Der Hamburgische Beauftragte für
Datenschutz und Informationsfreiheit

Hinweise zur Risikoanalyse und Vorabkontrolle nach dem Hamburgischen Datenschutzgesetz

Dr. Sebastian Wirth

(Stand: 31. Januar 2008)

1 Grundlagen

1.1 Rechtliche Grundlagen

Die Risikoanalyse und Vorabkontrolle ist im Hamburgischen Datenschutzgesetz (HmbDSG) festgeschrieben. In der Broschüre “Hamburgisches Datenschutzrecht 2001” sind insbesondere rechtliche Erläuterungen zu der Regelung enthalten.

§ 8 Abs. 4 HmbDSG

"Vor der Entscheidung über die Einführung oder die wesentliche Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, haben die Daten verarbeitenden Stellen zu untersuchen, ob und in welchem Umfang mit der Nutzung dieses Verfahrens Gefahren für die Rechte der Betroffenen verbunden sind. Die Einführung und die wesentliche Änderung eines automatisierten Verfahrens sind nur zulässig, soweit derartige Gefahren durch technische und organisatorische Maßnahmen wirksam beherrscht werden können, es sei denn, dass solche Maßnahmen gemäß Absatz 1 Satz 2 nicht erforderlich sind. Ergibt die Untersuchung, dass von einem Verfahren eine besondere Gefährdung für die Rechte der Betroffenen ausgeht, so ist das Ergebnis der Untersuchung vor der Einführung oder wesentlichen Änderung des Verfahrens der bzw. dem behördlichen Datenschutzbeauftragten oder, falls keine behördliche Datenschutzbeauftragte bzw. kein behördlicher Datenschutzbeauftragter bestellt wurde, der bzw. dem Hamburgischen Datenschutzbeauftragten zur Stellungnahme zuzuleiten."

Auch im § 4d Abs. 5 des Bundesdatenschutzgesetzes (BDSG) ist die Vorabkontrolle verankert.

www.datenschutz.hamburg.de
E-Mail: mailbox@datenschutz.hamburg.de
Klosterwall 6c - D-20095 Hamburg - Tel.: 040 - 4 28 54 – 40 40 - Fax: 040 - 4 28 54 – 40 00
Vertrauliche Informationen sollten auf elektronischem Weg nur verschlüsselt an uns übermittelt werden. Unser öffentlicher PGP-Schlüssel ist im Internet verfügbar (Fingerprint: 53D9 64DE 6DAD 452A 3796 B5F9 1B5C EB0E)

1.2 Ziele der Risikoanalyse

Mit der Risikoanalyse sollen bereits vor der technischen Realisierung die spezifischen Risiken für die Rechte und Freiheiten der Betroffenen abgeschätzt werden, die mit der Einführung bzw. der wesentlichen Änderung eines DV-Verfahrens verbunden sind. Auch soll geprüft werden, ob mit alternativen Verfahren, die mit geringeren Risiken für die Betroffenen verbunden sind, die geplanten Ziele erreicht werden können.

Durch eine frühzeitige Risikoanalyse lassen sich Fehlentwicklungen innerhalb eines DV-Projektes vermeiden. Datenschutzanforderungen können bereits in der Konzeptphase berücksichtigt werden. Da der Aufwand für Veränderungen von technischen Konzepten häufig um so höher ist, je später diese einfließen, kann so auch der Aufwand für eine datenschutzgerechte Lösung verringert werden. Die Abwägung zwischen Nutzen und Aufwand einzelner Maßnahmen kann so für die Betroffenen zu einem günstigeren Ergebnis führen.

1.3 Einordnung der Risikoanalyse

Eine Risikoanalyse ist vor jeder Entscheidung über die Einführung bzw. Änderung des Verfahrens zu erstellen (Abb.1). Dieser frühe Zeitpunkt führt dazu, dass gerade bei komplexen Verfahren wesentliche technische und organisatorische Details nicht festgelegt sind. Dem Zielkonflikt zwischen der frühzeitigen Erstellung und der Berücksichtigung von technischen und organisatorischen Einzelheiten kann man durch ein iteratives Vorgehen begegnen. Dabei werden die einzelnen Stufen der Risikoanalyse mehrfach, mit zunehmendem Detaillierungsgrad und zunehmender Vollständigkeit durchlaufen, so dass auch Erfahrungen aus dem technischen Realisierungsprozess genutzt werden können. Diese projektbegleitende Vorgehensweise hat den Vorteil, dass parallel zum Projektverlauf Risiken aufgedeckt und Fehlentwicklungen vermieden werden.

Auch nach der Pilotierung und Einführung eines Verfahrens kann eine erneute Risikoanalyse zu diesem Verfahren notwendig werden. Dies ist immer dann der Fall, wenn sich an den Rahmen- und Einsatzbedingungen gravierende Änderungen ergeben. Beispiele dafür sind, dass durch eine gesteigerte Leistungsfähigkeit der Hardware Verschlüsselungsalgorithmen nicht mehr als sicher gelten oder solche Algorithmen aufgebrochen wurden. Auch wenn mit einem bestehenden Verfahren zukünftig Daten von Personen mit einem deutlich höheren Schutzbedarf als bisher verarbeitet werden sollen, ist die Risikoanalyse fortzuschreiben, die bei der Einführung er-

stellt wurde. Eine erneute Risikobetrachtung ist auch erforderlich, wenn sich der Aufwand für bisher aus Kostengründen verworfene Schutzmaßnahmen gravierend verringert, so dass diese Maßnahmen zukünftig auch in Betracht zu ziehen sind, da sie nun in einem angemessenen Verhältnis zur Schutzwürdigkeit der Daten stehen.

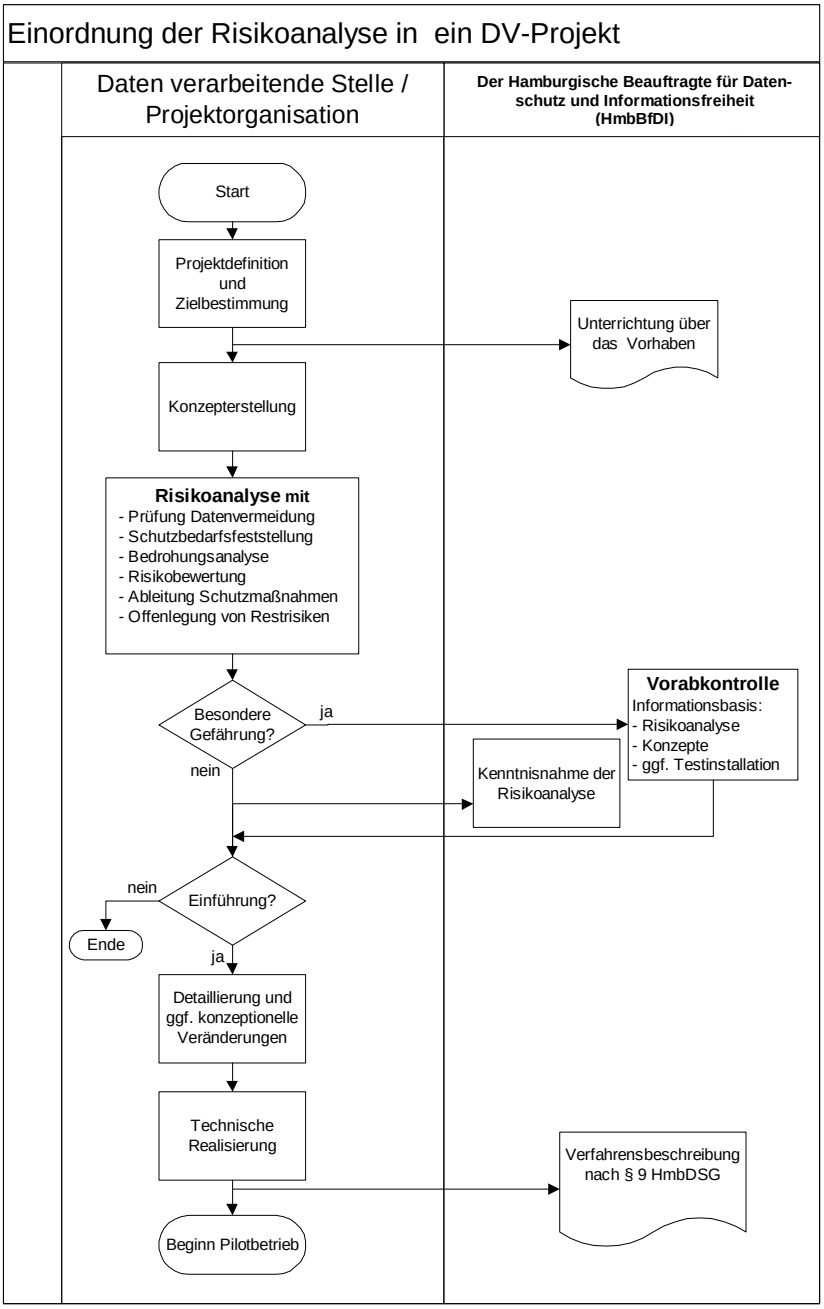

Abb. 1.: Einordnung der Risikoanalyse in ein DV-Projekt

Verantwortlich für die Erstellung ist die „**Daten verarbeitende Stelle**“. Der Begriff „Daten verarbeitende Stelle“ ist im Hamburgischen Datenschutzgesetz definiert. Er bezeichnet die Stelle, die für die Bearbeitung der Fachaufgabe zuständig ist. Häufig ist die Daten verarbeitende Stelle

eine Abteilung oder ein Amt in der Behörde und nicht die gesamte Behörde. Innerhalb einer Behörde gibt es unterschiedliche Daten verarbeitende Stellen, denen unterschiedliche Fachaufgaben (Funktionen) übertragen sind. Die Daten verarbeitende Stelle ist nicht der Dienstleister wie z.B. Dataport, der ggf. die Software oder die Server betreut. Dieser Dienstleister betreibt Datenverarbeitung im Auftrag, nämlich im Auftrag der Daten verarbeitenden Stelle.

2 Stufen der Risikoanalyse

Durch das HmbDSG wird kein bestimmtes formalisiertes Verfahren vorgeschrieben. Die im Folgenden vorgestellte Vorgehensweise ist als Hilfestellung für die Daten verarbeitenden Stellen zu verstehen, eine Risikoanalyse zu erstellen. Die Vorgehensweise basiert auf den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Zu jeder Stufe sind **Leitfragen** angeführt, die die Daten verarbeitende Stelle im Zuge der Risikoanalyse beantworten und darlegen sollte.

2.1 Prüfung der Datenvermeidung

Ein grundlegendes Gebot des Datenschutzrechtes ist das Gebot der Datenvermeidung bzw. Datensparsamkeit. Dieses Gebot ist im § 5 Abs. 4 des Hamburgischen Datenschutzgesetzes und auch im § 3a des Bundesdatenschutzgesetzes festgeschrieben.

Im Rahmen dieses Schrittes werden sowohl unterschiedliche Konzeptionen als auch die zur Auswahl stehenden technischen Alternativen geprüft. Dabei sollten der gesamte Verarbeitungsprozess und die einzelnen Teilprozesse betrachtet werden. Auf diese Weise fließen die Datenschutzkriterien bereits in den Entscheidungsprozess der Systemauswahl mit ein. Folgende Fragen gilt es zu klären:

- **Können die Ziele oder einzelne Teilziele ohne die Verarbeitung personenbezogener Daten erreicht werden?**
- **Kann der Umfang der erforderlichen personenbezogenen Daten reduziert werden?**
- **Muss der Personenbezug über den gesamten Verarbeitungsablauf erhalten bleiben? Wenn nein, wie lange muss der Personenbezug erhalten bleiben?**
- **Kann eine Anonymisierung erfolgen (vgl. § 3 Abs. 9 HmbDSG)? Wenn ja, zu welchem Zeitpunkt?**
- **Kann eine Pseudonymisierung erfolgen (vgl. § 3 Abs. 10 HmbDSG)? Wenn ja, zu welchem Zeitpunkt?**

2.2 Schutzbedarfsfeststellung

Für die näher in Betracht zu ziehende Alternative wird der Schutzbedarf festgestellt. Hierbei werden die Fragestellungen beantwortet:

- **Welche Verfahren und welche zu verarbeitenden Informationen werden betrachtet?**
- **Wie hoch sind die Schutzbedarfe zu bewerten?**

Der Schutzbedarf kann mit einer 3-Stufigen Skala bewertet werden.

Schutzbedarf	Skalen-Wert	Beispiele
normal	1	• Daten für die Personalabrechnung wie z.B. Vergütungsgruppe • KFZ-Zulassungsdaten • Adressdaten von Beschäftigten
hoch	2	• Sozialdaten • Gesundheitsdaten • Religionszugehörigkeit
sehr hoch	3	• Medizinische Daten lebenserhaltender Systeme • Identitätsdaten von verdeckten Ermittlern

Abb. 2: Schutzbedarf

Für eine differenzierte Betrachtung kann der Anhang A herangezogen werden.

Als Schutzziele sollten die im § 8 Abs. 2 HmbDSG festgeschriebenen Ziele definiert werden: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Revisionssicherheit. Ein Fragenkatalog zur differenzierten Bewertung ist im Anhang B enthalten. Der Fragenkatalog kann situationsabhängig angepasst und ergänzt werden.

Eine große Transparenz kann erzielt werden, wenn man den Schutzbedarf differenziert betrachtet und tabellarisch darstellt (Tab 1). Die Beteiligten können so das Ergebnis leichter nachvollziehen.

Bedrohtes Objekt	Wert der Vertraulichkeit	Wert der Integrität	Wert der Verfügbarkeit	Wert der Authentizität	Wert der Revisionsfähigkeit
1. Laptop mit gespeicherten Daten	2	2	1	2	2
2. ...					

Abb. 3: Ergebnis der Schutzbedarfsfeststellung (Beispiel)

2.3 Bedrohungsanalyse

Für die Bedrohungsanalyse werden die Fragestellungen beantwortet:

- **Welche Objekte werden bedroht ?**
- **Welchen Bedrohungen sind die Objekte ausgesetzt ?**

Bei der Bedrohungsanalyse werden die bereits vorhandenen Schutzmaßnahmen berücksichtigt. Das Ergebnis der Bedrohungsanalyse ist eine **vollständige Aufzählung aller möglicher Bedrohungen**, die einen Einfluss auf das zu erstellende Sicherheitskonzept haben. An dieser Stelle sollte die Vollständigkeit der Auflistung im Vordergrund stehen. Welche Bedeutung die einzelnen Bedrohungen für das Verfahren haben, ist Gegenstand der folgenden Stufe und ergibt sich z.T. auch erst aus der Gesamtschau der möglichen Bedrohungen. Die Bedrohungen können in unterschiedlichem Detaillierungsgrad dargestellt werden. Der zuvor festgestellte Schutzbedarf liefert dafür wichtige Hinweise. Bei einem hohen Schutzbedarf sollten die Bedrohungen differenziert dargestellt werden. Insbesondere neuartige Bedrohungen sollten ausführlich erläutert werden. Zum einen kann auf diese Weise eine gemeinsame Beurteilung durch alle Beteiligten leichter erzielt werden, da ein gleiches Verständnis der Sachlage geschaffen wird. Zum anderen können sich daraus später wichtige Hinweise für technische und organisatorische Schutzmaßnahmen ergeben.

Bedrohtes Objekt	Darstellung der Bedrohung	Bedrohtes Schutzziel
1. Laptop mit gespeicherten Daten	Diebstahl	Vertraulichkeit, Verfügbarkeit
2. Laptop mit gespeicherten Daten	Unberechtigter Zugriff z.B. bei Sitzungspausen	Vertraulichkeit, Integrität, Authentizität
3. ...		

Abb. 4: Ergebnis der Bedrohungsanalyse (Beispiel)

2.4 Risikobewertung

In der Risikobewertung werden der Schutzbedarf und die ermittelten Bedrohungen zusammengeführt und die Eintrittswahrscheinlichkeit möglicher Schäden bestimmt.

Es wird die Frage beantwortet:

- **Wie hoch ist der mögliche Schaden, der bei den einzelnen Objekten auftreten kann?**

Für die einzelnen bedrohten Objekte wird der Schaden jeweils durch den höchsten Wert einer Zeile aus Tab. 1 bestimmt. Es gilt das **Maximumprinzip**. Die größten negativen Auswirkungen bestimmen damit maßgeblich die Risikobewertung.

Ergänzend kann noch betrachtet werden, ob einzelne Objekte deutlich häufiger Bedrohungen ausgesetzt sind. Die höhere Eintrittswahrscheinlichkeit eines Schadens sollte dann dazu führen, für dieses Objekt stärkere Schutzmaßnahmen abzuleiten. Folgende Faktoren beeinflussen die Eintrittswahrscheinlichkeiten:

- der Nutzen, den Angreifer aus dem Angriff ziehen können; es sind materielle als auch immaterielle Werte in Betracht zu ziehen
- der Aufwand (zeitlich, finanziell, Ressourcen), der betrieben werden muss, um einen Angriff zu ermöglichen
- die notwendigen Kenntnisse, die für einen Angriff erforderlich sind
- die Gefahr für den Angreifer erkannt zu werden,
- die Schwere der Sanktionen für einen Angreifer,
- die Häufigkeit der Angriffsmöglichkeiten, z.B. die Häufigkeit der Datenübertragungen
- die Zugänglichkeit der einzelnen Komponenten des Verfahrens
- die Anzahl der Personen, die Zugang zum Verfahren haben oder sich Zugang verschaffen können.

Die Ergebnisse der Risikobewertung werden in einer Tabelle zusammengestellt:

Bedrohtes Objekt	**Darstellung der Bedrohung**	**Bedrohtes Schutzziel**	**Schutz-bedarf**	**technisch/ organisatorische Maßnahmen erforderlich?**
1. Laptop mit gespeicher-ten Daten	Diebstahl	Vertraulich-keit, Verfüg-barkeit	2	ja
2. Laptop mit gespeicher-ten Daten	Unberechtigter Zugriff z.B. bei Sitzungspausen	Vertraulich-keit, Integri-tät, Authen-tizität	2	Ja
3. ...				

Abb. 5: Ergebnis der Risikobewertung (Beispiel)

2.5 Ableitung von Schutzmaßnahmen

Für alle untragbaren Risiken müssen geeignete technische und organisatorische Maßnahmen getroffen werden, die Schadensauswirkungen so weit reduzieren, dass die Schwelle der tolerierten Risiken unterschritten wird. Die zusätzlich durchzuführenden Schutzmaßnahmen dürfen dabei nicht isoliert betrachtet werden. Es sind sowohl gegenseitige Abhängigkeiten als auch die Einbettung in den bestehenden technischen und organisatorischen Rahmen zu berücksichtigen. Die Kompatibilität der Einzelmaßnahmen muss gegeben sein. Auch organisatorische Abhängigkeiten wie z.B. die Widerspruchsfreiheit zu bestehenden Regeln und Betriebsvereinbarungen muss gewährleistet sein bzw. durch entsprechende Anpassungen hergestellt werden. Darüber hinaus sind auch personalbezogene Aspekte zu berücksichtigen; hier vor allem die Akzeptanz der Nutzer sowie ihre Qualifikation, damit die Maßnahmen in der Praxis auch greifen. Ggf. sind auch gezielte Fortbildungsmaßnahmen durchzuführen.

3 Vorabkontrolle

Die Daten verarbeitende Stelle hat vor jeder Entscheidung über die Einführung oder wesentlichen Änderung eines DV-Verfahrens, mit dem personenbezogene Daten verarbeitet werden, eine Risikoanalyse durchzuführen. Eine Vorabkontrolle durch die behördlichen Datenschutzbeauftragte bzw. den behördlichen Datenschutzbeauftragten oder, falls diese bzw. dieser nicht bestellt wurde, durch die Hamburgische Beauftragte bzw. den Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (HmbBfDI) findet im Anschluss an die Risikoanalyse immer dann statt, wenn die Risikoanalyse ergibt, dass von dem DV-Verfahren eine besondere Gefährdung für die Rechte der Betroffenen ausgeht. Eine besondere Gefährdung ist beispielsweise dann gegeben, wenn ein hoher Schutzbedarf und eine hohes Risiko bestehen oder wenn aus den Ergebnissen der Bearbeitung gravierende nachteilige Folgen für die Betroffenen gezogen werden sollen. Der bzw. dem HmbBfDI sind die Ergebnisse der Risikoanalyse und die Darstellung des Verfahrens mit den entsprechenden Begründungen in einer Form vorzulegen, die ohne weiteres eine Beurteilung ermöglicht.

Die Vorabkontrolle basiert auf den Konzepten des Verfahrens und der erstellten Risikoanalyse. Die Beschreibung des Verfahrens sollte die in § 9 Abs. 1 HmbDSG festgeschriebenen Punkte

umfassen. So wird Doppelarbeit vermieden, da eine solche Verfahrensbeschreibung vor der Einführung eines Verfahrens zu erstellen ist[1]. Die Verfahrensbeschreibung enthält:

- Namen und die Anschrift der Daten verarbeitenden Stelle
- Bezeichnung des Verfahrens und seine Zweckbestimmung
- Art der verarbeiteten Daten sowie die Rechtsgrundlage ihrer Verarbeitung oder die Ziele, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist
- Kreis der Betroffenen
- Empfängerinnen oder Empfänger oder Kreis der Empfängerinnen und Empfänger, die Daten erhalten können
- beabsichtigte Datenübermittlungen nach § 17 Abs. 2 und 3 HmbDSG an Stellen außerhalb der Europäischen Union oder an über- oder zwischenstaatliche Stellen
- Fristen für die Sperrung und Löschung der Daten
- technische und organisatorische Maßnahmen nach § 8 HmbDSG
- Art der Geräte, die Stellen, bei denen sie aufgestellt sind, sowie das Verfahren zur Übermittlung, Sperrung, Löschung, Auskunftserteilung und Benachrichtigung.

Erforderlich ist eine übersichtliche, strukturierte und aus sich heraus verständliche Aufbereitung der Unterlagen über das Verfahren. Im Rahmen der Vorabkontrolle können ggf. ergänzende Informationen aus einer Testinstallation bei der Daten verarbeitenden Stelle gewonnen werden. Auf dieser Informationsgrundlage kann eine schriftliche Stellungnahme gegenüber der Daten verarbeitenden Stelle abgegeben werden.

4 Quellen

- Der Hamburgische Datenschutzbeauftragte: Hamburgisches Datenschutzrecht 2001
- IT-Sicherheitshandbuch. BSI (Hrsg.) 1992
- IT-Grundschutzhandbuch. www.bsi.de
- Orientierungshilfe Internet. Der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern (Hrsg.)
- IT-Sicherheitskonzepte: Planung, Erstellung Umsetzung, Backup-Magazin Nr. 1, ULD, 2002

[1] Die Orientierung an der Verfahrensbeschreibung nach § 9 HmbDSG darf nicht so missverstanden werden, dass eine Risikoanalyse nur in den Fällen notwendig ist, in denen auch eine Verfahrensbeschreibung erfolgen muss. Eine Risikoanalyse ist auch für die in § 9 Abs. 2 HmbDSG genannten Verfahren notwendig.

Anhang A

Schadens-szenario	Schutzbedarf "normal"(1)	Schutzbedarf "hoch" (2)	Schutzbedarf "sehr hoch" (3)
1. Verstoß gegen Gesetze/ Vorschriften/ Verträge	• Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen	• Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen • Vertragsverletzungen mit erheblichen Haftungsschäden	• Fundamentaler Verstoß gegen Vorschriften und Gesetze • Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	• Eine Beeinträchtigung des informationellen Selbstbestimmungsrechts würde durch den Einzelnen als tolerabel eingeschätzt werden. • Ein möglicher Missbrauch personenbezogener Daten hat nur geringfügige Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen.	• Eine erhebliche Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. • Ein möglicher Missbrauch personenbezogener Daten hat erhebliche Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse des Betroffenen	• Eine besonders bedeutende Beeinträchtigung des informationellen Selbstbestimmungsrechts des Einzelnen erscheint möglich. • Ein möglicher Missbrauch personenbezogener Daten würde für den Betroffenen den gesellschaftlichen oder wirtschaftlichen Ruin bedeuten.
3. Beeinträchtigung der persönlichen Unversehrtheit	• Eine Beeinträchtigung erscheint nicht möglich.	• Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.	• Gravierende Beeinträchtigungen der persönlichen Unversehrtheit sind möglich. • Gefahr für Leib und Leben
4. Beeinträchtigung der Aufgabenerfüllung	• Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist größer als 24 Stunden.	• Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.	• Die Beeinträchtigung würde von allen Betroffenen als nicht tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Außenwirkung	• Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	• Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	• Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, evtl. sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	• Der finanzielle Schaden bleibt für die Institution tolerabel.	• Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.	• Der finanzielle Schaden ist für die Institution existenzbedrohend.

Anhang B

B. Schadenszenarien

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat Schadensszenarien beschrieben. Diese wurden entsprechend der im Hamburgischen Datenschutzgesetz niedergelegten Zielrichtungen technisch und organisatorischer Maßnahmen ergänzt.

B.1 Schadensszenario "Verstoß gegen Gesetze/Vorschriften/Verträge"

Beispiele für relevante Gesetze und Verordnungen sind:
Grundgesetz, Bürgerliches Gesetzbuch, Strafgesetzbuch, Bundesdatenschutzgesetz und Datenschutzgesetze der Länder, Sozialgesetzbuch, Handelsgesetzbuch, Personalvertretungsgesetz, Betriebsverfassungsgesetz, Urheberrechtsgesetz, Patentgesetz, Informations- und Kommunikationsdienstegesetz (IuKDG), Gesetz zur Kontrolle und Transparenz im Unternehmen(KonTraG),Telekommunikations-Überwachungsverordnung (TKÜV)

Beispiele für relevante Vorschriften sind:
Verwaltungsvorschriften und Dienstvorschriften.

Beispiele für Verträge:
Dienstleistungsverträge im Bereich Datenverarbeitung, Verträge zur Wahrung von Betriebsgeheimnissen.

Fragestellungen:

Verlustart	Fragestellung	Antwort
Verlust der Vertraulichkeit	Erfordern gesetzliche Auflagen die Vertraulichkeit der Daten?	
Verlust der Vertraulichkeit	Ist im Falle einer Veröffentlichung von Informationen mit Strafverfolgung oder Regressforderungen zu rechnen?	
Verlust der Vertraulichkeit	Sind Verträge einzuhalten, die die Wahrung der Vertraulichkeit bestimmter Informationen beinhalten?	
Verlust der Integrität	Erfordern gesetzliche Auflagen die Integrität der Daten?	
Verlust der Integrität	In welchem Maße wird durch einen Verlust der Integrität gegen Gesetze bzw. Vorschriften ver-	

	stoßen?	
Verlust der Verfügbarkeit	Sind bei Ausfall der IT-Anwendung Verstöße gegen Vorschriften oder sogar Gesetze die Folge? Wenn ja, in welchem Maße?	
Verlust der Verfügbarkeit	Schreiben Gesetze die dauernde Verfügbarkeit bestimmter Informationen vor?	
Verlust der Verfügbarkeit	Gibt es Termine, die bei Einsatz der IT-Anwendung zwingend einzuhalten sind?	
Verlust der Verfügbarkeit	Gibt es vertragliche Bindungen für bestimmte einzuhaltende Termine?	
Verlust der Authentizität	Erfordern gesetzliche Auflagen die Authentizität der Daten	
Verlust der Revisionssicherheit	Erfordern gesetzliche Auflagen die Revisionssicherheit der Daten	
Verlust der Revisionssicherheit	Ist der Zeitraum durch Gesetze Festgelegt, für die Revisionssicherheit zu gewährleisten ist?	

B.2 Schadensszenario "Beeinträchtigung des informationellen Selbstbestimmungsrechts"

Beispiele für die Beeinträchtigung des informationellen Selbstbestimmungsrechts sind:
Unzulässige Erhebung personenbezogener Daten ohne Rechtsgrundlage oder Einwilligung,
unbefugte Kenntnisnahme bei der Datenverarbeitung bzw. der Übermittlung von personenbezogenen Daten,
unbefugte Weitergabe personenbezogener Daten,
Nutzung von personenbezogenen Daten zu einem anderen, als dem bei der Erhebung zulässigen Zweck und
Verfälschung von personenbezogenen Daten in Ist-Systemen oder bei der Übertragung.

Die folgenden Fragen können zur Abschätzung möglicher Folgen und Schäden herangezogen werden:

Fragestellungen:

Verlustart	Fragestellung	Antwort
Verlust der Vertraulichkeit	Welche Schäden können für den Betroffenen entstehen, wenn seine personenbezogenen Daten nicht vertraulich behandelt werden?	
Verlust der Vertraulichkeit	Werden personenbezogene Daten für unzulässige Zwecke verarbeitet?	
Verlust der Vertraulichkeit	Ist es im Zuge einer zulässigen Verarbeitung personenbezogener Daten möglich, aus diesen Daten z. B. auf den Gesundheitszustand oder die wirtschaftliche Situation einer Person zu schließen?	
Verlust der Vertraulichkeit	Welche Schäden können durch den Missbrauch der gespeicherten personenbezogenen Daten entstehen?	
Verlust der Integrität	Welche Schäden würden für den Betroffenen entstehen, wenn seine personenbezogenen Daten unabsichtlich verfälscht oder absichtlich manipuliert würden?	
Verlust der Integrität	Wann würde der Verlust der Integrität personenbezogener Daten frühestens auffallen?	
Verlust der Verfügbarkeit	Können bei Ausfall der Ist-Anwendung oder bei einer Störung einer Datenübertragung personenbezogene Daten verloren gehen oder verfälscht werden, so dass der Betroffene in seiner gesellschaftlichen Stellung beeinträchtigt wird oder gar persönliche oder wirtschaftliche Nachteile zu befürchten hat?	
Verlust der Authentizität	Kann der Verlust der Authentizität zur Beeinträchtigung des informationellen Selbstbestimmungsrechts führen?	
Verlust der Revisionssicherheit	Kann der Verlust der Revisionssicherheit zur Beeinträchtigung des informationellen Selbstbestimmungsrechts füh-	

	ren?	

B.3 Schadensszenario "Beeinträchtigung der persönlichen Unversehrtheit"

Die Fehlfunktion eines Ist-Systems oder einer Ist-Anwendung kann unmittelbar die Verletzung, die Invalidität oder den Tod von Personen nach sich ziehen. Die Höhe des Schadens ist am direkten persönlichen Schaden zu messen.

Beispiele für solche Ist-Anwendungen und -Systeme sind:
medizinische Überwachungsrechner,
medizinische Diagnosesysteme,
Flugkontrollrechner und
Verkehrsleitsysteme.

Fragestellungen:

Verlustart	**Fragestellung**	**Antwort**
Verlust der Vertraulichkeit	Kann durch bekannt werden personenbezogener Daten eine Person physisch oder psychisch geschädigt werden?	
Verlust der Integrität	Können durch manipulierte Programmabläufe oder Daten Menschen gesundheitlich gefährdet werden?	
Verlust der Verfügbarkeit	Bedroht der Ausfall der IT-Anwendung oder des IT-Systems unmittelbar die persönliche Unversehrtheit von Personen?	
Verlust der Authentizität	Kann der Verlust der Authentizität zur Beeinträchtigung der persönlichen Unversehrtheit führen?	
Verlust der Revisionssicherheit	Kann der Verlust der Revisionssicherheit zur Beeinträchtigung der persönlichen Unversehrtheit führen?	

B.4 Schadensszenario "Beeinträchtigung der Aufgabenerfüllung"

Die Schwere des Schadens richtet sich nach der zeitlichen Dauer der Beeinträchtigung und nach dem Umfang der Einschränkungen der angebotenen Dienstleistungen.

Beispiele sind:
Fristversäumnisse durch verzögerte Bearbeitung von Verwaltungsvorgängen,
verspätete Lieferung aufgrund verzögerter Bearbeitung von Bestellungen,
fehlerhafte Produktion aufgrund falscher Steuerungsdaten und
unzureichende Qualitätssicherung durch Ausfall eines Testsystems.

Fragestellungen:

Verlustart	**Fragestellung**	**Antwort**
Verlust der Vertraulichkeit	Gibt es Daten, deren Vertraulichkeit die Grundlage für die Aufgabenerfüllung ist (z. B. Strafverfolgungsinformationen, Ermittlungsergebnisse)?	
Verlust der Integrität	Können Datenveränderungen die Aufgabenerfüllung dergestalt einschränken, dass die Institution handlungsunfähig wird?	
Verlust der Integrität	Entstehen erhebliche Schäden, wenn die Aufgaben trotz verfälschter Daten wahrgenommen werden? Wann werden unerlaubte Datenveränderungen frühestens erkannt?	
Verlust der Integrität	Können verfälschte Daten in der betrachteten IT-Anwendung zu Fehlern in anderen IT-Anwendungen führen?	
Verlust der Integrität	Welche Folgen entstehen, wenn Daten fälschlicherweise einer Person zugeordnet werden, die in Wirklichkeit diese Daten nicht erzeugt hat?	
Verlust der Verfügbarkeit	Kann durch den Ausfall der IT-Anwendung die Aufgabenerfüllung der Institution so stark beeinträchtigt werden, dass die Wartezeiten für die Betroffenen nicht mehr tolerabel sind?	
Verlust der Verfügbarkeit	Sind von dem Ausfall dieser IT-Anwendung andere IT-Anwendungen betroffen?	
Verlust der Verfügbarkeit	Ist es für die Institution bedeutsam, dass der Zugriff auf IT-Anwendungen nebst Programmen und Daten ständig gewährleistet ist?	
Verlust der Authentizität	Wird die Aufgabenerfüllung eingeschränkt, wenn die Authentizität nicht gegeben ist?	
Verlust der Revisionsfähigkeit	Können bestimmte aufgaben nicht erfüllt werden, wenn die Revisionsfähigkeit eingeschränkt ist?	

B.5 Schadensszenario "Negative Außenwirkung"

Beispiel:
Ansehensverlust einer Behörde bzw. eines Unternehmens,
Vertrauensverlust gegenüber einer Behörde bzw. einem Unternehmen,
Beeinträchtigung der wirtschaftlichen Beziehungen zusammenarbeitender Unternehmen,
verlorenes Vertrauen in die Arbeitsqualität einer Behörde bzw. eines Unternehmens und
Einbuße der Konkurrenzfähigkeit.
Die Höhe des Schadens orientiert sich an der Schwere des Vertrauensverlustes oder des Verbreitungsgrades der Außenwirkung.

Ursachen für diese Schäden können vielfältiger Natur sein:
Handlungsunfähigkeit einer Institution durch IT-Ausfall,
fehlerhafte Veröffentlichungen durch manipulierte Daten,
Fehlbestellungen durch mangelhafte Lagerhaltungsprogramme,
Nichteinhaltung von Verschwiegenheitserklärungen,
Weitergabe von Fahndungsdaten an interessierte Dritte und
Zuspielen vertraulicher Informationen an die Presse.

Fragestellungen:

Verlustart	Fragestellung	Antwort
Verlust der Vertraulichkeit	Welche Konsequenzen ergeben sich für die Institution durch die unerlaubte Veröffentlichung der für die IT-Anwendung gespeicherten schutzbedürftigen Daten?	
Verlust der Vertraulichkeit	Kann der Vertraulichkeitsverlust der gespeicherten Daten zu einer Schwächung der Wettbewerbsposition führen?	
Verlust der Vertraulichkeit	Entstehen bei Veröffentlichung von vertraulichen gespeicherten Daten Zweifel an der amtlichen Verschwiegenheit?	
Verlust der Vertraulichkeit	Können Veröffentlichungen von Daten zur politischen oder gesellschaftlichen Verunsicherung führen?	
Verlust der Integrität	Welche Schäden können sich durch die Verarbeitung, Verbreitung oder Übermittlung falscher oder unvollständiger Daten ergeben?	
Verlust der Integrität	Wird die Verfälschung von Daten öffentlich bekannt?	
Verlust der Integrität	Entstehen bei einer Veröffentlichung von verfälschten Daten Ansehensverluste?	
Verlust der Integrität	Können Veröffentlichungen von verfälschten Daten zur politischen oder gesellschaftlichen Verunsicherung führen?	

Verlust der Integrität	Können verfälschte Daten zu einer verminderten Produktqualität und damit zu einem Ansehensverlust führen?	
Verlust der Verfügbarkeit	Schränkt der Ausfall der IT-Anwendung die Informationsdienstleistungen für Externe ein?	
Verlust der Verfügbarkeit	Wird der (vorübergehende) Ausfall der IT-Anwendung extern bemerkt?	

B.5 Schadensszenario "Finanzielle Auswirkungen"

Beispiele :

unerlaubte Weitergabe von Forschungs- und Entwicklungsergebnissen,

Manipulation von finanzwirksamen Daten in einem Abrechnungssystem,

Ausfall eines IT-gesteuerten Produktionssystems und dadurch bedingte Umsatzverluste,

Einsichtnahme in Marketingstrategiepapiere oder Umsatzzahlen,

Ausfall eines Buchungssystems einer Reisegesellschaft,

Ausfall eines E-Commerce-Servers,

Zusammenbruch des Zahlungsverkehrs einer Bank,

Diebstahl oder Zerstörung von Hardware.

Die Höhe des Gesamtschadens setzt sich zusammen aus den direkt und indirekt entstehenden Kosten, etwa durch Sachschäden, Schadenersatzleistungen und Kosten für zusätzlichen Aufwand (z. B. Wiederherstellung).

Fragestellungen:

Verlustart	Fragestellung	Antwort
Verlust der Vertraulichkeit	Kann die Veröffentlichung vertraulicher Informationen Regressforderungen nach sich ziehen?	
Verlust der Vertraulichkeit	Gibt es in der IT-Anwendung Daten, aus deren Kenntnis ein Dritter (z. B. Konkurrenzunternehmen) finanzielle Vorteile ziehen kann?	
Verlust der Vertraulichkeit	Werden mit der IT-Anwendung Forschungsdaten gespeichert, die einen erheblichen Wert darstellen? Was passiert, wenn sie unerlaubt kopiert und weitergegeben werden?	
Verlust der Vertraulichkeit	Können durch vorzeitige Veröffentlichung von schutzbedürftigen Daten finanzielle Schäden entstehen?	
Verlust der Integrität	Können durch Datenmanipulationen finanzwirksame Daten so verändert werden, dass finanzielle Schäden entstehen?	
Verlust der Integrität	Kann die Veröffentlichung falscher Informationen Regressforderungen nach sich ziehen?	
Verlust der Integrität	Können durch verfälschte Bestelldaten finanzielle Schäden entstehen (z. B. bei Just-in-Time Produktion)?	
Verlust der Integrität	Können verfälschte Daten zu falschen Geschäftsentscheidungen führen?	
Verlust der Verfügbarkeit	Wird durch den Ausfall der IT-Anwendung die Produktion, die Lagerhaltung oder der Vertrieb beeinträchtigt?	
Verlust der Verfügbarkeit	Ergeben sich durch den Ausfall der IT-Anwendung finanzielle Verluste aufgrund von verzögerten Zahlungen bzw. Zinsverlusten?	

Verlust der Verfügbarkeit	Wie hoch sind die Reparatur- oder Wiederherstellungskosten bei Ausfall, Defekt, Zerstörung oder Diebstahl des IT-Systems?	
Verlust der Verfügbarkeit	Kann es durch Ausfall der IT-Anwendung zu mangelnder Zahlungsfähigkeit oder zu Konventionalstrafen kommen?	
Verlust der Verfügbarkeit	Wie viele wichtige Kunden wären durch den Ausfall der IT-Anwendung betroffen?	
Verlust der Authentizität	Entstehen Schäden, wenn die Authentizität nicht gewährleistet ist?	
Verlust der Revisionsfähigkeit	Können Regressforderungen aufgrund mangelnder Revisionsfähigkeit entstehen?	