Datenschutzrichtlinie

(Richtlinie IT und Datenschutz)

Regelungen zur Nutzung der IT-Infrastruktur

für

GEIGER
GmbH & Co. KG

–nachfolgend „Unternehmen“ genannt –

Inhaltsverzeichnis

1. Allgemeines

1.1 Einleitung

(1) Für das Unternehmen ist die Verfügbarkeit der IT-Systeme und der Daten von entscheidender Bedeutung. Ohne die IT-Systeme und Daten könnten zahlreiche Geschäftsprozesse nicht oder nur sehr eingeschränkt aufrechterhalten werden.

(2) Für das Unternehmen ist es daher wichtig, durch geeignete technische Vorkehrungen und organisatorische Maßnahmen dafür zu sorgen, dass die Verfügbarkeit der IT-Systeme und der Daten dauerhaft sichergestellt ist sowie Risiken für die IT-Systeme und die Daten möglichst auf ein Minimum reduziert werden.

(3) Ein Schutz der IT-Systeme kann dabei nur gelingen, wenn sich alle Mitarbeiter gemeinsam für die Sicherheit der IT-Systeme verantwortlich fühlen.

(4) Die IT-Abteilung entspricht der igepa papertec GmbH oder dem RZ-Dienstleister, die HRI IT-Services GmbH, beide mit Sitz in Berlin Brückenstraße 5a

1.2 Ziele der Richtlinie

(1) Die vorliegende Richtlinie IT und Datenschutz (die „Richtlinie“) soll verbindliche Regelungen treffen, wie die IT-Systeme und die Daten genutzt werden dürfen und zu schützen sind. DieRichtlinie soll alle wesentliche Aspekte der Nutzung der IT-Systeme regeln und damit als Orientierung für alle Mitarbeiter dienen.

(2) Eines der wesentlichen Ziele der Richtlinie ist der Schutz der IT-Systeme und Daten vor den Folgen eines Missbrauchs. Als Missbrauch kommen dabei sowohl vorsätzliche Handlungen in Betracht als auch unbeabsichtigte Verhaltensweisen.

1.3 Anwendungsbereich

(1) Die Richtlinie gilt für sämtliche IT-Systeme des Unternehmens, die den Mitarbeitern zur Nutzung zur Verfügung gestellt werden oder mit denen Mitarbeiter auf andere Weise in Betracht kommen.

(2) Die Richtlinie ist von allen Mitarbeitern verbindlich zu beachten. Soweit externe Dienstleister Zugang zu den IT-Systemen des Unternehmens erhalten, ist darauf zu achten, dass auch insoweit die Vorgaben der Richtlinie beachtet werden.

1.4 Definitionen

(1) IT-Systeme im Sinne der Richtlinie sind alle Hard- und Softwaresysteme (technische Einrichtungen, Betriebs- und Anwendungssysteme) einschließlich der Peripheriegeräte, digitaler Nebenstellenanlagen und Netzwerke. Typische IT-Systeme sind beispielsweise Arbeitsplatzrechner, E-Mail-Systeme, Internet-Zugänge und Telefonanlagen.

(2) Mitarbeiter sind alle Personen, die als Angestellte dauerhaft bei dem Unternehmen beschäftigt sind oder auf andere Weise, sei es vorübergehend oder langfristig, für das Unternehmen tätig sind. Praktikanten, Werkstudenten und ähnliche Personen gelten dabei ausdrücklich als Mitarbeiter.

(3) Personenbezogene Daten sind solche Daten, die sich auf eine konkrete natürliche Person beziehen, wobei der Bezug entweder bestehen muss oder zumindest hergestellt werden kann. Anonymisierte Daten oder aggregierte bzw. statistische Daten sind keinepersonenbezogenen Daten.

2. Generelle Verhaltensregeln

2.1 Erwartungshaltung des Unternehmens

(1) Die IT-Systeme dienen in erster Linie und vorrangig betrieblichen Zwecken des Unternehmens. Soweit nach Maßgabe der Richtlinie oder auf anderer Grundlage eine private Nutzung gestattet ist, darf diese sich keinesfalls negative auf die IT-Systeme oder die Produktivität der Mitarbeiter auswirken.

(2) Jeder Mitarbeiter hat im Rahmen der Nutzung der IT-Systeme darauf zu achten, dass sorg sammit den IT-Systemen umgegangen wird und jegliche Risiken für die IT-Systeme nach Möglichkeit ausgeschlossen werden oder, sofern dies nicht möglich ist, zumindest auf ein Minimum reduziert werden.

2.2 Explizit untersagtes Verhalten

(1) Bei der Nutzung der IT-Systeme sind jedwede Handlungen untersagt, die geeignet sind, Interessen des Unternehmens zu beeinträchtigen. Dies umfasst insbesondere Handlungen, die Gesetze, sonstige Rechtsvorschriften oder Rechte Dritter verletzen sowie sonstige Handlungen, die für das Unternehmen Nachteile mit sich bringen können und/oder das Ansehen des Unternehmens in der Öffentlichkeit beeinträchtigen.

(2) Bei der Nutzung der IT-Systeme sind insbesondere die nachfolgend aufgeführten Handlunge untersagt.

a) Abrufen, Anbieten oder Verbreiten von Inhalten, die gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungenverstoßen;

b) Herunterladen von Software, Musik oder urheberrechtlich geschützten Inhaltenunter Verletzung von Lizenzen und/oder Urheberrechten, selbst wenn esvermeintlich zu geschäftlichen Zwecken geschieht;

c) Abrufen, Anbieten oder Verbreiten beleidigender, verleumderischer, verfassungsfeindlicher, rassistischer, gewaltverherrlichender, sexistischer oder pornografischer Äußerungen, Abbildungen oder Inhalte;

d) Anbieten oder Verbreiten weltanschaulicher oder politischer Aussagen;

e) Verbreiten von Computer-Viren oder sonstiger Schadsoftware;

f) Abrufen, Anbieten oder Verbreiten von für unser Unternehmen kostenpflichtigen Internet-Seiten oder sonstigen kostenpflichtigen Leistungen zu nicht betrieblichen Zwecken;

g) Nutzung von Chat-Funktionalitäten und -angeboten zu privaten Zwecken.

3. Nutzung der IT-Systeme

3.1 Bereitstellung von IT-Systemen

(1) Das Unternehmen stellt den Mitarbeitern IT-Systeme zur Erfüllung der ihnen zugewiesenen Aufgaben zur Verfügung. Ein Anspruch auf eine bestimmte Ausstattung eines Arbeitsplatzes besteht nicht.

(2) Die Entscheidung, welche IT-Systeme den Mitarbeiter zur Verfügung gestellt werden, liegt alleine bei dem Unternehmen. Das Unternehmen ist insbesondere berechtigt, jederzeit diev orhandenen IT-Systeme auszutauschen, etwa im Rahmen einer Erneuerung der IT-Systeme.

3.2 Umgang mit IT-Systemen

(1) Der Umgang mit den IT-Systemen hat mit Rücksicht auf die Interessen des Unternehmens zuerfolgen.

(2) Die Hardware ist pfleglich zu behandeln. Beschädigungen der Hardware und Störungen der IT-Systeme sind der IT-Abteilung zu melden.

3.3 Nutzung von IT-Infrastruktur

(1) Die IT-Systeme dürfen ausschließlich für die vorgesehenen Zwecke verwendet werden; jede zweckwidrige Nutzung hat zu unterbleiben.

(2) Die Umgehung von Schutzmaßnahmen und die Ausnutzung von Sicherheitslücken sind untersagt.

4. Zugangsdaten

4.1 Berechtigungskonzept

(1) Die Mitarbeiter nutzen die IT-Systeme auf Grundlage eines von dem Unternehmenerarbeiteten Berechtigungskonzepts. Zugangsberechtigungen werden dabei so vergeben, dass die Mitarbeiter jeweils nur Zugang zu den IT-Systemen oder deren Teilbereichen haben,die für die jeweilige Aufgabenerfüllung erforderlich sind.

(2) Bestandteil des Berechtigungskonzepts ist die Vergabe von individuellen Zugangsdaten für jeden Mitarbeiter, die aus einem Benutzernamen und einem Passwort bestehen. Für unterschiedliche IT-Systeme kann es dabei unterschiedliche Zugangsdaten geben.

4.2 Vertraulichkeit von Zugangsdaten

(1) Die Mitarbeiter sind verpflichtet, die Zugangsdaten vertraulich zu behandeln. Die Zugangsdaten dürfen ausschließlich von den Mitarbeitern persönlich verwendet werden.

(2) Die Gestattung der Benutzung der IT-Systeme durch Dritte ist untersagt; gleiches gilt für die Weitergabe der eigenen Zugangsdaten, auch gegenüber anderen Mitarbeitern.

(3) Die Mitarbeiter der IT-Abteilung benötigen ebenfalls nicht die Passwörter von anderen Mitarbeitern; auch insoweit gilt die Pflicht zur Wahrung der Vertraulichkeit hinsichtlich der Zugangsdaten.

(4)Soweit ein Mitarbeiter den Verdacht hat, dass Dritten die eigenen Zugangsdaten bekanntgeworden sein könnten, sind die Zugangsdaten unverzüglich zu ändern; gleichzeitig ist die IT-Abteilung zu informieren.

(5) Zum Schutz der Zugangsdaten ist es untersagt, diese am Arbeitsplatz zu notieren.

4.3 Passwörter

(1) Die Passwörter müssen von den Mitarbeitern spätestens alle 12 Monate geändert werden.

(2) Die IT-Systeme weisen auf den Ablauf des jeweiligen Passwortes in einem angemessenen Abstand hin. Eine Anleitung zur Änderung des Passwortes wird mitgeliefert.

(3) Die Passwörter müssen mindestens acht Zeichen lang sein und – sofern das jeweilige IT-System entsprechenden Vorgaben erlaubt - mindestens zwei Buchstaben und eine Zahl enthalten.

(4) Es gelten die nachfolgend aufgeführten Passwortanforderungen:

- Die letzten 24 Passwörter dürfen nicht verwendet werden.
- Ein Passwort darf maximal 365 Tage alt sein.
- Ein Minimum für das Passwortalter gibt es nicht.
- Die Mindest-Passwortlänge sind 8 Zeichen.
- Komplexität: 3 Characters von Großbuchstaben, Kleinbuchstaben, Zahlen, Sonderzeichen.
- Der Anmeldename darf nicht im Passwort enthalten sein.

5. Persönliche Laufwerke

5.1 Einrichtung von Laufwerken

(1) Zur Speicherung persönlicher Daten können den Mitarbeitern persönliche Laufwerke zur Verfügung gestellt werden.

(2) Ein Anspruch auf die Bereitstellung oder die Verfügbarkeit der persönlichen Laufwerke besteht nicht.

(3) Das persönliche Laufwerk obliegt einer Quota. Diese Quota kann nicht überschritten werden Ist der Meldebestand erreicht, bekommt der Mitarbeiter eine Information zum Einhalten derGrenze. Die Daten sind zum Einhalten entsprechend zu löschen oder zu archivieren.

5.2 Nutzung der Laufwerke

(1) Von einer Speicherung von Daten, die für das Unternehmen wichtig sind, auf dem persönlichen Laufwerk wird ausdrücklich abgeraten. Bei einer Speicherung von Daten auf einem persönlichen Laufwerk ist beachten, dass andere Mitarbeiter während der Abwesen heit keinen Zugriff auf diese Daten haben.

(2) Die Organisation der Daten auf dem persönlichen Laufwerk liegt in der Verantwortung des Mitarbeiters. Der Mitarbeiter hat darauf zu achten, dass nicht mehr benötigte Daten gelöscht werden. Aufbewahrungspflichten Daten sind so abzuspeichern, dass diese dem Unternehmen während der Aufbewahrungsdauer zur Verfügung stehen.

5.3 Sicherung der Daten

Die Daten auf den persönlichen Laufwerken werden in die Datensicherung einbezogen. Soweit Daten nicht auf dem persönlichen Laufwerk, sondern beispielsweise auf einem lokalen Laufwerk abgespeichert werden, ist eine Datensicherung dagegen nicht gewährleistet.

5.4 Zugriff durch Dritte

(1) Es ist nicht gestattet, Dritten die Möglichkeit des Zugriffs auf das persönliche Laufwerk zuverschaffen. Das Unternehmen bleibt jedoch berechtigt, im Rahmen der allgemeinen Verwaltung und Betreuung der IT-Systeme auch Zugriff auf die persönlichen Laufwerke zunehmen, beispielsweise zur Überprüfung der auf dem persönlichen Laufwerk hinterlegte Daten auf Viren und andere Schadsoftware.

(2) Bei Ausscheiden des Mitarbeiters ist das persönliche Laufwerk zu bereinigen. Mit dem Ausscheiden ist das Unternehmen berechtigt, die auf dem persönlichen Laufwerk vorhandenen Daten zu sichten und über deren weitere Aufbewahrung bzw. Löschung zu entscheiden.

6. Software

6.1 Installation von Software

(1) Auf den IT-Systemen, die für die Nutzung durch Mitarbeiter vorgesehen sind, ist standardmäßig eine Auswahl von Software installiert, die für dienstliche Zwecke genutztwerden kann.

(2) Die Software wird im Rechenzentrum oder auf den lokalen Rechnern zur Verfügung gestellt.

(3) Eine Installation von weiterer Software auf den IT-Systemen ist mit der IT-Abteilung abzustimmen. Die Erlaubnis zur Installation von Software zu privaten Zwecken wird regelmäßig nicht erteilt.

(4) Ein Anspruch auf Vorhaltung der aktuellsten Versionen der jeweiligen Software besteht nicht.

(5) Die IT-Abteilung inventarisiert die eingesetzte Software und achtet darauf, dass für alle Installationen von Software ausreichende Lizenzen vorhanden sind. Die IT-Abteilung sorgt fürfehlerkorrigierende und sicherheitsrelevante Patche.

6.2 Freigabe von Software

(1) Die IT-Abteilung führt eine Übersicht über Software, die für den Einsatz auf IT-Systemen desUnternehmens freigegeben ist. Eine Software darf nur dann für die Nutzung freigegeben werden, wenn zuvor eine Prüfung der jeweiligen Software im Hinblick auf Risiken für die IT-Systeme des Unternehmens erfolgt ist.

(2) Die Erweiterung oder grundsätzliche Nutzung für bestimmte Softwareprodukte ist über den Benutzerantrag geregelt. Dieser ist vom Verantwortlichen zu stellen.

6.3 Nutzung von Software

Freigegebene Software ist entsprechend der Dokumentation der Software und den Vorgabender IT-Abteilung zu nutzen. Soweit Nutzungsbeschränkungen für die Software bestehen, sind diese zwingend einzuhalten.

7. Internet

7.1 Nutzung des Internets

(1) Das Unternehmen stellt den Mitarbeitern IT-Systeme zur Verfügung, die teilweise über einenInternet-Zugang verfügen. Ein Anspruch auf Gewährung eines Internet-Zugangs für alle Mitarbeiter besteht nicht.

(2) Soweit ein Internet-Zugang besteht, ist dieser primär für betriebliche Zwecke gedacht. Sofernzusätzlich auch eine private Nutzung gestattet ist, gelten hierfür ebenfalls die Regelungen der Richtlinie.

7.2 Filtersysteme

(1) Das Unternehmen ist jederzeit berechtigt, zur Verhinderung und weiteren Reduzierung vonRisiken eines Missbrauchs technische Vorkehrungen zu treffen, die insbesondere dafür sorgen, dass bestimmte Internetseiten und/oder Inhalte blockiert werden und gar nicht abrufbar sind. Hierzu zählen insbesondere softwaregestützte Filtersysteme, die den Zugriffauf bestimmte Internetseiten unterbinden.

(2) Das Unternehmen kann Filtersysteme im eigenen Ermessen konfigurieren. Es kann dabei auch geboten sein, Inhalte, die verschlüsselt übertragen werden, ebenfalls einer Prüfung zu unterziehen.

(3) Der Mitarbeiter bekommt die Informationen der Blockung im direkten Dialog kenntlich gemacht. Sollte die Blockung ungerechtfertigt sein und den Mitarbeiter in seiner Tätigkeit einschränken, kann er sich an die IT-Abteilung wenden, dass die Blockung aufgehoben wird Eine Freigabe vom Vorgesetzten ist hier erforderlich.

8. E-Mail

8.1 Nutzung von E-Mail

(1) Die Nutzung von E-Mails dient der schnellen und reibungslosen Kommunikation der Mitarbeiter. Über E-Mails kann sowohl eine interne Kommunikation der Mitarbeiter erfolgen als auch ein Austausch von Informationen mit Dritten.

(2) Jeder Mitarbeiter erhält eine eigene E-Mail-Adresse und ein damit verknüpftes Postfach, das für die Kommunikation genutzt werden kann.

(3) Die Postfächer sind in ihrer Kapazität beschränkt. Jeder Mitarbeiter hat daher sein Postfach so zu organisieren, dass die Kapazitätsgrenzen eingehalten werden, etwa durch das Löschenoder Archivieren nicht mehr benötigter E-Mails.

(4) Über das E-Mail-System können beliebige Anlagen empfangen oder versandt werden. Zur Vermeidung von Risiken sind PDF-Dateien gegenüber Dateien in einem Microsoft-Office Format zu bevorzugen. Ausführbare Dateien (.exe, .com, .bat) dürfen nur in Absprache mit der IT-Abteilung gespeichert und geöffnet werden.

(5) Das Unternehmen ist berechtigt, eingehende E-Mails entsprechend den Regelungen zur Internets zu überprüfen und zu filtern. Das Unternehmen darf insbesondere Spam-Filtereinsetzen und den Empfang von E-Mails bestimmter Absender blockieren. Sofern ein Absender zu Unrecht blockiert wird oder ein Absender zusätzlich blockiert werden soll, ist dies der IT-Abteilung mitzuteilen.

(6) Bei dem Versand von E-Mails ist vor dem Absenden zu überprüfen, ob die richtigen Empfänger angegeben sind. Im Hinblick auf die Unterrichtung weiterer Mitarbeiter sind nur solche Mitarbeiter aufzunehmen, die mit dem Vorgang befasst sind. Eine E-Mail an alle Mitarbeiter hat nur zu erfolgen, wenn die Information wirklich für alle Mitarbeiter relevantist.

(7) Sollen E-Mails verschlüsselt oder elektronisch signiert werden bzw. solche E-Mails empfangen werden, sind die technischen Voraussetzungen hierfür mit der IT-Abteilung abzustimmen.

(8) Verschlüsselte E-Mails von einem externen Empfänger werden zur Minimierung der Sicherheitsrisiken entschlüsselt, dann gescannt und wieder verschlüsselt zum beabsichtigten Empfänger weitergeleitet. Ein Scannen von verschlüsselten E-Mails ist nicht möglich.

8.2 Signaturen

(1) Das E-Mail-System ist so konfiguriert, dass Bestandteil jeder E-Mail eine Signatur ist, diesewohl den Namen des konkreten Mitarbeiters als auch die Pflichtenangaben des Unternehmens beinhaltet.

(2) Die Signaturen werden von der IT-Abteilung zentral gepflegt. Jede Veränderung der Signaturen ist mit der IT-Abteilung abzustimmen. Es ist nicht erlaubt, die Signaturen bei externer Kommunikation zu deaktivieren oder eigenmächtig zu verändern.

8.3 Stellvertretung

(1) Sofern eine E-Mail im Auftrag eines anderen Mitarbeiters versendet werden soll, ist dies entsprechend kenntlich zu machen. Entweder hat im Rahmen der eingerichteten Stellvertretungen ein Hinweis auf den Versand „im Auftrag“ zu erfolgen oder es hat eine Klarstellung im Rahmen der Signatur zu erfolgen.

(2) Es ist unzulässig, E-Mails über das Postfach eines anderen Mitarbeiters zu versenden, ohne dass dies ersichtlich wird.

8.4 Archivierung

(1) Das Unternehmen ist verpflichtet, geschäftliche Korrespondenz zu archivieren. Die Archivierungspflicht gilt dabei auch für eine Kommunikation per E-Mail.

(2) Die Archivierung von E-Mails kann dabei so erfolgen, dass bereits zentral vor der Weiterleitung der E-Mails in die einzelnen Postfächer eine Erfassung aller E-Mails erfolgt oder die Pflicht zur Archivierung der relevanten Nachrichten jedem Mitarbeiter einzeln zugewiesen wird.

9. Telefonie

9.1 Telefonanlage

(1) Das Unternehmen verfügt über eine zentrale Telefonanlage, die für interne Kommunikationund für Telefonate mit Dritten genutzt werden kann.

(2) Die Telefonanlage erfasst die Rufnummern aller eingehenden und ausgehenden Telefonate pro Nebenstellenanschluss einschließlich Datum und Dauer. Zusätzlich kann das Unternehmen von dem jeweiligen Diensteanbeiter einen Einzelverbindungsnachweis erhalten; eine Pflicht zur Kürzung der dort angegebenen Rufnummern besteht nicht. Eine Aufzeichnung oder Auswertung der Inhalte der unter Nutzung der Telefonanlage geführten Gespräche erfolgt nicht.

(3) Das Unternehmen ist berechtigt, einzelne Telefonnummer insgesamt oder an bestimmten Nebenstellenanschluss zu sperren, beispielsweise Auslandsverbindungen oderMehrwertdiensterufnummern.

(4) Das Unternehmen duldet private Telefongespräche, sofern diese nicht den Arbeitsablauf beeinträchtigen. Private Telefongespräche können über die CTI-Software am Client vom Anwender kenntlich gemacht werden.

9.2 Telefonbuch

(1) Alle Namen und Telefonnummern der Mitarbeiter werden in einem zentralen Telefonbucherfasst, dass von jedem Mitarbeiter für dienstliche Zwecke genutzt werden kann. Die Weitergabe des Telefonbuchs an Dritte, die nicht Mitarbeiter des Unternehmens sind, ist nicht vorgesehen.

(2) Soweit das Telefonbuch um weitere Informationen erweitert werden kann (etwa private Telefonnummern der Mitarbeiter o.ä.), werden solche Erweiterungen ausschließlich auf Basis einer Einwilligung des Mitarbeiters vorgenommen. Die Einwilligung im Hinblick auf diese weiteren Daten kann jederzeit widerrufen werden; ein Widerspruch gegen die Veröffentlichung von Name und Telefonnummer im internen Telefonbuch ist dagegen nich möglich.

10. Datenträger

10.1 USB-Sticks

(1) Die IT-Systeme des Unternehmens verfügen teilweise über USB-Anschlüsse, an die auch USB-Sticks angeschlossen werden können. Für die Nutzung innerhalb des Unternehmens stellt dasUnternehmen USB-Sticks zur Verfügung, die über die IT-Abteilung bei Bedarf erhältlich sind.

(2) Wegen der damit verbundenen Risiken dürfen eigene (private) USB-Sticks und USB-Sticks von Dritten nur in Abstimmung mit und gegebenenfalls nach Prüfung durch die IT-Abteilung verwendet werden.

10.2 Cloud Speicherdienste

(1) Die Nutzung von Cloud Speicherdiensten wie Google Drive o.ä. ist grundsätzlich untersagt, die Ausnahme bildet Microsoft One Drive im Rahmen der Nutzung Ihres Unternehmensbenutzerkontos.

10.3 Sonstige Datenträger

Die vorstehenden Regelungen gelten entsprechend auch für sonstige Datenträger, die an die IT-Systeme des Unternehmens angeschlossen werden können. Sonstige Datenträger können dabei vor allem externe Festplatten, aber auch Medien wie CD und DVD sein.

11. Datenübermittlung

11.1 Interner Datenaustausch

(1) Der freie Austausch von Informationen und Daten innerhalb des Unternehmens ist ausdrücklich erwünscht. Gleichzeitig ist jedoch im Hinblick auf vertrauliche Informatione und personenbezogene Daten zu überprüfen, inwieweit Gründe gegen einen internen Austausch sprechen.

(2) Sofern Informationen und Daten auch innerhalb des Unternehmens besonders geschützt werden sollen, kommt die Speicherung auf dem persönlichen Laufwerk oder eine gesonderte Verschlüsselung in Betracht.

11.2 Verschlüsselung

(1) Bei der Übermittlung an Dritte ist zu beachten, dass ein Versand per E-Mail standardmäßig ohne besondere Sicherheitsvorkehrungen erfolgt. Es ist daher vorab zu prüfen, ob unter Berücksichtigung der Relevanz der Daten für das Unternehmen und der gesetzliche Vorgaben besondere Sicherheitsvorkehrungen getroffen werden müssen, beispielsweise in Form einer Verschlüsselung.

(2) Neben der Verschlüsselung von E-Mails kommt auch die Verschlüsselung von Dateien in Betracht, die dann E-Mail oder mit Hilfe eines mobilen Datenträgers an dem Empfänger übermittelt werden können. In solchen Fällen ist dann darauf zu achten, dass die Informationen zur Entschlüsselung der Daten separat übermittelt werden müssen.

11.3 Weitergabe von Datenträgern

Eine Weitergabe von Datenträgern, die Daten des Unternehmens enthalten, ist grundsätzlich untersagt. Sofern ein Austausch von Daten mit Hilfe eines externen Datenträgers erfolgen soll, sind ausschließlich hierfür vorgesehene Datenträger zu verwenden, die von der IT-Abteilung zu beschaffen sind. Als durch die IT beschafften Datenträger gilt ebenfalls das One Drive Laufwerk Ihres Unternehmensbenutzerkontos. Für die Weitergabe von personenbezogenen oder sensiblen Daten ist grundsätzlich die Genehmigung der Geschäftführung oder des Datenschutzbeauftragen einzuholen. Als sensible Daten gelten zusätzlich zu den gesetzlich als solche Deklarierten: Finanzauskünfte den Unternehmens, Einkaufsverträge und Einkaufskonditionen, Lieferantenverträge, Produktinformationen….

12. Zusammenarbeit mit externen Dienstleistern

12.1 Auftragsdatenverarbeitung

(1) Soweit externe Dienstleister zumindest die Möglichkeit der Kenntnisnahme von personenbezogene Daten von Mitarbeitern oder Kunden haben, ist vor der Zusammenarbeitmit diesen Dienstleistern eine Vereinbarung zur Auftragsverarbeitung gemäß den datenschutzrechtlichen Vorschriften abzuschließen.

(2) Die Übermittlung von personenbezogenen Daten oder die Gewährung des Zugriffs auf solche Daten darf erst dann erfolgen, wenn die Vereinbarung zur Auftragsverarbeitung in unterschriebener Form vorliegt.

(3) Alle Vereinbarungen zur Auftragsverarbeitung werden im Unternehmen zentral erfasst; zusätzlich ist der Datenschutzbeauftragte bei dem Abschluss von Vereinbarungen zur Auftragsverarbeitung einzubeziehen.

12.2 Überwachung von Dienstleistern

(1) Die Dienstleister sind in regelmäßigen Abständen hinsichtlich der bei Ihnen getroffenen Maßnahmen zur Gewährung von Datenschutz und Datensicherheit zu kontrollieren. Eine Kontrolle kann dabei auch durch die Übersendung von Fragebögen oder die Anforderungen von Berichten des Dienstleisters erfolgen.

(2) Soweit sich bei einem Dienstleister Anzeichen für Datenschutzverstöße oder einen nicht ordnungsgemäßen Umgang mit Daten zeigen, ist der Datenschutzbeauftragte des Unternehmens zu informieren.

13. Fernwartung

13.1 Vorgaben zur Fernwartung

(1) Die Fernwartung ermöglicht Dienstleistern den Zugriff auf die IT-Systeme des Unternehmens,ohne dass der Dienstleister vor Ort im Unternehmen sein muss. Wegen der damitverbundenen Risiken ist eine Fernwartung nur unter besonderen Voraussetzungen zulässig.

(2) Eine Fernwartung findet nur statt, soweit der Fernwartungsdienstleister eine Vereinbarung zur Auftragsverarbeitung abgeschlossen hat. Etwas anderes gilt nur, wenn eine Kenntnisnahme von personenbezogenen Daten durch den Dienstleister vor der Fernwartung sicher ausgeschlossen werden kann.

(3) Jeder Fall, bei dem eine Verbindung zur Fernwartung mit IT-Systemen des Unternehmensaufgebaut wird, ist zuvor abzustimmen. Eine Fernwartung ohne Abstimmung mit dem Unternehmen ist unzulässig. Die Fernwartung ist nach Möglichkeit so zu konfigurieren, dass der Verbindungsaufbau durch das Unternehmen erfolgt.

13.2 Kontrolle der Fernwartung

(1) Die Durchführung der Fernwartung ist von mindestens einem Mitarbeiter des Unternehmen zu überwachen. Der Mitarbeiter muss jederzeit die Möglichkeit, die Fernwartungsverbindun zu unterbrechen.

(2) Nach Abschluss der Fernwartung ist von dem Dienstleister ein Protokoll der durchgeführten Tätigkeiten zu übersenden.

14. Mobile Endgeräte

14.1 Mobile Device Management

(1) Unser Unternehmen behält sich vor, ein System für das Mobile Device Management einzusetzen, mit dem die Verwaltung, Kontrolle und Konfiguration der mobilen Endgeräte (z. B. Smartphones, Tablets, Laptops) erfolgen kann.

(2) Bei Einführung eines Mobile Device Management Systems sind die zugrundeliegenden rechtlichen und tatsächlichen Gesichtspunkte der Einführung zu dokumentieren.

14.2 Sicherheitsvorgaben (PIN / Passwort)

Der Mitarbeiter hat die auf dem mobilen Endgerät gespeicherten Daten durch geeignete Sicherheitsmaßnahmen vor dem unberechtigten Zugriff durch Dritte zu schützen, insbesondere durch die Nutzung der Bildschirmsperre und die Nutzung eines PIN-Codes bzw. Passworts.

14.3 Installation von Software / Apps

(1) Soweit Mitarbeiter des Unternehmens mobile Endgeräte benutzen, sollen diese vorbehaltlich anderer Regelungen lediglich zu dienstlichen Zwecken verwendet werden. Die Regelungen zur Installation und Nutzung von Software nach der Richtlinie gelten auch für mobile Endgeräte.

(2) Sofern das Unternehmen keine anderen Anweisungen erteilt, ist der Mitarbeiter verpflichtet, das Betriebssystem des privaten mobilen Geräts auf dem jeweils für das Gerät supporteten Patchlevel der IT-Abteilung zu halten. Der Mitarbeiter hat zu diesem Zweck alle vom Hersteller verfügbaren bzw. von der IT-Abteiilung freigegebenen Sicherheits-Patches, Updates und Upgrades unverzüglich zu installieren.

(3) Dem Mitarbeiter ist es vorbehaltlich anderer Regelungen untersagt, das Betriebssystem oder die auf dem mobilen Gerät installierte Software zu verändern. Dies betrifft insbesondere sogenannte „Jailbreaks“ oder „Roots“ durch die vom Hersteller implementierte technische Nutzungsbeschränkungen umgangen oder beseitigt werden.

14.4 Datenspeicherung

(1) Die Speicherung von nicht betriebsbezogenen Daten auf dem mobilen Endgerät ist untersagt, soweit eine Privatnutzung nicht ausdrücklich gestattet wurde.

(2) Im Hinblick auf dienstliche Daten hat der Mitarbeiter eigenständig dafür Sorge zu tragen, dass wesentliche Daten für den Fall des Verlustes von Daten oder des mobilen Endgerätes gesichert werden. Lösungen von Drittanbietern, insbesondere cloudbasierte Backupsysteme, dürfen hierfür nur dann eingesetzt werden, wenn diese von der IT-Abteilung freigegeben wurden.

14.5 Nutzung durch Dritte

(1) Es ist nicht gestattet, Dritten die Nutzung von dienstlichen mobilen Endgeräten zu ermöglichen.

(2) Eine Weitergabe der Zugangsdaten an Dritte einschließlich Familienangehörige und andere Mitarbeiter des Unternehmens ist untersagt.

14.6 Verlust eines Gerätes

(1) Im Falle des Verlusts, der Beschädigung oder der Gefährdung des mobilen Endgerätes bzw. der darauf gespeicherten oder darüber zugänglichen dienstlichen Daten, z. B. durch Späh- oder Schadsoftware, hat der Mitarbeiter das Unternehmen unverzüglich zu informieren. Eine solche Information hat auch zu erfolgen, wenn der Mitarbeiter den begründeten Verdachthat, dass ein unbefugter Dritter auf das Endgerät zugegriffen hat oder er das mobile Endgerätnur für eine längere Zeitspanne (mehr als 24 Stunden) nicht auffinden kann.

(2) Der Mitarbeiter wird das Unternehmen in einem solchen Fall im Rahmen des Zumutbaren unterstützen, um negative Folgen für die Vertraulichkeit, Integrität und Verfügbarkeit der dienstlichen Daten zu vermeiden.

14.7 Herausgabe des Gerätes

(1) Auf Verlangen des Unternehmens haben Mitarbeiter die betrieblichen mobilen Endgeräte an das Unternehmen herauszugeben. Eine Herausgabe kann insbesondere zur Aktualisierung der Software oder der Daten auf dem mobilen Endgerät, zur Kontrolle der Einstellungen auf dem mobilen Endgerät und zum Austausch des mobilen Endgerätes erfolgen.

(2) Das Unternehmen ist berechtigt, jederzeit über alle Inhalte und Daten zu verfügen, die auf dem mobilen Endgerät gespeichert sind.

(3) Die IT-Abteilung hält sich vor, die auf dem Gerät befindlichen Daten und/oder Apps zu verwalten und bei Missbrauch zu löschen oder das Gerät selbst zu deaktivieren.

15. Einsatz von privaten Geräten

15.1 Nutzung von privaten Geräten

(1) Vorbehaltlich abweichender Regelungen und Vereinbarungen ist die Nutzung privater Geräte für dienstliche Zwecke nicht gestattet. Die Mitarbeiter können aber im Einzelfall von dem Unternehmen berechtigt werden, ihre privaten Geräte auch zu dienstlichen Zwecken zunutzen. Umfang und Ausmaß der Privatnutzung werden in diesem Fall zwischen dem Unternehmen und dem Mitarbeiter abgestimmt; insbesondere können spezielle für die Nutzung zu dienstlichen Zwecken zugelassene Gerätetypen festgelegt werden.

(2) Die Mitarbeiter haben dafür Sorge zu tragen, dass sie ihre privaten Geräte zu dienstlichen Zwecken verwenden dürfen und insbesondere im Fall von mobilen Endgeräten der hierfür gegebenenfalls abgeschlossene Mobilfunkvertrag eine solche Nutzung gestattet.

(3) Bei der Verwendung von privaten Geräten sind die dienstlichen Daten von den privaten Daten des Mitarbeiters zu trennen.

(4) Wird das Gerät an Dritte weitergeben, so sind sämtliche Daten auf dem Gerät zu löschen. Das Gerät ist auf Werkseinstellung zurückzusetzen. Die IT-Abteilung hält sich vor, diese Aktion durchzuführen und zu kontrollieren.

(5) Die unter Punkt 14 angegebenen Richtlinien gelten auch für private Geräte.

15.2 Übertragung von Daten auf private Geräte

(1) Die Übertragung von geschäftlichen Daten unseres Unternehmens auf private Geräte ist nurzulässig, soweit die dienstliche Nutzung des privaten Geräts durch unser Unternehmen gestattet wurde.

(2) Es ist demnach insbesondere nicht zulässig, dienstliche Daten auf mobilen Datenträgern zu speichern, diese anschließend an private Geräte anzuschließen, dort die dienstlichen Datenweiterzubearbeiten und anschließend wieder auf die IT-Systeme des Unternehmens zuübertragen.

15.3 Weiterleitung von E-Mails auf private Geräte

(1) Die Weiterleitung von E-Mails auf private Geräte ist nur zulässig, soweit die dienstliche Nutzung des privaten Geräts im Einzelfall durch das Unternehmen gestattet ist.

(2) Ohne eine entsprechende Gestattung ist es nicht zulässig, eine Weiterleitung in der Weise einzurichten, dass E-Mails, die an das Postfach des Mitarbeiters gehen, von dort auf eine private E-Mail-Adresse des Mitarbeiters weitergeleitet werden.

16. Heimarbeitsplätze

16.1 Anforderungen bei Heimarbeit

(1) Mit Einwilligung unseres Unternehmens dürfen Mitarbeiter auch von außerhalb über einen gesicherten Zugang (VPN) auf die IT-Systeme des Unternehmens zugreifen („Heimarbeit“).

(2) Für die Heimarbeit erhalten die Mitarbeiter in der Regel in mobiles Endgerät. Im Einzelfall ist es auch denkbar, dass auf privaten Geräten, die für die dienstliche Nutzung freigegeben sind, ein VPN-Zugang zu den IT-Systemen des Unternehmens eingerichtet wird. In diesem Fall ist im Vorfeld die Lizenzbedingung mit dem Unternehmen zu klären.

(3) Der VPN-Zugang ist mit einer Zweitidentifizierung versehen. Die sogenannteTransaktions-kennung (TAK) wird nach erfolgreicher Erstidentifikation per SMS oder per E-Mail mitgeteilt. Die TAK ist 30 Sekunden gültig.

(4) Der VPN-Zugang muss über den Benutzerantrag eingestellt werden.

(5) Mitarbeiter haben dafür Sorge zu tragen, dass das in der Richtlinie beschriebene Schutzniveau auch im Falle von Heimarbeit nicht unterschritten wird. Insbesondere sind Vorkehrungen zu treffen, dass Dritten keine Möglichkeit zur Kenntnisnahme von Daten des Unternehmens geschaffen wird.

(6) Ein Anspruch auf Heimarbeit wird durch die Richtlinie nicht begründet.

16.2 VPN-Zugang

(1) Soweit von außerhalb eine Verbindung zu den IT-Systemen des Unternehmens erfolgt, muss dies über die hierfür vorgesehenen Verbindungen erfolgen, insbesondere unter Nutzung eines VPN-Zugangs.

(2) Der VPN-Zugang ist zwingend von der IT-Abteilung einzurichten. Soweit hierfür besondere Zugangsdaten erforderlich sind, gelten hierfür die allgemeinen Regelungen der Richtlinie.

16.3 Zugriff auf zentrale IT-Infrastruktur

Jede andere Form des Fernzugriffs auf die zentrale IT-Infrastruktur des Unternehmens und einzelne IT-Systeme ist untersagt. Die Gewährung eines Zugriffs auf die IT-Systeme durc Dritte unter Nutzung von mobilen Endgeräten und privaten Geräten hat zu unterbleiben.

17. Videoüberwachung

17.1 Vorgaben zur Videoüberwachung

(1) Das Unternehmen ist berechtigt, unter Beachtung der gesetzlichen Bestimmungen einzelne Bereiche des Betriebsgeländes mit Hilfe einer Videoüberwachung zu kontrollieren. Die Video überwachung darf unter keinen Umständen dazu führen, dass Mitarbeiter während ihrer Tätigkeit für das Unternehmen dauerhaft im Erfassungsbereich der Videoüberwachung tätig sein müssen. Die Einzelheiten der Videoüberwachung mit dem Datenschutzbeauftragten abzustimmen und von diesem zu dokumentieren.

(2) Soweit eine Videoüberwachung stattfindet, sind die überwachten Bereiche durch geeignete Hinweise, beispielsweise ein Piktogramm zur Kennzeichnung von Videoüberwachung gemäß DIN 33450, zu kennzeichnen. Unter dem Piktogramm ist die für die Videoüberwachung verantwortliche Stelle zu benennen, sofern diese nicht ohnehin ersichtlich ist.

17.2 Dokumentation der Videoüberwachung

(1) Vor der Einführung einer Videoüberwachung sind die zugrundeliegenden rechtlichen und tatsächlichen Gesichtspunkte, die für die Videoüberwachung maßgeblich sind, in einem Bericht zu dokumentieren.

(2) Die Dokumentation umfasst mindestens eine Darstellung der technischen und organisatorischen Umsetzung sowie der berücksichtigten schutzwürdigen Interessen der Betroffenen. Bestandteil der Dokumentation muss auch eine datenschutzrechtliche Interessenabwägung aller in Frage kommender Interessen sein.

18. Private Nutzung

18.1 Private Internet-Nutzung

(1) Mitarbeiter haben keinen Anspruch auf die Gestattung der privaten Nutzung eines Internet Zugangs des Unternehmens. Soweit das Unternehmen eine Privatnutzung gestattet, erfolg diese Gestattung freiwillig und steht im alleinigen Ermessen unseres Unternehmens. Das Unternehmen ist jederzeit berechtigt, die Gestattung der Privatnutzung ganz oder teilweise zu widerrufen und/oder zu beenden. Dies gilt insbesondere, wenn Mitarbeiter die sich aus der Richtlinie ergebenden Pflichten verletzen.

(2) Zwar sprechen einige Gerichtsentscheidungen dafür, dass das Unternehmen bei einer Gestattung der Privatnutzung betrieblicher Internet-Accounts nicht an das Fernmeldegeheimnis nach § 88 des Telekommunikationsgesetzes (nachfolgend „TKG“)gebunden ist. Angesichts dessen, dass diese Entscheidungen keinen Bestand haben könnten oder sich die insoweit ohnehin umstrittene Rechtslage ändern sollte, steht die Gestattung der Privatnutzung stets unter dem Vorbehalt, dass der jeweilige Mitarbeiter eine Zusatzvereinbarung unterzeichnet und so das Unternehmen durch die ausdrückliche Einwilligung von den Beschränkungen des Fernmeldegeheimnisses nach § 88 TKG befreit.

(3) Die Einwilligung des jeweiligen Mitarbeiters ist freiwillig und der Mitarbeiter kann dieser jederzeit mit Wirkung für die Zukunft widerrufen. Ab Zugang des Widerrufs entfällt gleichzeitig mit Wirkung für die Zukunft die Berechtigung zu der Privatnutzung des Internetzugangs. Sofern keine berechtigten Interessen des jeweiligen Mitarbeiters entgegestehen, ist ein Widerruf der Einwilligung allerdings insoweit ausgeschlossen, wie dadurch die Verarbeitung und Nutzung von Informationen in Zusammenhang mit der Nutzung des Internet-Zugangs aus dem Zeitraum vor dem Widerruf eingeschränkt würde. Damit bleibt das Unternehmen auch im Falle eines Widerrufs der Einwilligung für Informationen in Zusammenhang mit der Nutzung des Internet-Zugangs für diejenigen Zeiträume von den Beschränkungen des Fernmeldegeheimnisses befreit, in denen die Privatnutzung gestattet war.

(4) Das Unternehmen gewährt dem Mitarbeiter keine Mindestverfügbarkeit und/oder Fehlerfreiheit des Internet-Zugangs und damit zusammenhängender technischer Einrichtungen. Der Mitarbeiter ist für eine etwaige Sicherung privater Inhalte selbst verantwortlich. Das Unternehmen ist gegenüber dem Mitarbeiter weder für etwaige Fehlerund/oder Ausfälle des Internet-Zugangs und damit im Zusammenhang stehender technischer Einrichtungen verantwortlich, noch für etwaige daraus folgende Schäden und andere Nachteile, insbesondere Datenverluste.

(5) Die Mitarbeiter haben eine Privatnutzung des Internet-Zugangs in Art und Umfang eigenverantwortlich so zu beschränken, dass Interessen des Unternehmens hierdurch nicht beeinträchtigt werden.

(6) Die Privatnutzung ist auf gelegentliche Fälle zu beschränken, so dass insbesondere die ordnungsgemäße Erfüllung der geschuldeten Arbeitsleistung und sonstiger dem jeweilige Mitarbeiter obliegender Pflichten sichergestellt ist und nicht beeinträchtigt wird. Eine solch Beeinträchtigung ist grundsätzlich nicht anzunehmen, wenn die Privatnutzung auf Pausenzeiten oder die Freizeit des jeweiligen Mitarbeiters beschränkt ist.

(7) Die Nutzung privater Browserprofile, die sich auf andere Geräte synchronisieren, ist untersagt.

18.2 Private E-Mails

(1) Die betrieblichen Postfächer sind ausschließlich betrieblich zu nutzen, eine private Nutzung ist untersagt. Um den Mitarbeitern gleichwohl die Möglichkeit zu geben, auch private E-Mails zu versenden und zu empfangen, können hierfür Webmail-Dienste genutzt werden Webmail-Diensten sind Angebote Dritter, die einem Mitarbeiter über eine Internetseite den Zugriff auf sein privates E-Mail-Account ermöglichen.

(2) Um den Mitarbeitern die Nutzung von Webmail-Diensten zu ermöglichen, wird das Unternehmen solche Angebote nicht generell sperren. Es besteht jedoch kein Anspruch darauf, dass der Zugriff auf bestimmte Webmail-Dienste über den Internet-Zugang des Unternehmens möglich ist.

(3) Das Unternehmen ist nicht dafür verantwortlich, wie die über den Internet-Zugang abrufbaren Webmail-Dienste verfügbar sind und welche Regelungen des Diensteanbieters für die Nutzung gelten. Es ist Sache der Mitarbeiter, Vereinbarungen mit den jeweiligen Diensteanbietern über die Nutzung der Webmail-Dienste zu treffen; das Unternehmen ist an solchen Vereinbarungen nicht beteiligt.

(4) Soweit die Nutzung der Webmail-Dienste über den Internet-Zugang erfolgt, unterliegt die Nutzung der Webmail-Dienste den gleichen Kontrollen wie die Nutzung sonstiger Internetseiten. Das Unternehmen wird insoweit aber eine Nutzung grundsätzlich nur im Rahmen der Missbrauchskontrolle und innerhalb der hierfür vorgesehenen Grenzen vornehmen.

(5) Mitarbeiter sind nicht berechtigt, Korrespondenz, die nicht ausschließlich privater Natur und damit zumindest auch betrieblicher Natur ist, über Webmail-Dienste abzuwickeln. E-Mails, die nicht ausschließlich private Inhalte sondern zumindest auch geschäftliche Inhalte zum Gegenstand haben, sind als betriebliche E-Mails anzusehen.

18.3 Private Nutzung der Telefonanlage und von mobilen Endgeräten

(1) Das Unternehmen toleriert die gelegentliche Privatgespräche unter Nutzung der Telefonanlage, soweit hierfür keine oder nur unwesentliche Kosten für das Unternehmen entstehen (Ortsgespräche, kurze Gespräche in Mobilfunknetze, o.ä.). Sofern ein Mitarbeite private Gespräche unter Beachtung dieser Beschränkungen führt, muss zugleich die Bereitschaft bestehen, dass dies Gesprächsdaten (ohne den Gesprächsinhalt) in gleicher Weise erfasst und ausgewertet werden wie dienstliche Telefonate.

(2) Soweit ein Mitarbeiter über ein mobiles Endgerät verfügt und eine Privatnutzung dieses Gerätes durch das Unternehmen gestattet worden ist, muss im Rahmen der technischen Möglichkeiten für eine Trennung von privaten und geschäftlichen Daten gesorgt werden. Eine Nutzung von geschäftlichen Daten für private Zwecke hat zu unterbleiben.

(3) Das Unternehmen kann „Computer Telephone Integrated“ (CTI) als Unterstützungs-softwareeinsetzen und dem Benutzer dazu berechtigen. Ein- und ausgehende Telefon-gespräche werden in diesem Fall gegen Datenbanken gegengeprüft. Die Prüfungen und daraus resultierenden Ergebnisse werden ausschließlich zu internen Zwecken genutzt. EineWeitergabe an Dritte findet nicht statt.

19. Abwesenheit und Ausscheiden von Mitarbeitern

19.1 Geplante Abwesenheit

(1) Die Mitarbeiter haben eigenständig Vorkehrungen zu treffen, dass für den Fall einer geplanten Abwesenheit (Urlaub, Fortbildung, o.ä.) eingehende E-Mails weitergeleitet werden und so eine Beantwortung möglich ist. Der Mitarbeiter soll die entsprechende Weiterleitung selbst einrichten.

(2) Zusätzlich kann im Ermessen des Mitarbeiters eine Abwesenheitsnachricht aktiviert werden. Soweit das Unternehmen entsprechende Textbausteine zur Verfügung stellt, soll der Mitarbeiter sich hier an orientieren.

(3) Ein weitergehender Zugriff auf Daten des Mitarbeiters, insbesondere auf sein persönliche Laufwerk und sein Postfach erfolgt grundsätzlich nicht, sofern nicht zwingende dienstliche Erfordernisse des Unternehmens einen solchen Zugriff rechtfertigen. Zuvor ist gegebenen-falls zu versuchen, mit dem Mitarbeiter in Kontakt zu treten, sofern dies als milderes Mittel anzusehen ist. Im Falle eines Zugriffs erfolgt die Einbeziehung des Datenschutzbeauftragten; der Mitarbeiter wird anschließend über den Zugriff informiert.

19.2 Ungeplante Abwesenheit

(1) Für den Fall einer ungeplanten Abwesenheit haben Mitarbeiter Vorkehrungen zu treffen, die die Fortführung ihrer dienstlichen Aufgaben ermöglichen. Hierzu können beispielsweis vorsorglich Stellvertretungen und Zugriffsberechtigungen eingerichtet werden.

(2) Das Unternehmen ist berechtigt, im Falle einer ungeplanten Abwesenheit für den Mitarbeite für die Dauer seiner Abwesenheit eine Weiterleitung und/oder Stellvertretung einzurichten Soweit darüber hinaus ein Zugriff auf Daten des Mitarbeiters erforderlich ist, gelten die Regelungen zur geplanten Abwesenheit entsprechend.

19.3 Ausscheiden von Mitarbeitern

(1) Bei Ausscheiden eines Mitarbeiters unterliegen die Daten des Mitarbeiters einschließlich des Postfachs und der Daten auf dem persönliche Laufwerk sowie die im Zusammenhang mit dessen Internetnutzung gespeicherten Daten weiterhin der ausschließlichen Verfügungsbefugnis des Unternehmens.

(2) Dem Mitarbeiter ist es untersagt, vor seinem Ausscheiden Daten zu löschen, die von dem Unternehmen weiter benötigt werden oder zu deren Aufbewahrung das Unternehmen verpflichtet ist. Sofern überhaupt Daten durch den Mitarbeiter gelöscht werden, darf sich dies daher ausschließlich auf private Daten beziehen.

(3) Nach dem Ausscheiden können in dem Postfach des Mitarbeiters eingehende E-Mails an einen vom Unternehmen zu benennenden anderen Mitarbeiter weitergeleitet werden, um die Bearbeitung eingehender Korrespondenz sicherzustellen.

(4) Die vorhandenen Daten des Mitarbeiters werden durch das Unternehmen gesichtet, anderenMitarbeitern – soweit erforderlich – zur weiteren Bearbeitung bzw. Fortführung überlassen und im Übrigen archiviert bzw. gelöscht.

(5) Die Aufbewahrungsfrist richtet sich nach der gesetzlichen Vorgaben.

20. Missbrauchskontrolle

20.1 Protokollierung

(1) Bei der Nutzung der IT-Systeme werden bestimmte Informationen protokolliert und gespeichert.

(2) Eine Unterscheidung zwischen dienstlicher und privater Nutzung ist nicht möglich, weil beide Nutzungsarten über dieselbe technische Infrastruktur erfolgen. Diese Informationen können auch personenbezogene Daten des Nutzers enthalten, insbesondere Informationen überbesuchte Websites und dort vorgenommene Aktivitäten des Nutzers.

20.2 Kontrolle durch IT-Abteilung

Die IT-Abteilung ist berechtigt, stichprobenartige Kontrollen der Nutzung der IT-Systemedurchzuführen, insbesondere bezogen auf die Einhaltung der Vorgaben der Richtlinie.

20.3 Einbeziehung des Datenschutzbeauftragten

Der Zugriff auf die Protokolldaten erfolgt durch die zuständigen Mitarbeiter der IT-Abteilungund den Datenschutzbeauftragten. Der Datenschutzbeauftragte ist im Vorfeld zu informieren; er kann auf seine Anwesenheit beim Zugriff verzichten oder seine Befugnisse delegieren.

20.4 Whistleblowing

(1) Soweit Mitarbeiter Anlass zu der Annahme haben, dass durch ein Fehlverhalten eines anderen Mitarbeiters eine Straftat verwirklicht wurde oder schwere Schäden für das Unternehmen oder Dritte drohen, besteht eine Meldepflicht gegenüber dem Unternehmen.

(2) Die Meldungen sollten offen und direkt gegenüber den zuständigen Vorgesetzten erfolgen. Nur in Fällen, in denen dem Hinweisgeber eine ihm zurechenbare Meldung unzumut-barerscheint, kann auch ein anonymer Hinweis erfolgen.

(3) Das Unternehmen schafft die Möglichkeit für alle Mitarbeiter, dass sich diese an eine Vertrauensperson wenden und so Meldungen abgeben können, ohne dass das Unternehmen über die meldende Person informiert wird.

(4) Jede Meldung soll so konkret wie möglich erfolgen und möglichst detaillierte Informationen über den zu meldenden Sachverhalt beinhalten.

21. Auswertung von Nutzungsdaten

21.1 Zulässige Auswertung

(1) Eine generelle Kontrolle der Nutzung der IT-Systeme findet nicht statt.

(2) Das Unternehmen ist jederzeit berechtigt, statistische Auswertungen über die Nutzung der IT-Systeme zu erstellen, soweit derartige Auswertungen keinen Personenbezug aufweisen.

(3) Soweit ein Verdacht besteht, dass der Mitarbeiter IT-Systeme rechtswidrig oder unter Verstoß gegen die Vorgaben der Richtlinie nutzt oder soweit entsprechende Rechtsverstöße des Mitarbeiters feststehen, ist das Unternehmen berechtigt, die gespeicherten Daten des betroffenen Mitarbeiters einzusehen und auszuwerten. Soweit die private Nutzung betroffen ist, kann der Mitarbeiter von der Privatnutzung vorübergehend oder dauerhaft ausgeschlossen werden.

(4) Über die Einsichtnahme und Auswertung wird ein Protokoll erstellt, von dem der Mitarbeiter eine Abschrift erhält. Das Protokoll wird erst nach Abschluss der Untersuchung übergeben, wenn andernfalls das Ergebnis der Untersuchung gefährdet werden kann.

21.2 Unzulässige Auswertung

Eine Auswertung zu Zwecken der Leistungskontrolle von Mitarbeitern erfolgt nicht.

21.3 Klärung von Streitfällen

In Streitfällen kann der Datenschutzbeauftragte hinzugezogen werden. Bis zu einer Klärung sollen die ausgewerteten Daten nicht weiter genutzt werden.

22. Datenschutz

22.1 Bestellung eines Datenschutzbeauftragten

Das Unternehmen hat einen Datenschutzbeauftragten bestellt, der von den Mitarbeitern jederzeit kontaktiert werden kann. Die Kontaktdaten des Datenschutzbeauftragten werde den Mitarbeiter auf geeignete Weise bekanntgegeben und können auch in der IT-Abteilung erfragt werden.

22.2 Aufgaben des Datenschutzbeauftragten

(1) Der Datenschutzbeauftragte ist Ansprechpartner für die Geschäftsführung, die Mitarbeiter, Kunden und sonstige Dritte sowie die Aufsichtsbehörde betreffend datenschutzrechtliche Fragen und Aufgabenstellungen. Bei Bedarf kann der Datenschutzbeauftragte in Ergänzung zu der Richtlinie Handlungsempfehlungen zu speziellen Themen herausgeben.

(2) Der Datenschutzbeauftragte koordiniert die datenschutzrechtlichen Aktivitäten desUnternehmens. Alle Mitarbeiter haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben und Aktivitäten zu unterstützen.

(3) Die Mitarbeiter sollen dem Datenschutzbeauftragten unverzüglich Bericht erstatten, wenn sie Kenntnis von einem Verstoß gegen die Richtlinie oder gesetzliche Bestimmungen haben, die sich auf den Schutz personenbezogener Daten beziehen. Der Datenschutzbeauftragteprüft falls notwendig ebenfalls, inwieweit eine Informationspflicht gegenüber den Aufsichtsbehörden besteht.

22.3 Datenschutzdokumentation

(1) Datenverarbeitungsvorgänge werden von dem Unternehmen entsprechend dendatenschutzrechtlichen Vorschriften dokumentiert.

(2) Um die Dokumentation auf dem aktuellen Stand zu halten, ist der Datenschutzbeauftragte über die Einführung neuer IT-Systeme und jede wesentliche Veränderungen bestehender IT-Systeme zu informieren.

22.4 Verpflichtung auf das Datengeheimnis

(1) Alle Mitarbeiter des Unternehmens sind auf das Datengeheimnis zu verpflichten. Es ist darüber zu belehren, dass es untersagt ist, personenbezogene Daten für private Zwecke zu nutzen, an Unbefugte zu übermitteln oder sie Unbefugten zugänglich zu machen. Die Verpflichtung auf das Datengeheimnis soll mit Beginn der Tätigkeit für unser Unternehmen erfolgen. Die Pflicht zur Wahrung der Vertraulichkeit besteht über das Ende der Tätigkeit für das Unternehmen hinaus, worauf im Rahmen der Verpflichtung hingewiesen wird.

(2) Auch innerhalb des Unternehmens ist darauf zu achten, dass Mitarbeiter nur Zugriff auf die Daten erhalten, die sie zur Erledigung ihrer Aufgaben für unser Unternehmen benötigten.

(3) Alle Mitarbeiter sollen zu Beginn der Tätigkeit und nachfolgend regelmäßig in Datenschutzthemen aufgeklärt werden. Diese Maßnahme kann auch online geschehen.

22.5 Grundzüge des Datenschutzes

(1) Bei jedem Vorgang der Datenverarbeitung ist zu prüfen, ob die beabsichtigte Erhebung, Speicherung oder Verarbeitung von personenbezogenen Daten zulässig ist. Bestehen Zweifel an der Zulässigkeit, soll der Datenschutzbeauftragte kontaktiert werden.

(2) Die Zulässigkeit der Datenverarbeitung kann sich aus verschiedenen rechtlichen Grundlagen ergeben. Zulässig ist insbesondere eine Datenverarbeitung dann, wenn der der Betroffene unter Beachtung der hierfür vorgesehenen Regelungen in die Datenverarbeitung seiner Daten eingewilligt hat. Auch ohne Einwilligung des Betroffenen kann die Datenverarbeitung zulässig sein, wenn eine andere gesetzliche Ermächtigungsgrundlage einschlägig ist. Fehlt es an einer Einwilligung und einer anderen gesetzlichen Ermächtigungsgrundlage, ist dieDatenverarbeitung unzulässig und hat zu unterbleiben.

(3) Im Rahmen der Prüfung der Zulässigkeit einer Datenverarbeitung ist zu untersuchen, ob die Datenverarbeitung unter Berücksichtigung des Grundsatzes der Datensparsamkeit notwendig ist. Bei der Erhebung, Speicherung und Verarbeitung personenbezogener Daten ist weiter derGrundsatz der Verhältnismäßigkeit zu beachten. Der Grundsatz der Verhältnismäßigkeit verlangt, dass die Datenverarbeitung dazu geeignet sein muss, einen legitimen Zweck zuerreichen; zusätzlich hat die konkrete Form der Datenverarbeitung geeignet, erforderlich undangemessen zu sein. Dazu darf kein milderes, gleichermaßen geeignetes Mittel zurErreichung des vorgesehenen Zwecks zur Verfügung stehen und es müssen im Rahmen derInteressenabwägung die überwiegenden schutzwürdigen Interessen des Betroffenen ausreichend beachtet werden.

(4) Im Rahmen der Verhältnismäßigkeitsprüfung ist dabei auch die Erhebung, Speicherung und Verarbeitung von aggregierten Daten oder sonstigen Daten ohne Personenbezug als milderes Mittel in Erwägung zu ziehen. Bei der Prüfung der Verhältnismäßigkeit kann insbesondereder Ursprung der personenbezogenen Daten (geschäftlich oder privat) zu berücksichtigen sein. Weiter ist das mit der Datenverarbeitung verbundene Risiko einer Beeinträchtigung von Persönlichkeitsrechten abzuschätzen.

(5) Für die Übermittlung von personenbezogener Daten gelten die vorstehenden Grundsätze entsprechend. Eine Übermittlung im rechtlichen Sinne liegt allerdings bei einer Weitergabe von Daten innerhalb des Unternehmens vor; außerdem sind Fälle der Auftragsverarbeitung privilegiert.

23. Kunden- und Mitarbeiterdaten

23.1 Kundendaten

(1) Unvollständige oder unrichtige personenbezogene Daten von Kunden sind auf Verlange des Betroffenen zu korrigieren. Die Korrektur ist dabei auch im Interesse des Unternehmens, da der gesamte Datenbestand möglichst richtig und von hoher Qualität sein soll. Soweit ein Mitarbeiter Kenntnis davon erlangt, dass beim Unternehmen gespeicherte Daten unvollständig sind, soll der Mitarbeiter unser Unternehmen informieren, damit eine Korrektur veranlasst werden kann.

(2) Eine von einem Betroffenen erteilte Einwilligung in die Erhebung, Speicherung und Verarbeitung von Daten ist jederzeit frei widerruflich. Der Betroffene ist auf die Möglichkeit des Widerrufs hinzuweisen. Der Widerruf gilt mit Wirkung für die Zukunft.

23.2 Mitarbeiterdaten

(1) Für Mitarbeiterdaten gelten die oben beschriebenen Regelungen zu Kundendaten entsprechend.

(2) Mitarbeiterdaten werden ausschließlich durch die Personalabteilung erhoben und verwaltet. Anderen Mitarbeitern (mit Ausnahme der Geschäftsführung) ist der Zugriff auf diese Datenuntersagt.

24. Anfragen und Untersuchungen

24.1 Interne Anfragen

Interne Anfragen im Hinblick auf Daten sind direkt gegenüber dem anfragenden Mitarbeiter zu beantworten. Für einer Beantwortung ist unter Beachtung der Vorgaben der Richtlinie die Zulässigkeit der Anfrage und ihrer Beantwortung zu prüfen; im Zweifelsfallen ist der Datenschutzbeauftragte zu konsultieren.

24.2 Kundenanfragen

(1) Kunden haben das Recht, sich über den Umgang mit ihren personenbezogenen Daten im Unternehmen zu informieren und zu beschweren. Derartige Anfragen sind unverzüglich anden Datenschutzbeauftragten weiterzuleiten.

(2) Soweit die Anfrage bzw. Beschwerde sich nicht auf datenschutzrechtliche Themen bezieht, erfolgt eine Weiterleitung an den Kundenservice. Soweit ein Kunde die Berichtigung seiner Daten wünscht, kann dies auch direkt durch den Kundenservice erfolgen; bei Auskunftsansprüchen von Kunden ist der Datenschutzbeauftragte zumindest einzubeziehen.

24.3 Anfragen und Untersuchungen der Aufsichtsbehörde

(1) Anfragen der Aufsichtsbehörden zu Datenschutzfragen werden im Außenverhältnis ausschließlich vom Datenschutzbeauftragten beantwortet; bei jeder Aktivität der Aufsichtsbehörden ist daher der Datenschutzbeauftragte unverzüglich zu informieren.

(2) Das Unternehmen arbeitet im Falle von Anfragen und Untersuchungen kooperativ und vertrauensvoll mit den Aufsichtsbehörden zusammen. Im Falle einer gesetzlichen Auskunftspflicht wird das Unternehmen die geforderten Auskünfte unverzüglich erteilen Maßnahmen und Feststellungen der Aufsichtsbehörden werden von unserem Unternehmen uneingeschränkt akzeptiert, soweit sie rechtmäßig sind.

24.4 Auskunftsersuchen anderer Behörden

Auskunftsersuchen anderer Behörden sind auf ihre datenschutzrechtliche Zulässigkeit zu prüfen, soweit personenbezogene Daten betroffen sind. Soweit die Prüfung eine Auskunftsverpflichtung oder zumindest eine Berechtigung zur Auskunftserteilung ergibt, sind bei der Beantwortung des Auskunftsersuchens nach Möglichkeit die berechtigten Interessen der Betroffenen zu berücksichtigen; in Zweifelsfällen ist Rücksprache mit dem Datenschutzbeauftragten zu halten.

24.5 Anfragen von Dritten

Anfragen von Dritten werden durch den jeweils fachlich zuständigen Mitarbeiter erteilt. Soweit die beabsichtigte Auskunft personenbezogenen Daten enthält, ist zuvor nach den allgemeinen Kriterien die Zulässigkeit der Übermittlung zu prüfen.

25. Datensicherheit

25.1 Grundzüge der Datensicherheit

(1) Für das Unternehmen ist von großer Bedeutung, dass die Sicherheit und Verfügbarkeit der Daten jederzeit gewährleistet ist. Vor diesem Hintergrund sind Daten unter anderem ausreichend gegen Verlust, gegen unbefugten Zugriff und vor anderen Gefahren zu schützen.

(2) Es ist daher dafür zu sorgen, dass angemessene Maßnahmen getroffen werden, um Daten des Unternehmens zu schützen.

25.2 Technische und organisatorische Maßnahmen (TOM)

(1) Die Datensicherheit ist durch geeignete technische und organisatorische Maßnahmen umzusetzen.

(2) Für die einzelnen Vorgänge der Datenverarbeitung sollen konkrete Schutzmaßnahmen dokumentiert und auf ihre Angemessenheit überprüft werden.

(3) Das Unternehmen behält sich das Recht vor, weitere Vorgaben für einzelne Vorgänge im Interesse der Datensicherheit zu erlassen.

26. Schlussbestimmungen

26.1 Publizität

(1) Die Richtlinie ist allen Mitarbeitern in geeigneter Weise zugänglich zu machen, insbesondere über das Intranet.

(2) Eine allgemeine Veröffentlichung der Richtlinie ist nicht vorgesehen, da es sich um eine interne Richtlinie des Unternehmens handelt.

26.2 Anpassung der Richtlinie

(1) Die IT-Systeme selbst und die Regelungen zur Nutzung der IT-Systeme unterliegen einem stetigen Wandel, der von Zeit zu Zeit auch Anpassungen der Richtlinie notwendig werden lässt.

(2) Das Unternehmen behält sich daher das Recht vor, die Richtlinie bei Bedarf zu ändern. Eine Änderung kann insbesondere erforderlich werden, um gesetzliche Vorgaben, bindende Verordnungen, Forderungen der Aufsichtsbehörden oder unternehmensinternen Verfahren zu entsprechen.

(3) In regelmäßigen Abständen soll geprüft werden, inwieweit technologische Veränderungen eine Anpassung der Richtlinie erfordern.

26.3 Verhältnis zu dienstlichen Anweisungen und anderen Regelwerken

(1) Die Richtlinie entbindet nicht von der Pflicht zur Beachtung dienstlicher Anweisungen. Soweit ein Mitarbeiter der Auffassung ist, eine ihm erteilte Weisung verstößt gegen die Vorgabender Richtlinie, ist hierauf hinzuweisen und eine Klärung herbeizuführen.

(2) Die Richtlinie beinhaltet grundlegende Vorgaben zur Nutzung der IT-Systeme. Es ist denkbar, dass im Einzelfall aufgrund besonderer Umstände eine andere Handhabung geboten sein kann. Es ist daher denkbar, dass speziellere Vorgaben vorrangig gegenüber der Richtlinie zubeachten sind.