BANKHAUS SCHEICH
WERTPAPIERSPEZIALIST AG

Datenschutzrichtlinie

Stand: 05.03.2024

Zuständigkeiten, Vertraulichkeitsstufe und Gültigkeitsbereich

Datum der Freigabe durch den Vorstand	06.03.2024
Fachlich verantwortlicher Bereich	Datenschutzbeauftragte
Einbezogene Fachbereiche	Compliance, Legal, ISB
Autoren	Hana Meyer
Vertraulichkeitsstufe	Intern
Gültigkeitsbereich	Bankhaus Scheich Wertpapierspezialist AG inkl. Filialen

Bekanntmachung

Datum der Bekanntmachung: 06.03.2024

Abkürzungsverzeichnis

Abkürzung	Beschreibung
BDSG	Bundesdatenschutzgesetz
BHS	Bankhaus Scheich Wertpapierspezialist AG
BSI	Bundesamt für Sicherheit in der Informations-technik
DSGVO	Datenschutzgrundverordnung; Richtlinie (EU) 2016/679
ErwGr	Erwägungsgrund
GoBD	Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form
ISB	Informationssicherheitsbeauftragter
NDA	Non-Disclosure Agreement
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
StGB	Strafgesetzbuch

Inhalt

1 Über diese Richtlinie

1.1 Zielsetzung

Das Bankhaus Scheich (BHS) verpflichtet sich im Rahmen seiner gesellschaftlichen Verantwortung zur Wahrung des Schutzes und der Sicherheit personenbezogener Daten. Mit der vorliegenden Datenschutzrichtlinie soll ein reibungsloser Betrieb des Unternehmensnetzwerkes sowie die Verhinderung von Datenmissbrauch gewährleistet werden.

Ziel dieser Richtlinie ist es, die Belegschaft für die Sicherstellung des Datenschutzes zu sensibilisieren und die ihnen hierfür erforderlichen Informationen an die Hand zu geben. Der gelebte Datenschutz ist die Basis für vertrauensvolle Geschäftsbeziehungen sowie ein gesundes Arbeitsverhältnis. Demgemäß legen wir großen Wert auf die Sicherheit der personenbezogenen Daten unserer Kunden und Mitarbeiter.

1.2 Geltungsbereich und Adressaten

Der Geltungsbereich dieser Richtlinie erstreckt sich auf alle Mitarbeiterinnen und Mitarbeiter des BHS inkl. Niederlassungen. Mitarbeiter im Sinne der nachfolgenden Bestimmungen sind alle Personen, die ein aktives Dienst-, Arbeits- oder Ausbildungsverhältnis mit BHS unterhalten. Hierzu zählen auch befristet tätige Arbeitnehmer sowie auch Zeitarbeitskräfte, studentische Aushilfen, Schüler, Praktikanten, freie Mitarbeiter und sonstige Externe. Als Mitarbeiter gelten auch die Mitglieder der Geschäftsleitung.

Diese Richtlinie gilt nicht nur für die Räumlichkeiten der BHS, sondern auch bei Telearbeit und an häuslichen Arbeitsplätzen und, soweit anwendbar, auch für externe Mitarbeiter, z. B. in Projektgruppen. Soweit erforderlich, ist für externe Mitarbeiter die Anwendung dieser Richtlinie durch geeignete Verpflichtungen oder vertragliche Regelungen sicherzustellen. Die Richtlinie gilt für jede Art von Hard- und Software sowie für alle im Unternehmen eingesetzten Datenverarbeitungsverfahren und mobile Datenträger einschließlich solcher, die für das Unternehmen von externen Stellen verwaltet werden.

Die Datenschutzrichtlinie regelt verbindlich für BHS und für alle bei BHS beschäftigten Mitarbeiter den sicheren Umgang mit Daten/Informationen, IT-Systemen, IT-Anwendungen und IT-basierten Abläufen. Verstöße gegen die Datenschutzrichtlinie sowie die sonstigen geltenden internen und externen Regelungen und Vorschriften bezüglich des Einsatzes der Informationstechnologie bzw. der ordnungsgemäßen und zuverlässigen Verarbeitung von Daten/Informationen können arbeitsrechtliche, haftungsrechtliche und ggf. strafrechtliche Konsequenzen haben.

1.3 Aktualisierung

Diese Richtlinie wird entsprechend unserer "Richtlinie zur Erstellung und Anpassung von Organisationsrichtlinien, Leitlinien und Arbeitsanweisungen" mindestens jährlich sowie anlassbezogen darauf hin überprüft, ob die Prozesse den aktuellen regulatorischen Vorgaben entsprechen und wenn

notwendig angepasst. Besonderes Augenmerk wird dabei auf die gegenwärtig sehr dynamische Regulierung des Geschäfts mit Kryptowerten gelegt.

1.4 Zentrale Ablage, Verbot der lokalen Speicherung

Diese Richtlinie wird in ihrer aktuellen Fassung unter dem Laufwerk “Organisationshandbuch” abgelegt. Lokale Speicherungen sind zu vermeiden, damit sichergestellt werden kann, dass keine veralteten Fassungen verwendet werden.

2 Grundlagen

Im folgenden Abschnitt erläutern wir die Grundlagen des Datenschutzes, wobei der Fokus insbesondere auf der DSGVO liegt. Wir bieten eine umfassende Übersicht über die Struktur und die zugrundeliegenden Prinzipien dieser Verordnung und legen dabei besondere Aufmerksamkeit auf die Bedeutung eines verantwortungsvollen Umgangs mit personenbezogenen Daten, um den rechtlichen Anforderungen und ethischen Verpflichtungen gerecht zu werden. Des Weiteren klärt dieser Abschnitt über die verschiedenen Rechte der Betroffenen auf und erläutert die Pflichten, die Unternehmen in Bezug auf Datensicherheit und -transparenz haben. Mit dieser Einführung soll sichergestellt werden, dass unsere Mitarbeiter ein klares Bild von der Art und Weise erhalten, wie personenbezogene Daten zu verarbeiten sind und wie unser Unternehmen Maßnahmen ergreift, um einen hohen Datenschutzstandard zu gewährleisten.

2.1 Datenschutz und Datensicherheit

Zweck des Datenschutzes ist es, den Einzelnen (z. B. Kunde, Mitarbeiter, Geschädigter) vor Beeinträchtigungen seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten zu schützen. Die Datenverarbeitungssysteme einschließlich der gesamten IT-Infrastruktur (Server, Netzwerke, Arbeitsplatz-PCs etc.) und der Datenbestände zählen zur unternehmenskritischen Infrastruktur. Der Schutz dieser Infrastruktur und der Datenbestände gegen Bedrohungen aller Art, z. B. durch Schadsoftware wie Computerviren, Trojaner etc., Spionage, Missbrauch und Fehlbedienung, ist für das Unternehmen von großer Bedeutung. Es ist deshalb für BHS von großer Wichtigkeit, den sicheren und sachgemäßen Umgang mit allen Arten von Informationstechnologie zu regeln und damit den Einzelnen sowie das Unternehmen vor Schaden zu schützen.

2.2 Begriffsbestimmungen

Dieser Datenschutzrichtlinie liegen die Begriffsbestimmungen des Art. 4 DSGVO zugrunde.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. (Name, Privatanschrift, E-Mail-Adresse usw.)

Besonders schutzwürdige personenbezogene Daten sind alle Informationen über die ethnische Herkunft, über religiöse oder weltanschauliche Überzeugungen, über die Gesundheit oder über die sexuelle Orientierung einer betroffenen Person.

Betroffener ist jede natürliche Person, über die personenbezogene Daten verarbeitet werden. (Mitarbeiter, Kunde oder Ansprechpartner)

Verarbeitungstätigkeit ist jeder Umgang mit personenbezogenen Daten. Eine Verarbeitungstätigkeit ist ein Bündel von Verarbeitungsschritten, das einem einheitlichen, übergeordneten Zweck dient. Hierunter fällt u.a. das Erfassen (z.B. per Formular, Software oder Kamera), Speichern (z.B. in einer Datenbank, Excel-Datei oder Personalakte), Ändern (z.B. Aktualisieren) und Übermitteln (z.B. an eine Behörde oder Unternehmen) von Daten.

2.3 Datenschutzrechtliche Grundsätze

Bei der Verarbeitung personenbezogener Daten haben alle Mitarbeiter die nachfolgend dargestellten Grundsätze gemäß Art. 5 DSGVO einzuhalten.

Rechtmäßigkeit und Transparenz: Personenbezogene Daten dürfen nur auf rechtmäßige Weise verarbeitet werden. Das heißt, für jede Datenverarbeitung muss eine Rechtsgrundlage bestehen. Weiterhin hat die Verarbeitung personenbezogener Daten auf nachvollziehbare Art und Weise zu geschehen. Betroffene müssen also über die Art und Auswirkung der Datenverarbeitung angemessen und nachvollziehbar informiert werden.

Treu und Glauben: Der Grundsatz der Verarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden. Unter diesem Gesichtspunkt sind insbesondere die Rechte der Betroffenen zu beachten und die Informationspflichten in verständlicher und nachvollziehbarer Form zu erfüllen.

Zweckbindung: Personenbezogene Daten dürfen nur für die Zwecke verarbeitet und genutzt werden, für die sie erhoben wurden und die dem Betroffenen auch als Erhebungszweck dargelegt worden sind. Für andere Zwecke werden die Daten nur genutzt, soweit dies nach den Vorschriften der DSGVO ausdrücklich zulässig ist. Bei einer Verarbeitung oder Nutzung für andere Zwecke (Zweckänderung) ist der Datenschutzbeauftragte zur Prüfung der Zulässigkeit der Zweckänderung einzuschalten oder alternativ eine weitere Einwilligung des Betroffenen einzuholen.

Datenminimierung: Daten dürfen nicht über das erforderliche Maß hinaus genutzt werden. Bei jeder Datenverarbeitung ist daher zu fragen, wofür und wie lange die Daten benötigt werden.

Speicherbegrenzung: Personenbezogene Daten müssen gelöscht werden, wenn Sie für den konkreten Nutzungszweck nicht mehr benötigt werden. Für alle Verarbeitungen sind deshalb Aufbewahrungs- und Löschfristen zu definieren und einzuhalten.

Richtigkeit: Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein.

Integrität und Vertraulichkeit: Personenbezogene Daten müssen vor unbefugter oder unrechtmäßiger Verarbeitung durch die Auswahl geeigneter technischer und organisatorischer Maßnahmen geschützt werden.

Pseudonymisierung: Soweit es der Zweck der Verarbeitung erlaubt, sind personenbezogene Daten in pseudonymisierter Form zu verarbeiten. Pseudonymisierung bedeutet, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer Person zugeordnet werden können. Die eigentlichen Daten und die Angaben, die eine Zuordnung zu einer Person erlauben werden also getrennt.

Rechenschaftspflicht: Der Grundsatz der Rechenschaftspflicht verlangt, dass die Einhaltung der o. g. Datenschutzgrundsätze nachgewiesen werden kann. Zur Erfüllung dieser Rechenschaftspflicht ist ein in sich stimmiges, systematisches und nachvollziehbares Datenschutzmanagement eingerichtet. Auf

der Grundlage der darüber geführten Datenschutzdokumentation ist eine Überprüfung der Einhaltung dieser Grundsätze durch Datenschutzprüfungen und Audits möglich. Die in diesem Datenschutzhandbuch zu diesem Zweck festgelegten Dokumentationen und Nachweise sind aktuell und vollständig zu führen.

2.4 Rechtsgrundlagen der Datenverarbeitung

Personenbezogene Daten dürfen nur verarbeitet oder an Dritte weitergegeben werden, wenn ein Erlaubnistatbestand nach Art. 6 DSGVO vorliegt. Im Folgenden werden die wichtigsten Rechtsgrundlagen dargestellt:

2.4.1 Einwilligung

Der Betroffene kann seine Einwilligung zur zweckbezogenen Verarbeitung oder Weitergabe erteilen. Hierfür müssen folgende Anforderungen erfüllt sein:

- Es muss eine unmissverständliche Erklärung vorliegen, mit der sich der Betroffene zur Verarbeitung seiner personenbezogenen Daten einverstanden zeigt,
- Die Einwilligung muss freiwillig erteilt worden sein,
- Die Einwilligung muss für den bestimmten Fall und in informierter Weise erteilt werden, d.h. es müssen das Unternehmen, die Daten und Nutzungszwecke genannt sein und
- Es muss auf die Widerrufbarkeit der Einwilligung hingewiesen werden.

Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Bei telefonischer Beratung kann die Einwilligung mündlich erteilt werden, jedoch muss die Erteilung anschließend dokumentiert werden.

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um die Einwilligung in verständlicher und leicht zugänglicher Sprache erfolgen. Der Betroffene muss über jede neue Art der Verarbeitung oder zu jedem einzelnen Zweck der Verarbeitung informiert werden und dieser einzeln zustimmen (Verkettungsverbot für Einwilligungen).

2.4.2 Datenverarbeitung aufgrund vertraglicher Beziehungen

Die Verarbeitung oder Weitergabe ist auch zulässig, soweit sie zur Begründung, Abwicklung, Beendigung oder Erfüllung eines bestehenden Vertrages erforderlich ist, etwa bei der Abfrage der Kontoverbindung von Mitarbeitern zur Auszahlung des Gehalts. Gleiches gilt für solche Verarbeitungsvorgänge die zur Durchführung vorvertraglicher Maßnahmen erforderlich sind, etwa in Fällen von Anfragen zu unseren Produkten oder Leistungen.

2.4.3 Rechtliche Verpflichtung

Eine Verarbeitung oder Weitergabe von personenbezogenen Daten kann auch dann erforderlich werden, wenn das Unternehmen einer rechtlichen Verpflichtung wie beispielsweise der Erfüllung steuerlicher Pflichten, unterliegt.

2.5 Rollen, Aufgaben und Verantwortlichkeiten

Der Datenschutz ist nicht nur eine gesetzliche Anforderung, sondern auch ein wichtiger Bestandteil unserer Unternehmenskultur. Die verschiedenen Rollen von der Geschäftsleitung bis zu den einzelnen Mitarbeitern sind hierbei zentral, um ein umfassendes Datenschutzkonzept erfolgreich umzusetzen.

2.5.1 Geschäftsleitung

Der Geschäftsleitung obliegt die Verantwortung für alle Datenverarbeitungsprozesse und -verfahren, IT-Systeme sowie Anwendungssysteme innerhalb des Unternehmens. Sie muss jederzeit sicherstellen und nachweisen, dass die Bestimmungen dieser Richtlinie und die gesetzlichen Datenschutzanforderungen von ihren Mitarbeitern eingehalten werden.

2.5.2 Datenschutzbeauftragter

Der Datenschutzbeauftragte hat zur Aufgabe, die Vorgaben der DSGVO umzusetzen und Datenschutzverletzungen zu verhindern. Er fungiert dabei als Vermittler zwischen Unternehmen, Betroffenen und Aufsichtsbehörden. In Kürze sind seine Aufgaben dargestellt:

- Der Datenschutzbeauftragte hat über einschlägige datenschutzrelevante Vorschriften und Vorgänge zu informieren und hat Mittel zur Behandlung bestehender datenschutzrechtlicher Probleme vorzuschlagen.
- Der Datenschutzbeauftragte kontrolliert die Einhaltung des einschlägigen nationalen und europäischen Datenschutzrechts sowie der Arbeitsanweisungen bzw. Richtlinien von BHS.
- Dem Datenschutzbeauftragten obliegt die Überwachung, dass ausreichend Sensibilisierungen und Schulungen zum Thema Datenschutz stattfinden.
- Der Datenschutzbeauftragte ist ausdrücklich zur Zusammenarbeit mit der Aufsichtsbehörde verpflichtet.

An unsere Datenschutzbeauftragte kann sich jederzeit mit Beschwerden, Auskunftsersuchen und sonstigen datenschutzrechtlichen Anliegen gewendet werden. Sie kann wie folgt erreicht werden:

E-Mail: Datenschutz@Bankhaus-Scheich.de
Telefonnummer: +49 69 348 79 66 771

2.5.3 Verarbeitungs-Verantwortlicher

Verarbeitungs-Verantwortlicher ist, wer im Unternehmen für ein Verfahren oder ein Projekt, bei dem personenbezogene Daten verarbeitet werden, fachlich verantwortlich ist. Er oder sie hat

- bei der Planung, Einführung und Änderung von Verarbeitungstätigkeiten das Formular für den Eintrag ins Verzeichnis der Verarbeitungstätigkeiten auszufüllen (**Anlage 4**),
- den Betroffenen darzulegen, wie mit ihren Daten umgegangen wird,
- bei der Datenverarbeitung die Einhaltung der Datenschutzgrundsätze sicherzustellen,
- ggf. Datenschutzfolgenabschätzungen durchzuführen und
- alle Datenschutz-Maßnahmen zu Nachweiszwecken transparent zu dokumentieren.

2.5.4 Jeder Mitarbeiter

Jeder Mitarbeiter ist beim Umgang mit personenbezogenen Daten dafür verantwortlich,

- den Datenschutzbeauftragten einzubinden und zu unterstützen,
- bei der Verarbeitung die Datenschutzgrundsätze zu beachten und
- Datenschutzpannen intern und umgehend zu melden.

Jeder Mitarbeiter kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen zum Datenschutz oder der Datensicherheit an den Datenschutzbeauftragten oder den IT-Koordinator wenden.

Anfragen und Beschwerden werden vertraulich behandelt. Die Entscheidungen des Datenschutzbeauftragten zur Abhilfe der Datenschutzverletzung sind durch die Geschäftsleitung zu berücksichtigen. Anfragen von Aufsichtsbehörden und Betroffenen sind immer dem Datenschutzbeauftragten zur Kenntnis zu bringen.

2.6 Vertraulichkeit der Datenverarbeitung

Wie aus dem vorherigen Kapitel hervorgeht, unterliegen alle Beschäftigten der Pflicht den Datenschutz einzuhalten („Datengeheimnis“). Eine unbefugte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist den Beschäftigten untersagt. Unbefugt handelt ein Mitarbeiter, wenn er personenbezogene Daten verarbeitet, ohne dazu zur Erfüllung seiner Tätigkeit beauftragt, angewiesen oder berechtigt zu sein. Die Verpflichtung gilt auch für andere Mitarbeiter, die unbeaufsichtigt in Räumen tätig sind, in denen personenbezogene Daten zugänglich sind. Verpflichtet werden auch Praktikanten, Werkstudenten, Teilzeitkräfte und sonstige externe Mitarbeiter, wenn sie im Rahmen ihrer Tätigkeiten personenbezogene Daten zur Kenntnis nehmen können.

Um ein hohes Maß an Vertraulichkeit zu gewährleisten, darf den Beschäftigten Zugang zu personenbezogenen Daten nur in dem Umfang eingeräumt werden, der konkret zur Erfüllung ihrer Tätigkeiten notwendig ist („Need-to-know-Prinzip“). Es ist ein detailliertes und vollständiges Berechtigungskonzept zu etablieren und sorgfältig zu pflegen, durch das die Beschäftigten entsprechend ihrer Rollen und Zuständigkeiten mit festgelegten Zugangsberechtigungen ausstattet sind.

2.6.1 Verpflichtungserklärung

Vor dem Hintergrund der obigen Ausführungen, müssen sich alle Beschäftigten, die Zugriff auf personenbezogene Daten haben, zur Vertraulichkeit und auf die Einhaltung der Grundsätze der DSGVO verpflichten. Dabei ist zu versichern, dass die im Rahmen der Tätigkeit erlangten personenbezogene Daten nicht für private oder wirtschaftliche Interessen genutzt, an Unbefugte weitergeleitet oder in sonstiger Weise zugänglich gemacht werden. Diese Pflicht besteht über das Ende des Beschäftigungsverhältnisses hinaus.

Die Verpflichtung erfolgt durch Unterzeichnung einer entsprechenden Erklärung. Die Datenschutz-Verpflichtung ist bei allen betroffenen Mitarbeitern und Dritten nach Inkrafttreten dieser Richtlinie einzuholen und sodann regelmäßig, spätestens alle 36 Monate, zu erneuern. Bei neu eingestellten Beschäftigten ist die Verpflichtung erstmals zusammen mit Unterzeichnung des Arbeitsvertrags einzuholen, bei Externen im Zusammenhang mit deren Beauftragung (**Anlage 5**).

2.6.2 Schulungen

Um ein hohes Datenschutzniveau im Unternehmen aufrechtzuerhalten, sind diejenigen Mitarbeiter im erforderlichen Umfang über datenschutzrechtliche Anforderungen fortzubilden, die regelmäßig oder fortlaufend personenbezogene Daten verarbeiten oder Zugang zu solchen haben. Verantwortlich für die Durchführung und die Dokumentation der Schulungen zum Datenschutz ist der Datenschutzbeauftragte. Dieser erstellt einen Schulungsplan und legt darin folgendes fest:

- nächste Schulung,
- Periodizität der Schulung,
- Art der Schulung (z.B. Online-Schulung oder Präsenzschulung),
- Schulungsinhalte (z.B. Basisschulung, IT-Sicherheit, Betroffenenrechte) und
- Stärkung des Bewusstseins für den Datenschutz (z.B. Fragerunden, Aushänge)

2.7 Betroffenenrechte

Jedem Betroffenen stehen sogenannte Betroffenenrechte zu. Möchte ein Betroffener eines seiner Betroffenenrechte geltend machen, so hat dieser das Anliegen unverzüglich an den Datenschutzbeauftragten zu übermitteln. Das Anliegen ist umgehend von der verantwortlichen Stelle zu bearbeiten und darf dem Betroffenen nicht zum Nachteil gereichen. Die durchgeführte Maßnahme ist dem Betroffenen innerhalb eines Monats anzuzeigen und zu dokumentieren. Der Prozessgang äußert sich folglich in drei Schritten:

1. Schritt: Das Anliegen und die Identität des Betroffenen werden geprüft.
2. Schritt: Erforderliche Informationen werden von den fachlichen Verantwortlichen eingeholt.
3. Schritt: Dem Betroffenen wird geantwortet.

Die einschlägigen Betroffenenrechte sind nachstehend aufgelistet: Garantierte Bonuszahlungen

2.7.1 Recht auf Auskunft

Betroffene können vom Unternehmen Auskunft verlangen, ob das Unternehmen über sie personenbezogene Daten verarbeitet und wenn dies der Fall ist,

- welche Datenkategorien für welche Zwecke verarbeitet werden,
- woher die Daten stammen,
- wem die Daten offengelegt werden,
- wie lange die Daten gespeichert werden und
- ob eine automatisierte Einzelentscheidung bzw. ein Profiling stattfindet.

Das Unternehmen hat dem Betroffenen auf Verlangen eine Kopie aller personenbezogenen Daten zur Verfügung zu stellen, die das Unternehmen über ihn oder sie verarbeitet. Die Auskunft ist binnen einer Frist von vier Wochen zu erteilen. Sofern das Auskunftsersuchen nicht elektronisch erfolgt ist, ist dem Betroffenen die Auskunft schriftlich zu erteilen. Stellt der Betroffene den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen.

2.7.2 Recht auf Berichtigung

Betroffene können verlangen, dass das Unternehmen unrichtige personenbezogene Daten unverzüglich berichtigt und unvollständige personenbezogene Daten ergänzt.

2.7.3 Recht auf Löschung bzw. „Vergessenwerden“

Der Betroffene hat einen Anspruch auf unverzügliche Löschung der ihn betreffenden personenbezogenen Daten, sofern einer der folgenden Löschungsgründe einschlägig ist (nicht abschließend):

- Der Zweck der Datenverarbeitung besteht nicht oder nicht mehr.
- Eine Rechtsgrundlage für die Datenverarbeitung fehlt oder ist weggefallen, da der Betroffene seine Einwilligung widerrufen hat.
- Der Betroffene widerspricht der Datenverarbeitung und es liegen keine berechtigten Gründe für die Verarbeitung vor.

Sofern personenbezogene Daten öffentlich bekannt gemacht wurden und BHS als Verantwortlicher zur Löschung der personenbezogenen Daten verpflichtet ist, trifft das Unternehmen unter Berücksichtigung der verfügbaren Technologien und Implementierungskosten angemessene Maßnahmen, um die Löschung durchzuführen. Hierfür werden andere für die Datenverarbeitung Verantwortliche, die die veröffentlichten personenbezogenen Daten verarbeiten, darüber in Kenntnis gesetzt, dass die betroffene Person von diesen die Löschung sämtlicher Links zu den personenbezogenen Daten sowie Kopien oder Replikationen verlangt hat.

2.7.4 Recht auf Einschränkung der Verarbeitung

Der Betroffene hat das Recht auf Einschränkung der Verarbeitung der ihn betreffenden personenbezogenen Daten, sofern einer der folgenden Gründe einschlägig ist:

- Der Betroffene bestreitet die Richtigkeit der personenbezogenen Daten. Eine Einschränkung erfolgt für den Zeitraum, in dem der Verantwortliche die Richtigkeit überprüft.

- Die Datenverarbeitung ist unrechtmäßig, jedoch verlangt der Betroffene die Nutzungseinschränkung anstelle einer Löschung der personenbezogenen Daten.

- Die personenbezogenen Daten werden vom Verantwortlichen für die Zwecke der Verarbeitung nicht mehr benötigt, die betroffene Person benötigt sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

- Der Betroffene hat gegen die Verarbeitung Widerspruch eingelegt. Eine Einschränkung erfolgt für den Zeitraum, in dem der Verantwortliche den Widerspruch überprüft.

Nach einer wirksamen Einschränkung der Verarbeitung dürfen die betreffenden personenbezogenen Daten nur mit Einwilligung des Betroffenen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutze Rechte anderer verarbeitet werden. Der Betroffene ist über die Aufhebung der Einschränkung zu informieren.

2.7.5 Recht auf Datenübertragbarkeit

Sofern die Datenverarbeitung auf einer Einwilligung beruht oder zur Durchführung eines Vertrages erforderlich war, hat der Betroffene das Recht, die ihn betreffenden personenbezogenen Daten an einen anderen Verantwortlichen zu übermitteln, soweit dies technisch möglich ist.

2.7.6 Recht auf Widerspruch

Der Betroffene hat jederzeit das Recht gegen die Datenverarbeitung Widerspruch einzulegen, die auf einer Einwilligung beruht oder zur Wahrung berechtigter Interessen erforderlich ist. Dafür muss das Ergebnis einer Abwägung ergeben, dass das aufgrund einer besonderen Situation ergebende, schutzwürdige Interesse des Betroffenen das Interesse des Unternehmens an der Verarbeitung überwiegt. Ein Widerspruchsrecht besteht nicht, wenn die Verarbeitung der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen dient.

2.8 Verzeichnis für Verarbeitungstätigkeiten (VVT)

BHS ist kraft Gesetzes dazu verpflichtet, alle Verarbeitungstätigkeiten in einem Verzeichnis zu dokumentieren, Art. 30 DSGVO. Die Verantwortung für die Eintragungen und die Vollständigkeit des Verfahrensverzeichnisses liegt bei den Fachabteilungen (Informationseigentümern).

Das Verzeichnis muss folgende Angaben beinhalten:

- den Namen und die Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten,
- die Zwecke der Verarbeitung,
- eine Beschreibung der Kategorien betroffener Personen und der personenbezogenen Daten,

- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden,
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland,
- wenn möglich, die vorgesehenen Fristen für die Löschung der Datenkategorien und
- wenn möglich, eine Beschreibung der technischen und organisatorischen Maßnahmen.

Zur Aufnahme der Verfahren in das Verzeichnis der Verarbeitungstätigkeiten ist der Datenschutzbeauftragte rechtzeitig vor Einführung von neuen Verfahren zu unterrichten. Dies gilt auch bei datenschutzrelevanten Änderungen an bestehenden Verfahren, z.B. bei einer Änderung des Datenkatalogs, zusätzlichen Übermittlungen oder Nutzungen oder Änderung des Verarbeitungsverfahrens.

Bei der Erfassung von Verarbeitungstätigkeiten ist zu beachten, dass eine zu feingliedrige Aufteilung zu Unübersichtlichkeit führt, während eine zu grobgliedrige Aufteilung keine sinnvolle Prüfung der Datenschutzkonformität erlaubt. Es bietet sich daher eine Orientierung an bestehenden Geschäftsprozessen oder Aufgabenbereichen an. Die Abgrenzung kann auch anhand der technischen Systeme erfolgen, die der Verarbeitungstätigkeit zugrunde liegen. Fällt jedoch eine Verarbeitungstätigkeit in die Verantwortlichkeit mehrerer Fachbereiche, kann eine Aufteilung sinnvoll sein.

2.8.1 Regelprüfung

Der Verarbeitungs-Verantwortliche nimmt in regelmäßigen Abständen sowie anlassbezogen eine Regelprüfung der Verarbeitungstätigkeiten vor. Das Intervall der Regelprüfung beträgt:

- bei Risikoklassifizierung „niedrig“: 36 Monate
- bei Risikoklassifizierung „mittel“: 24 Monate
- bei Risikoklassifizierung „hoch“: 12 Monate.

Im Rahmen der Regelprüfung prüft der Verarbeitungs-Verantwortliche, ob der jeweilige Eintrag im Verzeichnis noch aktuell ist, und ob die getroffenen Maßnahmen wirksam und ausreichend sind. Erforderlichenfalls aktualisiert er die Datenschutz-Dokumentation.

2.8.2 Änderung, Beendigung und Abschluss von Verarbeitungstätigkeiten

Die Änderung, Beendigung oder der Abschluss einer Verarbeitungstätigkeit ist vom Verarbeitungs-Verantwortlichen zu dokumentieren. Hierfür vermerkt er im Verzeichnis der Verarbeitungstätigkeit das Datum der letzten Änderung fest und unterzeichnet das Dokument.

- Eine wesentliche Änderung liegt vor, wenn die bisherige Dokumentation unvollständig oder unzutreffend ist.
- Eine Beendigung liegt vor, wenn Daten nur noch zu Zwecken der Einhaltung von Aufbewahrungspflichten verarbeitet werden.
- Ein Abschluss liegt vor, wenn im Rahmen der Verarbeitungstätigkeit keinerlei Daten mehr verarbeitet werden.

Die Datenschutz-Dokumentation samt begleitender Unterlagen ist für weitere drei Jahre ab Abschluss der Verarbeitungstätigkeit aufzubewahren. Hierbei ist folgendes zu beachten:

- Änderungen sind mit Datum und Verfasser kenntlich zu machen,
- Altfassungen müssen abrufbar bleiben und
- Änderungen sind dem Datenschutz-Manager mitzuteilen.

2.9 Auftragsverarbeitung durch Dienstleister

Werden personenbezogene Daten durch Dienstleister im Auftrag des Unternehmens verarbeitet stellt der Verarbeitungs-Verantwortliche sicher, dass mit dem Dienstleister die erforderlichen Datenschutz-Vereinbarungen geschlossen und die Dienstleister ausreichend überprüft werden.

2.9.1 Vorliegen einer Auftragsverarbeitung

Eine Auftragsverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird.

2.9.2 Prüfung der Dienstleister

Bevor ein Auftragsverarbeiter eingeschaltet wird, ist dieser daraufhin zu prüfen, ob er die Bestimmungen der DSGVO einhalten. Die Prüfung ist vom Verarbeitungs-Verantwortlichen zu veranlassen und erfolgt durch den Datenschutzbeauftragten. Die nachstehenden Aspekte sind zu prüfen:

- Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen,
- Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren,
- Die bereitgestellten Vertragsstandards müssen beachtet werden,
- Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.

Der Datenschutzbeauftragte dokumentiert Inhalt und Ergebnis der Prüfung. Der Datenschutzbeauftragte wiederholt die Prüfung regelmäßig, in der Regel alle 24 Monate. Wurde das Risiko für die der Auftragsverarbeitung zu Grunde liegenden Verarbeitungstätigkeit mit „hoch“ klassifiziert, erfolgt die Prüfung in der Regel alle 12 Monate, wurde sie mit „niedrig“ klassifiziert alle 36 Monate.

2.9.3 Verträge mit Dienstleistern

Bevor Verarbeitungsleistungen von Auftragsverarbeitern in Anspruch genommen werden ist mit diesen ein Vertrag zur Auftragsverarbeitung zu schließen, der den Anforderungen des Art. 28 DSGVO

genügt. Bei der vertraglichen Ausgestaltung einer Auftragsverarbeitung sind in jedem Fall die folgenden Fragen zu reflektieren:

- Zu welchem Zweck werden die Daten verarbeitet?
- Wie lange werden die Daten gespeichert?
- Welche Daten werden genutzt?
- An wen werden die Daten weitergegeben?

Wird ein Vertragsmuster des Auftragsverarbeiters verwendet, bedarf die finale Fassung der Freigabe durch den Datenschutzbeauftragten

3 Risikomanagement

Im folgenden Abschnitt konzentrieren wir uns auf die datenschutzrechtliche Risikobewertung. Wir bieten eine umfassende Übersicht über die Struktur und die zugrunde liegenden Prozesse unseres Risikomanagementansatzes und legen dabei das Hauptaugenmerk auf die Bedeutung der regelmäßigen Prüfung und Überwachung datenschutzrelevanter Vorgänge. Diese Maßnahmen sind essentiell, um den rechtlichen Anforderungen und ethischen Verpflichtungen im Datenschutz gerecht zu werden.

Des Weiteren klärt dieser Abschnitt über spezielle Bewertungsmethoden wie die Datenschutzfolgenabschätzung auf. Diese ist insbesondere bei neuen Projekten oder Änderungen in der Datenverarbeitung notwendig und hilft, potenzielle Risiken frühzeitig zu erkennen und zu minimieren. Darüber hinaus gehen wir auf das Vorgehen bei Datenschutzvorfällen ein, einschließlich der Meldepflichten und der Kommunikation mit den betroffenen Personen.

3.1 Allgemeine Prüfung

Das Unternehmen hat jederzeit den Schutz von personenbezogenen Daten vor unbefugten Zugriff, unrechtmäßiger Verarbeitung oder unberechtigtem Verlust sicherzustellen. Jede Datenverarbeitung ist darauf zu überprüfen, welche Risiken sie für den Betroffenen mit sich bringt.

3.1.1 Identifizierung personenbezogener Daten und beteiligter Parteien

Zunächst wird im Rahmen einer Identifizierungsphase festgestellt, welche personenbezogenen Daten im Unternehmen erhoben werden. Diese Phase ist in drei nachfolgend erläuterte Schritte gegliedert. Ist die Identifizierungsphase abgeschlossen, werden entsprechende Listen erstellt, die alle IT-Systeme, Datenbanken, Software-Anwendungen, Verarbeitungstätigkeiten und Prozesse des Unternehmens erfassen.

Schritt 1: Identifizierung der datenverarbeitenden Einheiten

Im ersten Schritt werden alle Abteilungen und die dazugehörigen Mitarbeiter, die an der Datenverarbeitung beteiligt sind, identifiziert und untergliedert. Zum Beispiel: IT-Abteilung, Personalwesen, Geschäftsleitung und Sales-Team.

Da eine Datenverarbeitung grundsätzlich in jeder Einheit stattfindet, ist hier das aktuelle Organigramm des Unternehmens zugrunde zu legen.

Schritt 2: Systematisierung der Daten

Im zweiten Schritt werden die verschiedenen Arten von Daten systematisiert, die in den jeweiligen Abteilungen verarbeitet und verwaltet werden. Dabei werden bspw. folgende Kategorien verwendet: Kundendaten, Finanzdaten, Personaldaten und rechtliche Dokumente. Während dieser Identifizierungsphase werden Interviews mit den beteiligten Parteien geführt, um Informationen über die Datenflüsse in ihrer Abteilung und ihre Rolle bei der Datenverarbeitung zu erhalten. Dabei sind mindestens die folgenden Punkte abzufragen:

- die Art der Daten, die gespeichert und erfasst werden sollen
- die zugrunde liegenden Technologien
- die Quellen, aus denen die Daten stammen
- die Dauer der Aufbewahrung bzw. Speicherung der Daten
- die Verantwortlichkeiten und Rechte der Personen, die auf die Daten zugreifen dürfen
- das Verfahren zur Sicherung der Daten

Schritt 3: Risikobeurteilung

Im Anschluss werden alle gesammelten Informationen daraufhin analysiert, ob sensible personenbezogene Daten verarbeitet werden.

Dies schließt auch eine Risikobewertung der Verarbeitungstätigkeiten und deren Dokumentation ein. Dabei ist festzustellen, ob es sich um besonders sensible personenbezogene Daten handelt oder ob es ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen gibt. Hierdurch sollen potenzielle Schwachstellen aufgedeckt werden, etwa unangemessene Zugriffsrechte, fehlende Sicherheitsvorkehrungen oder Verstöße gegen die Datenschutzrichtlinien. Um beurteilen zu können, welches Schutzniveau erforderlich ist, werden die Daten der einzelnen Datenverarbeitungsverfahren nach dem Grad ihrer datenschutzrechtlichen und betriebswirtschaftlichen Sensibilität beurteilt:

- Die **datenschutzrechtliche Sensibilität** der personenbezogenen Daten beurteilt sich danach, inwieweit der Betroffene bei einer Datenschutzverletzung in seinen Persönlichkeitsrechten oder seinem persönlichen oder wirtschaftlichen Ansehen verletzt oder eingeschränkt ist bzw. verletzt oder eingeschränkt werden kann.
- Die **betriebswirtschaftliche Sensibilität** der Daten beurteilt sich am Ausmaß der möglichen Störungen der Betriebsabläufe, der betrieblichen Erwerbstätigkeit oder der Beeinträchtigung des Ansehens des Unternehmens in der Öffentlichkeit, bei den Beschäftigten, den Kunden oder Geschäftspartnern, wenn die erforderlichen Daten nicht oder nicht rechtzeitig zur Verfügung stehen, nicht richtig sind oder in unbefugte Hände geraten.

3.1.2 Risikobeurteilung

Voraussetzung einer Risikobeurteilung ist eine konkrete Beschreibung des zugrunde gelegten Sachverhalts, für den das Risiko abgeschätzt werden soll. Zur Risikobeurteilung sind die im Folgenden beschriebenen Phasen zu durchlaufen:

1. Risikoidentifikation
2. Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden
3. Zuordnung zu Risikoabstufungen

Zur Identifikation von Datenschutzrisiken sind insbesondere die folgenden Fragen zu beantworten:

- Welche Schäden können für Personen aufgrund der zu verarbeitenden Daten entstehen?
- Durch welche Ereignisse kann es zu dem Schaden kommen?

- Durch welche Handlungen und Umstände kann es zum Eintritt dieser Ereignisse kommen?

Schäden können physischer, materieller oder immaterieller Natur sein und sind nicht auf monetär bezifferbare Schäden begrenzt. Es müssen die negativen Folgen der geplanten Verarbeitung selbst betrachtet werden. Dazu gehören auch Einschränkungen von Rechten und Freiheiten, beispielsweise wenn betroffene Personen aus Angst vor Nachteilen auf die Ausübung ihrer Rechte verzichten. Auch negative Folgen von Abweichungen von der geplanten Verarbeitung müssen betrachtet werden (z.B. Datenzugang durch unbefugte Personen oder Stellen, unbefugte Offenlegung oder Verknüpfung von Daten oder zufällige Vernichtung von Daten). Die Abweichungen können zu einer unrechtmäßigen oder einer die Datenschutzgrundsätze verletzenden Verarbeitung führen.

Durch jede Verarbeitung personenbezogener Daten erfolgt mindestens eine Beeinträchtigung des Grundrechts auf Schutz personenbezogener Daten. Daneben können weitere Grundrechte betroffen sein, wie z.B. die Achtung des Familienlebens oder das Recht auf Nichtdiskriminierung. Diese Beeinträchtigungen führen zu Schäden, wenn Sie nicht gerechtfertigt sind. Letztlich müssen alle denkbaren negativen Folgen der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen, ihre wirtschaftlichen, finanziellen und immateriellen Interessen, ihren Zugang zu Gütern oder Dienstleistungen, für ihr berufliches und gesellschaftliches Ansehen, für ihren gesundheitlichen Zustand und für alle ihre sonstigen legitimen Interessen betrachtet werden. Beispiele möglicher Schäden sind unter anderem:

- Diskriminierung
- Identitätsdiebstahl oder -betrug
- finanzieller Verlust
- Rufschädigung
- wirtschaftliche oder gesellschaftliche Nachteile
- Erschwerung der Rechtsausübung
- Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten
- Profilerstellung oder -nutzung durch Bewertung persönlicher Aspekte
- körperliche Schäden infolge von Handlungen auf der Grundlage fehlerhafter oder offengelegter Daten

Für jeden bereits identifizierten möglichen Schaden werden die Ereignisse ermittelt, die zu seiner Verwirklichung führen können. Diese bestehen in der Nichteinhaltung der Datenschutzgrundsätze Art. 5 Abs. 1 DSGVO sowie der Nichtgewährung der Betroffenenrechte nach Art. 12 ff DSGVO, insbesondere:

- Unbefugte oder unrechtmäßige Verarbeitung
- Verarbeitung wider Treu und Glauben
- Für den Betroffenen intransparente Verarbeitung
- Unbefugte Offenlegung von und Zugang zu Daten
- Unbeabsichtigter Verlust, Zerstörung oder Schädigung von Daten
- Verweigerung der Betroffenenrechte
- Verwendung der Daten durch den Verantwortlichen zu inkompatiblen Zwecken
- Verarbeitung nicht vorhergesehener oder richtiger Daten
- Verarbeitung über die Speicherfrist hinaus

Bei Schäden, die sich aus der Verarbeitung selbst ergeben, besteht das Ereignis in eben dieser Verarbeitung.

3.1.3 Risikoquellen

Ein relevanter Teil der Risikoquellen ist dem Bereich des Verantwortlichen oder Auftragsverarbeiters und der von diesen plangemäß durchgeführten Verarbeitungen zuzuordnen.

Dabei ist auch in Betracht zu ziehen, inwieweit Personen im Bereich des Verantwortlichen oder etwaiger Auftragsverarbeiter bewusst oder unbeabsichtigt den für die Verarbeitung vorgesehenen Rahmen überschreiten könnten (z.B. eine Vertriebsabteilung, die die Zweckbindung von Kundendaten ändern könnte, etwa um eine Zielvorgabe zum Umsatz zu erfüllen). Ein weiteres Beispiel sind Beschäftigte, die vorsätzlich gegen Anweisungen zum Umgang mit personenbezogenen Daten verstoßen oder vorsätzlich in Verfolgung eigener Interessen unbefugt handeln.

Weiter sind Risiken durch unbefugte Angreifer wie Cyberkriminelle zu berücksichtigen. Risikoquellen können ggf. auch staatliche Stellen sein, die sich unbefugt Zugang verschaffen können. Schließlich können Risikoquellen bei Kommunikationspartnern liegen, mit denen personenbezogene Daten befugt ausgetauscht werden, oder bei Herstellern und Dienstleistern, die Informationstechnik einschließlich der mit ihr verwendeten Software, die für die Verarbeitung personenbezogener Daten oder in ihrem Umfeld eingesetzt wird, bereitstellen oder warten. Schließlich sind technische Fehlfunktionen und äußere Einflüsse, z.B. durch höhere Gewalt, als Risikoquellen zu berücksichtigen.

3.1.4 Abschätzung von Eintrittswahrscheinlichkeit und Schadenshöhe

Für jeden möglichen Schaden werden die Eintrittswahrscheinlichkeit und Schwere abgeschätzt. Diese lassen sich nur in ganz wenigen Ausnahmefällen mathematisch erfassen. Dennoch verlangt die

DSGVO, das Risiko anhand objektiver Kriterien zu beurteilen (ErwGr.76). Insbesondere in Fällen immaterieller Schäden, wie z. B. einer Rufschädigung, muss auch – auf Basis objektiver Kriterien – beurteilt werden, als wie schwerwiegend die möglichen negativen Folgen für die Lebensführung der betroffenen Personen einzustufen sind. Eine Möglichkeit für die Bemessung eines Risikos besteht darin, eine Abstufung der Ausprägungen von Schwere und Eintrittswahrscheinlichkeit eines möglichen Schadens auf einer Skala – mit beispielsweise vier Ausprägungen darzustellen. Sowohl für die Differenzierung der Eintrittswahrscheinlichkeit als auch für die mögliche Schwere eines Schadens könnten jeweils folgende Abstufungen verwendet werden:

- geringfügig
- überschaubar
- substanziell
- groß

Die vier Begrifflichkeiten lassen sich folgendermaßen mit der Eintrittswahrscheinlichkeit und der Schwere eines Schadens in Beziehung bringen:

Risikoeinstufung	**Schwere des Schadens**	**Eintrittswahrscheinlichkeit**
geringfügig	Der mögliche Schaden hat sehr geringe Auswirkungen.	Der mögliche Schaden tritt selten bis nie ein.
überschaubar	Der mögliche Schaden zieht größere Unannehmlichkeiten nach sich.	Es bedarf eines hohen Aufwandes, um einen Schaden anzurichten.
substanziell	Der Datenmissbrauch bringt hohe Folgeschäden mit sich.	Es bedarf eines geringen Aufwandes, um einen Schaden anzurichten.
groß	Der mögliche Schaden ist schwerwiegend und ggf. irreversibel.	Der mögliche Schaden ist sehr einfach anzurichten.

3.1.4.1 Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit eines Risikos beschreibt, mit welcher Wahrscheinlichkeit ein bestimmtes Ereignis (das selbst auch ein Schaden sein kann) eintritt und mit welcher weiteren Wahrscheinlichkeit es zu Folgeschäden kommen kann. Handelt es sich zum Beispiel bei dem Schadensereignis um die ungewollte Offenlegung der sexuellen Orientierung einer Person, so ist die

Wahrscheinlichkeit sowohl dieser Offenlegung, als auch der hieraus resultierenden weiteren Schäden einzuschätzen. Die Wahrscheinlichkeiten der verschiedenen Wege, die zu einer solchen Offenlegung führen können, summieren sich hierbei. Im genannten Beispiel gehören unzureichende Vorkehrungen des Verantwortlichen, sorgloser Umgang von Beschäftigten unter seiner direkten Verantwortung mit der Information, technische Fehlfunktionen oder Ausspähung durch Dritte zu möglichen Wegen.

3.1.4.2 Die Schwere des möglichen Schadens

Die Schwere eines möglichen Schadens muss in jedem Einzelfall unter Berücksichtigung von Art, Umfang, Umständen und Zwecken der Verarbeitung bestimmt werden (ErwGr. 76). Wesentliche Faktoren sind insbesondere:

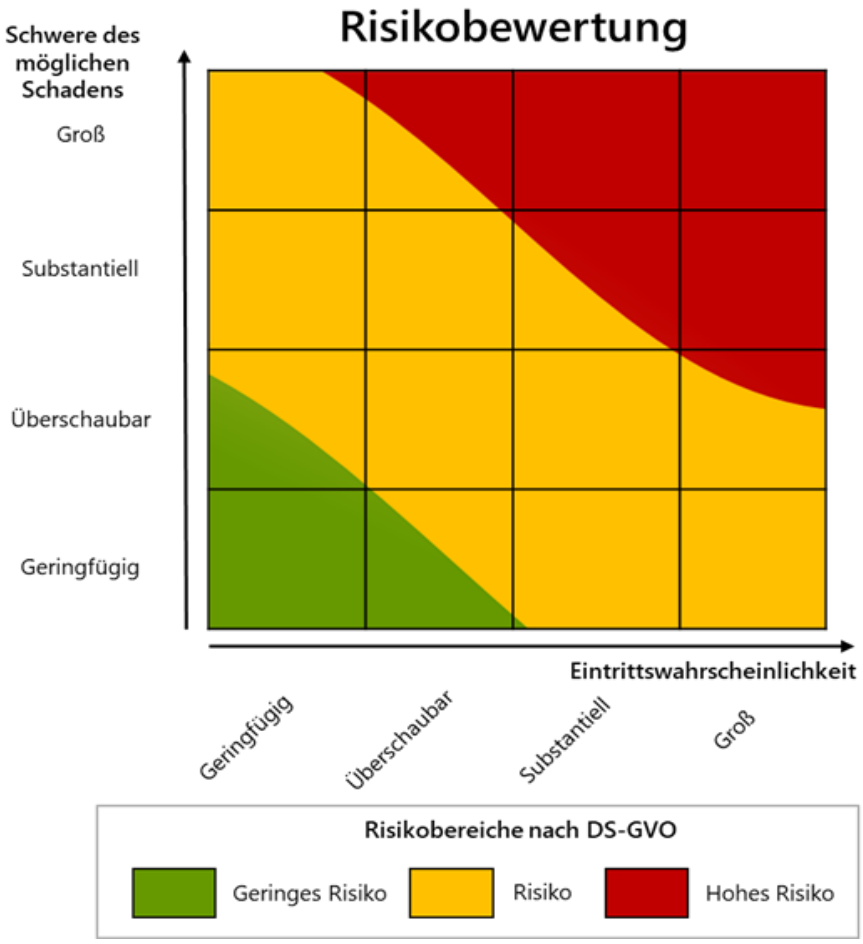
- Die Verarbeitung besonders geschützter Daten im Sinne von Art. 9 und 10 DSGVO, bei denen die DSGVO ausdrücklich eine gesteigerte Schutzbedürftigkeit vorsieht.
- Verarbeitung von Daten schützenswerter Personengruppen (z.B. Beschäftigte).
- Verarbeitung nicht veränderbarer und eindeutig identifizierenden Daten wie z. B. eindeutigen Personenkennzahlen im Vergleich zu pseudonymisierten Daten.
- Automatisierte Verarbeitungen, die eine systematische und umfassende Bewertung persönlicher Aspekte (z.B. Profiling) beinhalten und auf deren Grundlage dann Entscheidungen mit erheblichen Rechtswirkungen für betroffene Personen getroffen werden.
- Wenn der Schaden nicht oder kaum reversibel ist oder die betroffene Person nur wenige oder beschränkte Möglichkeiten hat, die Verarbeitung selbst zu prüfen oder sich dieser Verarbeitung zu entziehen, etwa, weil sie von der Verarbeitung gar keine Kenntnis hat.
- Wenn die Verarbeitung eine systematische Überwachung ermöglicht.
- Die Anzahl der betroffenen Personen, die Anzahl der Datensätze und die Anzahl der Merkmale in einem Datensatz sowie die geographische Abdeckung, die mit den verarbeiteten Daten erreicht wird.

3.1.5 Zuordnung zu Risikoabstufungen

Nachdem die Eintrittswahrscheinlichkeit und die Schwere möglicher Schäden bestimmt wurden, müssen diese den Risikoabstufungen „geringes Risiko“ „Risiko“ und „hohes Risiko“ zugeordnet werden. Wie diese Abbildung konkret erfolgt, wird in der DSGVO nicht näher beschrieben – es besteht daher grundsätzlich Spielraum für verschiedene Modelle.

Als Risiko der Verarbeitung insgesamt ist grundsätzlich die höchste Risikoklasse der Einzelrisiken anzunehmen. Sollten in dieser Risikoklasse viele Einzelrisiken vorhanden sein, kann es jedoch im Einzelfall erforderlich sein, eine höhere Risikoklasse anzunehmen.

Für die Abschätzung des Risikos der Verarbeitung gemäß der Eintrittswahrscheinlichkeit und der Schwere des möglichen Schadens kann die folgende Matrix verwendet werden:



Sind beispielsweise sowohl die Schwere als auch die Eintrittswahrscheinlichkeit des Schadens als „geringfügig“ einzustufen, so ergibt sich für die Risikobewertung das eindeutige Ergebnis eines „geringfügigen“ möglichen Schadens. Dies gilt auch bei Abstufungen, die nicht gleich sind, etwa wenn der Schaden zwar nur „geringfügig“ wahrscheinlich ist, jedoch die Schwere „substantiell“. Dann ergibt sich für die anschließende Risikobewertung ebenfalls das klare Ergebnis eines „substantiellen“ möglichen Schadens.

Bei der Abschätzung des Risikos anhand der Matrix können sich jedoch auch Fälle ereignen, in denen der Eintritt des Schadens „substantiell“ wahrscheinlich und auch die Schwere des Schadens „substantiell“ und damit schwerwiegend ist. In dieser Konstellation sind die Grenzbereiche zweier Risikoabstufungen („Risiko“ und „hohes Risiko“) betroffen, was sich in dem entsprechenden Feld der Matrix dadurch äußert, dass es zwei Farben (gelb und rot) ausweist. Dies macht deutlich, dass in bestimmten Grenzfällen eine Einzelfallbetrachtung notwendig ist. Im Zweifel führt die Entscheidung über die Risikoeinschätzung dazu, dass trotz des Ergebnisses der generischen Abschätzung anhand der

Matrix, der Einzelfall so schwerwiegend ist, dass nicht nur ein „Risiko“, sondern ein „hohes Risiko“ gegeben ist.

Mit der bis zu diesem Punkt beschriebenen Vorgehensweise wird das Ausgangsrisiko einer Datenverarbeitung unter Berücksichtigung aller Umstände bestimmt.

3.1.6 Eindämmung des Risikos

Im Wege der Datenschutz-Folgeabschätzung oder – falls voraussichtlich kein hohes Risiko vorliegt – in einem vereinfachten Verfahren sind als nächster Schritt die Maßnahmen zur angemessenen Eindämmung der Risiken zu ermitteln.

Das Risiko einer Verarbeitung ist mittels entsprechender technischer und organisatorischer Maßnahmen (TOMs) einzudämmen, die geeignet sind, die Rechte und Freiheiten der betroffenen natürlichen Personen angemessen zu gewährleisten. Ziel ist es mithilfe der Abhilfemaßnahmen die Eintrittswahrscheinlichkeit und/oder die Schwere des möglichen Schadens auf ein Minimum zu beschränken. In Betracht kommen folgende Maßnahmen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten,
- die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung,
- die rasche Wiederherstellung personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall und
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Das Sicherheitskonzept ist kontinuierlich zu überprüfen und an die technisch-organisatorischen Änderungen und Entwicklungen zum Schutz von personenbezogenen Daten anzupassen.

3.1.7 Restrisiko

Das nach Umsetzung dieser Maßnahmen verbleibende Risiko wird als Restrisiko bezeichnet. Wenn dieses Restrisiko als hoch einzustufen ist, besteht die Pflicht zur vorherigen Konsultation gemäß Art. 36 DSGVO. Der Verantwortliche muss genau prüfen (und gem. Art. 5 Abs. 2 DSGVO als Nachweis für die Erfüllung der Anforderungen der DSGVO dokumentiert haben), ob er alle ihm nach dem Grundsatz der Verhältnismäßigkeit möglichen Maßnahmen zur Eindämmung des Risikos ergriffen hat, bevor er mit einer Verarbeitung beginnt.

Nach Umsetzung der Abhilfemaßnahmen müssen diese auf ihre Wirksamkeit getestet und kontinuierlich überwacht werden. Möglicherweise zeigt sich bei der Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind.

3.2 Datenschutzfolgenabschätzung

Erscheint eine bestimmte Verarbeitung von personenbezogenen Daten für Betroffene besonders risikoreich, muss vor Beginn der Verarbeitung eine Datenschutzfolgenabschätzung durchgeführt werden. Die Datenschutzfolgenabschätzung ist von dem für die Verarbeitung der personenbezogenen Daten verantwortlichen Bereich durchzuführen. Der Datenschutzbeauftragte ist beratend hinzuzuziehen.

Eine Datenschutzfolgenabschätzung wird insbesondere dann erforderlich, wenn neue Technologien verwendet werden und aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Der Verarbeitungs-Verantwortliche führt die Datenschutzfolgenabschätzung durch und hat diese zu dokumentieren. Der Verarbeitungs-Verantwortliche

- bezieht diejenigen Fachbereiche ein, die bei der Ermittlung und Bewertung der Risiken, sowie bei der Umsetzung von Abhilfemaßnahmen fachliche Informationen oder Expertise zuliefern,
- holt ggf. den Standpunkt der Betroffenen ein,
- zieht ggf. externe Expertise hinzu (z.B. zur IT-Sicherheitsexperten) und
- dokumentiert den Prozess der Datenschutzfolgenabschätzung

Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden. Zur Beherrschung der Risiken für die Rechte und Freiheiten der betroffenen Personen sind geeignete technische und organisatorische Maßnahmen zu ergreifen und zu dokumentieren. Verbleibt trotzdem für die Rechte und Freiheiten der betroffenen Personen ein hohes Restrisiko, ist der Vorstand zu unterrichten. Der Vorstand entscheidet über die Einstellung oder Weiterentwicklung des Verfahrens und veranlasst im Fall einer Weiterentwicklung die vorherige Konsultation der Aufsichtsbehörde.

3.3 Umgang mit Datenschutzvorfällen

Das Unternehmen ist verpflichtet, Datenschutzvorfälle zu dokumentieren und in bestimmten Fällen der Datenschutz-Aufsichtsbehörde innerhalb von 72 Stunden zu melden. Die wesentlichen Schritte sind nachfolgend dargestellt:

3.3.1 Vorliegen eines Datenschutzvorfalls

Ein Datenschutzvorfall ist jede Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität personenbezogener Daten. Zum Beispiel:

- Eine E-Mail mit Mitarbeiterdaten wurde versehentlich an den falschen Adressaten gesendet.
- Ein USB-Stick oder Laptop mit personenbezogenen Daten kommt abhanden.
- Es wurden Änderungen im Datensatz eines falschen Mitarbeiters eingetragen.

3.3.2 Interne Meldepflicht

Ein Datenschutzvorfall ist regelmäßig zu melden. Bei der internen Meldung ist folgendermaßen vorzugehen:

a) Jeder Mitarbeiter meldet einen Datenschutzvorfall sowie jeden konkreten Verdacht auf einen Datenschutzvorfall bei Bekanntwerden sofort intern an den Datenschutzbeauftragten.
b) Die interne Meldung muss schnellstmöglich erfolgen, insbesondere bei schwerwiegenden Datenschutzvorfällen und solchen, bei denen zum Schutz der Betroffenen Schutzmaßnahmen durch das Unternehmen getroffen werden können. Die Meldung kann in jeder Form erfolgen. Mündliche Meldungen sind unverzüglich schriftlich (z.B. per E-Mail) nachzuholen.
c) In der Meldung sind folgende Fragen zu beantworten:
    1. Was ist im Detail passiert?
    2. Um wessen personenbezogene Daten geht es?
    3. Wie groß ist der betroffene Datensatz?
    4. Welche Arten von personenbezogenen Daten sind betroffen?
    5. Seit wann (Datum und Uhrzeit) besteht Kenntnis von dem Datenschutzvorfall?
    6. Was sind die wahrscheinlichen Folgen des Datenschutzvorfalls?
    7. Welche Maßnahmen zur Behebung des Datenschutzvorfalls wurden bereits ergriffen oder werden vorgeschlagen?

3.3.3 Nachforschung und Sicherungsmaßnahmen

Bestätigt sich der Verdacht des Datenschutzvorfalls, dokumentiert der Datenschutzbeauftragter Datum und Uhrzeit. Dieser Zeitpunkt ist für den Beginn der 72-Stunden Frist zur etwaigen Meldung an eine Datenschutz-Aufsichtsbehörde maßgeblich. Soweit erforderlich leitet der Datenschutzbeauftragte Sofortmaßnahmen zur Behebung des Datenschutzvorfalls oder zur Abmilderung möglicher nachteiliger Auswirkungen des Datenschutzvorfalls ein:

- Sperrung von Zugängen,
- Änderung von Passwörtern,
- Einspielen von Backups.

3.3.4 Information von Auftraggebern bei Auftragsverarbeitung

Betrifft der Datenschutzvorfall eine Verarbeitung, die das Unternehmen für einen anderen im Auftrag als Auftragsverarbeiter durchführt, informiert der Datenschutzbeauftragter unverzüglich den Auftraggeber.

3.3.5 Risikoanalyse

Der Datenschutzbeauftragte ermittelt im Rahmen einer Risikoanalyse, ob der Datenschutzvorfall

- zu keinem Risiko [grüne Kategorie],
- zu einem Risiko [gelbe Kategorie] oder

- zu einem hohen Risiko [rote Kategorie]

für die Rechte und Freiheiten natürlicher Personen führt.

3.3.6 Ggf. Meldung an die Datenschutz-Aufsichtsbehörde

Führt ein Datenschutzvorfall voraussichtlich zu einem Risiko für die Rechte und Freiheiten einer natürlichen Person (gelbe oder rote Kategorie) ist eine Meldung an die Datenschutz-Aufsichtsbehörde gemäß Art. 33 DSGVO vorzunehmen. Die Meldung gegenüber der Datenschutz-Aufsichtsbehörde muss unverzüglich und möglichst binnen 72 Stunden ab Kenntnis erfolgen. Wenn und soweit die Informationen nicht vollständig oder nicht rechtzeitig bereitgestellt werden können, sind die Angaben unverzüglich schrittweise der Aufsichtsbehörde bereitzustellen.

3.3.7 Ggf. Benachrichtigung von Betroffenen

Führt ein Datenschutzvorfall voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten einer natürlichen Person (rote Kategorie) so sind die Betroffenen von dem Datenschutzvorfall gemäß Art. 34 DSGVO zu benachrichtigen, sofern das Unternehmen die Daten nicht lediglich im Auftrag eines anderen verarbeitet hat und kein Ausnahmefall nach Art. 34 Abs. 3 DSGVO vorliegt.

3.3.8 Dokumentation im Verzeichnis für Datenschutzvorfälle

Jeder Datenschutzvorfall ist folgendermaßen festzuhalten:

- Beschreibung aller im Zusammenhang mit dem Datenschutzvorfall stehende Fakten,
- Beschreibung der Auswirkungen des Datenschutzvorfalls,
- Beschreibung der ergriffenen Abhilfemaßnahmen zur Eindämmung des Datenschutzvorfalls,
- Erwägungen und Ergebnis der Risikoeinschätzung zum Datenschutzvorfall.

Die Dokumentation muss der Datenschutz-Aufsichtsbehörde die Überprüfung der Einhaltung der Meldepflicht nach Art. 33 DSGVO ermöglichen und auf Anfrage dieser vorgelegt werden, Art. 33 Abs. 5 DSGVO.

3.3.9 Arbeitsrechtliche Konsequenzen

Wurde ein Datenschutzvorfall, ein Verstoß gegen diese Richtlinie oder ein Verstoß gegen andere datenschutzrechtliche Bestimmungen fahrlässig oder vorsätzlich verursacht, zieht dies arbeitsrechtliche Konsequenzen nach sich. Eine fristlose oder ordentliche Kündigung sind hierbei einbegriffen. Daneben können strafrechtliche und zivilrechtliche Sanktionen in Erwägung gezogen werden, etwa die Geltendmachung von Schadensersatzansprüchen.

4 Praktische Gestaltungsfragen

Im folgenden Abschnitt beschäftigen wir uns mit verschiedenen praktischen Gestaltungsfragen des Datenschutzes, die in der alltäglichen Arbeit in unserem Unternehmen relevant sind. Wir bieten eine umfassende Übersicht über die Struktur und die Prinzipien, die bei der Implementierung effektiver Datenschutzmaßnahmen zu beachten sind. Des Weiteren klärt dieser Abschnitt über konkrete Herausforderungen und Lösungen in Bezug auf die Datenspeicherung und -sicherung sowie die Transparenz und Nachvollziehbarkeit der Datenverarbeitung auf.

4.1 Besondere Gestaltungsfragen

Nachstehende Regelungskomplexe stehen in Zusammenhang mit den in **Anlage 3** beschriebenen technischen und organisatorischen Maßnahmen und stellen in Bezug auf die genannten Gestaltungsfragen ergänzende Vorgaben dar.

4.1.1 Projektmanagement

Alle Projektvorhaben sind daraufhin zu überprüfen, ob Datenschutz- und Datensicherheitsbezüge gegeben sind. In jedem Projekt ist sicherzustellen, dass der Datenschutz- und Datensicherheitsbezug geprüft und dokumentiert wird. Der Datenschutzbeauftragte ist daher frühzeitig in die Projektentwicklung einzubeziehen. Die Durchführung eventuell erforderlicher Vorabkontrollen gemäß Art. 35 DSGVO ist sicherzustellen.

4.1.2 Datentransfer in EU- und Drittstaaten

Die Datenverarbeitung innerhalb der EU ist im Rahmen des Bundesdatenschutzgesetzes grundsätzlich zulässig, wenn eine Zulässigkeitsgrundlage besteht, die die Verarbeitung innerhalb Deutschlands ermöglicht. Werden personenbezogene Daten in ein Land übermittelt, das nicht Mitglied der EU ist („Drittland“), so stellt der Verarbeitungs-Verantwortliche sicher, dass die Anforderungen der Artikel 44 ff. DSGVO an einen Datenexport eingehalten werden. Keine Drittländer sind auch die anderen Länder des Europäischen Wirtschaftsraums (Island, Liechtenstein und Norwegen). Eine Übermittlung in ein Drittland ist nach diesen Bestimmungen nur zulässig, wenn

- ein Ausnahmefall nach Art. 49 DSGVO vorliegt,
- die Datenübermittlung auf Grundlage eines Angemessenheitsbeschlusses nach Art. 45 DSGVO erfolgt, insbesondere in ein Land, für das die EU-Kommission beschlossen hat, dass dieses ein angemessenes Schutzniveau aufweist (z.B. Schweiz oder USA),
- das Unternehmen geeignete Garantien im Sinne des Artikel 46 DSGVO vorgesehen hat.

Der Verarbeitungs-Verantwortliche hat die Übermittlung personenbezogener Daten in ein Drittland vorher mit dem Datenschutz-Manager abzustimmen, außer die Übermittlung erfolgt nur vereinzelt und nur in geringem Umfang. Der Verarbeitungs-Verantwortliche dokumentiert im Verzeichnis der

Verarbeitungstätigkeiten, die Übermittlung in das Drittland sowie die Basis für deren rechtliche Zulässigkeit.

4.1.3 Entsorgung und Löschung von Dokumenten und Datenträgern

Alle Mitarbeiter haben sicherzustellen, dass sowohl Papierdokumente als auch elektronische Dokumente und Datenträger datenschutzgerecht entsorgt werden. Soweit die Entsorgung durch externe Dienstleister erfolgt, müssen diese über entsprechende Zertifikate verfügen. Die datenschutzgerechte Entsorgung ist in diesem Fall durch schriftliche Bestätigung des Entsorgungsunternehmens zu dokumentieren.

4.1.4 Grundsätze für Administratoren

Administratoren dürfen ihre Rechte nur entsprechend ihrer Arbeitsplatzbeschreibung und/oder Arbeitsanweisungen und der ihnen zugewiesenen Aufgabenbereiche durchführen. Maßgeblich ist die Datenschutzrichtlinie von BHS. Administratoren werden bezüglich einschlägiger Rechtsvorschriften (TKG, TMG, besondere Zweckbindung gem. § 26 BDSG) besonders unterwiesen. Bei besonders sensiblen oder risikoreichen Administrationsaufgaben ist das Vier-Augen-Prinzip, z. B. durch ein geteiltes Passwort oder ein festgelegtes Freigabeverfahren, anzuwenden. Diese besonderen Administrationsaufgaben sind im Administrationshandbuch festzulegen.

Eine Einsichtnahme in betriebliche Inhaltsdaten durch den Administrator ist nur auf Anordnung des zuständigen Bereichsverantwortlichen und in private Inhalte, z. B. private E-Mails, nur mit Einwilligung des Betroffenen, möglichst im Vier-Augen-Prinzip oder im Beisein des Betroffenen, zulässig. Davon unberührt bleiben Zugriffe, soweit sie bei einem Verdacht auf eine Straftat im Beschäftigungsverhältnis angeordnet oder zur Gefahrenabwehr (Gefahr im Verzug) erforderlich sind.

4.1.5 Einsatz von Protokollierung

Protokolle mit Personenbezug unterliegen der besonderen Zweckbindung nach § 76 BDSG. Sie dürfen zu keinem anderen Zweck als dem ordnungsgemäßen Betrieb von Systemen, zur Datensicherung oder zur Datenschutzkontrolle verwendet werden. Insbesondere sind Protokolle nur in dem Umfang zu führen, in dem sie auch für den beabsichtigten Zweck ausgewertet bzw. verwendet werden können. Eine Protokollierung „auf Vorrat“ ohne eindeutig bezeichneten Zweck ist unzulässig. Die Aufbewahrungsfrist ist am bezeichneten Zweck zu orientieren. Nach Ablauf dieser Frist sind Protokolle und Protokolleinträge sicher zu löschen. Folgende Sachverhalte sind zu protokollieren:

4.1.6 Protokollierung der Einrichtung und des Betriebs von IT-Systemen

- Dokumentation von Systemumfang, Komponenten/Modulen des eingesetzten IT-Systems
- Testfälle, Testung, Testergebnisse
- Fachliche und technische Freigabe und Freigabe zum Einsatz

4.1.6.1 Einrichtung/Änderung von Benutzern und Rechten

- Dokumentation aller berechtigten Nutzer

- Rechteprofile der berechtigten Nutzer
- Dokumentation von Änderungen von Nutzern/Rechten
- Dokumentation, wer die Benutzer und Rechte angeordnet hat
- Dokumentation, wer die Rechte eingerichtet hat
- Historie über die eingerichteten Nutzer und Rechte

4.1.6.2 Systemänderungen

- Dokumentation von funktionalen Systemänderungen/Erweiterungen einschließlich Testfällen, Testung, Testergebnissen und Freigabe
- Änderungen der Dateiorganisation oder des Dateiverwaltungssystems

Protokollierung von Eingaben und Veränderungen auf Systemebene

4.1.6.3 Zugriffe und Zugriffsversuche

- Zugriff auf Dateien mit personenbezogenen oder vertraulichen personenbezogenen Inhalten
- Unbefugte und abgewiesene Zugriffsversuche
- Wiederholte Eingabe von fehlerhaften Passwörtern zu einem Login
- Unbefugtes Einloggen und Überschreiten von Befugnissen
- Benutzung von Admin-Accounts
- Warnungen über unbefugtes Eindringen

4.1.6.4 Systemüberwachung

- Änderungen und Änderungsversuche von Gateway- und Firewall-Policies
- Systemprotokollausnahmen
- Netzmanagementalarme
- Zugriffe auf die Server-Registry, Veränderung relevanter Einstellungen
- Überwachung von Routern und Switches
- Überwachung von Druckern, Kopierern und Multifunktionsgeräten

4.1.6.5 Archivsysteme

- Datum und Uhrzeit von Zugriffen
- Kennung des Benutzers
- Ausgeführte Aktionen, insbesondere Lösch- und Kopiervorgänge
- Entfernung von Datenträgern
- Fehlermeldungen
- Exports, Downloads und Versand von vertraulichen Dokumenten und Daten

4.1.6.6 Verwaltung der Protokolldaten

- Protokollierung der Abschaltung von Protokollfunktionen
- Warnungen über unbefugtes Eindringen

- Überlauf von Protokolldateien
- Nachträgliche Änderung oder Löschung von Protokolleinträgen
- Protokollierung der Bearbeitung oder Löschung von Protokolldaten
- Protokollierung von Zugriffen auf die Protokolldateien
- Änderung von Meldetypen
- Speicherung der Protokolleinträge

4.1.7 Firewall und Internetschutz

Die Internetnutzung ist nur für dienstliche Zwecke und ggf. gemäß Betriebsvereinbarung zulässig. Jegliche E-Mail-Kommunikation aus dem Netz des BHS, insbesondere zu Endkunden, die personenbezogene Daten oder sensible Unternehmensdaten beinhalten, hat verschlüsselt zu erfolgen. Eine E-Mail-Kommunikation ist allerdings auch unverschlüsselt zulässig, wenn der Betroffene in die unverschlüsselte E-Mail-Kommunikation nachweislich eingewilligt hat oder keine personenbezogenen Daten sowie keine sensiblen Unternehmensdaten enthalten sind.

Zusätzlich zu den zentralen Vorkehrungen sind alle PCs und Notebooks auch durch eine lokal installierte Firewall und ein Anti-Virus-Programm geschützt. Eine entsprechende Anleitung und Benutzerhinweise stehen zur Verfügung. Die Geräte sind damit auch bei einem Internetzugang von externen Standorten aus entsprechend geschützt.

Um einen ständigen Schutz der Geräte zu gewährleisten, darf nur die von der IT-Abteilung freigegebene und installierte Sicherheitssoftware installiert und betrieben werden. Ferner darf die Konfiguration der Schutzsoftware nicht verändert oder die Schutzsoftware deaktiviert oder deinstalliert werden. Die Konfiguration der Firewall und deren Funktionsfähigkeit sind von der IT-Abteilung in angemessenen Abständen zu überprüfen.

4.1.8 Mobile Geräte/Heimarbeitsplätze

Der Einsatz von mobilen Geräten und Datenträgern bedarf einer entsprechenden Genehmigung durch den Arbeitgeber. Tele- und Heimarbeitsplätze dürfen nur nach Genehmigung von der Fachabteilung eingerichtet und betrieben werden. Bei der Genehmigung dieser Arbeitsplätze ist darauf zu achten, dass aufgrund der baulichen und räumlichen Verhältnisse angemessene Sicherheitsmaßnahmen vorhanden sind bzw. geschaffen werden können (z. B. separater Arbeits- bzw. Bürobereich, Möglichkeiten einer vertraulichen Behandlung/Aufbewahrung von Unterlagen, Schutz vor Einsichtnahme und Zugriff durch unbefugte Personen – auch durch Familienangehörige und Freunde etc.). Die Fachabteilung, die die Verlagerung der Tätigkeit auf Heimarbeitsplätze durchführt, ist dafür verantwortlich, dass die Heimarbeitsplätze den vorgenannten Anforderungen entsprechen und hat hierzu entsprechende Kontrollprozesse zu definieren und durchzuführen.

4.1.9 Einsatz und Freigabe von Datenverarbeitungsverfahren

Alle für die Erhebung, Verarbeitung und Nutzung von personenbezogenen und sonstigen vertraulichen Daten erforderlichen Datenverarbeitungssysteme und Programme (Hard- und Software) dürfen nur

nach einer erfolgreichen Prüfung und Freigabe eingesetzt werden. Der Umfang der im Einzelfall erforderlichen Prüfung und der Freigabe ist in der jeweiligen Verfahrensdokumentation festzulegen.

4.1.10 Private Nutzung von betrieblichen Geräten, Hard- und Software

Ein Einsatz privater Hard- und Software (Notebooks, USB-Sticks, Speicherkarten, mobile Laufwerke etc.) für betriebliche Zwecke und die Verwendung privater Datenträger (Disketten, CDs, USB-Sticks etc.) an Firmen-PCs ist untersagt und nur nach gesonderter Genehmigung durch die IT-Administration und für festgelegte Zwecke, ggf. nach näheren Anweisungen durch die IT-Administration bzw. durch den IT-Sicherheitsbeauftragten, zulässig.

4.2 Informationsübertragung

Primäre Zielgruppe: IT-Abteilung, Personalabteilung, Informationssicherheitsverantwortliche bzw. ISB.

Bei der Übertragung von Informationen (unter anderem per E-Mail oder Telefon) gelten folgende Vorgaben:

- Die Beschäftigten sind darauf hinzuweisen, dass sie keine vertraulichen Gespräche in der Öffentlichkeit, in offenen Büros oder an Versammlungsorten führen dürfen.
- Es sind Maßnahmen und Beschränkungen in Verbindung mit der Nutzung von Kommunikationseinrichtungen festzulegen und umzusetzen (z.B. Weiterleitung von beruflichen E-Mails an externe E-Mail-Adressen).
- Informationen des Unternehmens können über folgende elektronische Kommunikationswege ausgetauscht werden: E-Mail, Downloads von Dateien aus dem Internet, Übertragung von Daten via Kundenportale des Unternehmens, Telefone, Faxgeräte, der Versand von SMS-Textnachrichten, tragbare Medien, sowie Foren und soziale Netzwerke.
- Der Informationssicherheitsverantwortliche bzw. ISB legt für jede Art von Information die zulässigen Kommunikationswege sowie mögliche Einschränkungen bezüglich der für deren Nutzung erforderlichen Erlaubnis fest, d.h. er legt fest, welche Aktivitäten verboten sind.
- In Ergänzung der in der Richtlinie zur Klassifizierung von Informationen festgelegten Maßnahmen, legt der Informationssicherheitsverantwortliche bzw. ISB auf Basis der Ergebnisse der Risikoeinschätzung zusätzliche Maßnahmen für jeden Datentyp und Kommunikationsweg fest.
- Vor dem Austausch von Informationen und/oder Software mit einer externen Partei muss eine Vereinbarung unterzeichnet werden, wofür der Informationssicherheitsverantwortliche bzw. ISB verantwortlich ist. Die Vereinbarung kann in Papierform oder in elektronischer Form bestehen (z.B. Zustimmung zu Allgemeinen Geschäftsbedingungen) und muss Klauseln entsprechend der Risikoeinschätzung enthalten, mindestens jedoch die Nachfolgenden:
    - Methode zur Identifizierung der anderen Partei
    - Zugangsberechtigungen zu Informationen
    - Sicherstellung der Nichtabstreitbarkeit
    - Technische Standards für die Datenübertragung

- Verfahren für den Umgang mit Vorfällen
- Kennzeichnung von und Umgang mit sensibler Information
- Urheberrecht
- Verträge/Vereinbarungen mit externen Parteien müssen im Einklang mit den Richtlinien für Lieferantenbeziehungen (A.15) verfasst werden.

4.3 Datensicherheit – Verhaltensrichtlinien

4.3.1 Eigentumsrecht an Daten und Informationen sowie Datenschutz

- Hardware, Software, portierbare Medien sowie alle Daten und Informationen, die darin erzeugt oder gespeichert werden oder über Computer und Telekommunikationsnetze des BHS übertragen werden oder im Papierdokumentenformat vorhanden sind, sind einzeln und zusammen Eigentum des BHS, sofern nicht ausdrücklich festgelegt ist, dass sie Eigentum eines Dritten sind.
- Jede Nutzung des Informationssystems des BHS einschließlich des Zugangs zu Internet und E-Mail gilt als geschäftliche Nutzung. Die Gesellschaft behält sich vor, alle in ihren Systemen gespeicherten oder mit den Systemen übertragenen Informationen einschließlich des Inhalts bestimmter E-Mails zu prüfen. Dieser Grundsatz steht der Duldung der Nutzung von Werkzeugen, die dem Personal zur Verfügung stehen, zu persönlichen Zwecken in angemessenem Umfang nicht entgegen.

4.3.2 Systemzugriff

Die System-IDs sind so eingerichtet, dass diese den Zugriffsbedürfnissen Rechnung tragen. Sie dürfen nicht mit anderen geteilt oder gemeinsam genutzt werden. Passwörter sollten sorgfältig ausgewählt und regelmäßig – in Übereinstimmung mit der Datensicherheitspolitik – geändert werden.

4.3.2.1 Rechner-ID

- Jeder Datennutzer, der Zugang zu Rechneranlagen hat – einschließlich kurzzeitig beschäftigter Mitarbeiter und Aushilfskräfte – muss eine eigene Rechner-ID haben.
- Niemand anderes darf die personalisierte ID benutzen. Der Inhaber ist für alle Tätigkeiten verantwortlich, die unter Verwendung der personalisierten ID ausgeführt werden. Wenn der Verdacht besteht, dass jemand anderes die personalisierte ID benutzt hat, ist unverzüglich die IT-Abteilung darüber zu informieren.
- IDs von Arbeitsgruppen, Gattungs-IDs oder gemeinschaftlich genutzte IDs müssen dem BHS gemeldet und von der IT-Abteilung schriftlich genehmigt werden und sind nur unter außergewöhnlichen Umständen zu erteilen.
- Es steht jedem System nur eine ID zu, sofern der Eigentümer der Daten dieses Systems nichts Anderes erlaubt.
- Es ist untersagt, sich bei einem System mit der ID von jemand anderem anzumelden.

4.3.2.2 Passwörter

- Passwörter müssen geheim gehalten werden.
- Passwörter müssen mind. 8 Zeichen lang sein und aus Buchstaben und Zahlen bestehen.
- Passwörter dürfen keine regulären Wörter, Namen, Daten oder Zahlenreihen sein.
- Passwörter müssen regelmäßig geändert werden.
- Die Konten werden bei mehrfacher Falscheingabe des Passwortes gesperrt. Ausschließlich der Systemadministrator kann das gesperrte Konto wieder freigeben.
- Passwörter, die in automatischen Verfahren eingeschlossen sind, müssen in dem größten technisch möglichen Umfang geschützt werden und das minimale Anforderungsprofil für den erfolgreichen Abschluss des Verfahrens sicherstellen.

4.3.2.3 Benutzerzugriff

- Der Zugriff auf die Informationen und Systeme des BHS muss begründet sein und vom Eigentümer der Informationen genehmigt werden.
- Der Eigentümer der Informationen wird die Zugriffsberechtigung in regelmäßigen Abständen prüfen – mindestens alle zwölf Monate.

4.3.3 Besitz von Informationen und Einstufung

Viele der von dem BHS erzeugten und genutzten Informationen sind entweder vertraulich oder sensibel. Die Einstufung der Informationen ermöglicht den Mitarbeitern zu verstehen, wie jedes Dokument geschützt werden sollte, und sie gilt für alle Arten von Informationsträgern, einschließlich – jedoch nicht beschränkt – auf Papier, Rechnersysteme und optische Vorrichtungen.

4.3.3.1 Besitz von Informationen

Einem Eigentümer von Informationen ist in Bezug auf alle bedeutenden Informationsgüter eine Identität zuzuordnen. Die Aufgaben umfassen, sind jedoch nicht beschränkt auf:

- Definition der Nutzung, der die Informationen unterzogen werden sollen
- Festlegung der Einstufung der Informationen und der erforderlichen Schutzstufen
- Gewährleistung, dass die gesetzlichen Erfordernisse eingehalten werden
- Durchführung einer Risikoanalyse zur Bestimmung der Sicherheitsmaßnahmen
- Überwachung der Datenintegrität
- Festlegung der Aufbewahrungsdauer
- Zugriffsgenehmigung

Einige dieser Aufgaben können dem IT-Eigentümer des Systems, in dem die Informationen gespeichert sind, dem IT-Sicherheitsbeauftragten oder dem IT-Servicecenter übertragen werden.

4.3.3.2 Einstufung von Informationen

Informationen werden nach dem folgenden Schema in eine von vier Klassen eingestuft:

Öffentlich: Informationen, die der Öffentlichkeit allgemein zur Verfügung stehen. Ein besonderer Schutz ist nicht erforderlich, außer sicherzustellen, dass das Urheberrecht nicht verletzt wird. Öffentliche Informationen sind „nicht schutzbedürftig".

Intern: Informationen, deren Benutzung, Verbreitung und Kenntnis seitens eines beliebigen Mitarbeiters innerhalb des BHS keine erkennbare Bedrohung darstellen würde, deren Offenlegung außerhalb des BHS jedoch ein geschäftliches Risiko bedeuten könnte.

Interne Informationen können an andere Unternehmen innerhalb des BHS ohne besondere Genehmigung des Eigentümers der Informationen weitergegeben werden.

Vertraulich: Informationen, deren Offenlegung gegenüber anderen (unabhängig davon, ob es sich um Angestellte des BHS handelt oder nicht) ein erhebliches geschäftliches Risiko darstellt. Das Risiko kann finanzieller oder persönlicher Art sein oder das Ansehen des BHS oder einer ihrer Gesellschaften, Anteilseigner oder Kunden betreffen. Diese Informationen schließen ein, sind aber nicht beschränkt auf:

- persönliche, finanzielle und medizinische Informationen des Anlegers
- Informationen über Kredite oder Kreditwürdigkeit
- Informationen über Angestellte oder Vertreter

Streng vertraulich: Informationen, deren Bekanntgabe eine erhebliche geschäftliche Bedrohung für das BHS oder einen ihrer Angestellten, Kunden oder Vertreter darstellen würde. Diese Informationen schließen ein, sind jedoch nicht beschränkt auf:

- Alle nicht öffentlichen Finanzdaten, Geschäftsgeheimnisse und Informationen zu bedeutenden Geschäftsvorfällen und Strategien, die dem BHS oder Dritten gehören.
- Alle Informationen, die an andere finanzielle Institutionen wie beispielsweise die Börse freigegeben werden (oder werden sollen), aber noch nicht offiziell verkündet worden sind.

Streng vertrauliche Informationen dürfen nur solchen Einzelpersonen übergeben werden, die vom Besitzer dieser Informationen ausdrücklich ermächtigt wurden, diese zu empfangen, d. h. auf der Grundlage „nur für Ihre Augen bestimmt". Streng vertrauliche Informationen müssen innerhalb des BHS verbleiben und dürfen nur bei der Erfüllung von Aufgaben des BHS benutzt werden. Schutzmaßnahmen müssen eine Überprüfung der Benutzung durch den Eigentümer der Informationen einschließen, um die strengste Vertraulichkeit und Integrität der Informationen zu gewährleisten. Die Anfertigung zusätzlicher Kopien oder das Drucken von zusätzlichen Exemplaren streng vertraulicher Informationen darf nicht ohne die vorherige Genehmigung des Besitzers solcher Informationen erfolgen. Eine Überwachung von Dokumentkopien ist notwendig.

Alle Informationen in den Klassen „Intern", „Vertraulich" und „Streng vertraulich" werden als „Schutzbedürftig" eingestuft. Alle schutzbedürftigen Informationen müssen in einer ihrer Einstufungsklasse entsprechenden Weise geschützt werden.

Informationen, die als „Vertraulich" oder „Streng Vertraulich" eingestuft sind, müssen auf jeder Seite, für die die Einstufung gilt, eindeutig als solche gekennzeichnet sein. Diese Klassen können durch Angabe des Bereichs, innerhalb dessen die Einschränkungen gelten, näher erläutert werden, z. B.:

- „Streng vertraulich": nur für Mitglieder der Geschäftsleitung
- „Vertraulich": nur für Mitarbeiter eines Fachbereiches
- „Intern": nur für Mitarbeiter des BHS

Sämtliche vertraulichen und streng vertraulichen Informationen müssen sicher entsorgt werden, zum Beispiel durch Benutzung von bereitgestellten Entsorgungstonnen oder Schreddern. Es sollte davon ausgegangen werden, dass alle Informationen ohne Einstufungskennzeichnung „Intern – nur Bankhaus Scheich" sind. Für die korrekte Einstufung ist der Urheber und Eigentümer der Informationen verantwortlich.

4.3.4 Unbefugter Zugriff

- Unbefugten ist es untersagt, sich Zugang zu Unternehmensinformationen zu verschaffen, die nicht für sie bestimmt sind oder unter Überwindung von passwortgesichertem Material Daten „ausspähen". Eine Verletzung dieser Regel wird gemäß § 202a StGB bestraft.
- Wenn Personen streng vertrauliche Informationen erhalten oder sehen und sich nicht im Klaren über ihre Berechtigung hierzu sind, sollten sie die Angelegenheit unverzüglich dem Besitzer der Informationen und der IT-Abteilung des BHS melden.

4.3.5 Rechner-Management

4.3.5.1 Arbeitsplatzrechner

Wenn ein Arbeitsplatzrechner genutzt wird, muss der jeweilige Mitarbeiter:

- alle unternehmensbezogenen elektronischen Daten auf dem entsprechenden Netzlaufwerk speichern
- am Ende eines Arbeitstages den PC vom Netz abmelden
- einen passwortgeschützten Bildschirmschoner verwenden

Es ist verboten, in dem Rechnernetz Dateien oder Programme der nachstehend genannten Art herunterzuladen oder zu speichern:

- Virenerzeugungs- oder Hackerwerkzeuge
- nicht autorisierte Datenverschlüsselungswerkzeuge
- stenographische Werkzeuge
- nicht genehmigte Spiele
- urheberrechtlich geschützte Inhalte wie Musik, Filme oder nicht genehmigte Software
- Dateien, die pornographische, anstößige, rassistische oder erniedrigende Fotos, Filme, Grafiken, Texte oder andere Bilder oder Beschreibungen enthalten

4.3.5.2 Laptops und Heimarbeitsplätze

Erfahrungsgemäß sind Laptops besonders diebstahlgefährdet. Daher ist zusätzliche Sorgfalt aufzuwenden, um schutzbedürftige Informationen auf diesen Geräten zu schützen.

4.3.5.3 Benutzung eines Laptops

- Es dürfen keine schutzbedürftigen Informationen auf tragbaren Datenträgern ohne Passwortschutz oder Verschlüsselung der Daten gespeichert werden
- Der Laptop ist zu sichern, sofern dieser unbeaufsichtigt gelassen wird
- Er darf niemals im öffentlichen Raum (z. B. in Zügen, Flugzeugen, Restaurants) ohne Aufsicht zurückgelassen werden.
- An den firmeneigenen Laptops oder sonstigen Heimarbeitsgeräten dürfen keine Änderungen vorgenommen werden, sofern nicht die Genehmigung der IT-Abteilung vorliegt.
- Die Methoden bei der Heimarbeit oder Außer-Haus-Arbeit müssen den aktuellen IT-Sicherheitsvorschriften des BHS entsprechen.

4.3.5.4 Keine Nutzung

Laptops dürfen nicht genutzt werden, um sicherheitsbedürftige Informationen im öffentlichen Raum zu betrachten, wo sie von Unbefugten eingesehen werden können.

4.3.5.5 Fremdrechner, Fremdunternehmen

Fremdrechner bzw. Rechner, die nicht durch die zuständige IT-Abteilung freigegeben wurden, dürfen grundsätzlich nicht an das Firmennetzwerk angeschlossen werden. Fremdrechner sind alle Rechner von anderen Stellen, die nicht unter der Kontrolle der firmeneigenen IT-Abteilung stehen, z. B. PCs von Kunden, Lieferanten, Geschäftspartnern, Beratungsunternehmen etc. Bei Bedarf ist die zuständige IT-Abteilung einzuschalten. Soweit Fremdunternehmen oder kooperierenden Unternehmen ein Zugang zu personenbezogenen oder sonstigen vertraulichen Daten gewährt werden muss, ist dies nur im zwingend erforderlichen Umfang und nur auf Anordnung des Fachbereichsverantwortlichen bzw. des Informationseigentümers zulässig. Der Zugang darf nur über sichere Verbindungen mit einer zuverlässigen Identifizierung und Authentifizierung der Benutzer und erst nach Freigabe durch die Geschäftsleitung ermöglicht werden. Die Sicherheitsmaßnahmen sind in Abhängigkeit vom Schutzbedarf der Daten und von den mit dem Zugang verbundenen Risiken festzulegen.

4.3.5.6 Netzwerkanschluss

Der Anschluss an die BHS-Netzwerke von PCs und Laptops, die nicht Eigentum des BHS sind und auch nicht von ihr betreut werden oder anderweitig zugelassen sind, ist verboten.

4.3.5.7 Software Dritter

Auf Geräten des BHS darf nur Software installiert werden, die durch das Verfahren des IT-Änderungsmanagements zugelassen ist.

4.3.5.8 Virenschutz

- Alle PCs, einschließlich Heimgeräte und Laptops, die im Besitz des BHS sind, müssen mit der neuesten zugelassenen Anti-Virus-Software ausgerüstet sein und diese anwenden.
- Jedes externe Speichermedium MUSS vor der Benutzung mit Hilfe der auf dem PC installierten Anti-Virus-Software gescannt werden.
- Internet und E-Mail sind Hauptvirenquellen, und jede Art von Datei – selbst Dokumente – können Viren enthalten. Alle aus dem Internet oder einer anderen externen Quelle heruntergeladenen oder empfangenen Dateien werden durch das Anti-Virus-Programm automatisch geprüft, sobald sie heruntergeladen werden. Dennoch
    - sind keine E-Mails zu öffnen, wenn der Nutzer sich über deren Herkunft nicht im Klaren ist oder andere Anhänge wie beispielsweise Programme enthalten sind.
    - dürfen keine Websites aufgerufen werden, die nicht von renommierten Organisationen betrieben werden. Es besteht ein größeres Risiko, dass von einer solchen Website versehentlich ein Virus heruntergeladen wird.
- Wenn eine E-Mail – besonders eine elektronische Grußkarte – auffordert, zum Lesen zusätzliche Software herunterzuladen, ist dies untersagt. Die IT-Abteilung ist um Rat zu fragen.
- Wenn der Mitarbeiter den Verdacht hat, dass sich ein Virus auf seinem Laptop befindet, muss er sich SOFORT mit der IT-Abteilung in Verbindung setzen, hierzu sind folgende Informationen zu transferieren:
    - Warum vermutet der Benutzer, dass es dort einen Virus gibt (Symptome)?
    - Was wurde bereits unternommen und mit welchem Ergebnis?
    - Welche Quelle der Infektion wird vermutet?
    - Was könnte getan worden sein, was zu einer Ausbreitung des Virus geführt haben könnte (z. B. Versendung einer E-Mail, Dateiübertragung an das Netzwerk)?

Alle potenziell betroffenen Kollegen sind über die Gefahr zu informieren und die IT-Abteilung wird veranlassen, dass der PC und alle anderen infizierten Geräte geprüft und gesäubert werden. Die IT-Abteilung kommuniziert, wann der PC wieder sicher benutzt werden kann.

4.3.5.9 Sichere Entsorgung von Ausrüstung

Bei Ausrüstungselementen, die Speichermedien enthalten (einschließlich, aber nicht beschränkt auf Festplatten, USB-Sticks und sonstige optische Speichervorrichtungen), müssen alle Daten vor der Entsorgung oder Verlagerung vollständig gelöscht oder überschrieben werden.

Die Vernichtung von schadhaften Vorrichtungen muss durch vertrauenswürdige, ermächtigte Personen erfolgen (Angestellte, Auftragnehmer oder eine externe Agentur, die einen entsprechenden Vertrag oder eine Geheimhaltungsvereinbarung unterschrieben haben) und eine Wiederherstellung unwahrscheinlich machen. Das Verzeichnis der Vermögensgegenstände muss nach der Vernichtung von Ausrüstung aktualisiert werden. Dies gilt es mit der IT-Abteilung abzustimmen.

4.3.5.10 Schutz von Daten bei Übertragung

Wie beim Schutz von Informationen, die auf Systemen des BHS gespeichert sind, ist es genauso bei der Übermittlung von Informationen an firmenexterne Empfänger wichtig, dass alles Mögliche unternommen wird, um den unbefugten Zugriff zu verhindern.

4.3.5.11 Fax-Richtlinien

Um die Informationsgüter des BHS rechtlich gegen ungewollte Bekanntgabe zu schützen, müssen alle ausgehenden Faxe die folgende Nachricht enthalten:

- „Bitte rufen Sie uns bei Übertragungsproblemen an. Der Inhalt dieses Faxes ist vertraulich und nur für den Empfänger bestimmt. Falls Sie nicht der Empfänger sind, beachten Sie bitte, dass jede Benutzung, Verbreitung, Versendung oder jedes Kopieren dieses Faxes streng verboten ist. Sollte Ihnen dieses Fax irrtümlich zugehen, benachrichtigen Sie unverzüglich den Absender. Vielen Dank."
- Vertrauliche oder streng vertrauliche Informationen (einschließlich Einzelheiten über Kredite) des BHS dürfen nicht durch einen ungesicherten Kommunikationsweg (z. B. per Fax, Internet, Handy oder USB-Stick) übermittelt werden, sofern sie nicht gemäß den aktuellen Verschlüsselungsvorschriften des BHS verschlüsselt wurden.
- Es gilt sicherzustellen, dass sich der richtige Empfänger am Standort des Adressaten befindet, bevor Sie schutzbedürftige Informationen faxen.

4.3.6 Übertragung von oder Zugriff auf schutzbedürftige Informationen

Eine genehmigte Vertraulichkeitsvereinbarung/-klausel oder eine Geheimhaltungsvereinbarung (NDA) muss von beiden Parteien unterzeichnet sein und vorliegen, bevor Dritte interne, vertrauliche oder streng vertrauliche Informationen des BHS hin- oder zurücksenden, darauf zugreifen oder bearbeiten. Der zuständige Mitarbeiter des BHS bzgl. Vertragswerke muss zu der Übereinkunft über eine Vertraulichkeitsvereinbarung hinzugezogen werden.

4.3.6.1 Physische Übermittlung von vertraulichen Informationen

Die Übermittlung von vertraulichen Informationen des BHS in Papierform muss über die untenstehenden Wege erfolgen:

- von Hand durch Mitarbeiter des BHS
- vorausgesetzt, dass die Informationen sicher verpackt sind, durch:
    - interne Postabteilung
    - staatlichen Postdienst oder renommierten Kurierdienst

4.3.6.2 Verbindungen zu externen IT-Ressourcen

Verbindungen von vernetzten PCs zu externen Systemen und Netzen dürfen nur über die von der IT-Abteilung freigegebenen und kontrollierten Verbindungswege hergestellt werden. Internetnutzungen bspw. über WLAN-Verbindungen, z. B. in Hotels, auf Flughäfen, Bahnhöfen oder in Zügen, sind im

erforderlichen Umfang zulässig, wenn die dafür vorgesehenen Schutzmechanismen vorhanden, aktuell und funktionsfähig sind.

4.3.6.3 Verhalten und (Fern-)Zugriff auf Reisen

Firmeninformationen und -vermögenswerte sind häufig am verletzlichsten, wenn Mitarbeiter auf Reisen sind. Wenn die nachstehenden Anweisungen befolgt werden, kann diese Bedrohung minimiert werden:

4.3.6.4 Vorsichtsmaßnahmen für die Besprechung von schutzbedürftigen Informationen

- Es dürfen keine schutzbedürftigen Informationen des BHS in öffentlichen Räumen wie Restaurants, Flugzeugen, Zügen oder Bars einschließlich öffentlicher Räume auf dem Firmengelände besprochen werden.
- Die Identität eines Anrufers, bevor mit ihm am Telefon über schutzbedürftige Informationen gesprochen wird, gilt es zu überprüfen.
- Es dürfen keine schutzbedürftigen Informationen auf einem Anrufaufzeichnungssystem hinterlassen werden.
- Nach Möglichkeit müssen Hotelzimmer-Safes für die Aufbewahrung von schutzbedürftigen Unterlagen oder Laptops genutzt werden.
- Vorträge vor Zuhörern, die nicht unter Geheimhaltungsvereinbarungen fallen, dürfen kein schutzbedürftiges Material des BHS enthalten. Vorträge dürfen keine Informationen enthalten, die europäischen oder nationalen Datenschutzgesetzen entgegenstehen.
- Es darf nicht über BHS-Informationen vor einem öffentlichen Forum oder mit Medienvertretern gesprochen werden, sofern die Person kein autorisierter Firmensprecher ist.

4.3.6.5 Fernzugriff

Ein Fernzugriff auf die Rechnersysteme des BHS kann nur mittels sicherer Methoden geschehen, die von der IT-Abteilung genehmigt worden sind.

Nur befugte Personen dürfen versuchen, sich mittels zugelassener Fernzugriffsmethoden mit den Rechnersystemen des BHS zu verbinden. Alle Versuche eines Fernzugriffs auf die Rechnersysteme des BHS werden protokolliert.

4.3.6.6 Verhalten auf Reisen

Notebooks und sonstige mobile Datenträger dürfen auf Reisen – z. B. in Zügen, aber bspw. auch während der Sicherheitskontrollen auf Flughäfen und an sonstigen öffentlichen Plätzen – nicht unbeaufsichtigt gelassen werden.

Notebooks dürfen nicht als Fluggepäck aufgegeben werden, sondern sind als Handgepäck mitzuführen und möglichst verborgen zu tragen. Bei Arbeiten auf dem Notebook in Zügen oder sonstigen einsehbaren Umgebungen ist auf einen ausreichenden Sichtschutz zu achten, z. B. durch Sichtschutzfolien, um ein Mitlesen durch unbefugte Personen zu verhindern. Ansonsten dürfen in öffentlichen Verkehrsmitteln keine personenbezogenen oder sonstigen sensiblen Daten verarbeitet werden.

4.3.7 E-Mail

4.3.7.1 Private Nutzung von E-Mail und Internet

Jede Nutzung der Rechnereinrichtungen des BHS, einschließlich des Zugangs zu Internet und E-Mail, wird als geschäftlich angesehen. Davon ausgenommen ist eine Nutzung aus betrieblichem Anlass/Interesse, z. B. zur Benachrichtigung von Familienangehörigen bei einem ungeplanten Anfall von Überstunden oder in sonstigen besonders begründeten Fällen. BHS behält sich das Recht vor, den Inhalt bestimmter E-Mails zu kontrollieren. Den Mitarbeitern ist dadurch nicht die Möglichkeit genommen, diese Werkzeuge in angemessener Weise für persönliche Zwecke zu benutzen.

4.3.7.2 Maßnahmen bei Verstößen

Bei einem Verdacht auf eine missbräuchliche oder unerlaubte Nutzung des Internetzugangs oder des E-Mail-Systems oder bei sonstigen Verstößen gegen diese Richtlinie oder sonstige Regelungen zur Nutzung der IT-Systeme werden auch weitere Überprüfungen, soweit möglich, ohne Personenbezug vorgenommen. Erhärtet sich der Verdacht auf eine missbräuchliche Nutzung und werden personenbezogene Überprüfungen erforderlich (z. B. Offenlegung der IP-Adresse des benutzten PCs), werden die Verdachtsmomente schriftlich dokumentiert (z. B. Systemprotokolle) und der Betroffene wird unter Beachtung der Regelungen des Bundesdatenschutzgesetzes (BDSG) und des Arbeits- und Tarifrechts über die vorgesehenen bzw. durchgeführten Überprüfungen und über die Ergebnisse informiert. Der Betroffene wird zu den Ergebnissen der Überprüfungen gehört. Die Unternehmensleitung behält sich vor, bei Verstößen gegen diese Richtlinie die private Nutzung des Internetzugangs und des E-Mail-Systems im Einzelfall zu untersagen.

4.3.7.3 Benutzung des E-Mail-Systems

Jedem berechtigten Mitarbeiter steht für betriebliche Zwecke ein persönliches E-Mail-Postfach zur Verfügung. Das E-Mail-System erlaubt sowohl eine Kommunikation über das interne Netz mit Mitarbeitern als über das externe Netz (Internet) mit Kunden und Geschäftspartnern.

Für den Betrieb des E-Mail-Systems sind ausschließlich die hierfür vorgesehenen und eingerichteten Programme zu benutzen.

4.3.7.4 Zugangsbereitschaft

Die Mitarbeiter haben bei Abwesenheit zur Information des Absenders den Abwesenheitsassistenten mit einer entsprechenden Benachrichtigung des Absenders einzuschalten. Bei einer unerwarteten Abwesenheit eines Mitarbeiters wird der Abwesenheitsassistent auf Anforderung des Vorgesetzten von der IT-Administration eingerichtet.

Eine Weiterleitung im Abwesenheitsfall an E-Mail-Adressen außerhalb des Firmennetzes und an private Adressen ist nicht zulässig.

4.3.7.5 Vertraulicher Versand von Daten und Informationen

Die E-Mails sind mit einer aussagekräftigen Betreffzeile zu versehen, um eine Identifikation des Absenders und Zuordnung der Nachrichten für Archivierungszwecke zu erleichtern.

Da der E-Mail-Verkehr nicht vertraulich ist, dürfen personenbezogene und sonstige vertrauliche Informationen, die den Vertraulichkeitsrichtlinien unterliegen, nicht im Klartext per E-Mail versandt werden. Personenbezogene und sonstige vertrauliche Informationen und Daten dürfen deshalb nicht oder nur verschlüsselt oder unter Nutzung eines anderen von der IT-Administration zur Verfügung gestellten ausreichend sicheren Verfahrens per E-Mail versandt werden.

Bei einem Versand einer E-Mail an mehrere Empfänger kann die Angabe aller Empfänger Datenschutzprobleme aufwerfen, da die einzelnen Empfänger aufgelistet sind und so voneinander erfahren. Falls die Empfänger nicht offenbart werden sollen, sind die E-Mails einzeln zu versenden oder es ist die Blindkopie-Funktion (BCC) zu benutzen.

4.3.7.6 E-Mails als Geschäftsbriefe

E-Mails aus der betrieblichen Korrespondenz können als Handels- oder Geschäftsbriefe gelten und müssen bezüglich der Fußleistenpflicht die Vorschriften des Gesetzes über elektronische Handelsregister und Genossenschaftsregister sowie das Unternehmensregister (EHUG) erfüllen.

Inhalt und Format dieser Signatur werden zentral verbindlich vorgegeben und dürfen für den externen Schriftverkehr in der jeweils aktuell vorliegenden Form und Ausführung nicht verändert werden. Diese Signaturregelung gilt auch für Abwesenheitsnotizen und für E-Mails, die von mobilen Geräten aus (z. B. Handys etc.) versendet werden.

4.3.7.7 Rechtliche Verbindlichkeit von E-Mails

Da E-Mails bei ihrer Übertragung verfälscht werden können, sind Authentizität und Integrität der E-Mail bzw. des Inhalts nicht gesichert und der Beweiswert ist als gering zu veranschlagen. Ist eine rechtsverbindliche E-Mail-Kommunikation erforderlich, darf dies nur mittels einer qualifizierten elektronischen Signatur oder eines anderen von der IT-Administration zur Verfügung gestellten ausreichend sicheren Verfahrens geschehen. Nicht signierte verbindliche Erklärungen sind über einen sicheren Kommunikationsweg, z. B. in Schriftform, zu bestätigen. Dies gilt auch für eingehende E-Mails.

4.3.7.8 Sonstige Verhaltensgrundsätze

E-Mails unbekannter Herkunft und mit nicht plausiblem Betreff oder nicht korrekter Sprache und Anhängen, sollten nicht geöffnet, sondern ungeöffnet gelöscht werden. In Zweifelsfällen ist die IT-Administration zur Prüfung der E-Mails einzuschalten. Es sollen nur inhaltlich plausible und von vertrauenswürdigen Stellen stammende E-Mails geöffnet werden.

Untersagt ist:

- der Versand oder eine Weiterleitung von Kettenbriefen und von sog. falschen Warnungen, z. B. vor Computerviren, oft in Verbindung mit der Aufforderung zur Änderung von Sicherheitseinstellungen oder Warnung von Freunden und Bekannten
- der Versand von E-Mails mit rechtswidrigen, beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, Gewalt verherrlichenden oder pornografischen

Äußerungen oder Abbildungen oder sonstigen anstößigen oder dem Ansehen des Unternehmens abträglichen Inhalten
- die Verbreitung von Inhalten, die gegen persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen
- das Verbreiten unbekannter Inhalte aus unsicheren Quellen, insbesondere mit Anhängen und ausführbaren Dateien
- die Verwendung der betrieblichen E-Mail-Adresse in öffentlichen Chat-Räumen oder Foren zum Zwecke der Zusendung von Spam oder Werbematerial
- die Veränderung oder die Aufhebung von Sicherheitseinstellungen des E-Mail-Programms oder von sonstigen Sicherheitseinstellungen

Private E-Mails sind unverzüglich aus den dem Benutzer zugeordneten Verzeichnissen zu löschen, um die Verzeichnisse von privaten Vorgängen zu entlasten.

4.3.7.9 Spamfilterung

Zum Schutz vor Spam-Mails, insbesondere solchen E-Mails, die aufgrund ihres Dateiformats schädliche Software enthalten können, aber auch um selbst keine Spam-Mails zu verbreiten, wird der ein- und ausgehende E-Mail-Verkehr elektronisch gefiltert und in einen Quarantäneordner verschoben. Die IT prüft den Inhalt des Quarantäneordners mehrmals täglich auf „positive“, d. h. fälschlicherweise als Spam eingeordnete, E-Mails und leitet diese an die entsprechenden Empfänger weiter. Festgestellte Schadsoftware wird aus Sicherheitsgründen im Zuge der Filterung sofort gelöscht.

Darüber hinaus behält sich das Unternehmen vor, im Rahmen der rechtlichen Möglichkeiten erforderlichenfalls E-Mails in einem automatisierten Prozess ohne persönliche Kenntnisnahme des Inhalts nach bestimmten Schlüsselwörtern zu durchsuchen, um unerwünschte Spam-Mails auszufiltern. Eine persönliche Kenntnisnahme des Inhalts, etwa durch den Systemadministrator, ist dabei unzulässig.

4.3.7.10 Erklärung über die private Nutzung

Jeder Beschäftigte erklärt schriftlich, ob er unter Anerkennung der Regelungen dieser Richtlinie den Internetzugang und das E-Mail-System auch für private Zwecke nutzen will. Mit dieser Erklärung willigt der Beschäftigte auch in die Protokollierung und Kontrolle der Verkehrsdaten im beschriebenen Umfang ein. Solange er diese Erklärung (**Anlage 1**) nicht abgibt bzw. die Nutzungsvereinbarung nicht unterzeichnet (**Anlage 2**), gilt für ihn ein Verbot der privaten Nutzung. Jeder Mitarbeiter sollte mit Eintritt in das BHS beide Anlagen vorgelegt bekommen und diese dann unterschreiben.

4.4 Erklärung zur privaten Nutzung der Kommunikationssysteme

Die Datenverarbeitungssysteme einschließlich der gesamten IT-Infrastruktur (Server, Netzwerke, Arbeitsplatz-PCs etc.) sowie der Datenbestände und Informationen zählen zur unternehmenskritischen Infrastruktur. Der Schutz dieser unternehmenskritischen IT-Infrastruktur sowie der Datenbestände und Informationen gegen Bedrohungen aller Art, z. B. durch Schadsoftware wie Computerviren, Trojaner etc., Spionage, Missbrauch und Fehlbedienung ist für das Unternehmen von großer Bedeutung.

Zum Schutz der Daten und Informationen vor diesen Risiken und auch zur Belegung der Ordnungsmäßigkeit und Sicherheit der Datenverarbeitung im Hinblick auf steuer- und handelsrechtliche Vorschriften sind Regelungen über Art und Umfang der Nutzung sowie eine Kontrolle der Nutzung und der Verarbeitungsabläufe einschließlich sicherheitsrelevanter Systemzustände und Aktionen erforderlich. Art und Umfang dieser Kontrollen und Protokollierungen sind in der Richtlinie „Informationssicherheit, Einsatz und Nutzung der IT-Systeme“ in der jeweils gültigen Fassung geregelt und in dem dort beschriebenen Umfang für den Bereich der betrieblichen Kommunikation unter dem Gesichtspunkt der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlagen auch datenschutzrechtlich zulässig.

5 Anlagen

Anlage 1 Erklärung zur Nutzung der IT-Infrastruktur innerhalb des BHS

240305_BHS_Anlage 1 - Datenschutzricht

Anlage 2 Vereinbarung über die Nutzung von Internet und E-Mail

240305_BHS_Anlage 2 - Datenschutzricht

Anlage 3 Technische und organisatorische Maßnahmen

240305_BHS_Anlage 3 - Datenschutzricht

Anlage 4 Verzeichnis der Verarbeitungstätigkeiten

240305_BHS_Anlage 4 - Datenschutzricht

Anlage 5 Verpflichtung der Mitarbeiter zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO)

240305_BHS_Anlage 5 - Datenschutzricht