

Risikoanalyse IT-Sicherheit und Datenschutz

Für Geschäftsprozesse



**Inhaltsverzeichnis**

**1. Einleitung** 3

**2. Allgemeines** 4

**3. Schadenshöhe** 5

**4. Eintrittswahrscheinlichkeit** 8

**5. Risiken** 10

**6. Risiko-Entscheidung** 12

**7. Maßnahmen zur Verminderung der Risiken** 13

**8. Unterschriften** 14

**1. Einleitung**

Die vorliegende Risikoanalyse für Informationssicherheit und Datenschutz soll dabei helfen, die Ri-siken, die mit der Verarbeitung von Informationen des Unternehmens, speziell bei der Verwendung von Informationstechnologie, sowie die Risiken, die mit der Verarbeitung von personenbezogenen Daten bestehen, transparent und bewertbar zu machen. Als Unterstützung finden Sie in der Vorlage ein geeignetes Beispiel.

Erst wenn Risiken bewertet sind, kann eine sinnvolle Risikostrategie gewählt, und – im Falle der Risikominderung – eine Investition in risikosenkende Maßnahmen beurteilt werden.

Die Informationssicherheitsrisiken treten immer in der Wertschöpfung auf, sie können nicht auf Dienstleister abgewälzt werden (Vertragsstrafen mindern den Schaden, können aber i.d.R. nicht alle Folgeeffekte auffangen). Für Datenschutzrisiken gilt dies auch: die Verantwortung für ein angemes-senes Risiko bei der Verarbeitung von personenbezogenen Daten liegt beim Unternehmen. Eine Entscheidung für eine bestimmte Technologie/einen bestimmten Prozess/eine Kooperation mit einem Dienstleister ist daher immer auch vor dem Hintergrund der damit verbundenen Risiken zu treffen.

Die Risikoanalyse ist ein strukturierter Ansatz, um Risiken zu bewerten, die für Informationen und Daten durch

* eine Offenlegung, einen Verlust oder eine Veränderung der Informationen/Daten oder
* eine Manipulation, einen Diebstahl oder eine Störung der für die Verarbeitung genutzten IT-Anwendungen und sonstigen Arbeitsmittel

bestehen. Durch die Risikoanalyse für **Informationssicherheit** werden die Risiken hinsichtlich ihrer Kritikalität **aus Sicht des Unternehmens** bewertet. Durch die Risikoanalyse für **Datenschutz** werden die Risiken hinsichtlich ihrer Kritikalität **aus Sicht des Betroffenen** bewertet. Dies ermöglicht eine Priorisierung der notwendigen Maßnahmen im Sinne von Effizienz und Wirtschaftlichkeit einerseits und Gesetzeskonformität andererseits.

Bei einer Risikoanalyse wird zum einen der mögliche entstehende Schaden, und zum anderen die Eintrittswahrscheinlichkeit für diese Schäden eingeschätzt. Die beiden Werte werden zu einem Risiko kombiniert; die Geschäftsleitung muss dann entscheiden, ob das Risiko akzeptiert wird oder Schutzmaßnahmen erforderlich sind.

Es empfiehlt sich, die Ergebnisse dieser Risikoanalyse für alle Geschäftsprozesse/Verarbeitungs-tätigkeiten in einer Tabelle zusammen zu fassen, und jährlich auf ggf. notwendige Anpassungen zu prüfen.

Eine beispielhaft für den Geschäftsprozess „Online-Bewerbung“ ausgefüllte Risikoanalyse können Sie sich unter [www.ihk.de/datensicherheit](https://www.ihk.de/datensicherheit) herunterladen (interaktive PDF-Datei).

**2. Allgemeines**

Es ist wenig hilfreich, für jedes einzelne Datum eine Risikobewertung durchzuführen. Besser ist eine thematisch zusammenhängende Gruppierung, etwa Geschäftsprozess oder Verarbeitungstätigkeit.

Geben Sie zum einen die verarbeiteten Informationen an, und zum andern – sofern es in dieser Ver-arbeitung auch um personenbezogene Daten geht – welche Art diese personenbezogenen Daten sind (also z.B. Adressdaten, Gesundheitsdaten etc.). Es kann sein, dass Sie die gleiche Kategorie in beiden Feldern eintragen – wenn diese Informationen sowohl für Sie als auch für den Betroffenen relevant ist.

Dokumentieren Sie auch, wer für die Verarbeitungstätigkeit/den Geschäftsprozess verantwortlich ist, und wann die Analyse durchgeführt wurde.

|  |  |
| --- | --- |
| Geschäftsprozess/Verarbeitungstätigkeit |  |
| Arten von verarbeiteten Informationen |  |
| Arten von personenbezogenen Daten |  |
| Verantwortliche Person |  |
| Datum der Analyse |  |

**3. Schadenshöhe**

Für jede Informationsart geben Sie an, wie hoch für Sie aus Unternehmenssicht der Schaden ist, und zwar nach den Aspekten **Vertraulichkeit** (wie wichtig ist es für Sie, dass die Informationen nicht öffentlich werden), **Verfügbarkeit** (wie wichtig ist es für Sie, dass die Informationen ständig verfügbar sind) und **Integrität** (wie wichtig ist es für Sie, dass die Informationen korrekt sind und nicht verändert wurden). Tragen Sie die Informationsarten in die jeweilige Zeile der Tabelle ein:

**Mögliche Schadenshöhen für die Informationsarten im Geschäftsprozess / in der Verarbeitungstätigkeit aus Unternehmenssicht:**

|  |  |  |
| --- | --- | --- |
| Schaden | Bewertungskriterien | Informationsarten |
| 1gering | Eine Veröffentlichung/Verfälschung/Nicht-Verfügbarkeit von Informationen hat nur einen geringen Effekt auf die Organisation (Kosten/ Lieferfähigkeit oder Reputation). |  |
| 2mittel | Eine Veröffentlichung/Verfälschung/Nicht-Verfügbarkeit von Informationen hat einen merklichen Effekt auf die Organisation (Kosten/ Lieferfähigkeit oder Reputation), die Ansehens- oder Vertrauensbeeinträchtigung ist tolerierbar. |  |
| 3hoch | Eine Veröffentlichung/Verfälschung/Nicht-Verfügbarkeit von Informationen verletzt rechtliche Bestimmungen oder verursacht hohe Folge- kosten. Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. |  |
| 4sehr hoch | Eine Veröffentlichung/Verfälschung/Nicht-Verfügbarkeit von Informationen führt zu gravierenden rechtlichen Konsequenzen für die Organisation/ihre Organvertreter und verursacht sehr hohe Folgekosten. In der Folge ist mit für die Organisation kritischen Reputationsschäden zu rechnen. |  |

Führen Sie die gleiche Bewertung für Arten von **personenbezogenen Daten** durch, diesmal aus Sicht der Betroffenen. Da jede Verarbeitung personenbezogener Daten einen Eingriff in die Grund-rechte der betroffenen Person darstellt, kann der Schaden niemals niedriger als „2 – mittel“ sein. Deshalb ist grundsätzlich davon auszugehen, dass jede Verarbeitung von personenbezogenen Da-ten (außer öffentlicher Identifikatoren wie E-Mail-Adressen o.ä.) mindestens ein Risiko mit mittlerem Schaden aufweist. Besondere Kategorien personenbezogener Daten führen aufgrund der höheren Schadenswirkung mindestens zu der Schadensklasse „3 – hoch“. Dazu gehören etwa:

* Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
* Genetische und biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,
* Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person,
* personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten:
* personenbezogene Daten, die eine Fähigkeits-, Leistungs- und/ oder Verhaltensbewertung ermöglichen,
* eindeutig identifizierende, hoch verknüpfbare Daten (z. B. lebenslang gültige Krankenversichertennummer, Steuer-ID),
* berufsgeheimnisbezogene Daten (Aufzeichnungen von Rechtsanwälten, Wirtschaftsprüfern, Betriebsräten etc.) sowie
* Bank- & Kreditkartenkontendaten (Zugangsinformationen).

Tragen Sie die Informationsarten in die jeweilige Zeile der Tabelle auf der nächsten Seite ein:

**Mögliche Schadenshöhen für die Arten von personenbezogenen Daten im**

**Geschäftsprozess/in der Verarbeitungstätigkeit aus Betroffenensicht:**

|  |  |  |
| --- | --- | --- |
| Schaden | Bewertungskriterien | Informationsarten |
| 1gering | Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts wird durch den Einzelnen als tolerabel eingeschätzt.Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.  |  |
| 2mittel  | Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen ist gegeben und für den Betroffenen spürbar.Ein möglicher Missbrauch personenbezogener Daten hat spürbare Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen. Eine Beeinträchtigung der persönlichen Unversehrtheit ist unwahrscheinlich, aber möglich. Eine Ansehens -oder Vertrauensbeeinträchtigung ist eher nicht zu erwarten  |  |
| 3Hoch | Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen ist möglich. Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden. Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten. |  |
| 4 hoch  | Eine besonders bedeutende Beeinträchtigung des sehr informationellen Selbstbestimmungsrechts des Einzelnen ist zu erwarten. Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich, es besteht Gefahr für Leib und Leben. Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. |  |

**4. Eintrittswahrscheinlichkeit**

Die Eintrittswahrscheinlichkeit beschreibt, wie wahrscheinlich es ist, dass der im letzten Kapitel angenommene Schaden eintreten kann. Es gibt viele Faktoren, die die Eintrittswahrscheinlichkeit beeinflussen. Bei KMUs besteht der dominierende Faktor in der Regel aus der Qualität der vorhandenen Schutzmaßnahmen.

Beschreiben Sie die Schutzmaßnahmen, die Sie einsetzen, um den in diesem Dokument untersuchten Geschäftsprozess/die in diesem Dokument beschriebene Verarbeitungstätigkeit zu schützen. Wenn Sie eine IT-Sicherheitsdokumentation haben, die die entsprechenden Informationen enthält, können Sie auch darauf verweisen.

**Schutzmaßnahmen für Geschäftsprozess/Verarbeitungstätigkeit:**

|  |
| --- |
|  |



Schätzen Sie nun ein, inwiefern die Schutzmaßnahmen geeignet sind, um die im vorigen Kapitel betrachteten Schäden abzuwenden. Wenn die Schutzmaßnahmen durch einen IT-Dienstleister erbracht werden, ermitteln Sie die Werte gemeinsam. Tragen Sie die betroffenen Informationsarten und die Arten von personenbezogenen Daten jeweils in die entsprechende Zeile ein.

**Eintrittswahrscheinlichkeit von Schäden im Geschäftsprozess/in der Verarbeitungstätigkeit**

|  |  |  |  |
| --- | --- | --- | --- |
| Eintrittswahr-scheinlichkeit | Bewertungskriterien | Informationsarten | Arten von personenbezogenen Daten |
| 1fast nie | Die Schutzmaßnahmen funktionieren so gut, dass der Schaden mit sehr hoher Wahrscheinlichkeit nicht eintreten wird. |  |  |
| 2manchmal | Die Schutzmaßnahmen sind überwiegend wirksam, aber es ist nicht ausgeschlossen, dass der Schaden eintreten kann. |  |  |
| 3häufig | Die Schutzmaßnahmen sind nicht gut geeignet, den Schaden zu vermeiden. Einige Schäden können aber dennoch vermieden werden. |  |  |
| 4fast sicher | Die Schutzmaßnahmen sind nicht geeignet, den Schaden zu vermeiden. |  |  |

**5. Risiken**

Tragen Sie nun die Informationen über Schäden und Eintrittswahrscheinlichkeiten zusammen und ordnen Sie diese nach der größten Risikohöhe, multiplizieren Sie dafür Schaden und Eintrittswahr-scheinlichkeit. Trennen Sie die Auflistung nach Informationssicherheit und Datenschutz.

Tipp: Beschreiben Sie alle Risiken, die größer oder gleich 8 sind, etwas ausführlicher.

**Informationssicherheitsrisiken im Geschäftsprozess/in der Verarbeitungstätigkeit:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Risiko für Informationsart... | Risikohöhe | Schaden | Eintrittsw. |
| I1 |  |  |  |  |
| I2 |  |  |  |  |
| I3 |  |  |  |  |

**Datenschutzrisiken im Geschäftsprozess/in der Verarbeitungstätigkeit:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Risiko für Art von personenbezogenen Daten... | Risikohöhe | Schaden | Eintrittsw. |
| D1 |  |  |  |  |
| D2 |  |  |  |  |
| D3 |  |  |  |  |
| D4 |  |  |  |  |

Zur besseren Übersicht können Sie nun die Risiken (mit den IDs) in einer Risikomatrix
angeben.

**Risikomatrix vor kompensierenden Maßnahmen im Geschäftsprozess/in der Verarbeitungstätigkeit:**

|  |
| --- |
| Schadenshöhe |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4- sehr hoch |  |  |  |  |
| 3- hoch |  |  |  |  |
| 2- mittel |  |  |  |  |
| 1- niedrig |  |  |  |  |
|  | 1 – fast nie | 2 – manchmal | 3 – häufig | 4 – fast sicher |

Eintrittswahrscheinlichkeit

Die Idee der Risikoanalyse ist es, sich nur mit den wesentlichen Risiken zu beschäftigen. Sie können daher nun hier festlegen, dass alle Risiken mit einer festzulegenden Risikohöhe grund-sätzlich nicht weiter betrachtet werden, d.h. die Geschäftsführung akzeptiert diese Risiken.

**Alle Risiken mit der Risikohöhe (hier: <2) werden im Geschäftsprozess/in der Verarbeitungstätigkeit nicht weiter betrachtet.**

Datenschutz-Risiken, die hoch oder sehr hoch sind, müssen von Gesetz wegen weiter betrachtet werden. Hierzu ist eine so genannte Datenschutz-Folgeabschätzung erforderlich.

[Ein Beispiel dafür finden Sie hier (PDF-Datei)](https://stiftungdatenschutz.org/fileadmin/Redaktion/Dossiers_Infoplattform/DSGVO-Info-Dossier_IV___Datenschutzfolgenabschaetzung_AR.pdf)

**6. Risiko-Entscheidung**

Bitte dokumentieren Sie hier, wie mit den verbleibenden Risiken umgegangen wird. Risiken werden **übergeben**, wenn sie, z.B. gegen eine finanzielle Gegenleistung, von jemand anderem übernommen werden (etwa durch eine Versicherung) – Vorsicht: meist ist diese Risikoübernahme, gedeckelt, es besteht dann also ein Rest-Risiko. Risiken werden **vermindert**, wenn eine Maßnahme ergriffen wird, um die Eintrittshäufigkeit und/oder den Schaden zu begrenzen. Risiken werden **vermieden**, wenn die Ursache für dieses Risiko nicht weiter existiert (z.B. eine Sammlung vonUnternehmensdaten gar nicht erst angelegt wird) – in der Praxis ist das eher selten der Fall.

**Risikoentscheidungen im Geschäftsprozess/in der Verarbeitungstätigkeit:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Risiko | Übergeben | Vermindern | Akzeptieren | Vermeiden |
| *I1* |  |  |  |  |  |
| *D1* |  |  |  |  |  |
| *D2* |  |  |  |  |  |
| *D3* |  |  |  |  |  |

Bei „AKZEPTIEREN“ begründen Sie bitte Ihre Entscheidung, bei „ÜBERGEBEN“ beschreiben Sie kurz, wieso die Übergabe an Dritte das Risiko mindert, und welches Restrisiko besteht.

|  |
| --- |
|  |

**7. Maßnahmen zur Verminderung der Risiken**

Bitte beschreiben Sie zusätzliche Maßnahmen, die die im vorigen Kapitel genannten Risiken kompensieren, d.h. mindern sollen. Tragen Sie ein, auf welche Risiken (verwenden Sie die IDs I1, I2, D1, etc.) sich diese Maßnahmen auswirken werden, und wie die Wirkung ist (z. B. Eintrittswahrscheinlichkeit 3 -> 2).

**Kompensierende Maßnahmen z. B. im Geschäftsprozess/in der Verarbeitungstätigkeit:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Maßnahme | Wirkt auf Risiko | Effekt | Verantwortlich | Kosten | Umgesetzt bis |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Geben Sie hier die Risikomatrix nach Anwendung der zusätzlichen Maßnahmen an:

**Risikomatrix nach kompensierenden Maßnahmen im Geschäftsprozess/in der** **Verarbeitungstätigkeit:**

|  |
| --- |
| Schadenshöhe |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 4- sehr hoch |  |  |  |  |
| 3- hoch |  |  |  |  |
| 2- mittel |  |  |  |  |
| 1- niedrig |  |  |  |  |
|  | 1 – fast nie | 2 – manchmal | 3 – häufig | 4 – fast sicher |

Eintrittswahrscheinlichkeit

**8. Unterschriften**

Hiermit wird dokumentiert, dass die Geschäftsleitung die Risikoanalyse im Geschäftsprozess/in der Verarbeitungstätigkeit zur Kenntnis genommen hat, die in Kapitel 6 vorge-schlagene Risiko-Entscheidung trifft und die in Kapitel 7 genannten Maßnahmen umsetzen wird.

Datum

Geschäftsleitung IT-Sicherheitsbeauftragte/r

(Risikoübernahme) (fachliche Korrektheit)