Datenschutzrichtlinie

der Kanzlei

Loserth Schranner & Partner

Inhalt

I. Datenschutzrichtlinie allgemeiner Teil

1 Präambel

Der Schutz von personenbezogenen Daten rückt zunehmend in den Fokus der betroffenen Personen, der Öffentlichkeit und der Gesellschaft. Dem trägt auch die Europäische Datenschutzgrundverordnung (DSGVO) Rechnung. Der Schutz von personenbezogenen Daten und Informationen (und ein großer Teil davon sind personenbezogene Daten) ist auch ein bedeutender Wirtschaftsfaktor und als solcher für unser Unternehmen von großer Bedeutung. Andererseits kann ein Missbrauch der Daten und Informationen nicht nur die Wirtschaftstätigkeit unseres Unternehmens und die betriebliche Funktion schwer beeinträchtigen, sondern auch die Umweltbeziehungen oder das Ansehen unseres Unternehmens erheblich beschädigen und dadurch großen Schaden verursachen. Die mit der Datenschutzgrundverordnung eingeführte Rechenschaftspflicht führt zu einer Beweislastumkehr mit der Folge, dass das Unternehmen in der Lage sein muss, die Einhaltung der Grundsätze und Vorschriften der Datenschutzgrundverordnung nachzuweisen. Diese Datenschutzrichtlinie ist ein wichtiges Instrument zur Führung dieses Nachweises und zur Erfüllung der Rechenschaftspflicht.

Das Anliegen dieser allgemeinen Datenschutzrichtlinie ist es deshalb, im Interesse der betroffenen Personen und auch des Unternehmens den Schutz der personenbezogenen Daten nach den Vorschriften der DSGVO zu regeln und in jeder Phase der Informationsverarbeitung die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Daten zu gewährleisten. Um dieses Ziel zu erreichen, müssen nicht nur die gesetzlichen Vorschriften zum Schutz der Daten eingehalten, sondern auch geeignete technische und organisatorische Maßnahmen und Verfahren eingerichtet und geregelt und deren Einhaltung und Wirksamkeit ähnlich wie nach den Methoden des Qualitätsmanagementsystems kontrolliert, dokumentiert und weiterentwickelt werden. Nicht zuletzt kommt es aber auch darauf an, dass sich alle Beschäftigten der mit dem Umgang mit personenbezogenen Daten sowie der Datenverarbeitung und der Benutzung der technischen Systeme und Kommunikationstechnologien verbundenen Risiken und Verantwortung bewusst sind und mit Daten und Systemen mit der erforderlichen Vorsicht und Sorgfalt umgehen. Bei Fragen zum Umgang mit personenbezogenen Daten ist der Vorgesetzte oder der betriebliche Datenschutzbeauftragte zu konsultieren.

2 Zweck des Dokuments

Die Datenschutzrichtlinie folgt in der Dokumentenstruktur dem Managementhandbuch und regelt als Kopfdokument des Datenschutzmanagements mit den darin angegebenen mitgeltenden Unterlagen die rechtlichen und die zum Schutz der personenbezogenen Daten erforderlichen technischen und organisatorischen Maßnahmen. Die Einzelheiten dazu befinden sich in den mitgeltenden Unterlagen. Soweit zu einzelnen Bereichen gesonderte Dokumentationen vorhanden sind (z. B. zu bestimmten Prozessen, technischen Systemen und besonderen Verfahren), wird, sofern es zum Verständnis der Sicherungsmaßnahmen erforderlich ist, auf diese Dokumentationen verwiesen.

Die Datenschutzrichtlinie beschreibt den Aufbau und die Prinzipien des Datenschutzmanagements und bezeichnet die mitgeltenden Unterlagen. Es vermittelt damit einen kompletten Überblick über den Aufbau und die Funktionsweise des Datenschutzmanagements und kann auch als Einstieg und Grundlage für Prüfungen und Zertifizierungen dienen. Darüber hinaus erfüllt dieses Dokument mit den mitgeltenden Unterlagen die in der DSGVO geforderten Dokumentations- und Nachweispflichten und erfüllt die Anforderungen an die Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO.
Weil ein wirksamer Datenschutz nicht alleine durch Regelungen und Bestimmungen erreicht werden kann, sondern von einem ausgeprägten Datenschutz- und Sicherheitsbewusstsein der Mitarbeiterinnen und Mitarbeiter getragen wird, ist es ein besonderes Anliegen dieser Richtlinie, Sie für das Anliegen des Datenschutzes zu sensibilisieren und Ihnen Informationen und Regelungen an die Hand zu geben, die es ermöglichen, die mit dem Betrieb komplexer und offener Datenverarbeitungs- und Kommunikationssysteme verbundenen Risiken zu erkennen und damit umzugehen.

Diese Richtlinie bildet mit den enthaltenen Verweisen auf korrespondierende Dokumente und mitgeltende Unterlagen eine vollständige Beschreibung aller technischen und organisatorischen Maßnahmen und stellt damit nicht nur eine vollständige und umfassende Informationsquelle für alle Mitarbeiterinnen und Mitarbeiter dar, sondern ist auch eine Prüfgrundlage für Revisoren, Qualitätsmanager und Auditoren.

Auf der Grundlage der Bewertung der datenschutzrechtlichen und betriebswirtschaftlichen Sensibilität der Daten und der anschließenden Einstufung in Schutz- und Vertraulichkeitsstufen konkretisieren sich die erforderlichen technischen und organisatorischen Maßnahmen. Damit besteht für Revisoren, Auditoren und auch für die Datenschutz-Aufsichtsbehörde eine fundierte und schlüssige Möglichkeit, die Vollständigkeit, Notwendigkeit und Angemessenheit der technischen und organisatorischen Maßnahmen zu beurteilen.

Bei Fragen zur Datenschutzrichtlinie und zu den datenschutzrechtlichen Regelungen konsultieren Sie bitte Ihren nächsten Vorgesetzten oder den betrieblichen Datenschutzbeauftragten.

1. Was ist eigentlich Datenschutz?

Ziel des Datenschutzes ist den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten bzw. durch deren unzulässige Verwendung in seinem Persönlichkeitsrecht beeinträchtig wird. Datenschutz dient dem Persönlichkeitsschutz und soll natürliche Personen im Bereich ihrer persönlichen Lebensführung vor dem willkürlichen Zugriff staatlicher und privater Stellen schützen. Die Grundrechtscharta der europäischen Union hat in Artikel 8 das Recht auf den Schutz personenbezogener Daten zu einem Grundrecht erhoben. Die Sorge um die **Datensicherheit**, die in den letzten Jahren durch bekannt gewordene Missbrauchsfälle einen immer breiteren Raum eingenommen hat (z.B. Computerviren, Trojaner, Phishing), hat vor allem das Ziel in

technischer Hinsicht Hardware, Software und verarbeitete Daten vor Verlust, Zerstörung und Missbrauch zu schützen.
Die **Erhebung, Verarbeitung und Nutzung** personenbezogener Daten sind nur zulässig, soweit die DS GVO oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Die Einwilligung muss immer ausdrücklich erfolgen und i.d.R. schriftlich sein.

Personenbezogene Daten sind

- „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind; (Art. 4)"

Besondere Arten personenbezogener Daten sind

- Angaben über die „rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person" (Art. 9).

Für besondere Arten personenbezogene Daten sieht die DS GVO einen besonderen Schutzbedarf.

Verarbeiten von personenbezogenen Daten heißt:

- „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung" (Art. 4)

Werden die Daten auf eine oder mehrere dieser Möglichkeiten verarbeitet, sind die Gesetze zum Datenschutz vollumfänglich anzuwenden. Ausgenommen hiervon ist lediglich die Nutzung von personenbezogenen Daten für persönliche oder familiäre Angelegenheiten oder Verarbeitung von vollständig anonymisierten Daten.

2. Datenschutzgrundsätze

Die Datenschutzgrundsätze sind in Art. 5 Abs. 1 DSGVO beschrieben und für die Verarbeitung von personenbezogenen Daten verbindlich. Die Nichtbeachtung dieser Grundsätze ist gem. Art. 83 DSGVO mit Bußgeld bedroht.

Für den Umgang mit personenbezogenen Daten werden nachfolgende Grundsätze besonders beachtet:

a. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben

Der Grundsatz der Rechtmäßigkeit schreibt vor, dass personenbezogene Daten nur unter dem Vorbehalt einer gesetzlichen Erlaubnis oder einer Einwilligung erhoben und verarbeitet werden dürfen. Dieser Grundsatz ist in Art. 8 Abs. 2 GRCh vorgegeben und entspricht auch dem Grundsatz des Verbots mit Erlaubnisvorbehalt nach den Vorschriften der DSGVO. Bei jeder Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist deshalb darauf zu achten, dass

eine Rechtsgrundlage nach den Datenschutzvorschriften vorhanden ist. Eine Rechtsgrundlage kann insbesondere

- ein Vertrag mit der betroffenen Person oder zur Erfüllung einer rechtlichen Verpflichtung,
- die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde oder
- ein berechtigtes Interesse des Unternehmens oder einer anderen Stelle unter Abwägung des Interesses und der Grundrechte und Grundfreiheiten der betroffenen Personen oder
- eine Einwilligung sein.

Für die einzelnen Datenverarbeitungsverfahren sind die Rechtsgrundlagen in der Beschreibung zum Verzeichnis über die Verarbeitungstätigkeiten beschrieben und geprüft.
Der Grundsatz der Verarbeitung nach Treu und Glauben setzt voraus, dass die betroffenen Personen in der Lage sind, das Vorhandensein einer Verarbeitung zu erfahren, und ordnungsgemäß und umfassend über die Bedingungen der Erhebung informiert zu werden, wenn Daten bei ihnen erhoben werden (siehe auch Transparenz). Es bedeutet aber auch, dass der Betroffenen stets davon ausgehen kann, dass die Verarbeitung seiner Daten nicht rechtsmissbräuchlich erfolgt und bei der Verarbeitung seiner Daten seine sonstigen Rechte angemessen berücksichtigt werden.

Praxishinweis: Die Rechtsgrundlage, auf welcher i.d.R. die Verarbeitung der personenbezogenen Daten in Ihrem Arbeitsbereich erfolgt ist die Insolvenzordnung und damit die Verarbeitung im öffentlichen Interesse bzw. in Ausübung öffentlicher Gewalt, die dem Insolvenzverwalter übertragen wurde bzw. das Mandatsverhältnis.

b. Transparenz

Der Grundsatz der Transparenz verlangt, dass jeder Betroffene wissen soll, wer welche Daten für welche Zwecke über ihn erhebt, speichert und verarbeitet und übermittelt und wie lange die Daten gespeichert werden, und dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Natürliche Personen sind über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu informieren und darüber aufzuklären, wie sie ihre diesbezüglichen Rechte geltend machen können. Hier sind die im Einzelnen geregelten Informationspflichten zu beachten.
Praxishinweis: Insolvenzschuldner und Mandanten werden über Ihre Rechte und die Einzelheiten der Verarbeitung zu Beginn des Verfahrens bzw. Mandats informiert. Dies erfolgt i.d.R. durch ein entsprechendes Merkblatt.

c. Zweckbindung

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Die Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, müssen eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. Eine Verarbeitung oder Nutzung von personenbezogenen Daten für andere als den Betroffenen im Zusammenhang mit der Datenerhebung kommunizierten Zwecke ist nur unter den gesetzlich festgelegten Bedingungen (Art. 6 Abs. 5 DSGVO) und ansonsten nur mit Einwilligung der Betroffenen zulässig. Sollen erhobene Daten auch für einen anderen als den der Erhebung zugrunde liegenden Zweck verwendet werden, z. B. zu Zwecken der Werbung oder des Profilings oder für Datenübermittlungen, ist vorher der Datenschutzbeauftragte zu konsultieren.

Praxishinweis: Sollten Sie im Rahmen Ihrer Tätigkeit Daten erheben oder erheben wollen, die nicht zwingend mit der Durchführung des Auftrags zusammenhängen oder hierfür nicht zwingend erforderlich sind, denken Sie daran, dass eine Zustimmungspflicht der Betroffenen besteht. In diesen Fällen konsultieren Sie bitte die IT oder den DSB.

d. Datenminimierung

Art und Umfang der Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dies schließt eine Begrenzung der Speicherfrist auf das erforderliche Mindestmaß ein. Hier ist darauf zu achten, dass nur diejenigen Daten von den Betroffenen erhoben werden, die für den jeweiligen Verarbeitungszweck auch wirklich erforderlich sind. Darüber hinausgehende Erhebungen und Verarbeitungen sind unzulässig. Zweifelsfragen zur Erforderlichkeit der Daten und zur Zulässigkeit der Datenverarbeitung sind mit dem Datenschutzbeauftragten abzuklären.

Praxishinweis: Ein Beispiel für die Grenze der Verhältnismäßigkeit im Sinne der Datenminiemirung ist z.B. die Erhebung der genauen privaten Verhältnisse des Schuldners für die Berichterstattung, also Krankheitsbilder als Begründung für die Arbeitsunfähigkeit, partnerschaftliche Verhältnisse u.ä. Die Insolvenzordnung schreibt lediglich vor über die wirtschaftlichen Verhältnisse des Schuldners zu berichten. In diesem Zusammenhang wäre im zutreffenden Fall über die Arbeitsunfähigkeit zu berichten, weil dies Auswirkungen auf die wirtschaftliche Situation des Schuldners hat, aber nicht über die Ursachen dieser Arbeitsunfähigkeit.

e. Richtigkeit

Die personenbezogenen Daten müssen im Hinblick auf die Zwecke ihrer Verarbeitung sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Die Verarbeitung unrichtiger Daten ist zu vermeiden. Unrichtige Daten sind unverzüglich zu berichtigen.

Praxishinweis: Ein nachvollziehbares Beispiel ist der Eintrag von Daten bei z.B. der Creditreform. Ein Anspruch auf Richtigkeit der Daten kann auf Grundlage der DS GVO durchgesetzt werden. Aber auch jedes andere Datum, das verarbeitet wird ist i.S. einer kontinuierlichen Datenpflege zukünftig aktuell zu halten.

f. Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie erhoben worden sind, erforderlich ist. Um sicherzustellen, dass personenbezogene Daten nicht länger als nötig gespeichert werden, sind Fristen für ihre Löschung oder regelmäßige Überprüfung vorzusehen und die Daten regelmäßig zu löschen bzw. zu vernichten. Die Aufbewahrungsfristen sind von den fachverantwortlichen Stellen festzulegen und die Löschung bzw. Vernichtung der Daten ist von diesen Stellen zu veranlassen, zu überwachen und, soweit erforderlich, zu dokumentieren. Die Verfahren für eine sichere Löschung von personenbezogenen Daten und die Vernichtung/Entsorgung von Geräten und Datenträgern sind mit dem betrieblichen Datenschutzbeauftragten abzustimmen.

Praxishinweis: Die regelmäßige Vernichtung von Altaktenbeständen und Daten hat sich an den Aufbewahrungsfristen zu orientieren. Eine Aufbewahrung darüber hinaus ist an strenge Auflagen geknüpft.

g. Integrität und Vertraulichkeit

Der Grundsatz der Integrität und Vertraulichkeit verlangt einen angemessenen Schutz und eine angemessene Sicherheit der personenbezogenen Daten vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung. Bei der Verarbeitung der personenbezogenen Daten ist durch geeignete

technische und organisatorische Maßnahmen eine angemessene Sicherheit der personenbezogenen Daten zu gewährleisten.

h. Rechenschaftspflicht

Der Grundsatz der Rechenschaftspflicht verlangt, dass die Einhaltung der o. g. Datenschutzgrundsätze nachgewiesen werden kann. Zur Erfüllung dieser Rechenschaftspflicht ist ein in sich stimmiges, systematisches und nachvollziehbares Datenschutzmanagement eingerichtet. Auf der Grundlage der dazu geführten Datenschutzdokumentation ist eine Überprüfung der Einhaltung dieser Grundsätze durch Datenschutzprüfungen und Audits möglich. Die in diesem Datenschutzhandbuch zu diesem Zweck festgelegten Dokumentationen und Nachweise sind aktuell und vollständig zu führen.

Für die Beachtung dieser Grundsätze und für die Gestaltung und Einhaltung der hierfür erforderlichen Regelungen ist die für den jeweiligen Fachprozess zuständige Stelle verantwortlich. Bei Zweifelsfragen zur Interpretation der Grundsätze und deren Anwendung ist der betriebliche Datenschutzbeauftragte zu konsultieren.

3. Datenschutzorganisation

Bestellung eines betrieblichen Datenschutzbeauftragten

Das BDSG schreibt mit § 38 für unser Unternehmen die Bestellung eines Datenschutzbeauftragten vor. Der Datenschutzbeauftragte ist gem. Art. 37 Abs. 8 DSGVO der Aufsichtsbehörde für den Datenschutz gemeldet.

Für den Datenschutzbeauftragten gelten folgende Regelungen:

1. Organisatorische Einrichtung im Unternehmen

   Der Datenschutzbeauftragte ist unmittelbar der Geschäftsleitung unterstellt und berichtet an diese.

2. Aufgaben des Datenschutzbeauftragten

   Dem Datenschutzbeauftragten sind folgende Aufgaben übertragen:

   a) Unterrichtung und Beratung der Geschäftsleitung und der Beschäftigten in allen Datenschutzfragen
   b) Überwachung der Einhaltung der Datenschutzvorschriften
   c) Sensibilisierung und Schulung/Unterweisung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter
   d) Durchführung von Datenschutzprüfungen nach eigenem Ermessen und im Auftrag der Geschäftsleitung
   e) Datenschutzrechtliche Freigabe von automatisierten Datenverarbeitungsverfahren zur Verarbeitung von personenbezogenen Daten und von datenschutzrelevanten Änderungen zur Anwendung. Die Freigabe erfolgt i. d. R. mit der Beschreibung der Verarbeitungsverfahren im Verzeichnis der Verarbeitungstätigkeiten und den damit verbundenen datenschutzrechtlichen Prüfungen.
   f) Beratung und Unterstützung bei der Zusammenarbeit mit der Aufsichtsbehörde

3. Informations- und Informationszugangsrechte des Datenschutzbeauftragten

   Der Datenschutzbeauftragte besitzt im Zusammenhang mit seiner Tätigkeit ein uneingeschränktes Informationsrecht zu allen Fragen des Umgangs mit personenbezogenen Daten und ein uneingeschränktes Zugangsrecht zu allen damit zusammenhängenden Unterlagen,

Informationen und Dokumenten. Die Unterlagen sind dem Datenschutzbeauftragten auf Verlangen vollständig und unverzüglich in geeigneter Weise zur Verfügung zu stellen.

4. Datenschutzberichte

Der Datenschutzbeauftragte berichtet regelmäßig (mindestens einmal jährlich) der o. g. Stelle über seine Tätigkeit und über seine Feststellungen (Jahresbericht). Bei besonderen Vorkommnissen berichtet er unverzüglich und unterrichtet die beteiligten Stellen zur Einleitung der erforderlichen Maßnahmen.

In seinem Jahresbericht beurteilt der Datenschutzbeauftragte nach dem vorgegebenen Dokumentations- und Bewertungssystem den Stand des Datenschutzes und in Abstimmung mit dem IT-Sicherheitsverantwortlichen auch den Stand der technischen und organisatorischen Maßnahmen zum Datenschutz.

Der Datenschutzbeauftragte berät in allen Fragen des Datenschutzes und soll, soweit möglich, auch bereits präventiv tätig sein. Aus diesem Grund ist er von den fachbereichs- bzw. projektverantwortlichen Stellen insbesondere bei den folgenden Vorhaben frühzeitig einzubeziehen:

- Neuentwicklung oder Änderung von IT-Systemen
- Einführung von Systemen zur Personal- oder Kundendatenverarbeitung
- Gestaltung der Telekommunikations-, Internet-, Intranet- oder E-Mail-Nutzung
- Abschluss von Betriebsvereinbarungen mit Bezug zum Umgang mit Mitarbeiterdaten
- Vergabe von Aufträgen im Rahmen einer Datenverarbeitung im Auftrag (Outsourcing)
- Übermittlung von personenbezogenen Daten an Stellen außerhalb des Unternehmens
- Gestaltung von Datenerhebungen für automatisierte Verfahren

Jeder von der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten Betroffene kann sich an den Beauftragten für den Datenschutz wenden. Ebenso kann sich jeder Mitarbeiter in allen Fragen des Datenschutzes an ihn wenden. Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen verpflichtet, soweit er nicht durch den Betroffenen davon entbunden ist. Zum Datenschutzbeauftragten wurde Fritz Spaeder bestellt. Die Kontaktdaten sind: dsb@berater-kanzlei.bayern

4. Datenschutzmanagement

1. Integration des Datenschutzmanagements in das Unternehmensmanagement

   Die Erfüllung der operativen Aufgaben des Datenschutzes bzw. die Ausführung der vorgeschriebenen Maßnahmen und Regelungen ist den für die einzelnen Fachbereiche bzw. für die Geschäftsprozesse verantwortlichen Fachbereichsleitern bzw. Geschäftsprozessverantwortlichen übertragen. Die für die einzelnen Geschäftsprozesse bzw. Fachbereiche relevanten Datenschutzvorgaben sind in den Datenschutzprozessen und in den Verfahrensbeschreibungen zur Übersicht über die Verarbeitungstätigkeiten verbindlich festgelegt. Die Vollständigkeit und Aktualität der Datenschutzprozesse und Verfahrensbeschreibungen wird vom betrieblichen Datenschutzbeauftragten regelmäßig überprüft.

2. Qualitätsmanagement

   a) Verankerung des Datenschutzes in den QM-Dokumenten

      Die datenschutzrechtlichen Vorgaben zu Unternehmenszielen und Strategien werden in den zutreffenden QM-Dokumenten beschrieben und ausgestaltet. Der QM-Verantwortliche und der Datenschutzbeauftragte wirken gemeinsam auf die Entwicklung geeigneter Datenschutzziele und -strategien hin. Der Datenschutzbeauftragte hat für die Entwicklung der Datenschutzziele und Strategien eine besondere

Beratungsaufgabe. Für die förmliche Ausgestaltung in der QM-Dokumentation ist der QM-Beauftragte verantwortlich.

b) Integration des Datenschutzes in den PDCA-Zyklus/Kontinuierlichen Verbesserungsprozess

Zur laufenden Aktualisierung und Fortentwicklung des Datenschutzes und zur Anpassung an sich verändernde Verhältnisse im Unternehmen ist der Datenschutz in den PDCA-Zyklus bzw. den Kontinuierlichen Verbesserungsprozess nach den eingerichteten Regeln des Qualitätsmanagements integriert. Der Datenschutzbeauftragte beobachtet die Rechtsentwicklung im Datenschutz und wendet für seinen Bereich in Abstimmung mit dem QM-Verantwortlichen die Prinzipien des PDCA-Zyklus an.

c) Integration des Datenschutzes in das Auditwesen

Der Datenschutzbeauftragte kann einen jährlichen Prüfplan über die durchzuführenden Datenschutzprüfungen erstellen. Die Prüfungen sind so zu gestalten, dass alle datenschutzrelevanten Bereiche, Prozesse und Datenverarbeitungsverfahren in einem angemessenen Rhythmus dahingehend überprüft und bewertet werden, ob die Anforderungen der Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO erfüllt werden.

Mitgeltende Unterlagen:

- Übersicht über die eingerichteten Datenschutzprozesse
- Ggf. Prüfplan des betrieblichen Datenschutzbeauftragten
- Auditplan

5. Datensicherheitsmanagement

1. Integration des Datensicherheitsmanagements in das Informations- und IT-Sicherheitsmanagement

a) Technische und organisatorische Maßnahmen zum Informations- und Datenschutz

Die beschriebenen Normen und technischen und organisatorischen Maßnahmen gelten auch für die personenbezogenen Daten. Soweit sich für die personenbezogenen Daten zusätzliche Anforderungen ergeben, sind diese dort ebenfalls zu berücksichtigen.

Mitgeltende Unterlagen:

- Prüfliste TOMs

6. Schutzziele und Schutzgrade der Daten, Vertraulichkeitsrichtlinie

Schutzeinstufung

Die einzelnen Datenverarbeitungsverfahren werden nach dem Grad ihrer datenschutzrechtlichen und betriebswirtschaftlichen Sensibilität beurteilt und einer Schutzstufe zugeordnet. Die Schutzeinstufungen sind eine mitgeltende Unterlage zur Beschreibung der einzelnen Verarbeitungsverfahren im Verzeichnis der Verarbeitungstätigkeiten. Die datenschutzrechtliche Sensibilität der personenbezogenen Daten beurteilt sich an der Frage, inwieweit der Betroffene bei einer Datenschutzverletzung in seinen Persönlichkeitsrechten oder seinem persönlichen oder wirtschaftlichen Ansehen verletzt oder eingeschränkt ist bzw. verletzt oder eingeschränkt werden kann.

Die Schutzstufe des gesamten Datenverarbeitungsverfahrens richtet sich nach den Schutzanforderungen der sensibelsten Datenkategorien des zugehörigen Datenbestands. Es bestehen aber für die personenbezogenen und sonstigen vertraulichen Daten noch weitere Schutzziele, und zwar die Gewährleistung der Verfügbarkeit, der Schutz der Integrität, der Authentizität und der Revisionsfähigkeit. Diese Schutzziele können je nach Schutzbedarf der Daten unterschiedlich hoch ausgeprägt

sein und werden bei Bedarf nach der in der nachstehenden Tabelle dargestellten Skalierung festgelegt.

Die Festlegung der Schutzziele und deren Skalierung trifft die über die Informationen und Daten verfügungsberechtigte Stelle.

Der Schutzgrad orientiert sich an dem Ausmaß der Verletzung des Persönlichkeitsrechts der Betroffenen und an der Höhe des Schadens, der sowohl dem Betroffenen als auch dem Unternehmen entstehen kann. Unter Datenschutzgesichtspunkten ist insbesondere auch dem erhöhten Schutz der besonderen Datenarten im Sinne von Art. 9 DSGVO Rechnung zu tragen.

Kriterien für die Festlegung der Schutzziele sind weitere gesetzliche Anforderungen an die Daten, die sich aus ihrer jeweiligen Rechtsnatur ergeben, z. B. nach steuer- und handelsrechtlichen Vorschriften, den Grundsätzen ordnungsgemäßer DV-gestützter Buchführungssysteme (GoBS) oder der ordnungsgemäßen Datenverarbeitung (GoDV) u. a., und Anforderungen unter dem Gesichtspunkt der Beweiskraft und Gerichtsverwertbarkeit der Informationen und Daten.

In Abhängigkeit von den Schutzzielen sind bei Bedarf von den fachverantwortlichen Stellen nach den Vorgaben in der Tabelle die im Einzelnen erforderlichen technischen und organisatorischen Maßnahmen abzuleiten und festzulegen. Dazu gehören:

- Die Festlegung der Verfügbarkeit, d. h. der maximal tolerierbaren Ausfallzeit der Daten
- Die Festlegung von Rechten an den Daten, insbesondere der Rechteprofile der Benutzer der Datenverarbeitungsverfahren, von Protokollierungen von Zugriffen und Veränderungen sowie ggf. von Signaturen zum Nachweis der Integrität der Daten
- Die Festlegung von Maßnahmen zum Nachweis der Authentizität der Daten, z. B. Protokollierung der Einstellung und Veränderung der Daten in Datenverarbeitungsverfahren bzw. elektronische Signatur
- Die Festlegung von Dokumentationen, Freigaben und Protokollierungen zum Nachweis der Revisionsfähigkeit der Datenverarbeitungsverfahren und der Daten

Der Umgang mit besonders vertraulichen Daten und Informationen ist in der Datenschutzrichtlinie geregelt. In dieser Richtlinie sind die besonders vertraulichen Daten und Informationen ihrer Art nach definiert und die Verantwortlichkeiten sowie der Umgang mit diesen Daten gesondert geregelt.

Mitgeltende Unterlagen:

- Verzeichnis über Verarbeitungstätigkeiten

7. Datenschutzdokumente

Die Datenschutzdokumentation enthält folgende Dokumente:

1. Übersicht über die eingerichteten Datenschutzprozesse
   Die Übersicht enthält alle gültigen und verbindlich eingerichteten Datenschutzprozesse und für jeden Prozess ein grafisches Modell mit einer Kurzbeschreibung. Für jeden Datenschutzprozess sind die zuständige Stelle, sonstige zu beteiligende sowie zu informierende Stellen, das Prüfintervall für die Prüfung durch den betrieblichen Datenschutzbeauftragten und die mitgeltenden Unterlagen festgelegt.

2. Verzeichnis über die Verarbeitungstätigkeiten
   Gemäß Art. 30 Abs. 1 DSGVO wird ein Verzeichnis über die Verarbeitungstätigkeiten geführt. Das Verzeichnis besteht aus den folgenden Dokumenten:

a) Beschreibung der einzelnen Verfahren

Die Beschreibung der einzelnen Verfahren enthält die Angaben lt. Art. 30 Abs. 1 lit. b bis f DSGVO. Die Beschreibung der Verfahren für Verantwortliche gem. Art. 30 Abs. 1 DSGVO enthält über die Pflichtangaben des Art. 30 Abs. 1 DSGVO hinaus alle zur Prüfung der Rechtmäßigkeit des Verfahrens und der Verarbeitung erforderlichen Angaben und unter Angabe der Rechtsgrundlage auch eine Prüfung der Zulässigkeit der einzelnen Verarbeitungstätigkeiten und der Erfüllung der datenschutzrechtlichen Voraussetzungen. Der Datenschutzbeauftragte bestätigt auf jeder einzelnen Verfahrensbeschreibung die datenschutzrechtliche Ordnungsmäßigkeit bzw. Konformität des Verfahrens und vermerkt das Datum der letzten Prüfung des Verfahrens. Stellt der Datenschutzbeauftragte bei der Prüfung eines Datenverarbeitungsverfahrens Abweichungen fest, vermerkt er diese und berichtet der Geschäftsleitung. Der Datenschutzbeauftragte überwacht die Erledigung der Abweichungen.

b) Beschreibung der Auftragsdatenverarbeitungen

Die Beschreibung der Auftragsverarbeitungen gem. Art. 30 Abs. 2 DSGVO enthält eine Übersicht über alle Datenverarbeitungsverfahren, die im Auftrag für andere Stellen durchgeführt werden. Für die Führung dieses Verzeichnisses ist <*Bezeichnung der Stelle*> zuständig. Die für die Verfahren zuständigen Stellen melden neue Verfahren rechtzeitig der <*Bezeichnung der Stelle*> und unterrichten den betrieblichen Datenschutzbeauftragten.

c) Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen

Diese Beschreibung enthält die übergreifenden und für alle Verarbeitungsverfahren gültigen allgemeinen technischen und organisatorischen Maßnahmen. Bestehende Verfahrensanweisungen und Regelungen zu den technischen und organisatorischen Maßnahmen werden als mitgeltende Unterlagen geführt. Soweit für einzelne Verfahren davon abweichende verfahrensindividuelle Maßnahmen bestehen, sind diese in den Verfahrensbeschreibungen zu den einzelnen Verfahren enthalten.

3. Risikobewertung und Verfahren zur Klassifizierung der personenbezogenen Daten nach Risikostufen und Schutzbedarfsfeststellung

   Das Risiko wird aus der Sicht der Betroffenen beurteilt und in folgende drei Risikostufen (Schutzklassen) eingeteilt:

   - Kein rechtserhebliches (geringes) Risiko
   - Mittleres, das allgemein vorhandene Risiko (Grundrisiko) übersteigende Risiko
   - Hohes Risiko

   Die Risiken und Risikogruppen sowie deren Eintrittswahrscheinlichkeit und Schwere sowie die daraus abzuleitende Schutzklasse der Daten sind ermittelt und zu dokumentiert. Das Ergebnis ist in der Verfahrensbeschreibung des Verzeichnisses über die Verarbeitungstätigkeiten zu den einzelnen Datenverarbeitungsverfahren angegeben. Für die Risikobewertung ist die für das jeweilige Verarbeitungsverfahren zuständige Stelle verantwortlich. Bei der Erstellung der Risikobewertung und bei Änderungen der Bewertung ist der betriebliche Datenschutzbeauftragte zuzuziehen.

4. Checklisten und Dokumentationen über die Erhebungen des Datenschutzbeauftragten zum Datenschutz und zur Datensicherheit und Bewertung des Standes des Datenschutzes und der technischen und organisatorischen Maßnahmen

Zum Nachweis der Einhaltung der datenschutzrechtlichen Vorschriften ist ein Dokumentations- und Bewertungsverfahren eingerichtet. Im Rahmen dieses Verfahrens werden die einzelnen datenschutzrechtlichen Sachverhalte anhand von vorgegebenen Checklisten erhoben und nach ihrem Erfüllungsgrad bewertet. Sie vermitteln einerseits einen vollständigen Überblick über alle datenschutzrechtlich relevanten Sachverhalte und deren Überprüfung und zeigen den Grad der Erfüllung der einzelnen datenschutzrechtlichen Voraussetzungen sowie eventuell noch offene Handlungsbedarfe. Anhand der Checklisten wird eine Bewertung des Erfüllungsgrades erstellt und damit der Nachweis zur Rechenschaftspflicht gem. Art. 5 Abs. 2 DSGVO geführt.

2. Verantwortlichkeit für die Führung der Datenschutzdokumentation
   Für die laufende Ergänzung und Aktualisierung der Datenschutzdokumentation, der Checklisten, des Dokumentations- und Bewertungssystems nach den ihm vorgelegten Meldungen und Informationen und für die regelmäßige Bewertung des Standes des Datenschutzes ist der betriebliche Datenschutzbeauftragte verantwortlich.

Mitgeltende Unterlagen:

- Risiko- und Schutzbedarfsermittlung
- Übersicht über die eingerichteten Datenschutzprozesse
- Verzeichnis über die Verarbeitungstätigkeiten
- Beschreibung der technischen und organisatorischen Maßnahmen
- Checklisten lt. Übersicht des Datenschutzbeauftragten

8. Datenschutzprozesse und Verfahren

Der Datenschutzbeauftragte überwacht die Führung einer verbindlichen Übersicht über die eingerichteten Datenschutzprozesse. Er legt mit den für die Fachprozesse bzw. Fachbereiche verantwortlichen Stellen die zugehörigen verbindlichen Checklisten fest. Die zugehörigen Verfahrensanweisungen werden vom zuständigen Fachbereichsverantwortlichen bzw. von den für den jeweiligen Fachprozess verantwortlichen Stellen verwaltet. Der Bestand dieser Datenschutzprozesse wird vom Datenschutzbeauftragten regelmäßig geprüft und ggf. ergänzt. Die Datenschutzprozesse werden anhand der Checklisten in den festgelegten Prüfintervallen geprüft und bewertet.

Mitgeltende Unterlagen:

- Übersicht über die eingerichteten Datenschutzprozesse
- Checklisten lt. Übersicht des Datenschutzbeauftragten

9. Rechte der Betroffenen

Vorgänge über die Wahrnehmung von Rechten der Betroffenen (Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und ggf. des Rechts auf Datenübertragbarkeit.) werden von der Kanzleileitung bearbeitet und dokumentiert und sind dieser unverzüglich zuzuleiten. Die Kanzleileitung regelt das weitere Verfahren nach den dazu bestehenden Datenschutzprozessen und veranlasst die umgehende Einschaltung des Datenschutzbeauftragten. Die Bearbeitung von Anträgen der Betroffenen zur Wahrnehmung ihrer Rechte ist eng mit dem Datenschutzbeauftragten abzustimmen.

Beschwerden der Betroffenen in Datenschutzangelegenheiten werden ebenfalls von der kanzleileitung nach den Vorgaben des Beschwerdemanagements bearbeitet und sind dem Datenschutzbeauftragten zu melden.

Mitgeltende Unterlagen:

- Prozesse über die Rechte der Betroffenen
- Dokumentation der bearbeiteten Vorgänge zu den Rechten der Betroffenen

10. Information der Betroffenen bei der Datenerhebung

Bei jeder Datenerhebung von den betroffenen Personen sind die Betroffenen in geeigneter Weise (z. B. durch einen schriftlichen Hinweis) über die in Art. 13 DSGVO genannten Sachverhalte zu informieren. Die Modalitäten des Art. 12 DSGVO sind dabei zu beachten.

Wenn die Daten nicht von der betroffenen Person erhoben worden sind, sind die Betroffenen fristgerecht (siehe Art. 14 Abs. 3 DSGVO) zu unterrichten. Die fachverantwortlichen Stellen sind für die Durchführung der vorgeschriebenen Informationen verantwortlich. Inhalt und Verfahren zur Information der betroffenen Personen sind mit dem betrieblichen Datenschutzbeauftragten abzustimmen.

Jeder Fachbereichsverantwortliche und der IT-Verantwortliche ist jeweils für seinen Bereich auch dafür verantwortlich, dass in der Datenschutzerklärung zum Internetauftritt des Unternehmens die erforderlichen Informationen zum Datenschutz enthalten sind.

Die Art und Weise der Unterrichtung sowie deren Form und Inhalt sowie die Datenschutzerklärung zum Internetauftritt sind mit dem Datenschutzbeauftragten abzustimmen.

Mitgeltende Unterlagen:

- Prozess „Informationspflicht bei einer Datenerhebung vom Betroffenen“
- Prozess „Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden“
- Datenschutzinformation der Betroffenen

11. Meldung von Datenschutzverletzungen

Bei einer möglichen Verletzung des Schutzes von personenbezogenen Daten, insbesondere bei einem Verlust der Vertraulichkeit durch eine unbefugte Offenbarung oder Datenübermittlung, unbefugte Zugriffe oder Verarbeitungen oder durch Verlust, Zerstörung oder Verfälschung der Daten, ist sofort der jeweilige Vorgesetzte zu informieren. Dieser leitet umgehend die erforderlichen Sofortmaßnahmen zur Behebung der Ursachen der Datenschutzverletzung ein und benachrichtigt die beteiligten Stellen, die Geschäftsleitung und den Datenschutzbeauftragten. Für die Vorgehensweise bei der Bearbeitung von Datenschutzverletzungen ist der Prozess „Melde- und Benachrichtigungspflicht“ und die Dokumentation zur Prüfung der Benachrichtigungspflicht gem. Art. 33, 34 DSGVO verbindlich.

Die Meldung an die Aufsichtsbehörde für den Datenschutz und die Information der Betroffenen erteilt die Geschäftsleitung. Für die Meldung an die Aufsichtsbehörde ist eine Frist von 72 Stunden einzuhalten. Die Kanzleileitung führt eine Übersicht über die Vorfälle.

Vorfälle bei Auftragsdatenverarbeitungen

Bei einer möglichen Verletzung des Schutzes von personenbezogenen Daten, insbesondere bei einem Verlust der Vertraulichkeit durch eine unbefugte Offenbarung oder Datenübermittlung, unbefugte Zugriffe oder Verarbeitungen oder durch Verlust, Zerstörung oder Verfälschung der Daten oder eine sonstige Störung der Auftragsdatenverarbeitung, ist sofort der jeweilige Vorgesetzte zu informieren. Dieser leitet umgehend die erforderlichen Sofortmaßnahmen zur

Behebung der Ursachen der Störung bzw. Datenschutzverletzung ein und benachrichtigt die beteiligten Stellen, die Geschäftsleitung und ggf. den Datenschutzbeauftragten.

Die Geschäftsleitung entscheidet über die weitere Vorgehensweise auf der Grundlage des bestehenden Vertrags über die Auftragsdatenverarbeitung und unterrichtet ggf. den Auftraggeber. Die Kanzleileitung führt eine Übersicht über die Vorfälle.

Mitgeltende Unterlagen:

- Datenschutzprozess „Melde- und Benachrichtigungspflicht“
- Formular zur Dokumentation zur Prüfung der Benachrichtigungspflicht gem. Art. 33, 34 DSGVO
- Dokumentation der Datenschutzvorfälle

12. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

1. Beschaffung von Software
   Bei der Beschaffung von Software zur Verarbeitung von personenbezogenen Daten ist auf die Erfüllung der Anforderungen hinsichtlich einer datenschutzfreundlichen Technikgestaltung zu achten. Kriterien für eine datenschutzfreundliche Technikgestaltung sind insbesondere eine Minimierung der Verarbeitung von personenbezogenen Daten und deren frühzeitige Pseudonymisierung, eine Rechtegestaltung nach dem Minimalprinzip sowie Funktionen zur Unterstützung der Wahrnehmung der Rechte der Betroffenen, insbesondere des Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und ggf. des Rechts auf Datenübertragbarkeit. Die ausreichende Erfüllung dieser Anforderungen ist ein Auswahlkriterium.

2. Softwareentwicklung
   Bei der Softwareentwicklung sind ebenfalls die unter a. bezeichneten Anforderungen zu beachten und zu erfüllen.

3. Implementation von Datenverarbeitungsverfahren
   Bei der Implementierung von Verfahren zur Verarbeitung von personenbezogenen Daten ist auf Beschränkung des Funktionsumfangs, eine Minimierung von personenbezogenen Daten, auf eine Rechtebeschränkung auf den nötigen Umfang und die Nutzung von Sicherheitsfunktionen zu achten.

Einzelheiten sind ggf. mit dem Datenschutzbeauftragten abzustimmen. Die Maßnahmen, Vorkehrungen und Funktionen zur datenschutzfreundlichen Technikgestaltung und zum datenschutzfreundlichen Design sind zu dokumentieren.

Mitgeltende Unterlagen:

- Dokumentationen über die eingerichteten Funktionen zum Datenschutz durch Technikgestaltung

13. Datenschutzfolgenabschätzung und vorherige Konsultation der Aufsichtsbehörde gem. Art. 35 u. 36 DSGVO

<u>Durchführung der Datenschutzfolgenabschätzung</u>

Die Datenschutzfolgenabschätzung ist von dem für die Verarbeitung der personenbezogenen Daten verantwortlichen Fachbereich nach den Vorgaben des Datenschutzprozesses

„Datenschutzfolgenabschätzung“ durchzuführen. Der betriebliche Datenschutzbeauftragte ist beratend zuzuziehen.

In einer Risikobeurteilung ist zunächst zu ermitteln, ob die Verarbeitung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt. Ist dies nicht der Fall, ist keine Datenschutzfolgenabschätzung durchzuführen und das Ergebnis der Beurteilung zu dokumentieren. Ergibt die Beurteilung, dass die Verarbeitung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten der betroffenen Personen führt, ist eine Datenschutzfolgenabschätzung nach den Regelungen des Datenschutzprozesses „Datenschutzfolgenabschätzung“ durchzuführen. Das Ergebnis der Risikobeurteilung und ggf. einer Datenschutzfolgenabschätzung ist in der Beschreibung des Verfahrens zur Übersicht über die Verarbeitungstätigkeiten zu vermerken.

Zur Beherrschung der Risiken für die Rechte und Freiheiten der betroffenen Personen sind geeignete technische und organisatorische Maßnahmen zu entwickeln und zu dokumentieren. Verbleibt trotzdem für die Rechte und Freiheiten der betroffenen Personen ein hohes Restrisiko, ist die Geschäftsführung zu unterrichten. Die Geschäftsführung entscheidet über die Einstellung oder Weiterentwicklung des Verfahrens und veranlasst im Fall einer Weiterentwicklung die vorherige Konsultation der Aufsichtsbehörde gem. Art. 36 DSGVO.

Mitgeltende Unterlagen:

- Prozess- und Verfahrensanweisung zur Datenschutzfolgenabschätzung
- Dokumentation der Risikobeurteilung
- Dokumentation der Datenschutzfolgenabschätzung
- Übersicht über die Verarbeitungstätigkeiten

14. Vertraulichkeit und Geheimhaltungspflichten

Die personenbezogenen Daten unterliegen der Vertraulichkeit gem. Art. 5 Abs. 1 DSGVO. Soweit personenbezogene Daten sonstigen Geheimnissen bzw. Geheimhaltungsvorschriften unterliegen, sind diese Geheimhaltungspflichten in der Übersicht über die Verarbeitungstätigkeiten bei den einzelnen Verarbeitungsverfahren zu dokumentieren, die Beschäftigten über diese Geheimhaltungs- bzw. Schweigepflichten nachweisbar zu unterrichten und auf die Einhaltung dieser Geheimhaltungsvorschriften zu verpflichten. Geheimnisse dieser Art können insbesondere das Telekommunikationsgeheimnis, Berufsgeheimnisse, vertragliche Geheimhaltungspflichten (z. B. aus Verträgen mit Kunden) oder Betriebsgeheimnisse sein.

Mitgeltende Unterlagen:

- Verpflichtung auf die Wahrung der Vertraulichkeit
- Ggf. weitere sonstige Geheimhaltungsvorschriften und Verpflichtungen
- Übersicht über die Verarbeitungstätigkeiten

15. Datenverarbeitung im Auftrag

1. Auswahl und Kontrolle der Auftragnehmer
   Bei der Auswahl der Auftragnehmer für eine Datenverarbeitung im Auftrag ist darauf zu achten, ob der Auftragnehmer durch technische und organisatorische Maßnahmen hinreichende Garantien für den Schutz der Rechte der betroffenen Personen bietet. Die eingerichteten technischen und organisatorischen Maßnahmen sind in Abstimmung mit dem Datenschutzbeauftragten in geeigneter Weise zu überprüfen. Die Überprüfung ist zu dokumentieren.

2. Verträge über eine Datenverarbeitung im Auftrag
   Über die Beauftragungen sind Verträge nach den Vorgaben des Art. 28 DSGVO abzuschließen bzw. entsprechende Ergänzungen vorzunehmen. Zum Vertragsabschluss und ggf. zu eventuellen Vertragsergänzungen ist der Datenschutzbeauftragte hinzuzuziehen. Bei einer Vergabe von Unteraufträgen ist darauf zu achten, dass die vertraglichen Verpflichtungen, denen der Auftragsverarbeiter gegenüber dem Auftraggeber unterliegt, in gleicher Weise an den Unterauftragnehmer weitergegeben werden.

3. Übersicht über Beauftragungen (Vertragsverzeichnis)
   Über die bestehenden Beauftragungen führt die Kanzleileitung eine Vertragsübersicht. Der Inhalt der Übersicht ist mit dem Datenschutzbeauftragten abzustimmen.

Mitgeltende Unterlagen:

- Vertragsverzeichnis
- Dokumentationen über die Prüfung von Auftragsverarbeitern
- Verträge über eine Datenverarbeitung im Auftrag

16. Zusammenarbeit mit der Aufsichtsbehörde

Einfache Anfragen und Einholung von Beratungen

Soweit einfache Anfragen und Beratungen unter Wahrung der Anonymität des Unternehmens eingeholt werden (insbesondere durch einen externen Datenschutzbeauftragten), nimmt der Datenschutzbeauftragte diese Kontakte in eigener Verantwortung und unabhängig wahr. Geschehen diese Anfragen im Namen des Unternehmens, ist vorher der zuständige Bereichsverantwortliche zu informieren.

Abgabe von verbindlichen Auskünften und Erklärungen

Verbindliche Auskünfte und Erklärungen werden vor ihrer Abgabe zwischen dem Datenschutzbeauftragten und den betroffenen Fachbereichsverantwortlichen, ggf. mit der Geschäftsleitung, abgestimmt und von den jeweiligen Fachbereichsverantwortlichen erteilt.

Bußgeldverfahren

Der Verkehr mit der Aufsichtsbehörde im Zusammenhang mit Bußgeldverfahren wird von der Geschäftsleitung in Abstimmung mit dem Datenschutzbeauftragten abgewickelt.

Anlaufstelle für die Aufsichtsbehörde

Der betriebliche Datenschutzbeauftragte ist für die Aufsichtsbehörde die Anlaufstelle in allen Datenschutzfragen. Der Datenschutzbeauftragte beteiligt in diesen Angelegenheiten die jeweils betroffenen Fachbereichsverantwortlichen und ggf. die Geschäftsleitung.

I. Spezieller Teil: Konkrete Regelungen und Verhaltensvorschriften

1. Verantwortlichkeiten

1.1. IT-/ Administrator und Datenschutzbeauftragter

Ansprechpartner für Administration des IT-Netzwerks und IT-Sicherheit ist Herr Johann Hinterberger. Der IT-Administrator ist Ansprechstelle für alle Stellen und Beschäftigten des Unternehmens in Fragen der IT-Sicherheit. Zu seinen Aufgaben gehören insbesondere die Konzeption und Steuerung/Überwachung von Sicherheitsprozessen, die Erstellung von Richtlinien zur IT-Sicherheit und die Entwicklung von Lösungen in allen Fragen der IT-Sicherheit.

In weiteren Fragen der Datensicherheit und des Datenschutzes ist der externe Datenschutzbeauftragte Fritz Spaeder Ansprechpartner. Der Datenschutzbeauftragte kann jederzeit unter dsb@berater-kanzlei.bayern erreicht werden.

2. Einsatz privater Hard- und Software und private Nutzung von betrieblichen Geräten

2.1. 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 nicht zulässig. Für die Berufsträger ist die Verwendung des privaten Telefons zu dienstlichen Zwecken zulässig.

2.2. 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 nicht zulässig. Dies gilt auch für eine betriebliche Nutzung von firmeneigenen mobilen Datenträgern an privaten Geräten. Die Überlassung an betriebsfremde Personen zur Nutzung, auch an Familienangehörige ist untersagt. Ausnahmen bedürfen der Genehmigung durch den Vorgesetzten und der Freigabe durch die IT-Administration.

Telefon: in Maßen erlaubt. Die Nutzung des betrieblichen EDV-Systems für die Teilnahme am Internet (Besuch von Web-Seiten) für private Zwecke ist in Maßen zulässig.

Für die Berufsträger ist die Nutzung der betrieblichen Laptops zu Hause zulässig. Bei der Nutzung sind jedoch alle Sicherheitshinweise dieser Datenschutzrichtlinie zu beachten.

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.

3. Datensicherheit

3.1. 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.

3.2. Verbindungen zu externen IT-Ressourcen

Verbindungen von vernetzten PCs zu externen Systemen und Netzen dürfen nur über die von der IT 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.

3.3. Fremdrechner, Fremdunternehmen

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

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.

3.4. 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, USB-Sticks, 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.

- 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 sind 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. Jeder Mandant hat ein personalisiertes Passwort, das ggf. anzuwenden ist. Daten werden per E-Mail und verschlüsselt versendet, insbesondere aus der Lohn- und Gehaltsabteilung.

- 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.

3.5. Firewall und Internetschutz

Um einen ständigen Schutz der Geräte zu gewährleisten, darf nur die von der IT-Abteilung freigegebene und installierte Sicherheitssoftware installiert und betrieben werden. Ferner darf die Konfiguration der Schutzsoftware nicht verändert oder die Schutzsoftware deaktiviert oder deinstalliert werden. Insbesondere dürfen die automatische Aktualisierung der Schutzsoftware nicht deaktiviert oder verändert und die Geräte nicht ohne aktuellen Schutz am Internet betrieben werden.

3.6. 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 die IT-Administration zulässig. Dabei müssen die von der IT 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.

3.7. Verwendung von Passwörtern

Der Zugang zu Datenverarbeitungsverfahren ist nur über ein sicheres Anmeldeverfahren zulässig. 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 fremdem 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 6 Zeichen lang sein. Es muss mindestens drei von vier der folgenden Kriterien enthält: Großschreibung, Kleinschreibung, Ziffern, Sonderzeichen. Beispiele: „9Xklug“ „2felhaft“ „Sper5ling“ „Früh3jahr“„Som6mer“ „Herb9Sept“ „Win12ter“.

- 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.

3.8. 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:

1. 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-Administrator 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 etc. Er leitet die erforderlichen Maßnahmen zur Schadensbegrenzung und zur Behebung der Störung ein. Mitbestimmungsrechte des Betriebsrats sind dabei zu beachten.

2. Jeder Vorfall ist nach Art und Ausmaß, betroffenen Verfahren, Daten und Stellen zu dokumentieren.

3. Die Art der Behebung des Vorfalls sowie die eingeleiteten rechtlichen, organisatorischen und technischen Maßnahmen sind zu dokumentieren.

4. 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 Schadensbericht zu erstellen.

5. Die Ursachen des Vorfalls sind zu analysieren, und es sind nach Möglichkeit Maßnahmen abzuleiten und einzurichten, um ähnliche Vorfälle in Zukunft zu vermeiden.

6. Bei einem Verlust der Vertraulichkeit der Daten sind eventuelle Informationspflichten der Betroffenen und der Datenschutzaufsichtsbehörde zu beachten.

7. 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.

8. 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.

4. Vertraulichkeitsschutz

4.1. 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. 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.

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 Soweit keine anderweitigen Regelungen entgegenstehen, sind abschließbare Einzelbüros bei Verlassen abzuschließen.

4.2. Besucher

Innerhalb des Unternehmens werden Besucher geführt und sind innerhalb von Sicherheitsbereichen zu beaufsichtigen. Besprechungen mit Besuchern werden nur in Ausnahmefällen in den Büros durchgeführt. Bevorzugt sind hierfür die Besprechungsbereiche zu nutzen.

Für Besucher ist ein Gäste-WLAN eingerichtet. Soweit erforderlich erhält der Besucher einen Zugang zur Nutzung des Gäste- WLANs. Ein Zugriff auf das Kanzlei- WLAN darf dem Gast nicht eingerichtet werden. Nur die Kanzleileitung zusammen mit dem IT-Administrator darf eine anderslautende Entscheidung treffen.

4.3. Verhalten außerhalb der Kanzlei (Heimarbeitsplätze / Arbeiten zu Hause oder 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 sondern als Handgepäck mitzuführen und möglichst verborgen zu tragen.

- Notebooks dürfen nicht sichtbar in Fahrzeugen abgelegt werden.

- 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.

- 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.

- 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.

- Zum Anschluss an unternehmensfremde Rechner dürfen nur mobile Geräte verwendet werden, die keine personenbezogenen oder sonstige vertrauliche Daten enthalten.

- Nach einem Anschluss an Fremdrechner müssen die mobilen Geräte auf Freiheit von Viren und sonstiger Schadsoftware geprüft werden.

- Jeder Diebstahl oder sonstige Verlust von mobilen Geräten oder Datenträgern ist sofort dem Vorgesetzten und der zuständigen IT-Abteilung zu melden. Von diesen Stellen werden die weiteren Schritte eingeleitet.

4.4. 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.

Insbesondere sind zurückzugeben:

- Der Hardware-Token, der zur Nutzung von DATEV am Heimarbeitsplatz benötigt wird
- Die DATEV-Smart-Card
- Der Schlüssel

Der Zugang wird nach Ausscheiden des Mitarbeiters gesperrt.

4.5. 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 mit der fachverantwortlichen Stelle unter Beachtung eventueller Aufbewahrungsfristen oder eines sonstigen Aufbewahrungsinteresses des Unternehmens oder der Betroffenen abzustimmen. 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 Entsorgung oder Rückgabe von Multifunktionsgeräten (Drucker, Kombifaxgeräte etc.) ist dafür zu sorgen, dass Dateien, die sich im Speicher, auf der Festplatte oder Cache befinden so gelöscht werden, dass sie von einem Dritten nicht mehr ausgelesen werden können.

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 Dienstleistungsunternehmen 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-Sicherheitsverantwortliche 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.

Entsorgung von Papierunterlagen

Da auch Papier vertrauliche Informationen enthalten kann, sind eine sorgfältige Sammlung von Altpapier und eine zuverlässige Entsorgung mit einer Bestätigung der datenschutzgerechten Vernichtung erforderlich. Dokumente mit personenbezogenen oder vertraulichen Daten werden in der roten Tonne entsorgt. Diese wird regelmäßig abgeholt und mit der erforderlichen Sicherheitsstufe vernichtet.

5. E-Mail/Internet

5.1. Private Nutzung von E-Mail und Internet

Eine Nutzung des Internets und des E-Mail-Dienstes für private Zwecke ist unzulässig. Davon ausgenommen ist eine Nutzung aus betrieblichem Anlass/Interesse, z.B. zur Benachrichtigung von Familienangehörigen bei einem ungeplanten Anfall von Überstunden oder in sonstigen besonders begründeten Fällen. Diese Nutzungen sind keine privaten Nutzungen im Sinne dieser Regelung.

5.2. Benutzung des E-Mail-Systems

- Jedem berechtigten Mitarbeiter steht für betriebliche Zwecke ein persönliches E-Mail-Postfach zur Verfügung. Der Mitarbeiter wird daher seine für den beruflichen E-Mail-Verkehr eingerichtete E-Mail-Adresse
    - nicht zum Versand privater E-Mails benutzen und
    - nicht als Adresse für den Empfang privater E-Mails weitergeben.
- Der Mitarbeiter stimmt ausdrücklich zu, dass entgegen dieser Regelung eingegangene Daten – insbesondere E-Mails und Anhänge zu E-Mails – durch den Kanzleiinhaber oder einem von ihm Beauftragten gelesen, bearbeitet und gelöscht werden.
- Der Mitarbeiter stimmt ausdrücklich zu, dass der Kanzleiinhaber oder ein von ihm Beauftragter die Daten aller E-Mails in die in der Kanzlei verwendeten Sicherungsmaßnahmen – z.B. Virenkontrolle – einbezieht und dass alle im Sinn der Sicherungsmaßnahmen bedenklichen Daten sofort gelöscht werden.
- Der Mitarbeiter ist verpflichtet, Absender privater E-Mails über diese Regelung zu verständigen, damit wiederholte Zusendungen unterbleiben.

5.3. 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.

5.4. 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 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.

Die Funktion des E-Mail-Clients, die Adresse eines E-Mail-Empfängers automatisch zu vervollständigen, sollte nicht verwendet werden bzw. Bedarf bei der Anwendung besonderer Sorgfalt. Bitte stellen Sie immer sicher, dass bei der automatischen Vervollständigung der Adressat wirklich der

beabsichtigte Adressat ist. Die potentielle Gefahr der Versendung von Mandantenpost an einen falschen Empfänger könnte nicht unerhebliche Folgen haben.

5.5. 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.

5.6. 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.

5.7. 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.

5.8. 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. 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.

5.9. Internet

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:

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 die IT 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.

Diese Regelungen gelten auch, sofern ein Mitarbeiter ein in seinem Eigentum stehendes EDV-Gerät innerhalb des betrieblichen EDV-Systems oder durch Anschluss an dieses betreibt oder anstelle des oder neben dem betrieblichen EDV-System verwendet.

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

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 der IT-Abteilung 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 die IT-Abteilung 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.

5.10. 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
- Verdachtsvolle Anhänge

Über die Internetnutzung wird nicht grundsätzlich protokolliert. Zur Gewährleistung der Systemsicherheit können jedoch folgende Protokolldaten erhoben werden:

- 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 maximal über einen Zeitraum von Frist 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 des IT-Administrators (Herr Hinterberger) und Herr Christian Schulz, (IT-Dienstleister) unter Beachtung der jeweils gültigen Datenschutzvorschriften und der arbeitsrechtlichen Vorschriften durchgeführt. Der Betroffene wird zum frühestmöglichen Zeitpunkt über diese Kontrollen und über die Ergebnisse unterrichtet.

Mühldorf, 26.10.2020

Unterschrift