich des Tools dient zur Erstellung eines DSFA-Berichts.

Um im Tool den Risikomanagementprozess so gut wie möglich umzusetzen, befinden sich im Tool eigene Arbeitsblätter, in denen sich mögliche Risikoquellen, die Kriterien für die Eintrittswahrscheinlichkeit und die Auswirkung, und der optimierte Maßnahmenkatalog befinden. Bei den Risikoquellen wurde zwischen menschlichen und nichtmenschlichen unterschieden. Für die Kriterien zur Eintrittswahrscheinlichkeit und die materielle und immaterielle Auswirkung wurde eine fünfstufige Skala festgelegt. Die Verfasserin dieser Arbeit wollte eine vierstufige Skala für die Raiffeisen-Landesbank Steiermark AG umsetzen, jedoch

stellte sich nach Absprache mit dem Datenschutzbeauftragten heraus, dass diese Möglichkeit nicht bestand, da das Computersystem die Änderung auf eine vierstufige Skala nicht zuließ. An dieser Stelle muss betont werden, dass eine vierstufige Skala mehr Vorteile gehabt hätte, denn bei einer fünfstufigen Skala wird der Risikoeigner eher dazu tendieren, die Auswahl in der Mitte zu treffen. Eine vierstufige Skala hingegen zwingt den Risikoeigner zur Entscheidung zu einer Seite, was bei einer fünfstufigen Skala nicht der Fall ist.

Auch der Maßnahmenkatalog wurde optimiert, indem Maßnahmen zur Risikovermeidung und weitere Risikominderungsmaßnahmen definiert wurden. Beispielsweise kann ein Risiko vermieden werden, indem personenbezogene Daten erst gar nicht erhoben werden oder man die Verarbeitungstätigkeit aufgrund des hohen Risikos einstellt. Die Maßnahmen der Risikominderung wurden um den Aspekt der Rechtmäßigkeit erweitert. Dazu zählen Maßnahmen wie die Einschränkung der Datenkategorien, Einschränkung des Datenumfangs, Einschränkung der Kategorien von Betroffenen, die Einschränkung der Anzahl von Betroffenen, die Einschränkung der Verarbeitungszwecke, die Einschränkung des Kreises der Zugangsberechtigten, die Einschränkung der Übermittlungsempfänger und die Einschränkung der Speicherdauer.

Im Zuge des vierten Kapitels wurde die Durchführung der DSFAs beschrieben. Dabei wurde aufgezeigt, für welche Geschäftsprozesse, in denen personenbezogene Daten verarbeitet werden, eine DSFA vorzunehmen ist. Die Verfasserin dieser Arbeit kam zum Ergebnis, dass für folgende sechs Prozesse eine DSFA durchzuführen ist, da bei den meisten Prozessen unter anderem das Kriterium „umfangreiche Verarbeitung der besonderen Kategorie personenbezogener Daten“ erfüllt ist:

- „Lebenspuzzle durchführen“
- „Kundenabwanderung vorbeugen und bearbeiten“
- „Revision durchführen“
- „Verwaltung physischer Sicherheitssysteme“
- „Finanzierung durchführen“
- „Maklergeschäft durchführen“

Mit Hilfe des konzipierten Tools wurden die einzelnen Workshops durchgeführt. In diesen Workshops hatte der Risikoeigner geschlossene als auch offene Fragen zu beantworten. Die Identifikation der Risiken erfolgte mithilfe der Brainstorming-Methode und einem im Voraus erstellten Risikokatalog. Die Verfasserin entschied sich für einen Risikokatalog, da zu den Vorteilen dieser Methode die einfache Handhabung, die individuelle Gestaltungsmöglichkeit und die Ermöglichung einer systematischen Vorgehensweise zählen. Außerdem ermöglichen Checklisten eine eindeutige Aufgabenzuordnung an Risikoverantwortliche, die Gestaltung eines

standardisierten Berichtssystems speziell für Risiken als auch eine Einbindung des Risikomanagements in existierende Planungs- und Berichtssysteme. Ein weiterer Vorteil standardisierter Fragenkataloge stellt die universelle Anwendbarkeit dar.

Die Brainstorming-Methode wurde gewählt, da dadurch die Kreativität der Beteiligten gefördert wird. Damit keine bedeutenden Risiken übersehen werden können, wurden für die Risikoidentifikation mehrere Methoden ausgewählt. Außerdem empfiehlt der Autor GLEIßNER die Methode des Risikokatalogs nicht als alleinige Methode anzuwenden, sondern diese mit anderen Methoden zu kombinieren, um nicht überbordende und unstrukturierte Risikolisten zu erhalten.

Für die Umsetzung des Risikomanagementprozesses im Tool wurde auch das Risk-Assessment-Sheet ausgewählt, da der Vorteil dieses Sheets die strukturierte Vorgehensweise darstellt. Ein Risikokatalog bietet eine abgeschlossene Auswahl an Lösungsmöglichkeiten, wobei Risk-Assessment-Sheets eine Kombination von offenen als auch geschlossenen Fragen darstellen. Ein großer Vorteil dieses Instruments ist, dass eine gewisse Mindeststruktur zur näheren Beschreibung des Risikos gegeben ist und die zu befragenden Personen nicht in der Nennung von Risiken eingeschränkt sind.

Des Weiteren wurden in den Workshops Szenarien erarbeitet. Beispielsweise wurden die Risikoquellen und die Folgen der identifizierten Risiken bestimmt. In weiterer Folge wurde eine Risikobeurteilung vor und nach definierten Maßnahmen durchgeführt. Bei den sechs Prozessen für die eine DSFA durchzuführen war, kam man durch die Workshops zum Ergebnis, dass nur geringe Risiken existieren für die keine weiteren Maßnahmen zu treffen sind. Da die Risikoeigner jedoch gewisse Risiken wie beispielsweise das Risiko eines unbefugten Zutritts zu personenbezogenen Daten durch einen Hacker oder das Risiko der Veränderung von personenbezogenen Daten im System nicht beurteilen konnten, wurde ein weiterer Workshop mit dem IT-Experten der Raiffeisen-Landesbank Steiermark AG durchgeführt. Dabei kam man zum Ergebnis, dass auch mittlere Risiken existieren.

Zu guter Letzt zeigte das fünfte Kapitel dieser Arbeit die TOP-5-Risiken, welche in der Risikoklasse „mittel“ einzustufen sind, auf. Die Risikopriorisierung ergab, dass zu den TOP-3-Risiken die Vernichtung von personenbezogenen Daten, der Verlust von personenbezogenen Daten, die möglicherweise von Dritten zur Kenntnis genommen werden können und die unbefugte Offenlegung von personenbezogenen Daten zählen. Alle 3 Risiken hätten bei Eintritt des Risikos entweder eine Diskriminierung, einen Identitätsdiebstahl, eine Rufschädigung oder eine Verletzung der Privatsphäre zur Folge. Zum TOP 4 Risiko wurde der unbefugte Zugang zu personenbezogenen Daten ermittelt. Dabei kann der Eintritt dieses Risikos einen Identitätsdiebstahl, eine Verletzung der Privatsphäre, eine Kreditschädigung als auch eine

betrügerische Verwendung zur Folge haben. Als TOP 5 Risiko wurde die Veränderung von personenbezogenen Daten identifiziert, welche einen Verlust der Vertraulichkeit der betroffenen Person mit sich bringen kann.

Um den Risiken der Vernichtung und dem Verlust von personenbezogenen Daten entgegenzuwirken wird in Zukunft verstärkt darauf geachtet, dass Verfügbarkeitskontrollen durchgeführt werden. Dabei schützt man sich gegen eine zufällige oder mutwillige Zerstörung bzw. den Verlust. Beispiele dafür wären eine Backup-Strategie, eine unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, Meldewege und Notfallpläne, mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum, Standardprozesse bei einem Wechsel oder Ausscheiden von Mitarbeitern. Auch auf eine rasche Wiederherstellbarkeit soll geachtet werden. Dadurch ist gewährleistet, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

Im Hinblick auf die Risiken der Offenlegung und dem unbefugten Zugang zu personenbezogenen Daten sollen in Zukunft Zutritts-, Zugangs-, und Zugriffskontrollen beachtet werden. Zutrittskontrollen dienen zum Schutz vor einem unbefugten Zutritt zu Datenverarbeitungsanlagen. Beispiele für diese Maßnahme wären Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Alarmanlagen und Videoanlagen. Zugangskontrollen sollen vor einer unbefugten Systembenutzung schützen, beispielsweise durch sichere Kennwörter, automatische Sperrmechanismen und der Verschlüsselung von Datenträgern. Zugriffskontrollen hingegen ermöglichen kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb eines Systems, beispielsweise durch einen Standardprozess für eine Berechtigungsvergabe, Protokollierung von Zugriffen, eine periodische Überprüfung der vergebenen Berechtigungen.

Das Risiko der Veränderung von personenbezogenen Daten soll mit Weitergabe-, und Eingabekontrollen reduziert werden. Bei Weitergabekontrollen wird kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport ermöglicht. Beispiele dafür wären eine Verschlüsselung, die Verwendung von Virtual Private Networks (VPN) oder eine elektronische Signatur. Mit Hilfe von Eingabekontrollen, kann festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, beispielsweise durch Protokollierung und dem Dokumentenmanagement. Des Weiteren dienen für alle TOP-5-Risiken die Einschränkung der Datenkategorien als auch regelmäßige Mitarbeiterschulungen als weitere Maßnahmen zur Risikoreduktion. Trotz dem Treffen von Maßnahmen verbleiben die TOP-5-Risiken in der Risikoklasse „mittel“.

6.2. Kritische Reflexion und Ausblick

Im Großen und Ganzen konnte der Praxisoutput mit Hilfe der verwendeten Literatur gut umgesetzt werden. Kritisch anzumerken ist aber, dass die Kriterien der DSGVO zur Überprüfung, ob eine DSFA durchzuführen ist, sehr vage in der DSGVO formuliert sind. Dadurch ergibt sich ein weiter Ermessensspielraum bei der Prüfung, ob für den jeweiligen Prozess, in dem personenbezogene Daten verarbeitet werden, eine DSFA durchzuführen ist oder auch nicht. Diesbezüglich sollte man darüber informiert bleiben, ob diese Kriterien noch konkretisiert werden. Falls in Zukunft weitere datenschutzrechtliche Änderungen erfolgen sollten, gilt es dabei herauszufinden, wie das Datenschutz-Risikomanagement an diese Veränderungen optimal angepasst werden kann.

Des Weiteren stellt die neue Regelung des Art. 35 DSGVO zwar einen bürokratischen Aufwand dar, jedoch kann die DSGVO zukünftig als Chance gesehen werden. Denn durch die DSFA und deren Veröffentlichung kann das Vertrauen des Kunden gestärkt und das Image der Raiffeisen-Landesbank Steiermark AG aufgewertet werden. Außerdem kann die Landesbank einen weiteren Vorteil aus der neuen Regelung generieren, da die Maßnahmen zum Schutz der personenbezogenen Daten der Kunden auch für die eigenen Unternehmensdaten verwendet werden können und somit auch zum Schutz der eigenen Daten dienen.

Im Hinblick auf das konzipierte Tool, so wird dieses auch in Zukunft die Raiffeisen-Landesbank bei der DSGVO-konformen Durchführung der DSFAs unterstützen. Denn mit Hilfe des Tools kann der Kooperationspartner die DSFAs effizienter durchführen, wodurch in weiterer Folge datenschutzrechtliche Sanktionen und damit verbundene Strafzahlungen vermieden werden können.

Abschließend sei erwähnt, dass die Raiffeisen-Landesbank Steiermark AG aufgrund der Ermittlung der TOP-5-Risiken über die wesentlichen Risiken informiert ist und somit entsprechende Maßnahmen umsetzen kann, um präventiv vorzugehen und somit Datenschutzverletzungen keinen Raum zu bieten.

Literaturverzeichnis

Bücher:

AHRENDTS, F./MARTON, A. [2008]: IT-Risikomanagement leben!: Wirkungsvolle Umsetzung für Projekte in der Softwareentwicklung, Heidelberg: Springer-Verlag Berlin Heidelberg, 2008.

BAUER, C./EICKMEIER, F./ECKARD, M. [2018]: E-Health: Datenschutz und Datensicherheit: Herausforderungen und Lösungen im IoT-Zeitalter, Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2018.

BOZKURT, Ö. [2018]: EU-DSGVO und Compliance: Rechtliche und wirtschaftliche Herausforderungen, Hamburg: Igel Verlag RWS, 2018.

BRÜHWILER, B. [2016]: Risikomanagement als Führungsaufgabe: Umsetzung bei strategischen Entscheidungen und operationellen Prozessen, 4. aktualisierte Auflage, Bern: Haupt, 2016.

BRÜHWILER, B./ROMEIKE, F. [2010]: Praxisleitfaden Risikomanagement: ISO 31000 und ONR 49000 sicher anwenden, Berlin: Erich Schmidt Verlag GmbH & Co. KG, 2010.

BURGER, A./BUCHHART, A. [2002]: Risikocontrolling, München: Oldenbourg Wissenschaftsverlag GmbH, 2002.

CALDER, A. [2017]: EU-DSGVO: Eine Kurzanleitung, Cambridgeshire: IT Governance Publishing, o.O.: o.V., 2017.

DENK, R./EXNER-MERKELT, K./RUTHNER, R. [2008]: Corporate Risk Management: Unternehmensweites Risikomanagement als Führungsaufgabe, 2. überarbeitete und erweiterte Auflage, Wien: Linde Verlag Wien Ges.m.b.H., 2008.

DIEDERICHS, M. [2017]: Risikomanagement und Risikocontrolling, 4. vollständig überarbeitete und ergänzte Auflage, München: Verlag Franz Vahlen München, 2017.

DIHEN, R. [2017]: Die neue Datenschutzgrundverordnung (EU-DSGVO): Auswirkungen auf die Social Media Marketing Strategie von Unternehmen in Deutschland, Norderstedt: Studylab, 2017.

FEILER, L./HORN, B. [2018]: Umsetzung der DSGVO in der Praxis: Fragen, Antworten, Muster, Wien: Verlag Österreich GmbH, 2018.

GEIST, R.,M. [2017]: EU-DSGVO: Neue Aufgaben für die Verwaltung, o.O.: Grin Verlag, 2017.

GLEIßNER, W. [2017]: Grundlagen des Risikomanagements: Mit fundierten Informationen zu besseren Entscheidungen, 3. vollständig überarbeitete und erweiterte Auflage, München: Verlag Franz Vahlen GmbH, 2017.

GLEIßNER, W./KLEIN, A. [2017]: Risikomanagement und Controlling: Chancen und Risiken erfassen, bewerten und in die Entscheidungsfindung integrieren, 2. Auflage, München: Haufe-Lexware GmbH & Co. KG, 2017.

GLEIßNER, W./ROMEIKE, F. [2005]: Risikomanagement: Umsetzung, Werkzeuge, Risikobewertung, München: Rudolf Haufe Verlag GmbH & Co. KG, 2005.

GOLA, P./JASPERS, A./MÜTHLEIN, T./SCHWARTMANN, R. [2018]: DS-GVO/BDSG im Überblick Informationen zur Datenschutz-Grundverordnung und dem Bundesdatenschutzgesetz bei der Anwendung in der Privatwirtschaft, 3. aktualisierte Auflage, Rheinbreitbach: Datakontext GmbH, 2018.

HECHENBLAIKNER, A. [2006]: Operational Risk in Banken: Eine methodenkritische Analyse der Messung von IT-Risiken, 1. Auflage, Wiesbaden: Deutscher-Universitäts-Verlag GWV Fachverlage GmbH, 2006.

HOEREN, T./HOLZNAGEL, B. [2018]: Direktmarketing im Licht der Europäischen Datenschutzgrundverordnung, Münster: LIT Verlag Dr. W. Hopf, 2018.

HOHN, W. [2018]: Berücksichtigung der EU Datenschutz-Grundverordnung (DSGVO) bei der privaten Vermietung und Verpachtung: Ein Praxisleitfaden, o.O.: o.V., 2018.

KNYRIM, R. [2016]: Datenschutz-Grundverordnung: Das neue Datenschutzrecht in Österreich und der EU, Wien: Manz’sche Verlags- und Universitätsbuchhandlung GmbH, 2016.

KÖNIGS, H.-P. [2013]: IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits- und IT Risiken, 4. Auflage, Wiesbaden: Springer Fachmedien Wiesbaden, 2013.

KRANIG, T./SACHS, A./GIERSCHMANN M. [2017]: Datenschutz-Compliance nach der DS-GVO: Handlungshilfe für Verantwortliche inklusive Prüfungsfragen für Aufsichtsbehörden, Köln: Bundesanzeiger Verlag GmbH, 2017.

KÜHLING, J./KLAR, M./SACKMANN, F. [2018]: Datenschutzrecht, 4. Auflage, Heidelberg: C.F. Müller GmbH, 2018.

KUGLER, S./ANRICH, F. [2018]: Digitale Transformation im Mittelstand mit System: Wie KMU durch eine innovative Kultur den digitalen Wandel schaffen, Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2018.

LEPPERHOF, N./MÜTHLEIN, T. [2018]: Leitfaden zur Datenschutz-Grundverordnung: Umsetzungshilfe für die betriebliche Praxis, 2. erweiterte Auflage, Rheinbreitbach: Datakontext GmbH, 2018.

MATTHEWS. A. [2018]: DSGVO für Ihre Webseite: Endlich verständlich, 1. Auflage, Senden: o.V., 2018.

MOOS, F./SCHEFZIG, J./ARNING M. [2018]: Die neue Datenschutz-Grundverordnung, Berlin: Walter de Gruyter GmbH, 2018.

MÜHLBAUER, H. [2018]: EU-Datenschutz-Grundverordnung (DSGVO): Praxiswissen für die Umsetzung im Unternehmen – Schnellübersichten, 2. durchgesehene Auflage, Berlin: Beuth Verlag GmbH, 2018.

MÜTHLEIN, T. [2017]: Datenschutz-Grundverordnung: General Data Protection Regulation, 2. aktualisierte Ausgabe, Rheinbreitbach: Datakontext GmbH, 2017.

OCHSENFELD, M.,F. [2017]: Datenschutz für Betriebsräte: Kurz und knackig, 2. Auflage, Norderstedt: BoD – Books on Demand, 2017.

REIMANN, G. [2018]: Betrieblicher Datenschutz Schritt für Schritt – gemäß EU-Datenschutz-Grundverordnung: Lösungen zur praktischen Umsetzung, 2. vollständig überarbeitete und erweiterte Auflage, Berlin: Beuth Verlag GmbH, 2018.

REINIS, M. [2017]: Privacy Impact Assessment: Datenschutz-Folgenabschätzung nach ISO/IEC 29134 und ihre Anwendung im Rahmen der EU-DSGVO, 1. Auflage, Norderstedt: Books on demand, 2017.

ROMEIKE, F. [2018]: Risikomanagement, Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2018.

ROMEIKE, F./FINKE, R. [2003]: Erfolgsfaktor Risiko-Management: Chancen für Industrie und Handel, Methoden, Beispiele, Checklisten, Wiesbaden: Gabler GWV Fachverlag GmbH, 2003.

ROMEIKE, F./HAGER, P. [2009]: Erfolgsfaktor Risiko-Management 2.0: Methoden, Beispiele, Checklisten, Praxishandbuch für Industrie und Handel, 2. Auflage, Wiesbaden: Gabler GWV Fachverlage GmbH, 2009.

ROßNAGEL, A. [2017]: Datenschutzaufsicht nach der EU –Datenschutz –Grundverordnung: Neue Aufgaben und Befugnisse der Aufsichtsbehörden, Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2017.

SCHMIDT, F./SCHWEIßGUTH, H./HOFFMANN J. H./HUMMEL, D. [2018]: Datenschutz in der Wohnungswirtschaft, 1. Auflage, Freiburg: Haufe-Lexware GmbH & Co. KG, 2018.

SCHWARTMANN, R./JASPERS, A. [2018]: Internet- und Datenschutzrecht: Vorschriftensammlung, Heidelberg: C.F. Müller GmbH, 2018.

SCHWARTMANN, R./JASPERS, A./THÜSING, G./KUGELMANN, D. [2018]: DS-GVO/BDSG: Datenschutzgrundverordnung: Bundesdatenschutzgesetz, Heidelberg: C.F. Müller GmbH, 2018.

SCHWICHTENBERG, S. [2018]: Datenschutz in drei Stufen: Ein Auslegungsmodell am Beispiel des vernetzten Automobils, Wiesbaden: Springer Fachmedien Wiesbaden GmbH, 2018.

STAPELKAMP, T. [2018]: DSGVO-Bibel: Datenschutz-Grundverordnung, Leipzig: Design is making Sense, 2018.

VANINI, U. [2012]: Risikomanagement: Grundlagen, Instrumente, Unternehmenspraxis, Stuttgart: Schäffer-Poeschel Verlag, 2012.

VOIGT, P./VON DEM BUSSCHE A. [2018]: EU-Datenschutz-Grundverordnung (DSGVO): Praktikerhandbuch, Berlin: Springer-Verlag GmbH, 2018.

VON WALTER, A. [2018]: Datenschutz im Betrieb: Die DSGVO in der Personalarbeit, 1. Auflage, Freiburg: Haufe-Lexware GmbH & Co. KG, 2018.

WYBITUL, T. [2017]: EU-Datenschutz-Grundverordnung, Frankfurt am Main: Deutscher Fachverlag GmbH, 2017.

Ar**tikel:**

BIEKER, F./BREMERT, B./HANSEN, M. [2018]: Die Risikobeurteilung nach der DSGVO, in: DuD – Datenschutz und Datensicherheit, 2018, Ausgabe 8/2018, S. 492-496.

FRIEDEWALD, M. [2017]: Datenschutz-Folgenabschätzung: Chancen, Grenzen, Umsetzung, in: TA TuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, Jahrgang 26 (2017), Ausgabe 1-2, S. 66-71.

HANSEN, M. [2016]: Datenschutz-Folgenabschätzung – gerüstet für Datenschutzvorsorge?, in: DuD – Datenschutz und Datensicherheit, 2016, Ausgabe 09/2016, S. 587-591.

KNYRIM, R./TIEN, K. [2017]: Die Datenschutz-Grundverordnung im Beschäftigtenkontext: Auswirkungen der DSGVO auf den Arbeitnehmerdatenschutz, in ASoK – Arbeits- und SozialrechtsKartei, Ausgabe 2017, S. 362-366.

MERTINZ, A. [2016]: Datenschutz in der Personaladministration, in: PV-Info – Fachzeitschrift für Personalverrechnung, Jahrgang 16, 2016, Ausgabe 07/2016, S. 16-23.

WEICHERT, T. [2015]: Führungsaufgabe „Datenschutz“ bei Banken, in: DuD – Datenschutz und Datensicherheit, 2015, Ausgabe 1/2015, S. 16-20.

WICHTERMANN, M. [2016]: Die Datenschutz-Folgenabschätzung in der DS-GVO: Die Folgenabschätzung als Nachfolger der Vorabkontrolle, in: DuD – Datenschutz und Datensicherheit, 2016, Ausgabe 12/2016, S. 797-801.

Sonstige Dokumente:

BITKOM LEITFADEN [2017]: Risk Assessment & Datenschutz-Folgenabschätzung: Leitfaden, https://www.bitkom.org/Bitkom/Publikationen/Risk-Assessment-Datenschutz-Folgenabschaetzung.html, [02.04.2019].

Datenschutzgruppe nach Artikel 29 [2017]: Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“, https://www.dsb.gv.at/europaischer_datenschutzausschuss_edsa, [02.04.2019]

Anhangsverzeichnis

Anhang

Startseite	Fragen zur Verarbeitungstätigkeit

Verarbeitungstätigkeit	
Befragte Person(en)	Prozesseigner, Prozesscoach
Datum	

Bitte beschreiben Sie systematisch die Verarbeitung von personenbezogenen Daten im Rahmen der von Ihnen durchgeführten Verarbeitungstätigkeit!

Was ist der Zweck der Erhebung, Verarbeitung, Übermittlung, Aufbewahrung und Vernichtung von personenbezogenen Daten in Ihrer Verarbeitungstätigkeit?

Wie notwendig und verhältnismäßig schätzen Sie Ihre Verarbeitungsvorgänge in Bezug auf den Zweck ein? (sind die personenbezogenen Daten hinsichtlich des Zwecks angemessen sowie auf das notwendige Maß beschränkt?)

nicht notwendig	4
eher wenig notwendig	3
eher notwendig	2
sehr notwendig	1

Bewertung der Notwendigkeit	

Begründung:

nicht verhätnismäßig	4
eher wenig verhältnismäßig	3
eher verhältnismäßig	2
sehr verhätnismäßig	1

Bewertung der Verhältnismäßigkeit	

Begründung:

Involvierte Parteien

Verantwortlicher	Auftragsverarbeiter

Startseite		Fragen zur Verarbeitungstätigkeit

Welche Personen sind im Rahmen Ihrer Verarbeitungstätigkeit betroffen?		
Kategorien betroffener Personen	**Erläuterung**	**Ja/Nein?**
Mitarbeiter	Dienstnehmer des Verantwortlichen, einschließlich ehemalige Mitarbeiter	
Angehörige von Mitarbeitern		
Bewerber	Externe und interne Stellenbewerber	
Vertragspartner	Lieferanten, Dienstleister, sonstige Vertragspartner, deren Beschäftigten und Vertreter	
Von Bildverarbeitung betroffene Personen		
Potenzielle Kunden und Interessenten		
Kunden	einschließlich Vertreter, Beschäftigte und wirtschaftliche Eigentümer von Kunden, auch zB Treuhänder und Treugeber, Stifter und Begünstigte von Privatstiftungen	
Sicherheitengeber	einschließlich deren Vertreter und Beschäftigte	
Eigentümer des Verantwortlichen	Gesellschafter, Aktionäre oder Genossenschaftsmitglieder	
Organe und Funktionäre des Verantwortlichen	Geschäftsführer, Vorstands- und Aufsichtsratsmitglieder	
Besucher und sonstige Zutrittsberechtigte		
Organe/Beschäftigte v. Konzernges. u. Sektorinst.		
Sonstige	**Bitte schreiben Sie in diese Zelle welche sonstigen Personen betroffen sind**	

Welche interne Empfängerkategorien werden im Rahmen ihrer Verarbeitungstätigkeit verarbeitet?		
Interne Empfängerkategorien	**Abteilung/Detail**	**Ja/Nein?**
Geschäftsbereich Vertragsverwaltung	Abteilungsleiter/Filialleiter/Gruppenleiter	
Aufsichtsrat	Aufsichtsrat	
Geschäftsbereich Privat- und Geschäftskunden	Correspondent Banking, ELBA, Filialen, Kundenhandel, Vertriebsunterstützung, Bauträger & Projektgesellschaften, Firmen-/Institutionelle Kunden, Sanierungskunden, Vertriebsunterstützung Firmenkunden	
Innenrevision	Innenrevision, IT Revision	
Marketing	Marketing	
Personalmanagement	Personalmanagement	
Rechnungswesen & Controlling	Rechnungswesen & Controlling	
Recht-/Geldwäsche- und Compliance	Recht-/Geldwäsche- und Compliance	
Risikomanagement	Risikomanagement	
Treasury	Treasury	
Vorstand/Geschäftsführung	Vorstand	

Startseite

Fragen zur Verarbeitungstätigkeit

Welche externe Empfängerkategorien werden im Rahmen ihrer Verarbeitungstätigkeit verarbeitet?

Externe Empfängerkategorien	Abteilung/Detail	Ja/Nein?
Kredit- und Finanzinstitute	andere Banken, Kreditkartenunternehmen	
Anwälte, Notare	Anwälte, Notare	
Verwaltungsbehörden		
Aufsichtsbehörden	FMA, OeNB	
Steuerberater und Wirtschaftsprüfer	Externe Prüfer oder Parteienvertreter	
Gerichte und Staatsanwaltschaften	Gerichte und Staatsanwaltschaften	
IT-Dienstleister	Rechenzentren	
Lieferanten	Lieferanten	
externe Revision	Revision	
Unternehmen des Raiffeisensektors	Raiffeisenbanken, Raiffeisenlandesbanken, RBI, Raiffeisenverband, Lagerhäuser etc.	
Versicherungen	sonstige Versicherung (zB Sperrscheinersatz)	
sonstige Auftragsverarbeiter EU	zB Kartenproduzenten, Callcenter	
sonstige Auftragsverarbeiter außerhalb EU		
Makler, Vermittler, Finanzdienstleister		
Bonitätsdatenbanken		
Geschäftspartner vermittelter Produkte	Teambank, Bausparkasse, Raiffeisen Leasing, Raiffeisen Versicherung	
gesetzlicher Vertreter oder Bevollmächtigter		
Sonstige		

Startseite

Fragen zur Verarbeitungstätigkeit

Welche personenbezogenen Datenarten werden im Rahmen Ihrer Verarbeitungstätigkeit verarbeitet?

Datenkategorien (Kurzname)	Erläuterung, Beispiele	Ja/Nein?
Persönliche Detailangaben	Name, Titel, Alter, Geschlecht, Geburtsort, Geburtsdatum, Nationalität, interne Identifikationsnummern (z.B. Kundennummer, Vertragspartnernummer)	
Haushaltsdaten und familiäre Verhältnisse	Familienstand, Hochzeitsdaten, Scheidungsdaten, Anzahl Kinder, unterhaltsberechtigte Personen und Haushaltsangehörige	
Daten zu Identitäts- und Reisedokumenten	Art des Ausweises, Ausstellende Behörde/Organisation, Nummer des Ausweises, Ausstellungsdatum	
Kontaktdaten	Aktuelle und frühere Adressen, Telefonnummern, Fax Nummer, E-Mail Adressen (jeweils beruflich und privat), Messenger & Social Media Accounts	
Lebenslauf u. Mitarbeiterqualifikation	Lebenslauf, frühere Arbeitgeber, Vorerfahrungen bei anderen Arbeitgebern, Name der Einrichtung, Zeugnisse/Diplome, Berufliche Abschlüsse und Ausbildungsdaten, Aus- und Fortbildungen, sonstige Ausbildungen, Kenntnisse, Fähigkeiten (zB Sprachkenntnisse, Erste Hilfe, Führerschein), akademische Titel, Beurteilungen, Einschätzungen iZm Arbeitsverhältnis	
Daten zu Beruf und Arbeitsverhältnis	Arbeitgeber, Funktionstitel, Beschreibung der Funktion, Jobgrade, Einstellungsdatum, Arbeitsort, Mitgliedschaft in innerbetrieblicher Arbeitnehmervertretung, Ersthelfer, Brandschutzbeauftragter, Referenzen, Probezeit, Arbeitsverhältnis, Datum des Ausscheidens, Gründe des Ausscheidens, Daten zur Pension (z.B. Antrittsdatum)	
Aufenthaltsstatus	Details über Aufenthaltstitel, Visum, Arbeitserlaubnis, Wohn- oder Reisebeschränkungen, an das Aufenthaltsrecht gebundene Sonderbedingungen	
Lohn- und Gehaltsdaten	Zahlungen, Lohn, Provisionen, Bonus, Zulagen, Spesen, Sachbezüge, Vergünstigungen, Darlehen, Gebühren, Firmen-KfZ, Abzüge (z.B. Steuer, Sozialversicherung)	
Steuerliche Daten und Sozialversicherungsdaten	zB UID und sonstige steuerliche Nummern / Registrierungen, Steuerbescheide, Steuerleistung, steuerlicher Sitz, Sozialversicherungsdaten	
Arbeitsorganisationsdaten	Personalnummer, Dienstausweis, Zutrittsdaten, Anwesenheiten, gegenwärtige Verantwortungen, Projekte, Arbeitszeiten, geleistete Stunden, Dienstreisen, Urlaubsanspruch, konsumierter Urlaub, Krankenstände, sonstige Abwesenheiten, Arbeitsmittel (z.B. Laptop, Mobiltelefon, Tablet), Berechtigungen, Sicherheitsprotokolle und Authentifizierungsdaten (Zutritt, Zugang, Zugriff, Weitergaben). Ergebnisse von Routinekontrollen, Besucherlisten, Raumbuchungsinformationen	
Beteiligungen, Organfunkt., Vertretungsbefugnisse	Detailinformationen zur jeweiligen Rolle (z.B. Art der Vertretungsbefugnis, Stimmrecht, Höhe der Beteiligung)	
Lebens- und Konsumgewohnheiten	Lebensstil, Angaben über Aufenthalte und Fahrten, Soziale Kontakte, Hobby, Sport, Mitgliedschaften (andere als berufliche, politische, gewerkschaftliche), andere Interessen	
Elektron. Protokoll- u. Identifikationsdaten	IP-Adressen, Cookies, Anschlusszeiten, elektronische Unterschrift, Online-Kennungen, Benutzernamen, Passwörter, Protokollierung von Systemaktivitäten insb.	
Elektronische Standort- und Bewegungsdaten	GPS-Daten, Mobilfunk-Daten, WLAN-Netzdaten	
Bild- und/oder Tonaufzeichnungen	Filme, Fotografien, Videoaufzeichnungen (z.B. Aufzeichnungen von Überwachungskameras, Mitschnitte von Videokonferenzen), digitale Fotos (z. B. Pass- oder Bewerbungsfotos, Firmenausweisfotos), Aufzeichnungen auf Tonbandträgern, Telefonaufzeichnung	
Bonitätsdaten	Art (und jeweilige Höhe) der Einkünfte: selbstständige/unselbstständige Tätigkeit, Invaliditäts-/Alterspension, Vermietung/Verpachtung, Einkünfte aus Unternehmens- oder Gesellschaftsbeteiligungen; Vermögen: Konto- oder Sparguthaben, Wertpapierdepots, Liegenschaften, Gesellschaftsbeteiligungen; Unterhaltspflichten (Kinder/Ehegatte), wiederkehrende Zahlungsverpflichtungen für Ausbildungskosten/Kinder, Kredittilgungen, Mieten, anhängige Exekutionsverfahren, anhängige/abgeschlossene Insolvenz-, Sanierungs- oder Schuldenrgulierungsverfahren, Bilanzdaten.	
Finanzidentifikationsdaten	IBAN/BIC, Daten von Kredit-, Debit- oder Prepaidkarten (Kartenart, Inhaber, Aussteller, Gültigkeitsdauer, verfügbarer Rahmen)	
Daten zu Kreditgeschäft	Kreditart (Einmal-/revolvierender Kredit), Kreditbetrag, Laufzeit, Verzinsungsart (fix/variabel/antizipativ/dekursiv), Angaben zur Tilgung (Tilgungsstruktur, Tilgungsraten, etc.), (Annuitätentilgung), Angaben zu Kreditsicherheiten (Sicherheitengeber, Art der Sicherheit: Hypothek, Bürgschaft, Garantie, Patronatserklärung, etc.), Basel-II relevante Daten (z.B. Default/Non Default-Status)	
Daten zu Einlagengeschäft	Kontoart (Spar-/Girokonto), Kontosalden, Kontoumsätze, Zeichnungs-/Verfügungsberechtigte, Disporahmen, etc.	
Daten zu Finanztermin-/Derivatgeschäft	Name/Angaben zur Gegenpartei, eigene/fremde Rechnung, Geschäftsart (FX, IRS, CDS, Put/Call Option), etc.	
Kassageschäft, Wertpapierverwahrung u. -verwaltung	Daten zu Devisenkassageschäften und Wertpapiergeschäften, Wertpapierdepotnummer, Wertpapierbestand/-bewegungen, steuerliche Anschaffungsdaten, (Wahl-)Dividenden/Kupons/Kapitalmaßnahmen, Name/Angaben zur Gegenpartei	

Startseite

Fragen zur Verarbeitungstätigkeit

Welche personenbezogenen Datenarten werden im Rahmen Ihrer Verarbeitungstätigkeit verarbeitet?

Datenkategorien (Kurzname)	Erläuterung, Beispiele	Ja/Nein?
Versicherungsdaten	Versicherungsart, Details über die gedeckten Risiken, Versicherungssumme, Versicherungsprämie, Deckungszeitraum, Fälligkeitsdatum, ausgeführte oder erhaltene Zahlungen und nicht ausgeführte Zahlungen, sonstige Konditionen	
Zahlungsverkehrs- und Clearing-Daten	Angaben über Auftraggeber, Empfänger/Begünstigten, Transaktionsbetrag, Transaktionswährung, IBAN/BIC-Daten von Auftraggeber- und Empfängerkonto, Details über Clearing, sonstige SWIFT-Daten	
Daten zu Fuhrparkmanagementgeschäft	KFZ Daten (techn. und preisl. KFZ-Daten ieS., Unfälle, Fahrzeugschäden/Reparaturen, Fahr- und Tankverhalten, Service und Wartung, KFZ Versicherung, etc.	
Daten zu Bauträgergeschäft	Käuferdaten (nat. und juristische Personen - deren Organe), Kaufobjekt und -preis, allfällige Angaben zu Sicherheiten (Sicherheitengeber, Art der Sicherheit: Hypothek, Bürgschaft, Garantie, Patronatserklärung, etc.), Daten iZm der Kaufpreisfinanzierung, Sonderausstattungen, Wohnungszweck (Eigennutzung / Vermietung)	
Daten zu Vermittlungsgeschäft	Vertragsdaten zu vermittelten Geschäften (zB Leasing, Bausparen, Versicherung, Kreditkarten)	
Daten zu Vermietungsgeschäft	Mietvertragsart, Miete, Kaution, Laufzeit, Mietobjekt samt Ausstattung, Mietzins und Betriebskosten bzw. sonstige Verpflichtungen des Mieters, Angaben zu Sicherheiten (Sicherheitengeber, Art der Sicherheit: Hypothek, Bürgschaft, Garantie, Patronatserklärung, etc.), Kaufoptionen	
AML- (Anti Money Laundering) und Compliance-Daten	Risikoeinschätzung, PEP, FISA, KYC (incl. Gap-Liste), Suspicious Activity Reports, Fraud checks, FATCA, CRS einschließlich öffentliche Mandate in gesetzgebenden Körperschaften, Mandate oder Mitgliedschaften in Interessensvertretungen, Einordnung als PEP (Politisch exponierte Person), Befugnisse, Ermächtigungen, Bevollmächtigungen	
Daten zu Marketing und Vertrieb	Kontakt- und Listendaten, Produktinteressen, Kommunikationshistorie, Geschäftshistorie	
Daten zu Safes und Schließfächern	Datum, Zeit, Grund des Zugriffs, Safe-Nummer	
Besondere Kategorien personenbezogener Daten	Besondere Kategorien personenbezogener Daten gem. Art 9 DSGVO, insbesondere: rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder weltanschauliche Überzeugungen, biometrische Identifikationsdaten, Gesundheitsdaten, Daten zum/r Sexualleben/-orientierung, körperliche Beschreibungsdaten usw.	
strafrechtliche Verurteilungen und Straftaten	inkl. Anschuldigungen, Strafregisterauszug	
Sonstige	Freies Textfeld	

Auf welcher Rechtsgrundlage basiert die Verarbeitung der personenbezogenen Daten?

Hat es in Ihrer Verarbeitungstätigkeit bereits eine Ihnen bekannte Datenschutzverletzung gegeben? Wenn ja, welche? (z.B. Datenverlust, Datendiebstahl, unautorisierter Zugriff)

Welche Risiken könnte es, bezogen auf die von Ihnen verarbeiteten Daten, für die Rechte und Freiheiten der betroffenen Personen geben? (gemeinsames Brainstorming)