Technisch-organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. B DSGVO)

- **Zutrittskontrolle**
  Die Geschäftsräume des Auftragnehmers sind alarmgesichert und werden durch ein externes Sicherheitsunternehmen außerhalb der Geschäftszeiten überwacht. Alle Flure sind mittels Bewegungsmeldern zusätzlich abgesichert. Die Geschäftsbereiche sind nur über ein elektronisches Zugangssystem / Transponder-Schließsystem erreichbar. Darüber hinaus ist der Zutritt zum Serverraum nur für den durch die Geschäftsführung bestätigten Personal erlaubt.

- **Zugangskontrolle**
  Über sichere Kennwörter in Verbindung mit dem Namen der Berechtigten ist der sichere Zugang gewährleistet.

- **Zugriffskontrolle**
  Die gesamte IT-Infrastruktur des Auftragsnehmers ist über ein mehrstufiges Firewall-System vor unerlaubten Zugriffen geschützt. Die Betreuung der Firewall-Systeme wird durch die Firma Starke Datensysteme abgesichert. Alle personenbezogenen Daten des Auftraggebers werden im eigenen Server vorgehalten und in einem Backup-System geschützt.
  Für die Lohn- und Gehaltsabrechnung ist die Firma BRZ Deutschland GmbH beauftragt. Personenbezogene Daten werden auch dort verwaltet. Mit der Firma BRZ Deutschland GmbH ist ein Auftragsverarbeitungsvertrag im Rahmen der EU-DSG-VO geschlossen.

Zugangskontrolle Standorte

- die Grundstücke sind über ein Tor gesichert
- alle Zugänge verfügen über Sicherheitsschlösser mit einem Schließsystem
- jeder berechtigte Mitarbeiter erhält einen oder mehrere Zugangsschlüssel für seinen Bereich
- die Vergabe und Kontrolle wird über eine Schlüsselliste geführt
- diese Liste und weitere verfügbare Schlüssel sind im Safe aufzubewahren

Zugangskontrolle EDV

- **jeder berechtigte Mitarbeiter hat über sein persönliches Passwort in Verbindung mit seinem Namen Zugang zu den für Ihr / Ihn persönlich festgelegten Programmen und Laufwerken**

- **die Vergabe und Kontrolle der Zugänge wird über eine Liste mit Namen und Berechtigungen geführt**

- **Administrationsrechte werden von der Geschäftsleitung festgelegt**

- **Administrationsrechte auf die Server der TSI GmbH & Co. KG:**
  - IT-Dienstleister (Starke Datensysteme GmbH)
  - Herr Michael Päßler

- **Administrationsrechte im BRZ-Kalkulationsprogramm:**
  - Herr Frank Höhne
  - Frau Cornelia Winkler

- **Administrationsrechte im BRZ-Buchhaltungsprogramm:**
  - Herr Dirk Meinhardt

- **Administrationsrechte im BRZ-Lohnprogramm:**
  - Herr Frank Höhne
  - Frau Cornelia Winkler

- **Administrationsrechte im DAKO-Programm:**
  - Herr Hans-Ulrich Kügler

- **Administrationsrechte im HILTI-Programm:**
  - Herr Hans-Ulrich Kügler

Konzept für Datenpannen

- **schwerwiegende Fälle**
  Bei schwerwiegenden Datenpannen werden, nach sofortiger Rücksprache mit dem externen Datenschutzbeauftragten, alle weiteren Maßnahmen und Vorgehensweisen besprochen bzw. umgesetzt.

- **kleinere bis minderschwerwiegende Fälle**
  Bei kleineren Datenpannen werden umgehend alle Maßnahmen ergriffen um die fehlerhaften bzw. falsch übermittelten Daten zu Löschen.

Lösch-Konzept

Dieses Konzept soll als Erweiterung der bereits im Verzeichnis von Verarbeitungstätigkeiten genannten Löschfristen eingehalten werden.

Vorwort

Personenbezogenen Daten gem. DSGVO dürfen nur so lange gespeichert werden, wie sie für die vorab festgelegten Zwecke benötigt werden. Sollten die Zwecke nicht mehr bestehen, so müssen diese Daten gelöscht werden. Es dürfen allerdings keine gesetzlichen Vorgaben entgegenstehen. Eine unbegrenzte Aufbewahrung von personenbezogenen Daten ist nicht zulässig. Darüber hinaus kann eine Löschung auch durch eine Anfrage eines Betroffenen ausgelöst werden.

Übergangsfrist bis zur Löschung:

Nach Ablauf der Löschfrist bis zur Durchführung der Löschung dürfen nicht mehr als 6 Monate vergehen.

Durchführung der Löschung

Daten werden, je nach Datenträger gem. DIN 66399 folgendermaßen gelöscht bzw. vernichtet:

- **Papier:**
  Einmal jährlich werden alle nicht mehr benötigten Ordner des vorangegangenen Geschäftsjahres dem jeweiligen Archiv hinzugefügt. Gleichzeitig werden alle, nach den gültigen Aufbewahrungsfristen, nicht mehr benötigten Ordner vernichtet. Bewerbungsunterlagen werden im Zuge der Ablehnung bzw. spätestens nach 6 Monaten anonymisiert.

- **Digitale Datenträger (z.B. Festplatte, USB-Stick, CD-ROM):**
  Löschung bzw. Vernichtung erfolgt durch einen externen IT-Dienstleister, nach den Vorgaben der gültigen IT-Sicherheitsrichtlinie.

Protokollierung:

Jede ordnungsgemäße Vernichtung wird dokumentiert. Daraus muss hervorgehen, wer was wann gelöscht/vernichtet hat.

Verantwortlichkeiten

Verantwortlich für das Löschen (d.h. für die Definition der Löschfristen, deren Einhaltung und tatsächlicher Durchführung) ist der jeweilige Dateneigentümer. Dateneigentümer ist der Leiter derjenigen Abteilung, welche hauptverantwortlich ist für die Speicherung und Verarbeitung der jeweiligen personenbezogenen Daten.

Aufbewahrungsfristen

Verfahrensart	Frist	(ggfs. Gesetzliche) Grundlage
Abmahnung	3 Jahre	Danach hat ein Arbeitnehmer grds. Recht auf Löschen aus der Personalakte (BAG, Urteil v. 27.11.2008, 2 AZR 675/07; BAG, Urteil v. 18.11.1986, 7 AZR 674/84, DB 1987, 1303)
Abrechnung Kassenpatienten	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Abrechnung Privatpatienten	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Akten von verkauften Fahrzeugen	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Angebote (die zum Auftrag geführt haben)	6 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO
Angebote (die nicht zum Auftrag geführt haben)	-	Keine gesetzliche Aufbewahrungspflicht
Antrag auf Nutzerzulassung	10 Jahre	§ 257 I Nr. 1, IV HGB
Antrag Bankvollmacht	6 Jahre	§ 147 I Nr. 5, III AO
Anwesenheitsliste	10 Jahre bei entgeltlicher Schulung/ Zeiterfassung ansonsten unmittelbar nachdem der Zweck erfüllt wurde	Soweit für Lohnbuchhaltung erforderlich, § 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b UStG Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt

Arbeitnehmerüberlassung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Arbeitsunfähigkeitsbescheinigung	5 Jahre nach entstehen (angemessen) 10 Jahre, wenn für Steuer relevant	§ 6 AAG § 257 I Nr. 1, IV HGB, § 147 I Nr. 1, 4, III AO
Arbeitsvertrag	grds. 3 Jahre 10 Jahre, wenn für Steuer relevant	§ 195 BGB regelmäßige Verjährungsfrist § 257 I Nr. 1, IV HGB, § 147 I Nr. 1, 4, III AO
Arbeitszeugnis	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Archivierung von Empfangsquittungen Anwenderhinweis	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Archivierung von Kundenakten	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO
Archivierung von Aufträgen und Gewährleistungsaufträgen	6 Jahre	§ 257 I Nr. 2, 3, IV HGB § 147 I Nr. 2, 3, 5, III AO
Archivierung von Empfangsquittungen	6 Jahre	§ 257 I Nr. 2, 3, IV HGB § 147 I Nr. 2, 3, 5, III AO
Archivierung von Leasing- und AfA-Rechnungen	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Archivierung von Mietverträgen	3 Jahre 10 Jahre, wenn für Steuer relevant	§ 195 BGB regelmäßige Verjährungsfrist § 257 I Nr. 1, IV HGB, § 147 I Nr. 1, 4, III AO

Archivierung von TÜV-Rechnungen Archivierung von Versicherungs- und Garantieabrechnungen	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Arztbriefe	10 Jahre	§ 630f III BGB, § 10 III MBO-Ä, § 51 III ÄrzteG
Aufhebungsvertrag	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Auftragsbestätigung	6 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO
Ausbildungsantrag	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Ausbildungsbericht	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Ausbildungsprogramm	6 Jahre	§ 147 I Nr. 5, III AO
Ausgangsschecks	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Aushändigung an Boten	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Auslagen/Rechnungen von Mitarbeitern	10 Jahre	§ 257 I Nr. 4, IV HGB, § 147 I Nr.4, III AO, § 14b I UStG
Backup		Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Bauantrag	Lebensdauer des Bauwerks	
Bankbelege	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG

Beantragung von Aufenthaltsgenehmigung	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Beförderung	6 Jahre	§ 147 I Nr. 5, III AO
Befundanfragen/ Sozialberichte	grds.10 Jahre 30 Jahre, wenn schutzwürdige Belange des Betroffenen beeinträchtigt werden können	§ 630f III BGB, § 10 III MBO-Ä, § 51 III ÄrzteG § 197 BGB Verjährungsfrist und Empfehlung aus Beweissicherungsgründen
Beschäftigungsverbot	min. 2 Jahre	§ 27 V MuSchG
Besucherregistrierung	6 Monate	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Betriebsdatenerfassung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Bewerber-Management Software	max. 6 Monate min. 2 Monate	Art. 17 I lit. a DSGVO, § 15 IV AGG
Bewerbungen (Email/Post)	max. 6 Monate min. 2 Monate	Art. 17 I lit. a DSGVO, § 15 IV AGG
Bewertungen		Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Blog	1 Jahr	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Bonitätsprüfung	6 Jahre	§ 147 I Nr. 5, III AO
Breitenausbildung	3 Jahre	§ 195 BGB Verjährungsfrist
Buchung von Dienstreisen	6 Jahre	§ 257 I Nr. 2, 3, IV HGB § 147 I Nr. 2, 3, 5, III AO

Buchung von Schulungen	6 Jahre	§ 257 I Nr. 2, 3, IV HGB § 147 I Nr. 2, 3, 5, III AO
Bußgeldbescheid	6 Monate bis 3 Jahre 2 bis 10 Jahre 10 Jahre	§ 31 II OWiG § 489 IV S. 2 StPO § 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO
Cookies		Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
CRM System mit Warenwirtschaft	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
CRM System ohne Warenwirtschaft	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Customer Identity und Access Management	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Datenmanagement	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Direktwerbung		Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Disposition	6 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO
Dokumentenmanagement	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Eignungstest	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist

E-Learning	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Elektronische Signatur	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Elektronischer Zahlungsverkehr	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Elternzeitantrag	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO
Entsendung von Mitarbeitern zu Baustellen	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 1, 4, III AO, § 14b I UStG
Erfassung von Gästewünschen	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
E-Mail	6 Jahre 10 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO Geschäftsbriefe, Mahnungen § 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO Buchungsbelege
Fahrtenauftrag	6 Monate	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Fahrtenbuch	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO
Fahrtenschreiber Verwaltung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO
Finanzbuchhaltung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Fotofinder	5 Jahre (Berichtsvordruck) 10 Jahre bei Frauen (Präparate und Befunde)	Anlage zur KFE-RL KFE-RL

Führerschein Prüfung Gültigkeit	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Fundsachen	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Geburtstags- und Jubiläumsverzeichnis	6 Monate nach Ausscheiden aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Gehaltspfändung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 1, III AO, § 14b I UStG
Geschäftswagenvertrag	6 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO
Gesellschafterverwaltung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Gewinnspiele	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 1, III AO
Globales Adressbuch	6 Monate nach dem Austritt aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
GPS-System	6 Monate 3 Jahre	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt § 195 BGB regelmäßige Verjährungsfrist
Gutscheine	6 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO
Haushaltsbefragung	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Hausnotruf	1 Monat	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung / Verarbeitung erfüllt

Hygienelisten	eigene Festlegungen zur Aufbewahrung treffen	§ 4a ApBetrO bestimmt keine Frist Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Inkasso	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Interne Mailinglisten	6 Monaten nach dem Austritt aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Interne Prozessabläufe	6 Monaten nach dem Austritt aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Internes Personalrundschreiben	6 Monate nach dem Austritt aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Intranet	6 Monate nach dem Austritt aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Kalender	6 Monate, nach Austritt aus dem Unternehmen 10 Jahre, wenn Kalender-einträge zum Verständnis und zur Überprüfung der für die Besteuerung gesetzl. vorgeschriebenen Aufzeichnungen von Bedeutung sind	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt § 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Kassenbuch	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Kaufvertrag	Regelmäßig 10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG

Kinderkrankschreibung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Kontaktdaten Geschäftspartner		Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Kontaktformular Internetseite	1 Monat	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt Art. 17 I lit. b DSGVO Einwilligung widerrufen Art. 17 I lit. c DSGVO Widerspruch
Kostenstellenverrechnung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b UStG
Kostenvoranschlag	6 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO
Krankenstatistik	keine	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt Daten müssen anonymisiert oder gelöscht werden!
Krankentagesgeldversicherung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Kreditkartenzahlungen	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Kundendatenerfassung über ein Webportal	6 Monate	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Kundendienst und -service	10 Jahre	§ 257 I Nr. 1, IV HGB,

		§ 147 I Nr. 4, III AO, § 14b I UStG
Kündigung	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Lohn- und Gehaltsabrechnung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Mahnung	10 Jahre ab Vertragsschluss	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Meinungsumfragen	6 Monate	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt Daten müssen anonymisiert oder gelöscht werden!
Meldung an Gemeinde bei Mieterwechsel	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Mietverträge	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO
Mitarbeiterbefragung	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Mitarbeiterbeurteilung	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Mitgliederverwaltung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Nebenkostenabrechnung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Newsletter	max. 1 Monat	Art. 17 I lit. a DSGVO, sobald

		der Zweck der Erhebung/Verarbeitung erfüllt Art. 17 I lit. b DSGVO Einwilligung widerrufen Art. 17 I lit. c DSGVO Widerspruch
Notfall-Kontaktdaten	Keine	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Nutzer/ Terminliste/ Poolfahrzeuge	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Organigramm	6 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO
Patientenaufnahme	3 Monate	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Patientendokumentation	10 Jahre nach der letzten Behandlung 30 Jahre nach der letzten Behandlung mit ionisierenden Strahlen 30 Jahre nach Blut-Spendenentnahme 30 Jahre	§ 630f III BGB allgemeine Frist § 70 VI StrlSchV § 11 I TFG § 197 BGB
Patientenkoordination	10 Jahre nach der letzten Behandlung 30 Jahren nach der letzten Behandlung mit ionisierenden Strahlen 30 Jahren nach Blut-Spendenentnahme 30 Jahren	§ 630f III BGB allgemeine Frist § 70 VI StrlSchV § 11 I TFG § 197 BGB
Patientenstudie	10 Jahre nach Arzneimittel	§13 X GCP-V

	Prüfungen	
Patiententerminierung	6 Monate	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Patientenverwaltung	grds.10 Jahre 30 Jahre, wenn schutzwürdige Belange des Betroffenen beeinträchtigt werden können	§ 630f III BGB, § 10 III MBO-Ä, § 51 III ÄrzteG § 197 BGB Verjährungsfrist und Empfehlung aus Beweissicherungsgründen
Personal Einarbeitungsplan	10 Jahre	§ 257 I Nr. 1, IV HGB
Personalfragebogen	3 Monate nach dem Austritt aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Personalmanagement Software	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Personalpläne/Dienstpläne/Schichtpläne	6 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO
Personalvermittlung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b UStG
Praktikant	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Rechnungen	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Reisekostenabrechnung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Reklamationen	10 Jahre	§ 257 I Nr. 1, IV HGB,

		§ 147 I Nr. 4, III AO, § 14b I UStG
Reservierungen	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Schadensmeldung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Schlüsselverwaltung/ Transponderverwaltung	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Seminarverwaltung	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Sozialversicherungsnachweise	grds. bis zum folgenden Kalenderjahr der letzten Prüfung	§ 28f V SGB IV
Sonderzahlung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Spesenabrechnung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Studienbescheinigung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 1, III AO
Talent Management	6 Monate nach dem Austritt aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Tankkarten	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Tätigkeitsnachweis/ Zeiterfassung	min. 2 Jahre 3 Jahre 6 Jahre	§ 16 II ArbZG § 195 BGB regelmäßige Verjährungsfrist § 147 I Nr. 5, III AO, wenn für Lohnbuchhaltung erforderlich
Telefonanlage	6 Monate nach Ausscheiden aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der

		Erhebung/Verarbeitung erfüllt
Telefondatenbank Privatnummern	6 Monate nach Ausscheiden aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Telefonzentrale	6 Monate nach Ausscheiden aus dem Unternehmen	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Terminverwaltung Patienten	3 Monate	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Testwaren	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
(Daten-) Übernahme	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Umsatzstatistiken	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 1, III AO, § 14b I UStG
Unfallbericht	5 Jahre	§ 24 VI BGV A 1
Unfallmeldungen Berufsgenossenschaft	min. 15 Jahre	Anforderungen nach § 34 SGB VII
Urlaubsplanung	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Urlaubsverwaltung	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
User Logdaten	Keine	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
Verbandsbuch	5 Jahre	§ 24 VI BGV A 1
Versicherungsangebotsrechner	6 Jahre 3 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO § 195 BGB regelmäßige Verjährungsfrist
Versicherungsvergleich	6 Jahre	§ 257 I Nr. 2, 3, IV HGB, § 147 I Nr. 2, 3, 5, III AO

	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Vertragsmanagement	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b UStG
Vertrieb Geschäftskunden		Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt Art. 17 I lit. b DSGVO Einwilligung widerrufen Art. 17 I lit. c DSGVO Widerspruch
Vertrieb Privatkunden	6 Monate	Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt Art. 17 I lit. b DSGVO Einwilligung widerrufen Art. 17 I lit. c DSGVO Widerspruch
Vorschlagswesen	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Websites		Art. 17 I lit. a DSGVO, sobald der Zweck der Erhebung/Verarbeitung erfüllt
WhatsApp	Aktualität der Einwilligung beachten!	Art. 17 I lit. b DSGVO Einwilligung widerrufen
Wiedereingliederungsmanagement	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Zeitarbeit	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 4, III AO, § 14b I UStG
Zeiterfassung	min. 2 Jahre 3 Jahre	§ 16 II ArbZG § 195 BGB regelmäßige

	6 Jahre	Verjährungsfrist § 147 I Nr. 5, III AO, wenn für Lohnbuchhaltung erforderlich
Zielvereinbarung	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist
Zollabwicklung	10 Jahre	§ 257 I Nr. 1, IV HGB, § 147 I Nr. 1, III AO, § 14b I UStG
Zuschläge	3 Jahre	§ 195 BGB regelmäßige Verjährungsfrist

IT-Sicherheitsrichtlinie

1 Allgemeine Regelungen

1.1 Anwendungsbereich und Grundlagen für den Umgang mit IT-Systemen

1.1.1 Anwendungsbereich

Diese Richtlinie gilt ohne Ausnahme für alle Beschäftigten des Unternehmens, auch bei Telearbeit und an häuslichen Arbeitsplätzen einschließlich aller Zweigstellen, Niederlassungen und Beteiligungsgesellschaften 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. Soweit in Ausnahmefällen von dieser Richtlinie abweichende Verfahrensweisen erforderlich werden, sind diese nur nach vorheriger Genehmigung durch die Geschäftsleitung in Absprache mit dem IT-Dienstleister zulässig.

1.1.2 Zweckbindung der Systeme und Arbeitsmittel

Sämtliche IT-Einrichtungen, PCs, Notebooks, USB-Sticks, Speicherkarten und mobile Laufwerke sowie sonstige mobile Geräte wie PDAs, BlackBerry-Geräte etc. (mobile Datenträger) zur geschäftlichen Nutzung werden vom IT-Dienstleister bereitgestellt und unterliegen den Regelungen dieser Richtlinie. Die Beschaffung von IT-Ausrüstung für den Einsatz im Unternehmen ist nur nach Prüfung und Freigabe durch den IT-Dienstleister und nur nach den von ihm festgelegten Spezifikationen zulässig. Der Einsatz von Hard- und/oder Software, die nicht nach den festgelegten Spezifikationen beschafft und eingerichtet worden ist, ist unzulässig. Ausnahmen sind nur nach Absprache mit dem IT-Dienstleister und schriftlicher Dokumentation möglich. Vor der Inbetriebnahme ist jegliche Art von Hard- und Software vom IT-Dienstleister technisch und, soweit erforderlich, auch fachlich freizugeben. Die Freigaben sind zu dokumentieren. Die Nutzung von nicht freigegebener Software ist unzulässig. Veränderungen sind nur auf Anordnung des IT-Dienstleisters zulässig und sind sowohl fachlogisch als auch technisch zu testen, zu dokumentieren und förmlich freizugeben. Die eingesetzten PCs, Server und sonstigen Geräte inklusive Notebooks, mobile Datenträger, PDAs u.a. dürfen einschließlich der zugelassenen und freigegebenen Arbeitsmittel wie Programme, Dateien, Datenträger usw. nur für sachgemäße betriebliche Aufgaben und unter Wahrung der Installations- und Benutzervorschriften eingesetzt werden.

1.1.3 Tele- und Heimarbeitsplätze

Die Regelungen dieser Richtlinie gelten grundsätzlich auch für Tele- und Heimarbeitsplätze. Tele- und Heimarbeitsplätze dürfen nur nach Genehmigung der Geschäftsleitung in Absprache mit dem IT-Dienstleister 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.). Darüber hinaus gelten für die Wahrung der Vertraulichkeit der Daten und Informationen die Regelungen dieser Richtlinie entsprechend. Soweit aufgrund der Sensibilität der Daten am häuslichen Arbeitsplatz Kontrollen bezüglich der Einhaltung von Sicherheits- oder Datenschutzauflagen erforderlich werden können, sind entsprechende vertragliche Vereinbarungen vorzusehen.

1.2 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 (Testung) und Freigabe eingesetzt werden. Dies gilt auch für die Einführung von Standardsoftware und für die Installation von Updates oder für sonstige Programm- oder Verfahrensänderungen. Der Umfang der im Einzelfall erforderlichen Prüfung und der Freigabe ist in der jeweiligen Verfahrensdokumentation festzulegen. Grundsätzlich müssen folgende Prüfungen, Dokumentationen und Freigaben durchgeführt werden:

1.2.1 Sachlogische Prüfung

Die sachlogische Prüfung prüft anhand von fachlichen Testfällen, ob das Datenverarbeitungsverfahren einerseits richtige Verarbeitungsergebnisse liefert und andererseits auch Falscheingaben erkennt und auf diese in der vorgesehenen Weise, z.B. durch Fehlermeldungen, reagiert. Zusätzlich werden in der sachlogischen Prüfung auch die Sicherheitsmechanismen der Programme wie Plausibilitätsprüfungen, Eingabe- und Grenzprüfungen auf ihr Vorhandensein, ihre Richtigkeit und Wirksamkeit hin überprüft. Art und Umfang der sachlogischen Prüfung richten sich nach den rechtlichen Anforderungen an die Verarbeitungsergebnisse. Die Prüfanforderungen an die sachlogische Prüfung, das Prüfverfahren, die Art und Weise ihrer Durchführung, die Testdaten und Testfälle sowie die Abnahmekriterien für die Freigabe sind deshalb in Abhängigkeit von diesen Anforderungen festzulegen und in der Verfahrensorder Testdokumentation oder in einem Testplan zu beschreiben. Für die Durchführung der Testung sind anonyme oder in geeigneter Weise anonymisierte Testfälle zu verwenden. Eine Testung mit Originaldaten ist unzulässig. Die sachlogische Freigabe erfolgt durch den zuständigen Fachbereich, eventuell ergänzt durch die Revision und den Datenschutzbeauftragten, wenn mit dem Verfahren personenbezogene Daten verarbeitet werden.

1.2.2 Technische Testung

Die technische Testung prüft und bestätigt die Ordnungsmäßigkeit und Sicherheit der Installation und der systemtechnischen Integration des Verfahrens in die vorhandene IT-Infrastruktur und die technische Umgebung des Datenverarbeitungsverfahrens sowie die Umsetzung aller für den Betrieb des Verfahrens erforderlichen technischen und organisatorischen Maßnahmen. Die technische Testung ist sowohl bei der Einführung des Datenverarbeitungsverfahrens als auch bei Verfahrensänderungen und bei Änderungen in der technischen Umgebung des Datenverarbeitungsverfahrens im erforderlichen Umfang durchzuführen. Die Anforderungen an die technische Testung (z.B. Zugriffsschutz, Datensicherung, Verfügbarkeit, Versions- und Identitätskontrolle und sonstige Sicherheitsanforderungen etc.) sind festzulegen und in der Verfahrens- oder Testdokumentation zu beschreiben. Die Testergebnisse sind nachvollziehbar zu dokumentieren und entsprechend der rechtlichen Anforderungen zugriffssicher aufzubewahren. Die Freigabe erfolgt durch den IT-Dienstleister.

1.2.3 Einrichtung der Verfahren

Im Zusammenhang mit der Einrichtung des Datenverarbeitungsverfahrens sind alle relevanten Systemeinstellungen, Protokollierungen und sonstige Überwachungsfunktionen, die Nutzer und ihre Berechtigungen (Nutzerprofile) und sonstige Zugangsberechtigungen zu dokumentieren. Die zugangsberechtigten Personen und ihre Rechteprofile sind von der Geschäftsleitung in Absprache mit dem IT-Dienstleister festzulegen. Sowohl die Festlegung der zugangsberechtigten Personen und ihre Rechteprofile als auch deren Einrichtung ist nachvollziehbar zu dokumentieren.

1.2.4 Datenübernahme

Soweit aus einem Vorgängerverfahren Daten übernommen werden müssen, sind das Übernahmeverfahren und die Testung der Richtigkeit der Datenübernahme einschließlich des Nachweises der Richtigkeit der Datenübernahme zu dokumentieren.

1.2.5 Freigabe zur Anwendung

Nach Abschluss aller vorgesehenen Testungen, Dokumentationen und Freigaben ist das Verfahren von der Geschäftsleitung in Absprache mit dem IT-Dienstleister zur Anwendung freizugeben. Erst nach dieser Freigabe darf das Verfahren produktiv eingesetzt werden.

1.2.6 Aufbewahrung der Testergebnisse und der Dokumentationen

Alle Testergebnisse sind nachvollziehbar zu dokumentieren und entsprechend der rechtlichen Anforderungen zugriffssicher aufzubewahren. Die Frist für die Aufbewahrung der Testergebnisse und Dokumentationen richtet sich nach der Rechtsnatur der mit den Datenverarbeitungsverfahren erzeugten Ergebnisse. Die Fristen sind in der jeweiligen Verfahrensdokumentation festzulegen.

1.3 Einsatz privater Hard- und Software und private Nutzung von betrieblichen Geräten

1.3.1 Einsatz privater Geräte

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

1.3.2 Nutzung betrieblicher Geräte für private Zwecke

Die Nutzung von betrieblicher Hard- und Software für private Zwecke und die Nutzung von betrieblichen mobilen Datenträgern an privaten Geräten ist untersagt. Dies gilt auch für eine betriebliche Nutzung von firmeneigenen mobilen Datenträgern an privaten Geräten. Ebenso ist deren Überlassung an betriebsfremde Personen zur Nutzung, auch an Familienangehörige, streng untersagt. Ausnahmen bedürfen der Genehmigung durch den Vorgesetzten und der Freigabe durch den IT-Dienstleister. Kopien von Programmen dürfen nur für betriebliche Zwecke angefertigt werden und auch nur insoweit, als es im Rahmen der Lizenzbedingungen zulässig und aus betrieblichen Gründen erforderlich ist. Die Kopien sind, sobald sie nicht mehr benötigt werden, wieder zu löschen bzw. zu vernichten. Kopien von Daten dürfen ebenfalls nur für betriebliche Zwecke und je nach Vertraulichkeitsgrad nur in Abstimmung mit dem Informationseigentümer angefertigt werden.

1.4 Verwaltung und Administration der Datenverarbeitungsverfahren

1.4.1 Verwaltung der Datenverarbeitungsverfahren

Zum Schutz vor unbefugten Zugriffen und vor Manipulationen sowie zur Gewährleistung der jederzeitigen Integrität der Verarbeitungsverfahren, Programme und Daten müssen die Produktions-, Test und Entwicklungsumgebungen zuverlässig voneinander getrennt werden. Hierzu sind die Möglichkeiten der Hard- und Softwaretrennung, z.B. Installation der Verfahren unter unterschiedlichen Computerprozessoren oder in verschiedenen Verzeichnissen oder Domänen, zu nutzen. Für die Produktions-, Test- und Entwicklungssysteme sind unterschiedliche Anmeldeprozeduren mit verschiedenen Passwörtern einzurichten. Programmierer dürfen keinen Zugriff auf Originalprogramme und Daten erhalten. Ist ein Zugriff der Programmierer auf Produktionsprogramme erforderlich, z.B. für die Durchführung von Programmänderungen, dürfen die Programme nur in einem kontrollierten Prozess zur Verfügung gestellt und erst nach

einer Testung und Freigabe gem. Ziff. 1.2 dieser Richtlinie in einem kontrollierten und dokumentierten Prozess in die Produktionsumgebung eingestellt werden.

1.4.2 Administrationsrechte

Administratoren dürfen nur insoweit mit privilegierten Rechten ausgestattet werden, als dies zur Durchführung ihrer jeweiligen Administrationsaufgaben erforderlich ist. Für Aufgaben, die ohne privilegierte Rechte durchgeführt werden können, sind Accounts mit Standardrechten zu benutzen. 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. Die Administratortätigkeit ist, soweit sie unter Nutzung von hohen Privilegien durchgeführt wird, zu protokollieren und regelmäßig und zeitnah auszuwerten. 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.

1.4.3 Nachweis der Programmidentität

Die Programmidentität ist durch Programmprotokolle wie Umwandlungsliste/Übersetzungsliste oder ggf. durch elektronische Signatur nachzuweisen und zu dokumentieren.

1.4.4 Überwachung von Schnittstellen und Zugängen

Soweit an PCs Schnittstellen zu externen Geräten, z.B. WLAN- oder USB-Schnittstellen, oder externe Laufwerke, z.B. CD- oder DVD-Laufwerke, nicht benötigt werden, sind sie zu deaktivieren. Für die Aufgabenerfüllung erforderliche Schnittstellen sind so zu überwachen, dass an diesen Schnittstellen keine unzulässigen oder nicht freigegebenen Geräte betrieben werden können. Nicht benötigte Netzwerkzugänge sind ebenfalls zu deaktivieren oder in einer geeigneten Weise zu überwachen, um den Anschluss unbefugter Geräte zeitnah zu erkennen und zu verhindern. Der Zugang mittels unbefugter Geräte ist zu protokollieren und automatisiert zu verhindern.

2 Nutzung von IT-Systemen

2.2 Datensicherheit

2.2.1 Allgemeine Grundsätze

Bei der Nutzung von IT-Systemen ist Folgendes zu beachten:
Personenbezogene Daten und Geschäftsdaten (auch E-Mails) dürfen nur in den vorgesehenen Laufwerken, Verzeichnissen und Ordnerstrukturen gespeichert werden. Innerhalb dieser Struktur kann der Mitarbeiter selbst Unterordner anlegen. Eine alleinige Speicherung von Originaldaten auf lokalen Datenträgern (mobile Festplatten, Speichersticks etc.) ist unzulässig. Erforderlichenfalls sind Kopien zu erstellen. Nicht mehr benötigte Dateien und E-Mails sind regelmäßig zu löschen.

2.2.2 Verbindungen zu externen IT-Ressourcen

Verbindungen von vernetzten PCs zu externen Systemen und Netzen dürfen nur über die vom IT-Dienstleister freigegebenen und kontrollierten Verbindungswege hergestellt werden. Internetverbindungen, z.B. 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. (Anmerkung: Aktueller Virenscanner, Firewall auf Notebooks)

2.2.3 Fremdrechner, Fremdunternehmen

Fremdrechner bzw. Rechner, die nicht durch den IT-Dienstleister freigegeben wurden, dürfen grundsätzlich nicht an das Firmennetzwerk angeschlossen werden. Fremdrechner sind alle Rechner von anderen Stellen, die nicht unter der Kontrolle des IT-Dienstleisters stehen, z.B. PCs von Kunden, Lieferanten, Geschäftspartnern, Beratungsunternehmen etc. Bei Bedarf ist der IT-Dienstleister 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 den IT-Dienstleister ermöglicht werden. Die Sicherheitsmaßnahmen sind in Abhängigkeit vom Schutzbedarf der Daten und von den mit dem Zugang verbundenen Risiken festzulegen. Servicepartnern darf ein Zugang nur über definierte sichere Zugänge und Pfade unter Gewährleistung einer sicheren und zuverlässigen Authentifizierung ermöglicht werden. Soweit Fremdunternehmen oder sonstigen betriebsfremden Personen ein Zutritt zu Sicherheitsbereichen oder Zugang zu personenbezogenen oder sonstigen vertraulichen Daten oder Informationen gewährt werden muss, sind diese Personen während ihrer Tätigkeit in geeigneter Weise zu beaufsichtigen. Die näheren Umstände und Sicherheitsanforderungen sind in den entsprechenden Verträgen und ggf. Vertraulichkeitsvereinbarungen zu regeln. Die zu vergebenden Berechtigungen sind unter Berücksichtigung des Schutzbedarfs der Daten und Informationen abzuwägen und nur im geringstmöglichen Umfang zu erteilen. Soweit möglich, sind die Aktionen dieser Stellen revisionssicher zu protokollieren und zu überprüfen.

2.2.4 Wechseldatenträger

Im Interesse eines vertraulichen Umgangs mit Unternehmensdaten ist bei der Nutzung von mobilen Datenträgern Folgendes zu beachten:
Um Datenverluste zu vermeiden, dürfen auf mobilen Datenträgern (mobile Plattenlaufwerke, USBSticks, Speicherkarten, CD/DVDs) nur Kopien von Firmendaten gespeichert werden. Soweit personenbezogene Daten oder sonstige nach den Regelungen der Vertraulichkeitsrichtlinie vertrauliche oder streng vertrauliche Daten gespeichert werden, sind diese Daten zu verschlüsseln. Als mobile Datenträger dürfen zur geschäftlichen Nutzung ausschließlich vom IT-Dienstleister freigegebene oder bereitgestellte Datenträger eingesetzt werden. Die Vergabe und die Vernichtung von mobilen Datenträgern werden revisionsfähig dokumentiert. Mobile Datenträger müssen regelmäßig, insbesondere nach einem Anschluss an fremde Systeme, einer Speicherung von Daten aus Quellen außerhalb des Unternehmens oder vor einem Transfer von Fremddaten in firmeneigene Systeme auf Virenfreiheit geprüft werden. Die Weitergabe von Daten und ein Kopieren auf fremde Datenträger ist nur im Rahmen der Vertraulichkeitsrichtlinien und nur insoweit erlaubt, als es für die Erfüllung betrieblicher Aufgaben zwingend erforderlich ist. Personenbezogene oder andere vertrauliche Daten dürfen nicht unverschlüsselt auf Wechseldatenträgern gespeichert werden. Mobile Datenträger dürfen nicht unbeaufsichtigt sein und müssen zugriffssicher verwahrt werden. Zum Anschluss an unternehmensfremde Rechner dürfen nur mobile Datenträger verwendet werden, die keine personenbezogenen oder sonstige vertrauliche Daten enthalten. Diese mobilen Datenträger müssen möglichst über einen Schreibschutz verfügen und sollen nur im schreibgeschützten Zustand verwendet werden. Auf mobilen Datenträgern nicht mehr benötigte Daten sind unverzüglich sicher zu löschen.

2.2.5 Firewall und Internetschutz

Zusätzlich zu den zentralen Vorkehrungen sind alle PCs und Notebooks auch durch eine lokal installierte Firewall und Internetschutz geschützt. Eine entsprechende Anleitung und Benutzerhinweise stehen zur Verfügung. Die Geräte sind damit auch bei einem Zugang zum Internet von externen Standorten aus entsprechend geschützt. Um einen ständigen Schutz der Geräte zu gewährleisten, darf nur die vom IT-

Dienstleister freigegebene und installierte Sicherheitssoftware installiert und betrieben werden. Ferner darf die Konfiguration der Schutzsoftware nicht verändert oder die Schutzsoftware deaktiviert oder deinstalliert werden. Insbesondere dürfen die automatische Aktualisierung der Schutzsoftware nicht deaktiviert oder verändert und die Geräte nicht ohne aktuellen Schutz am Internet betrieben werden. Die Konfiguration der Firewall und deren Funktionsfähigkeit sind vom IT-Dienstleister in angemessenen Abständen zu überprüfen.

2.2.6 Schutz der Informationen vor unbefugter Kenntnisnahme

In Räumen mit Publikumsverkehr sind IT-Arbeitsplätze so anzuordnen, dass betriebsfremde Personen keinen unmittelbaren Einblick in die Bildschirme haben, ggf. sind die Monitore mit Sichtschutzfolien gegen unbefugte Einsichtnahme zu schützen. Ebenso dürfen Drucker nur so aufgestellt werden (z.B. in Sicherheitszonen), dass unbefugte Personen keinen Zugang zu den Druckerzeugnissen besitzen. Ausdrucke sind nach Veranlassung des Druckprozesses unverzüglich vom Drucker abzuholen. Nach Möglichkeit, insbesondere für vertrauliche Vorgänge, sind vertrauliche Druckfunktionen zu benutzen. Bei Verlassen des Arbeitsplatzes hat sich der Benutzer am System abzumelden oder die Tastatur/ Bildschirmsperre (passwortgeschützter Bildschirmschoner) zu aktivieren. Unabhängig davon muss diese automatisch nach einer Zeitspanne von fünf bis zehn Minuten ohne Benutzereingabe wirksam werden. Datenträger, Ausdrucke oder sonstige Unterlagen mit vertraulichem/streng vertraulichem Inhalt sind grundsätzlich bei Verlassen des Arbeitsplatzes unter Verschluss zu halten. Bei Arbeitsende sind Endgeräte wie PCs oder Drucker auszuschalten. Nicht durch ein Kabelschloss gesicherte Notebooks sind bei Arbeitsende einzuschließen. Soweit keine anderweitigen Regelungen entgegenstehen, sind abschließbare Einzelbüros bei Verlassen abzuschließen.

2.2.7 Diebstahl und Verlust von Datenträgern

Um Diebstählen vorzubeugen, sind Notebooks und Docking-Stations beim stationären Betrieb nach Möglichkeit zu sichern, z.B. durch Sicherung mit einem Kabelschloss. Jeder Diebstahl oder sonstige Verlust von mobilen Geräten oder Datenträgern ist sofort dem Vorgesetzten und dem IT-Dienstleister zu melden. Von diesen Stellen werden die weiteren Schritte eingeleitet.

2.2.8 Verhalten auf Reisen

Notebooks und sonstige mobile Datenträger dürfen auf Reisen, z.B. in Zügen, aber z.B. auch während der Sicherheitskontrollen auf Flughäfen und an sonstigen öffentlichen Plätzen nicht unbeaufsichtigt gelassen werden. Notebooks dürfen nicht als Fluggepäck aufgegeben werden. Notebooks dürfen nicht sichtbar in Fahrzeugen abgelegt werden. Bei einer Verwahrung des Notebooks im Auto ist das Notebook nach Möglichkeit im Kofferraum mit einem Kabelschloss an der Karosserie zu befestigen. Im Hotel müssen Notebooks oder sonstige mobile Datenträger möglichst mitgeführt oder im Hoteltresor verwahrt werden. Die Zimmertresore sind häufig nicht ausreichend sicher. Bei einer Nutzung von Taxi oder Mietwagen ist darauf zu achten, keine Datenträger im Fahrzeug zu verlieren. Notebooks sind auf Reisen als Handgepäck mitzuführen und möglichst verborgen zu tragen. Bei Auslandsreisen sind die jeweils geltenden besonderen Risiken, Vorkehrungen und Auflagen zu beachten. 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 sonstige sensible Daten verarbeitet werden. Auf Reisen erfasste Daten und erstellte Verarbeitungsergebnisse sind laufend über eine sichere Verbindung auf die zentralen Systeme oder auf mobile Datenträger zu sichern. Die Sicherungsdatenträger sind zu verschlüsseln und getrennt vom Notebook zu verwahren.

2.2.9 Arbeiten in fremden Umgebungen

Bei einer Nutzung von Notebooks oder mobilen Datenträgern in fremden Umgebungen, z.B. bei Kunden, sind folgende mögliche Risiken zu beachten:
Arbeitsplatzrechner (Desktops, Notebooks, Handhelds, usw.) sowie Peripheriegeräte sind einzuschließen, wenn sie nicht unter Aufsicht sind. Bei Gesprächen und Besprechungen über vertrauliche Sachverhalte ist darauf zu achten, dass diese Gespräche nicht von unbefugten Personen belauscht werden können. Das Speichern oder Verarbeiten von internen und vertraulichen Informationen auf fremden Systemen ist unzulässig. Interne und vertrauliche Informationen dürfen nur auf Druckern ausgedruckt werden, bei denen die Ausgabe geeignet geschützt ist und sind umgehend vom Drucker abzuholen. Drucker und Kopierer mit umfangreichen Speicherfunktionen sollten für einen Ausdruck von vertraulichen Informationen vermieden werden.

2.2.10 Meldung von Sicherheitsvorfällen und Verhalten bei Systemausfällen und Störungen

Sicherheitsvorfälle sind Vorfälle mit dem Verlust oder dem Risiko des Verlusts oder der Zerstörung von Daten oder deren Vertraulichkeit, Integrität, Authentizität und Revisionsfähigkeit. Störungen sind sonstige Vorfälle und Betriebsstörungen ohne Gefährdung der Daten oder deren Vertraulichkeit, Integrität, Authentizität und Revisionsfähigkeit, meist in Verbindung mit einer vorübergehenden Störung der Verfügbarkeit der Daten, von Hard- oder Software oder der Funktionsfähigkeit von Datenverarbeitungsverfahren. Beim Auftreten von Sicherheitsvorfällen oder bei einem entsprechenden Verdacht und bei sonstigen Störungen ist folgendermaßen zu verfahren:
Ausfall oder Störungen von IT-Systemen sind unabhängig von der Art und der Schwere des Vorfalls und der Anzahl der betroffenen Systeme/Arbeitsplätze unverzüglich dem IT-Dienstleister zu melden. Dieser entscheidet je nach Art des Vorfalls über die weitere Vorgehensweise und über die zu benachrichtigenden bzw. einzuschaltenden Stellen, z.B. fachverantwortliche Stellen, Personalabteilung, Datenschutzbeauftragter oder Geschäftsleitung. Er leitet die erforderlichen Maßnahmen zur Schadensbegrenzung und zur Behebung der Störung ein. Mitbestimmungsrechte des Betriebsrats sind dabei zu beachten. Jeder Vorfall ist nach Art und Ausmaß, betroffenen Verfahren, Daten und Stellen zu dokumentieren. Die Art der Behebung des Vorfalls sowie die eingeleiteten rechtlichen, organisatorischen und technischen Maßnahmen sind zu dokumentieren. Der durch den Vorfall entstandene Schaden ist zu bewerten. Dabei sind auch immaterielle Schäden zu berücksichtigen, z.B. Auswirkungen auf Kunden, Beschäftigte, Öffentlichkeit etc., und es ist ein Schadens-bericht zu erstellen. Die Ursachen des Vorfalls sind zu analysieren, und es sind nach Möglichkeit Maßnahmen abzuleiten und einzurichten, um ähnliche Vorfälle in Zukunft zu vermeiden. Bei einem Verlust der Vertraulichkeit der Daten sind eventuelle Informationspflichten der Betroffenen und der Datenschutz-aufsichtsbehörde zu beachten. Mitarbeiter dürfen nicht versuchen, den Vorfall selbst aufzuklären oder etwas gegen den Verursacher zu unternehmen. Grundsätzlich ist dabei Folgendes zu beachten:

- Laufende Programme sind zu beenden.
- Neue Programme dürfen nicht mehr gestartet werden.
- Es dürfen keine Daten oder E-Mails mehr versandt werden.
- Systemhinweise und Systemmeldungen sind festzuhalten.

Die Dokumentationen über Sicherheitsvorfälle sind regelmäßig statistisch aufzuarbeiten und nach Art, Umfang, Kosten, Risiko- und Gefahrenpotenzial der Vorfälle auszuwerten. Aus den Auswertungen sind unter dem Gesichtspunkt des Lernens aus Vorfällen Maßnahmen zur künftigen Vermeidung ähnlicher Vorfälle und zur Verbesserung der Informationssicherheit abzuleiten.

2.3 Sicherungsmaßnahmen

2.3.1 Sicherung von zentralen Datenbeständen

Die Datensicherung erfolgt auf der Grundlage eines festgelegten Sicherungskonzepts auf vorgesehene Systeme und Datenträger. Die Lesbarkeit der Sicherungsbestände ist regelmäßig zu kontrollieren und die erfolgreiche Durchführung der Sicherungsaktivitäten lückenlos zu überwachen und zu protokollieren. Die Sicherungsdatenträger sind auf ihre Haltbarkeit und die zulässige Zahl von Schreibzyklen zu überprüfen und rechtzeitig auszusondern. Je nach Sensibilität und Bedeutung der Daten für das Unternehmen ist die Wiederherstellung der Datenbestände aus den Sicherungsdaten regelmäßig (mindestens einmal jährlich) zu testen und zu dokumentieren. Die Sicherungsdatenträger sind getrennt von den Datenverarbeitungssystemen, zumindest in einem anderen Brandabschnitt in einem feuerhemmenden Tresor der Schutzklasse S60 oder S120, zu lagern.

2.3.2 Sicherung von lokalen Datenbeständen

Daten auf lokalen Festplatten, z.B. von Arbeitsplatz-PCs oder auf sonstigen mobilen Datenträgern, werden nicht gesichert und sind im Schadensfall verloren. Ungesicherte Laufwerke, z.B. lokale oder persönliche Laufwerke, dürfen deshalb nicht als alleiniger Speicherort für geschäftskritische Daten verwendet werden.

2.3.3 Protokollierung

Folgende Sachverhalte, Ereignisse und Aktionen sind in geeigneter Weise zu protokollieren bzw. zu regeln:

- Dokumentation von Systemumfang, Komponenten/Modulen des eingesetzten IT-Systems
- Fachliche und technische Freigabe und Freigabe zum Einsatz
- 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
- Systemänderungen
- Dokumentation von funktionalen Systemänderungen/Erweiterungen einschließlich Testfällen, Testung, Testergebnissen und Freigabe
- Dokumentation von Versionsänderungen oder Änderungen der technischen Umgebung des IT-Systems
- Änderungen der Dateiorganisation oder des Dateiverwaltungssystems
- Protokollierung von Eingaben und Veränderungen auf Systemebene
- 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
- Systemüberwachung
- Benutzte Programme
- Systemstart und –stop
- Anschluss und Entfernung von Ein- und Ausgabegeräten

- Aktivitäten im Zusammenhang mit Fremdwartung und Fernwartung
- Systemwarnungen oder Systemfehler
- Konsolwarnungen und Konsolmeldungen
- Am Paketfilter wegen Regelverstoß abgewiesene Pakete
- 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
- VoIP-Systeme
- Verkehrsdaten
- Konfigurationsänderungen
- Anlegen und Löschen von Benutzern
- 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
- 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
- Auswertung der Protokolle

Die Protokolle sind regelmäßig und zeitnah auf sicherheitsrelevante und sonstige kritische Aktivitäten und Zustände auszuwerten. Nach Möglichkeit sind für die Kontrolle, Auswertung und Meldung der Vorfälle und Zustände geeignete automatisierte Werkzeuge zu verwenden. Die Protokolldaten dürfen nach den Vorschriften des Bundesdatenschutzgesetzes nur zum Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs der Datenverarbeitungsanlagen gespeichert und verwendet werden. Soweit die Protokolldaten nicht aus Rechtsgründen, z.B. zur Verfolgung von Rechtsansprüchen, länger erforderlich sind, sind sie nach Ablauf einer Frist von zwölf Monaten zu löschen. Die Protokolldaten sind vor unbefugten Zugriffen zuverlässig geschützt zu speichern.

2.3.4 Verwendung von Passwörtern

Der Zugang zu Datenverarbeitungsverfahren ist nur über ein sicheres Anmeldeverfahren zulässig. Das Anmeldeverfahren ist insbesondere bei sensiblen Verfahren so zu gestalten, dass bei einem Anmeldevorgang Datum und Uhrzeit des letzten vorhergegangenen erfolgreichen oder erfolglosen Anmeldeversuchs angezeigt werden. Die Anzahl der erfolglosen Anmeldeversuche ist auf drei Versuche zu begrenzen. Erfolglose Anmeldeversuche sind zu protokollieren. Die Identifizierung und Authentifizierung der Benutzer geschieht durch ein persönliches Login, das jeder Mitarbeiterin und jedem Mitarbeiter zugeteilt ist

und durch ein zusätzliches Passwort. Mit dem Login sind im System die Berechtigungen des Eigentümers verknüpft, während das Passwort der Identifikation des Berechtigten dient. Für den Fall, dass Passwörter vergessen oder der Zugang durch Überschreiten der zulässigen Anzahl von Fehlversuchen gesperrt worden ist, darf das Passwort nur in einem geregelten Verfahren, das eine eindeutige Identifizierung des Benutzers gewährleistet (z.B. durch Einsatz eines Passwort-Reset-Managementsystems oder eines anderen geeigneten Verfahrens), zurückgesetzt werden. Das Passwort ist der persönliche Schlüssel zu diesen Systemen und Daten und muss absolut vertraulich behandelt werden. Da Passwörter auch ausgespäht und entschlüsselt werden können, müssen bestimmte Regeln beachtet werden, um ein sicheres Passwort zu gewährleisten. Die folgenden Passwortregeln sind unter diesen Sicherheitsanforderungen erarbeitet worden und bieten bei einer konsequenten Anwendung ein hohes Maß an Sicherheit:

- Jeder PC-Benutzer ist verpflichtet, ihm zur Verfügung gestellte bzw. von ihm benutzte Passwörter vertraulich zu behandeln und geheim zu halten, sodass sie Dritten nicht zugänglich sind. Passwörter dürfen nicht an Dritte, nicht an Kolleginnen und Kollegen und auch nicht an IT-Administratoren weitergegeben werden. Passwörter dürfen nicht in Dateien oder Skripten gespeichert und auch nicht am Arbeitsplatz, z.B. auf Zetteln, hinterlegt oder auf Funktionstasten gespeichert werden.
- Die Anmeldung darf niemals unter einem fremden Benutzernamen/Passwort erfolgen.
- Bei einem Verdacht auf Verlust der Vertraulichkeit oder Ausspähung ist das Passwort sofort zu ändern. Ansonsten sind Passwörter in Abständen von drei Monaten zu ändern. Es ist ein von den bisher genutzten Passwörtern abweichendes Passwort zu wählen. Voreingestellte Passwörter (z. B. des Herstellers oder der IT-Administration bei Auslieferung/Installation von Systemen) dürfen nur einmalig verwendbar sein (sog. Einmalpasswörter) und sind unverzüglich durch individuelle Passwörter zu ersetzen.
- Bereits benutzte Passwörter dürfen nach einem Passwortwechsel nicht wieder verwendet werden.
- Passwörter sind verdeckt einzugeben, um eine Kenntnisnahme durch Unbefugte zu verhindern. Bei Verdacht von Missbrauch ist unverzüglich die IT-Systemadministration einzuschalten.
- Das Passwort muss mindestens acht Zeichen lang sein. Es muss aus Groß- und Kleinbuchstaben und mindestens aus einer Ziffer und einem Sonderzeichen (z.B.*"§$%& etc.) bestehen und darf nicht mehr als zwei aufeinander folgende identische Zeichen enthalten. Es dürfen keine Trivialpasswörter verwendet werden, dazu gehören aufeinander folgende Buchstaben und Zahlen, z.B.123456 oder abcdefg oder aufeinander folgende Tastaturzeichen, z.B. asdfgh, Es dürfen auch keine Passwörter verwendet werden, die mit dem einzelnen Mitarbeiter in Verbindung gebracht werden können, z.B. Name, Wohnort, Kfz-Kennzeichen etc. und keine Namen/Begriffe, die in Wörterbüchern stehen können.
- Die Benutzerkennung darf nicht Bestandteil des Passworts sein. Die von einigen Browsern angebotene Funktion „Passwort speichern" darf nicht verwendet werden.
- Passwörter, welche innerhalb des Unternehmens verwendet werden, dürfen nicht in anderen Umgebungen (z.B. im Internet, Kundenportale etc.) gleichlautend verwendet werden.

Um im Falle einer Kompromittierung des Passworts die Risiken möglichst gering zu halten, darf auch innerhalb des Unternehmens für mehrere Zugänge bzw. Applikationen nicht das gleiche Passwort verwendet werden. Die Einhaltung dieser Passwortregeln ist in einem ausreichenden Umfang automatisiert zu kontrollieren und zu erzwingen. Nach einer mehrmaligen Falscheingabe (drei Fehlversuche) ist der Zugang zu blockieren und darf erst nach einer zweifelsfreien Identifikation des Benutzer wieder freigegeben werden.

2.4 Einrichten und Verwalten von Benutzerkonten und Zugriffsrechten

Die Benutzer dürfen nur auf solche Programme, Laufwerke, Ordner und Dateien Zugriff erhalten, die sie für die Erledigung ihrer betrieblichen Aufgaben benötigen. Dies geschieht über direkt dem Mitarbeiter zugewiesene Rechte und Berechtigungen für die eingesetzten Systeme bzw. Anwendungen und Daten. Berechtigungen sind restriktiv zu handhaben und dürfen deshalb nur in dem Umfang vergeben werden, wie es zur Erledigung der betrieblichen Aufgaben erforderlich ist. Im Einzelnen gelten folgende Regelungen:

- Mitarbeiter dürfen sich nur innerhalb der Systeme und Datenbereiche bewegen, welche sie zur Erfüllung ihres Arbeitsauftrags benötigen. Sollte im Einzelfall aufgrund einer unzureichenden Rechtevergabe oder aufgrund technischer Mängel ein Zugriff auf Ressourcen möglich sein, die außerhalb des Aufgabengebiets des Benutzers liegen, darf von diesen Rechten nicht Gebrauch gemacht werden. Der Vorgesetzte oder der IT-Dienstleister ist zu verständigen.
- Die Benutzerkonten und Zugriffsrechte werden von der IT-Administration nach schriftlicher Anforderung der Fachvorgesetzten eingerichtet. In der Anforderung sind die freizugebenden Anwendungen und die erforderlichen Rechte festzulegen. Den Mitarbeitern dürfen keine Administratorrechte übertragen werden. Ausnahmen sind eingehend zu begründen. Soweit die Vergabe von Administrationsrechten erforderlich ist, z.B. bei lokalen Geräten mit lokalem Betriebssystem, dürfen diese Administrationsrechte nur im erforderlichen Umfang für betriebliche Aufgaben eingesetzt werden. Sicherheitsrelevante Einstellungen oder Standardsystemeinstellungen der Systeme dürfen nicht verändert werden.
- Bei Ausscheiden des Mitarbeiters, Versetzungen oder Wechsel von Aufgaben und Zuständigkeiten ist von den jeweiligen Vorgesetzten unverzüglich die Löschung von eventuell nicht mehr benötigten Berechtigungen zu veranlassen. Neue Zugriffsrechte sind entsprechend dem neuen Aufgabengebiet zu beauftragen und einzurichten.

Zur Rechtekontrolle ist jährlich von den Fachvorgesetzten zu prüfen, ob die eingerichteten Berechtigungen zur Aufgabenerfüllung noch erforderlich sind, und die Erforderlichkeit der IT-Administration zu bestätigen. Nicht mehr erforderliche Rechte sind zu löschen.

2.5 Verantwortlichkeit für Daten

2.5.1 Ausscheiden, Umsetzung und Abwesenheit von Beschäftigten

Jeder Mitarbeiter ist verpflichtet, vor seinem Ausscheiden, seiner Umsetzung bzw. Abwesenheit alle für das Unternehmen noch relevanten und aufbewahrungspflichtigen Dokumente und Daten zu übergeben und private bzw. nicht mehr erforderliche Vorgänge zu löschen. Die Übergabe der Daten und Dokumente ist vom Vorgesetzten und die Löschung der privaten Vorgänge vom Betroffenen zu bestätigen.

2.6 Computersicherheit, Computerviren und sonstige bösartige Software

Um den Risiken durch Schad- und Spionagesoftware vorzubeugen, ist Folgendes zu beachten: Verbindungen von vernetzten PCs zu externen Netzen außerhalb des Unternehmens sind nur im zwingend erforderlichen Umfang und nur nach sicherheitstechnischer Prüfung und Freigabe durch den IT-Dienstleister zulässig. Dabei müssen die vom IT-Dienstleister eingerichteten Schutzmaßnahmen vorhanden, aktuell und funktionsfähig sein. Alarme der Virenscanner, Computeranomalien und Systemereignisse oder sonstige Auffälligkeiten, die auf die Aktivierung unbekannter Software hindeuten (z.B. Datenverluste, längere Ladezeiten von Programmen, unerklärbare und vermehrte Festplattenzugriffe, Programmabstürze etc.), sind der IT-Systemadministration unverzüglich zu melden. Die eigenmächtige Veränderung von Sicherheitseinstellungen, z.B. am Virenscanner oder am Browser, ist unzulässig.

Bei Verdacht auf eine Vireninfektion ist wie folgt zu verfahren:

- Neue Programme dürfen nicht mehr gestartet werden.
- Es dürfen keine Daten mehr eingegeben und keine E-Mails mehr versandt werden.
- Das Betriebssystem und laufende Programme sind zu beenden.
- Alle Systemhinweise und Meldungen sind zu notieren.
- Die IT-Administration ist umgehend zu verständigen.
- Zusätzlich gelten die Sicherheitsmaßnahmen bei der Nutzung von E-Mail und Internet.

2.7 Notebooks und mobile Kommunikationsgeräte

Um Datenverluste zu vermeiden, dürfen auf Notebooks und mobilen Kommunikationsgeräten (Mobiltelefonen, PDAs etc.) nur Kopien von Firmendaten gespeichert werden. Soweit personenbezogene Daten oder sonstige vertrauliche oder streng vertrauliche Daten nach den Regelungen der Vertraulichkeitsrichtlinie gespeichert werden, sind diese Daten zu verschlüsseln. Darüber hinaus sind folgende Vorsichtsmaßnahmen zu beachten:
Jedes mobile Gerät ist mit einem sicheren Passwort nach den Vorgaben dieser Richtlinie oder durch ein anderes sicheres und zugelassenes Verfahren zu sichern. In Privaträumen ist ein unbefugter Zugang auszuschließen. Ein Zugriff durch unbefugte Personen oder eine Überlassung des Notebooks an Dritte, auch an Familienangehörige, zur Nutzung ist unzulässig. Werden Notebooks von wechselnden Benutzern oder in unsicheren bzw. unbekannten Umgebungen eingesetzt, sind sie einem regelmäßigen Sicherheitscheck zu unterziehen. In öffentlichen Räumen, z.B. in Verkehrsmitteln etc., sind an den Notebooks Blickschutzfilter zu verwenden, ansonsten ist eine Verarbeitung von personenbezogenen oder sonstigen sensiblen Daten unzulässig. Mobile Geräte dürfen nicht unbeaufsichtigt sein und müssen zugriffssicher verwahrt werden. Zum Anschluss an unternehmensfremde Rechner dürfen nur mobile Geräte verwendet werden, die keine personenbezogenen oder sonstige vertraulichen Daten enthalten. Nach einem Anschluss an Fremdrechner müssen die mobilen Geräte auf Freiheit von Viren und sonstiger Schadsoftware geprüft werden.

2.8 Weitergabe, Löschung und Entsorgung von Geräten und Datenträgern

2.8.1 Weitergabe von elektronischen Datenträgern

Eine Weitergabe von Datenträgern an Dritte darf nur im Rahmen der vorgesehenen Verfahren und nur an befugte Personen erfolgen. Ausnahmen bedürfen der vorherigen Genehmigung durch den IT-Dienstleister. Der Empfang von personenbezogenen oder sonstigen vertraulichen Daten ist von den Empfängern zu quittieren. Bei einem Versand von Datenträgern ist ein zuverlässiger Versandweg zu wählen, über den der Versand und der Empfang der Datenträger nachweisbar sind. Personenbezogene oder sonstige vertrauliche Daten sind vor dem Versand zu verschlüsseln.

2.8.2 Löschung und Entsorgung von elektronischen Datenträgern

Alle personenbezogenen und sonstigen Unternehmensdaten sind unverzüglich zu löschen, wenn sie für die Aufgabenerfüllung nicht mehr benötigt werden und keinen Aufbewahrungsfristen unterliegen bzw. die Aufbewahrungsfristen abgelaufen sind. Die Löschung ist von der fachverantwortlichen Stelle unter Beachtung eventueller Aufbewahrungsfristen oder eines sonstigen Aufbewahrungsinteresses des Unternehmens oder der Betroffenen schriftlich anzuordnen. Für die Löschung von elektronischen Datenträgern sind sichere Löschverfahren, z.B. Löschprogramme, einzusetzen, die durch mehrmaliges Überschreiben die gespeicherten Daten zuverlässig und nicht wiederherstellbar überschreiben. Bei der Vernichtung und Entsorgung von Datenträgern ist darauf zu achten, dass keine personenbezogenen oder sonstige vertrauliche Daten in unbefugte Hände geraten. Für jede Art von Daten und Datenträgern sind deshalb die nachstehenden Regelungen zu beachten. Bei einer Vernichtung durch Dienstleistungs-

unternehmen sind die Vorschriften des § 11 BDSG zur Datenverarbeitung im Auftrag zu beachten. Zu entsorgende elektronische Datenträger sind vom Benutzer an der von der IT eingerichteten Sammelstelle abzugeben. Dort werden sie gesammelt, aufbereitet oder vernichtet oder in geeigneter Weise entsorgt. Enthalten die Datenträger personenbezogene Daten oder Daten, die nach den Vertraulichkeitsrichtlinien der Vertraulichkeit unterliegen, sind diese Datenträger vor ihrer Weitergabe zur Vernichtung mit einem Löschprogramm nach dem jeweiligen Stand der Technik sicher zu löschen. Kann der Datenträger wegen eines Defekts nicht mehr angesprochen werden, ist der Datenträger zu vernichten. In Gewährleistungsfällen oder sonstigen besonders gelagerten Fällen kann der IT-Dienstleister je nach den Umständen des Einzelfalls (Art des Datenträgers, Art und Sensibilität der gespeicherten Daten, Garantiefall oder sonstiger Reparaturtausch) unter Berücksichtigung der Sicherheitsanforderungen eine abweichende Entscheidung treffen. Enthält der Datenträger besonders sensible oder sonstige besonders vertrauliche Daten (z.B. Personaldaten) und ist eine sichere Löschung nicht möglich, ist der Datenträger ausnahmslos zu vernichten. Da auch Papier vertrauliche Informationen enthalten kann, sind eine sorgfältige Sammlung von Altpapier und eine zuverlässige Entsorgung mit einer Bestätigung der datenschutzgerechten Vernichtung erforderlich. Die Vernichtung von Papier ist in der Norm DIN 32757-1 geregelt. Für geheim zu haltendes Schriftgut ist nach dieser Norm die Vernichtung nach Sicherheitsstufe 3 mit einem Streifenschnitt von maximal 2 mm Breite und einer Teilchenfläche von max. 594 mm² oder einem Partikelschnitt von 4 mm x 80 mm und kleiner und einer Teilfläche von max. 320 mm² erforderlich. Bei der Papierentsorgung ist darauf zu achten, dass diese Anforderungen eingehalten und vom Entsorgungsunternehmen schriftlich bestätigt werden.

3 E-Mail/Internet

3.1 Gemeinsame Regelungen

3.1.1 Private Nutzung von E-Mail und Internet

Die Nutzung von Internet und E-Mail-Dienst für private Zwecke ist zulässig, soweit die betrieblichen Aufgabenerfüllung sowie die Verfügbarkeit des IT-Systems für betriebliche Zwecke nicht beeinträchtigt wird. Ein Abruf von erheblichen Datenmengen wie z.B. Musikdateien oder die Nutzung von Internet- Radio, Internet-TV o.Ä. ist wegen der damit verbundenen Netzbelastung unzulässig. Das Abrufen von kostenpflichtigen Informationen oder die Nutzung von kostenpflichtigen Diensten für den Privatgebrauch ist unzulässig. Im Rahmen der zugelassenen privaten Nutzung dürfen keine kommerziellen oder sonstige eigene geschäftliche Zwecke verfolgt werden. Eine Unterscheidung von betrieblicher und privater Nutzung auf technischem Weg erfolgt nicht. Die Protokollierung und Kontrolle der Verkehrsdaten erstreckt sich deshalb auch auf den Bereich der privaten Nutzung. Ein Verstoß gegen diese Nutzungsregelung kann neben den arbeitsrechtlichen auch Schadensersatzansprüche oder strafrechtliche Folgen nach sich ziehen. Die Unternehmensleitung behält sich vor, den Zugang zu bestimmten Internetadressen zu sperren oder bei Verstößen gegen diese Vereinbarung die private Nutzung des Internetzugangs im Einzelfall zu untersagen. Die Erlaubnis der Nutzung von Internet und E-Mail-Dienst für private Zwecke steht unter dem Vorbehalt der organisatorischen, technischen und rechtlichen Rahmenbedingungen und kann bei einer Änderung dieser Umstände oder aus sonstigen Gründen jederzeit einseitig widerrufen werden.

3.1.2 Einweisung/Schulung

Jeder Beschäftigte wird mit der Zurverfügungstellung des E-Mail/Internet-Dienstes in die Nutzung der Dienste eingewiesen. Dabei werden die Beschäftigten in die unternehmensspezifischen Regelungen eingewiesen und über die mit der Nutzung der Dienste verbundenen Risiken und die zu beachtenden Sicherheitsmaßnahmen unterrichtet. Die Teilnahme an der Einweisung ist nachvollziehbar zu dokumentieren.

3.1.3 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 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.

3.2 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. Die Größe der E-Mails ist, unabhängig ob sie versendet oder empfangen werden, nicht beschränkt.

3.2.1 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.

3.2.2 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.

3.2.3 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. BlackBerry, PDA etc.) versandt werden.

3.2.4 Rechtliche Verbindlichkeit von E-Mails

Da E-Mails bei ihrer Übertragung verfälscht werden können, sind Authentizität und Integrität der Mail bzw. des Inhalts nicht gesichert und der Beweiswert ist 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.

3.2.5 Sonstige Verhaltensgrundsätze

Die Nutzung von E-Mail-Programmen unterliegt verschiedensten Risiken. So können empfangene E-Mails gefälscht worden sein oder einen anderen Absender vortäuschen oder mit Schad- oder Spionagesoftware infiziert sein. Besondere Vorsicht ist deshalb bei E-Mails von unbekannten Absendern und insbesondere bei Anhängen von E-Mails geboten, weil diese ausführbare Dateien und damit auch Schadsoftware enthalten können. Es sind deshalb folgende Verhaltensgrundsätze zu beachten:
E-Mails unbekannter Herkunft und mit nicht plausiblen Betreffs oder nicht korrekter Sprache und Anhängen (insbesondere mit ausführbaren Dateien), sollten nicht geöffnet, sondern ungeöffnet gelöscht und auch keine Lesebestätigung abgegeben werden. In Zweifelsfällen ist die IT Administration zur Prüfung der E-Mails einzuschalten oder beim Absender nachzufragen. 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.

3.2.6 Spamfilterung

Zum Schutz vor Spam-Mails, insbesondere solchen 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 auf Schadsoftware überprüft. In Abhängigkeit von den technischen Gegebenheiten des Spamfilters werden die Benutzer über die Spamfilterung unterrichtet und die ausgefilterten E-Mails in einem Quarantäneordner zur Einsicht zur Verfügung gestellt und nach Ablauf einer Frist von einem Monat gelöscht. Festgestelle 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.

3.3 Nutzung des Internetsystems

3.3.1 Allgemeines

Der Internet-Zugang wird den Beschäftigten als Arbeitsmittel im Rahmen der betrieblichen Aufgabenerfüllung zur Verfügung gestellt und dient insbesondere der Verbesserung der internen und externen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse. Der uneingeschränkte Zugang für den betrieblichen Zweck ist an eine gesonderte, vom jeweiligen Vorgesetzten zu beantragende Berechtigung gebunden. Bei der Nutzung des Internetzugangs sind folgende Regeln und Vorsichtsmaßnahmen zu beachten:

3.3.2 Nutzung des Internetzugangs

Für die Nutzung des Internets darf nur die vom Unternehmen bereitgestellte Hard- und Software eingesetzt werden. Das Einbringen und Installieren von privater Hard- und/oder Software oder von externen Dienstprogrammen, von Dokumenten und Daten aller Art in das lokale Netz ist ohne explizite Freigabe aus Sicherheitsgründen unzulässig. Ebenso ist das Ausführen von über das Internet beschafften Programmen oder ausführbarem Programmcode ohne vorherige Prüfung auf Virenbefall und Freigabe durch den IT-Dienstleister untersagt. Jede absichtliche oder wissentliche Nutzung des Internets, die den Interessen des Unternehmens oder dessen Ansehen in der Öffentlichkeit schaden oder die Sicherheit des Firmennetzes beeinträchtigen kann oder die gegen geltende Rechtsvorschriften oder ggf. vorhandene Richtlinien oder Verfahrensanweisungen für die Nutzung des IT-Systems verstößt, ist unzulässig. Dies gilt insbesondere für das Abrufen und Verbreiten von Inhalten, die gegen strafrechtliche, urheberrechtliche oder persönlichkeitsrechtliche Bestimmungen verstoßen, das Abrufen und Verbreiten von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, Gewalt verherrlichenden oder pornografischen Äußerungen oder Abbildungen, das Abrufen und Verbreiten von weltanschaulichen, parteipolitischen oder sonstigen Inhalten, die den Interessen oder dem Ansehen des Unternehmens in der Öffentlichkeit schaden können, das Abrufen und Verbreiten unbekannter Inhalte aus unsicheren Quellen, insbesondere mit Anhängen und ausführbaren Dateien. Soweit für die Nutzung oder für den Zugang zu gewünschten Informationen die Eingabe von Benutzerkennung und Passwort verlangt wird, dürfen keine internen Kennungen und Passwörter verwendet werden. Unzulässig ist auch jede Veröffentlichung von Inhalten oder eine Teilnahme an Diskussionsforen oder sonstigen Plattformen im Namen des Unternehmens oder in einer Form, die den Eindruck erweckt, dass es sich um einen offiziellen Beitrag des Unternehmens handelt. Veröffentlichungen im Namen des Unternehmens sind vorab von der Geschäftsleitung freizugeben. Bei jeder Veröffentlichung und auch bei der Teilnahme an sozialen Netzwerken, z.B. Facebook u.a., ist streng darauf zu achten, dass keine internen oder vertraulichen Informationen veröffentlicht werden.

3.3.3 Allgemeine Sicherheitsregeln

Für die Nutzung des Internets gelten folgende Sicherheitsregeln:

- Eine Ergänzung des Browsers, z.B. durch sog. Add-on oder Plug-in, oder eine Veränderung der Sicherheitseinstellungen des Browsers durch die Benutzer ist unzulässig.
- Werden Daten aus dem Internet heruntergeladen, sind diese Daten unverzüglich nach dem Datentransfer mit dem Virenscanner auf Schadsoftware zu überprüfen.
- Der Download von Sicherheits- oder Hacker-Werkzeugen und deren Nutzung ist unzulässig.
- Da immer wieder Internetseiten gehackt oder Phishing-Seiten eingerichtet werden, sollte nur vertrauenswürdigen Links gefolgt werden. Ferner sind verändertes Aussehen und Verhalten von

bislang bekannten seriösen Webseiten sofort dem IT-Dienstleister zur Überprüfung der Authentizität der Seiten zu melden. Software aus dem Internet darf nicht von den Benutzern heruntergeladen werden, weil über derartige Software die Gefahr des Einbringens von Schadsoftware besteht. Wird der Einsatz derartiger Software gewünscht, ist der IT-Dienstleister einzuschalten und mit einem eventuellen Download und Prüfung der Software zu beauftragen.

- Bei einer Nutzung von Internetdiensten dürfen keine intern verwendeten Passwörter eingesetzt werden.
- Ebenso dürfen für die Nutzung von mehreren Internetdiensten nicht identische Passwörter eingesetzt werden.

Untersagt sind:

- die Verfolgung von privaten geschäftlichen Zielen,
- der Download von Musik- und Videodateien,
- der Abruf von kostenpflichtigen Informationen und Diensten,
- die Beteiligung an Tauschbörsen, Onlinespielen oder ähnlichen Aktionen,
- die Beteiligung an Diskussionsforen mit offensichtlich rechtswidrigen oder sonstigen fragwürdigen Inhalten.

Das Unternehmen behält sich vor, den Zugang zu rechtswidrigen oder sonstigen sicherheitskritischen oder mit den Grundsätzen des Unternehmens nicht zu vereinbarenden Internetseiten zu sperren. Nicht gesperrte Seiten dieser Art sind sofort zu verlassen.

4 Protokollierung der E-Mail- und Internetnutzung

Zur Überprüfung der Einhaltung der Regelungen dieser Vereinbarung werden regelmäßige nichtpersonenbezogene Stichproben in den Protokolldateien durchgeführt. Ergänzend wird eine Übersicht über das jeweilige Gesamtvolumen des ein- und ausgehenden Datenverkehrs erstellt. Zur Gewährleistung der Systemsicherheit, zum Erkennen, Eingrenzen, Beheben und Vorbeugen von Störungen sowie zur Missbrauchskontrolle bzw. zur Erkennung und Verhinderung unbefugter Handlungen und Sicherstellung eines ordnungsgemäßen Betriebs werden bestimmte Benutzeraktivitäten, Systemaktivitäten und Systemzustände protokolliert und ausgewertet. Dabei handelt es sich regelmäßig um Daten über Art und Zeitpunkt der Benutzeraktivität und nähere Daten, z.B. wodurch bzw. von wem die Aktivität veranlasst wurde. Diese Protokollierungen sind erforderlich, um die Ordnungsmäßigkeit und Nachvollziehbarkeit des IT-Betriebs zu gewährleisten. Über die Nutzung des E-Mail-Systems werden folgende Protokolldaten gewonnen:

- Datum und Uhrzeit des Vorgangs
- Absender und Empfänger
- Größe der E-Mails und von Anhängen
- Dateiformate

Über die Internetnutzung werden folgende Protokolldaten gespeichert:

- Datum und Uhrzeit des Vorgangs
- Adresse der besuchten Seiten
- IP-Adresse des benutzen PCs

Die aufgezeichneten Protokolldaten unterliegen der Zweckbindung des § 31 Bundesdatenschutzgesetz und dürfen nur für Administrationszwecke nach den Regelungen dieser oder weiterer Richtlinien zum Betrieb der IT-Systeme, für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs der Datenverarbeitungsanlagen (insbesondere zur Gewährleistung der Systemsicherheit, Analyse und Korrektur technischer Fehler, Optimierung des Netzes, zur

Missbrauchskontrolle etc.) gespeichert und verwendet werden. Die Daten werden nicht für eine Leistungs- und Verhaltenskontrolle genutzt. Die Protokolle werden über einen Zeitraum von sechs Monaten gespeichert. Soweit sie nicht als Beweismittel für aufgetretene Störungen oder Unregelmäßigkeiten benötigt werden, werden sie nach Ablauf dieser Frist durch die IT-Systemadministration gelöscht. Im Rahmen der laufenden Kontrollmaßnahmen werden keinerlei Inhaltsdaten zur Kenntnis genommen oder aufgezeichnet. Soweit aus besonderen Gründen, z.B. bei einem Verdacht auf eine missbräuchliche Nutzung, personenbezogene Auswertungen der Protokolldaten oder sonstige personenbezogene Kontrollmaßnahmen erforderlich werden, werden diese nur unter Beteiligung der Rechts-/Personalabteilung, des Betriebsrats, des Datenschutzbeauftragten unter Beachtung der jeweils gültigen Datenschutzvorschriften (z.B. Bundesdatenschutzgesetz, Telekommunikationsgesetz) und der arbeitsrechtlichen Vorschriften durchgeführt. Der Betroffene wird zum frühestmöglichen Zeitpunkt über diese Kontrollen und über die Ergebnisse unterrichtet.

5 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 (siehe Anlage) nicht abgibt, gilt für ihn ein Verbot der privaten Nutzung.

6 Überprüfung der Richtlinie „Informationssicherheit, Einsatz und Nutzung der IT-Systeme"

Diese Richtlinie ist neben ihrer laufenden Anpassung an Veränderungen der Rahmenbedingungen im Abstand von jeweils zwölf Monaten auf ihre Aktualität, Vollständigkeit und Konformität zu den vorhandenen rechtlichen, technischen und organisatorischen Rahmenbedingen zu überprüfen und ggf. zu ergänzen bzw. zu aktualisieren.