Datenschutz-Handbuch

(Stand Mai 2018)

Liebe Mitarbeiterinnen und Mitarbeiter,

durch die stetige Entwicklung der Digitaltechnik erhält die Bedeutung des Datenschutzes immer mehr Aufmerksamkeit und stellt die GreenGate AG regelmäßig vor große Herausforderungen, weil Datenerfassung, Datenhaltung, Datenweitergabe und Datenanalyse immer einfacher werden.
Deshalb gilt der Grundsatz:
Wo Daten gespeichert und gesendet werden, muss ein hohes Maß an Datenschutz und Datensicherheit gewährleistet sein. Dies gilt für Daten von Kunden, Interessenten und Geschäftspartnern genauso wie für Mitarbeiterdaten. Denn Datenschutz ist Schutz der Person.

Es ist der Anspruch der GreenGate AG, nicht nur herausragende Dienstleistungen und Produkte anzubieten, sondern auch einen hohen Standard beim Datenschutz zu setzen. Deshalb liegt es in der Pflicht des Unternehmens, den gesetzlichen Anforderungen zu entsprechen, die mit der Verarbeitung personenbezogener Daten verbunden sind. Es hat oberste Priorität, einen einheitlichen gültigen Standard für das Unternehmen beim Umgang mit personenbezogenen Daten sicherzustellen. Denn die Persönlichkeitsrechte und die Privatsphäre eines jeden Einzelnen zu wahren, ist die Basis für vertrauensvolle Geschäftsbeziehungen.

In diesem Datenschutz-Handbuch sind die notwendigen Voraussetzungen für die Verarbeitung personenbezogener Daten von Kunden, Interessenten, Geschäftspartnern und Mitarbeitern geregelt. Dies entspricht den Anforderungen der Europäischen Datenschutzgrundverordnung und stellt deren Einhaltung sicher. Dadurch setzt die GreenGate AG einen gültigen Datenschutz- und Datensicherheitsstandard im Unternehmen und regelt den Datenaustausch intern sowie mit externen Partnern.

Als Maßstab wurden Prinzipien für die Verarbeitung personenbezogener Daten festgelegt, darunter Transparenz, Datensparsamkeit und Datensicherheit. Sämtliche Führungskräfte und Mitarbeiter sind verpflichtet, die im „Datenschutz-Handbuch“ niedergelegten Grundsätze bei Ihrer Arbeit zu beachten, um weiterhin das hohe Ansehen des Hauses, der Produkte und Dienstleistungen zu gewährleisten.

Als Beauftragter für den Datenschutz trage ich dafür Sorge, dass die gesetzlichen Regelungen und Prinzipien zum Datenschutz in der GreenGate AG geachtet werden.

Stephan Hartinger
Datenschutzbeauftragter (TÜV)

Inhalt

Für die GreenGate AG ist die effektive Nutzung moderner Informations- und Kommunikationstechnologien ein wichtiger Bestandteil der Geschäftsprozesse. Eine nicht sachgerechte oder missbräuchliche Verwendung dieser Technologie kann zur Verletzung von Persönlichkeitsrechten führen. Bei der Gestaltung der Informationsgesellschaft soll ein Ziel sein, den Schutz der Persönlichkeitsrechte in den Vordergrund zu stellen. Perfekte Betreuung und zuverlässige Auftragsabwicklung sind bedeutende Ziele der GreenGate AG und erfordern auch, auf Datenschutzbelange unserer Kunden, Vertragspartner und Mitarbeiter einzugehen. Im Bewusstsein dieser Ziele verpflichtet sich das Unternehmen, die nachfolgenden Richtlinien einzuhalten.
Jeder Mitarbeiter der GreenGate AG ist verpflichtet, die im „Datenschutz-Handbuch" niedergelegten Grundsätze bei seiner täglichen Arbeit zu beachten, um weiterhin das hohe Ansehen der GreenGate AG, unserer Produkte und Dienstleistungen zu gewährleisten.
Das „Datenschutz-Handbuch" kann nicht jede mögliche Situation des beruflichen Alltags abbilden. Aus diesem Grund stehen für weitere Hinweise und Rückfragen sowohl der Datenschutzbeauftragte selbst als auch die Ansprechpartner bei der GreenGate AG zur Verfügung, die im „Datenschutz-Handbuch" aufgeführt sind.

§ 1 Ziel des Datenschutz-Handbuches

Ziel des Datenschutz-Handbuches ist es, für das gesamte Unternehmen einheitliche, adäquate Datenschutz- und Datensicherheitsstandards aufzustellen, um den aus der Datenschutzgrund-verordnung (DSGVO)[1] und nationalen Gesetzen[2] folgenden Anforderungen an den grenzüberschreitenden Datenverkehr zu genügen. Das Datenschutz-Handbuch schafft in diesem Zusammenhang ein einheitliches Datenschutzniveau, ersetzt aber nicht die Legitimation, die jeder Verarbeitung oder Übermittlung zu Grunde liegen muss. Daneben sollen die Mitarbeiter und Führungskräfte dabei unterstützt werden, Datenschutzbelange unserer Kunden und Vertragspartner in die Gestaltung von Produkten und Dienstleistungen unseres Hauses zu integrieren. Dieser Paragraph soll im Einklang mit den folgenden Paragraphen dieses Handbuches, insbesondere mit § 3, der die Geltung des einzelstaatlichen Rechts regelt, interpretiert werden.

§ 2 Geltungsbereich

Das Datenschutz-Handbuch ist eine Unternehmensrichtlinie und gilt sowohl für die Verarbeitung personenbezogener Mitarbeiter- und Kundendaten, als auch für die personenbezogenen Daten von Dritten, Beratern und anderen Vertragspartnern im gesamten Unternehmen.

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EU (Datenschutz-Grundverordnung).
[2] Speziell das Bundesdatenschutzgesetz (BDSG-NEU) in der vom Deutschen Bundestag am 27.04.2017 und dem Deutschen Bundesrat am 12.05.2017 beschlossenen Fassung.

§ 3 Geltung einzelstaatlichen Rechts

Durch die Europäische Datenschutz-Grundverordnung (EU-DSGVO) wurde ein einheitlich hohes Datenschutzniveau in der Europäischen Union geschaffen. Sie ist als europäische Verordnung unmittelbar geltendes Recht. Alle EU-Länder sind verpflichtet, die darin zusammengefassten Maßnahmen, welche bei der Verarbeitung von personenbezogenen Daten eingehalten werden müssen, umzusetzen. Eine Verarbeitung von personenbezogenen Daten in einem Drittland ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die zur Datenübermittlung niedergelegten Bedingungen erfüllt und auch die sonstigen Bestimmungen der Europäischen-Datenschutz-Grundverordnung beachtet.

Eine Übermittlung ist danach zulässig, wenn die Europäische Kommission entschieden hat, dass ein angemessenes Schutzniveau besteht.

Hierzu bedarf es eines gesonderten Beschlusses der Europäischen Kommission. Bisher hat die Europäische Kommission dies lediglich für einzelne Länder festgelegt und entsprechende Feststellungen getroffen

Gem. Art. 45 Abs. 8 DSGVO veröffentlicht die Kommission im Amtsblatt der Europäischen Union und auf ihrer Website eine Liste aller Drittländer, für die festgestellt wurde, dass ein angemessenes Schutzniveau gewährleistet bzw. nicht mehr gewährleistet ist.

Hat die Kommission keine solche Entscheidung getroffen, darf ein Verantwortlicher oder ein Auftragsverarbeiter personenbezogene Daten in ein Drittland nur übermitteln, sofern er geeignete Garantien vorgesehen hat und durchsetzbare Rechte sowie wirksame Rechtsbehelfe zur Verfügung stehen, u. a. rechtlich bindende und durchsetzbare Instrumente zwischen Behörden oder öffentlichen Stellen, unternehmensinterne Datenschutzvorschriften oder Standarddatenschutzklauseln, die von der Kommission oder der Aufsichtsbehörde in einem bestimmten Verfahren angenommen werden.

§ 4 Definitionen

- ***Betroffene*** im Sinne dieses Datenschutz-Handbuches sind alle Personen, mit denen eine Vertragsbeziehung besteht oder geplant ist, d.h. z. B. Kunden und Mitarbeiter aber auch zukünftige Kunden und Mitarbeiter in der Anbahnungsphase, allerdings nur, soweit personenbezogene Daten über diese Personen betroffen sind.
- ***Personenbezogene Daten*** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“/“Betroffener“) 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.
- ***Verarbeitung*** personenbezogener Daten ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.

- ***Befugte*** sind Mitarbeiter welche eine Erklärung zur Einhaltung der Datenschutzvorschriften unterzeichnen und entsprechend unterwiesen / sensibilisiert wurden.
  Diese Mitarbeiter dürfen je nach Aufgabenstellung nur die für Ihren Aufgabenbereich relevanten personenbezogenen Daten verarbeiten.
- ***Pseudonymisierung*** meint die Verarbeitung personenbezogener Daten in einer Weise, dass die personenenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.
- ***Anonymisierung*** ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche und sachliche Verhältnisse nicht mehr oder nur mit reinem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können
- ***Verantwortlich*** für die Datenverarbeitung ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.
- ***Auftragsverarbeiter*** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
- ***Dritter*** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.
- ***Einwilligung*** der betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.
  Die Einwilligung muss vor Beginn der Erhebung oder der Verarbeitung der Daten erfolgen. Eine rückwirkende Legitimation einer Verarbeitung kann durch eine Einwilligung nicht erfolgen.
- ***Profiling*** wird verstanden als jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Personen zu analysieren oder vorherzusagen.
- ***Privacy by Design*** beschreibt die bereits datenschutzfreundliche Entwicklung von Hard- und Software, was eine nachträgliche Anpassung und den damit verbundenen Mehraufwand vermeiden soll.

- ***Privacy by Default*** sieht eine datenschutzfreundliche Grundeinstellung von Hard- und Software vor, bei der die Nutzer im zweiten Schritt entscheiden können, ob und wie ihre Daten genutzt werden dürfen.
- Die ***Angemessenheit des Datenschutzniveaus*** wird in einem förmlichen Verfahren anerkannt. Die EU-Kommission hat die Möglichkeit, nach entsprechender Prüfung das Bestehen eines angemessenen Schutzniveaus in einem bestimmten Drittland festzustellen. Die Feststellung kann auch auf ein bestimmtes Gebiet oder einen bestimmten Sektor in dem Drittland oder auch auf bestimmte Datenkategorien beschränkt sein. Ein angemessenes Schutzniveau besteht dann, wenn in dem Drittland auf Grundlage seiner innerstaatlichen Rechtsvorschriften und deren Anwendung, der Existenz und der wirksamen Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden sowie seiner eingegangenen internationalen Verpflichtungen ein Schutzniveau existiert, welches dem in der DS-GVO gewährten Schutzniveau gleichwertig ist.
- Die ***Belastbarkeit*** betreffend ist derzeit noch nicht final absehbar, welche konkreten Maßnahmen hierbei der Verantwortliche oder Auftragsverarbeiter tatsächlich zu treffen hat, um eine Sicherstellung auch hinsichtlich der Nachweisbarkeit zu gewährleisten. Vorstellbar ist, dass der Begriff der Belastbarkeit eine wesentliche Rolle im Bereich des Notfallmanagements spielen kann. Die Datenschutzaufsichtsbehörden sind derzeit bemüht, auch diesen Begriff näher zu durchleuchten und die Anforderungen daran baldmöglichst zu veröffentlichen.
- Die ***Datenschutz-Folgeabschätzung*** hat den Rechten der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest Folgendes zu enthalten:
  1. Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke,
  2. Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge,
  3. Eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und
  4. Maßnahmen, mit denen bestehenden Gefahren abgeholfen werden.

§ 5 Grundsätze für die Verarbeitung personenbezogener Daten

1. Bei der Datenverarbeitung müssen die Persönlichkeitsrechte der Betroffenen gewahrt werden.
2. Im Datenschutzrecht gilt das sogenannte Verbot mit Erlaubnisvorbehalt (Rechtmäßigkeit). Das heißt die Datenverarbeitung ist generell verboten, so lange sie nicht durch ein Gesetz ausdrücklich erlaubt ist oder der Betroffene in die Verarbeitung eingewilligt hat.

   Widerspricht ein Betroffener der Verarbeitung personenbezogener Daten, hat die Datenverarbeitung zu unterbleiben, sofern sie nicht trotz des Widerspruchs erlaubt ist.
3. Die Verarbeitung ist rechtmäßig, wenn sie auf einer entsprechenden Grundlage beruht (Rechtsgrundlage, Einwilligung etc.) und der Zweck der Verarbeitung von der Rechtsgrundlage bzw. der Einwilligung umfasst ist.
4. Die Daten dürfen nur für die genannten Zwecke verarbeitet werden. Ausnahmen sind vorgesehen für sog. kompatible Zwecke, also Zweckänderungen, die aber mit dem ursprünglichen Zweck sachlich eng zusammenhängen.

   Unter bestimmten Voraussetzungen können personenbezogene Daten auch weiterverarbeitet werden, wenn die Verarbeitung nicht dem ursprünglichen Zweck entspricht. Hierfür muss der neue Zweck mit dem alten kompatibel sein, darf also für die betroffene Person nicht überraschend sein.

Der Verantwortliche muss eine genaue, dokumentierte Prüfung anhand folgender festgelegter Kriterien durchführen:

- Jede Verbindung zwischen den Zwecken,
- Der Zusammenhang der Erhebung der Daten, insbesondere hinsichtlich des Verhältnisses zwischen der betroffenen Person und dem Verantwortlichen,
- Die Art der personenbezogenen Daten (z. B. besonders sensible Daten),
- Die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,
- Vorhandene Verschlüsselungen oder Pseudonymisierung der Daten.

Ergibt die Prüfung, dass der Zweck nicht kompatibel ist, ist eine darauf gestützte Verarbeitung unzulässig, es sei denn, der Verantwortliche holt für den neuen Zweck wiederum eine Einwilligung ein.

5. Personenbezogene Daten müssen sachlich richtig und nach Möglichkeit aktuell gehalten werden. Es sind Maßnahmen dafür zu treffen, dass nichtzutreffende oder unvollständige Daten gelöscht bzw. berichtigt werden. Auch sind Maßnahmen zu treffen, dass Datensätze gesperrt werden können, um diese nach Ablauf von etwaigen Aufbewahrungsfristen löschen zu können.
6. Personenbezogene Daten dürfen nur in einer Form gespeichert werden, die die Identifizierung der Person solange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist. Sobald die Speicherung personenbezogener Daten für den Verarbeitungszweck nicht mehr erforderlich ist, müssen die personenbezogenen Daten gelöscht oder die Identifizierung der betroffenen Person aufgehoben werden. Ausnahmen ergeben sich für im öffentlichen Interesse liegenden Archivzwecke, für wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke.
7. Zugriff auf personenbezogene Daten dürfen nur Mitarbeiter haben, in deren Tätigkeitsbereich der Umgang mit diesen Daten fällt. Die Zugriffsberechtigung ist nach Art und Umfang des jeweiligen Tätigkeitsfeldes zu begrenzen.
8. Die betroffene Person muss wissen, wer welche Daten für welchen Zweck verarbeitet. Daher gibt es umfangreiche Betroffenenrechte (z. B. Informationspflichten, Auskunftsrechte, Recht auf Berichtigung der Daten, Widerspruchsrecht etc.). Eine nähere Definition der einzelnen Punkte befindet sich unter § 8 Betroffenenrechte.
9. Die Datenverarbeitung hat sich an dem Ziel auszurichten nur die erforderlichen personenbezogenen Daten, d. h. so wenig wie möglich, zu verarbeiten ***(Datenminimierung)***. Die Verarbeitung muss dabei in diesem Umfang verhältnismäßig (angemessen), zur Erreichung eines legitimen Zieles geeignet (erheblich) und nicht über das zur Zweckerreichung notwendige Maß hinausgehend sein. Die Instrumente der ***Anonymisierung*** und ***Pseudonymisierung*** sind zu nutzen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Statistische Auswertungen oder Untersuchungen, die auf der Basis anonymisierter oder pseudonymisierter Daten erfolgen, sind nicht datenschutzrelevant, soweit über diese Datensätze keine Rückschlüsse mehr auf die betroffenen Personen hergestellt werden kann.

10. Zum Schutz der personenbezogenen Daten hat die GreenGate AG die Grundsätze des Datenschutzes durch Technik (privacy by design) und durch datenschutzfreundliche Voreinstellungen (privacy by default) zu berücksichtigen und geeignete interne Strategien festzulegen sowie entsprechende Maßnahmen zu setzen.

    Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).
11. Entscheidungen, die für den Betroffenen eine rechtliche Wirkung nach sich ziehen oder ihn in ähnlicher Weise erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten (einschließlich Profiling) gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale wie z.B. der Kreditwürdigkeit dient. Die Informationstechnik darf grundsätzlich nur als Hilfsmittel für eine Entscheidung herangezogen werden, ohne dabei deren einzige Grundlage zu bilden.

    Das heißt, es sollte gewährleistet werden, dass in automatisierten Datensystemen keine personenbezogenen Daten weiterverarbeitet und verändert werden. Sofern im Einzelfall die sachliche Notwendigkeit bestehen sollte, automatisierte Entscheidungen zu treffen, muss der Betroffene über eine automatisierte Verarbeitung und die Möglichkeit des Widerspruchs informiert werden. Der Verantwortliche muss angemessene und geeignete Maßnahmen treffen, um die Rechte, Freiheiten und berechtigten Interessen des Betroffenen zu wahren. Bei Datenverarbeitungsvorhaben, aus denen sich hohe Risiken für die Rechte und Freiheiten der Betroffenen ergeben können, ist der Bereich Datenschutz schon vor Beginn der Verarbeitung zu beteiligen und gegebenenfalls vorab eine Datenschutz-Folgenabschätzung vorzunehmen. Dies gilt insbesondere für die in Art. 35 Abs. 3 DSGVO aufgezählten Fälle
12. Das gesamte Unternehmen ist verantwortlich für den Datenschutz und seine Beachtung. Um die Einhaltung des Datenschutzes nachweisen zu können, muss eine entsprechende Dokumentation vorhanden sein.

§ 6 Unterrichtung und Einwilligung der Betroffenen

1. Die vertragliche Beziehung

Personenbezogene Daten des Betroffenen dürfen auf der Grundlage bzw. zur Durchführung eines Vertrags-, bzw. Vertragsanbahnungsverhältnisses verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners nach Abschluss des Vertrages, sofern dies im Zusammenhang mit dem Vertragszweck steht.

Bereits bei der Erhebung, ist der Betroffene darauf hinzuweisen, dass er über Auskunfts- und Berichtigungsrechte hinsichtlich seiner personenbezogenen Daten verfügt. Ferner sollte der Betroffene über die Freiwilligkeit der Angabe von Daten für Zwecke des Marketings unterrichtet werden.

Bei der Erhebung muss der Betroffene Folgendes erkennen können (Transparenz) und entsprechend informiert werden:

- Name und Kontaktdaten des Verantwortlichen, ggf. dessen Vertreters;
- Ggf. die Kontaktdaten des Datenschutzbeauftragten;
- Zweck der Datenverarbeitung samt Rechtsgrundlage für die Verarbeitung;
- Die verfolgten berechtigten Interessen, wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erfolgt;
- Ggf. Dritte oder Kategorien von Dritten, an die die Daten übermittelt werden;
- Ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln;
- Dauer der Speicherung oder Kriterien für die Festlegung dieser Dauer;
- Das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- Wenn die Verarbeitung aufgrund einer Einwilligung des Betroffenen erfolgt, das Bestehen des Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- Das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- Ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsschluss erforderlich ist, inwieweit der Betroffene verpflichtet ist, diese Daten bereitzustellen, und welche Folgen die Nichtbereitstellung hätte;
- Inwiefern eine automatisierte Entscheidungsfindung erfolgt (Profiling).

2. Beziehung ohne Vertragsverhältnis

Im Vorvertragsverhältnis ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Gleiches gilt für die Verarbeitung zur Erfüllung eines Vertrages mit der betroffenen Person. Sollten personenbezogene Daten erhoben werden, die über das zur Vertragsdurchführung oder -anbahnung Erforderliche hinausgehen, so ist eine Einwilligung des Betroffenen einzuholen.

Dasselbe gilt, wenn eine weitere Verarbeitung oder Nutzung von Daten außerhalb des ursprünglichen Erhebungszweckes erfolgen soll. Vor der Einwilligung muss der Betroffene wie unter § 6 Ziffer 1 unterrichtet werden.

Die Einwilligungserklärung ist aus Beweisgründen regelmäßig schriftlich einzuholen. Handelt es sich z. B. um eine Einwilligung, die im Zusammenhang mit dem Abschluss eines Kaufvertrages eingeholt wird, muss diejenige Vertragsklausel, die die Einwilligung enthält, auf dem Kaufvertragsformular getrennt von sonstigen Regelungen und optisch hervorgehoben werden. In der Einwilligungserklärung müssen Umfang und Zweck der Datenverarbeitung spezifiziert werden. Im Falle besonderer Umstände, z. B. bei telefonischer Beratung, kann die Einwilligung ausnahmsweise auch mündlich erteilt werden. Für die Gestaltung von online abzugebenden Einwilligungserklärungen sind die Datenschutz- und Qualitätsstandards für e-Business zu beachten.

3. Datenerhebung bei einem Dritten/Datenaustausch

Grundsätzlich sind personenbezogene Daten beim Betroffenen selbst zu erheben. Sofern Daten bei Dritten erhoben bzw. von Dritten übermittelt werden, ist sicherzustellen, dass der Betroffene bei der ersten Ansprache entsprechend wie unter § 6 Ziffer 1 informiert ist oder wird, sofern nicht eine Ausnahme gem. § 33 Abs. 1 Nr. 2 BDSG vorliegt.

Im Falle eines Datenerwerbs muss sichergestellt sein, dass die Daten im Rahmen des jeweils geltenden Rechts rechtmäßig erhoben wurden und rechtmäßig weitergegeben werden.

Eine Bonitätsprüfung bedarf keiner Einwilligung des Betroffenen, wenn ein überwiegendes berechtigtes Interesse besteht. Dieses liegt nur bei Kauf auf Rechnung vor.

Bei Zahlung per Lastschrift oder Vorkasse liegt kein solches überwiegendes berechtigtes Interesse vor und ist somit unzulässig. Weiterhin möglich ist eine Bonitätsprüfung jedoch, sofern der Betroffene hierin eingewilligt hat.

4. Datenaustausch innerhalb des Unternehmens

Die einzelnen Unternehmen einer Unternehmensgruppe sind zueinander grundsätzlich als Dritte anzusehen. Sofern ein Unternehmen personenbezogene Daten, für die es verantwortlich ist, gegenüber anderen Unternehmen, die derselben Unternehmensgruppe angehören, offenlegt, muss diese Offenlegung datenschutzrechtlich abgesichert werden:

Als verantwortliches Unternehmen kann die GreenGate AG andere Unternehmen innerhalb der Unternehmensgruppe als Auftragsverarbeiter einsetzen. Verantwortliche, die Teile einer Unternehmensgruppe sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln.

Hierzu muss ein Vertrag zur Auftragsverarbeitung mit jedem Unternehmen oder mit dem Mutterkonzern, welcher wiederum die anderen Unternehmen als weitere Auftragsverarbeiter einsetzt, abgeschlossen werden.

Der Verantwortliche, der Teil einer Unternehmensgruppe ist, darf daher personenbezogene Daten innerhalb der Unternehmensgruppe übermitteln, sofern die empfangenden Unternehmen dieser Unternehmensgruppe ebenso angehören, die empfangenden Unternehmen dieser Unternehmensgruppe ihren Sitz innerhalb der EU/des EWR haben, es internen Verwaltungszwecken dient und im Falle einer gemeinsamen Verarbeitung eine Vereinbarung geschlossen wurde.

Für eine Weiterübermittlung an Dritte, die nicht zur Unternehmensgruppe gehören, müssen sowohl die Voraussetzungen des § 6 Ziffer 1 und 2 vorliegen.

§ 7 Besondere Kategorien personenbezogener Daten

Die Verarbeitung personenbezogener Daten, aus denen 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 sind untersagt, sofern sich die Rechtmäßigkeit der Verarbeitung nicht aus einer gesetzlichen Erlaubnis oder aus einem gesetzlichen Erfordernis ergibt.

Eine Verarbeitung besonderer Kategorien personenbezogener Daten ist ferner beispielsweise zulässig für die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche auch im Rahmen eines Rechtsstreits, wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung überwiegt oder der Betroffene in die Verarbeitung eingewilligt hat.

§ 8 Rechte der Betroffenen

Betroffene können sich mit Fragen und Beschwerden entweder direkt an den Datenschutzbeauftragten oder an den hierfür zuständigen Ansprechpartner im Unternehmen wenden. Insbesondere, wenn sie ihre nachfolgenden Rechte wahrnehmen, müssen diese Anfragen umgehend bearbeitet werden.

1. Recht auf Auskunft

Der Betroffene hat das Recht eine Bestätigung darüber zu verlangen, ob personenbezogene Daten seiner Person verarbeitet werden.

Wenn seine personenbezogenen Daten verarbeitet werden, kann Auskunft darüber verlangt werden, welche personenbezogenen Daten (Kategorien), aus welcher Herkunft und zu welchem Zweck gespeichert werden und welchen Empfängern (Kategorien) die personenbezogenen Daten offengelegt werden. Wenn möglich ist dem Betroffenen auch die geplante Dauer der Speicherung mitzuteilen. Falls dies nicht möglich ist, sind die Kriterien für die Festlegung der Speicherung mitzuteilen. Der Betroffene ist ferner über seine Rechte auf Berichtigung oder Löschung seiner personenbezogenen Daten und auf Einschränkung der Verarbeitung der Daten zu informieren.

Dem Betroffenen sind darüber hinaus sein Widerspruchsrecht und das Recht der Beschwerde bei einer Aufsichtsbehörde aufzuzeigen. Wenn eine automatisierte Entscheidungsfindung (Profiling) genutzt wird, ist der Betroffene über die involvierte Logik und Tragweite der angestrebten Auswirkungen zu informieren. Bei einer Übermittlung der Daten an ein Drittland oder eine internationale Organisation ist der Betroffene über geeignete Garantien gemäß Art. 46 DSGVO im Zusammenhang mit der Übermittlung in Kenntnis zu setzen.

2. Recht auf Berichtigung

Sollte sich beispielsweise im Rahmen der Bearbeitung des Auskunftsrechts herausstellen, dass personenbezogene Daten unrichtig oder unvollständig sind, ist der Betroffene berechtigt, ohne unangemessene Verzögerung die Berichtigung bzw. Vervollständigung zu verlangen.

3. Recht auf Einschränkung der Verarbeitung

Eine betroffene Person kann vom Verantwortlichen unter folgenden Voraussetzungen die Einschränkung der Verarbeitung verlangen:

- Die Richtigkeit der Daten wird vom Betroffenen bestritten;
- Die Verarbeitung ist unrechtmäßig;
- Der Zweck der Verarbeitung hat sich erledigt, die Daten sind aber zur Geltendmachung von Rechtsansprüchen des Betroffenen notwendig;
- Es liegt ein Widerspruch des Betroffenen vor.

4. Recht auf Löschung

Die betroffene Person hat unter folgenden Voraussetzungen das Recht, die unverzügliche **Löschung** ihrer Daten zu verlangen („Recht auf Vergessenwerden“):

- Die Speicherung der Daten ist nicht mehr notwendig;
- Der Betroffene hat seine Einwilligung zur Datenverarbeitung widerrufen;
- Die Daten wurden unrechtmäßig verarbeitet;
- Es besteht eine Rechtspflicht zum Löschen nach EU- oder nationalem Recht.

Das Recht auf Vergessenwerden findet unter folgenden Voraussetzungen keine Anwendung:

- Bei Überwiegen des Rechts auf freie Meinungsäußerung bzw. der Informationsfreiheit;
- Die Datenspeicherung dient der Erfüllung einer rechtlichen Verpflichtung (z. B. Aufbewahrungspflichten);
- Archivzwecke stehen der Löschung entgegen;
- Speicherung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.

Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht, muss die für die Verarbeitung der Daten verantwortliche Stelle unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten angemessene Maßnahmen treffen und alle weiteren mit der Verarbeitung Beteiligten darüber informieren, dass eine betroffene Person die Löschung aller Links, Kopien oder Replikationen seiner personenbezogenen Daten verlangt hat. Die Berichtigung, Löschung oder Einschränkung der Verarbeitung muss dem Betroffenen mitgeteilt werden. Insoweit wird auf die Richtlinie zum Löschen personenbezogener Daten (DS-RI 015) verwiesen.

5. Recht auf Datenübertragbarkeit

Der Betroffene hat das Recht die ihn betreffenden personenbezogenen Daten, welche dieser einem Verantwortlichen bereitgestellt hat, in einem gängigen Format zu erhalten und diese ohne Behinderung durch den Verantwortlichen an einen anderen Verantwortlichen weiterleiten zu lassen, sofern bspw. eine Einwilligung des Betroffenen vorliegt und die Verarbeitung mittels eines automatisierten Verfahrens erfolgt. Betroffene sollen dadurch leichter von einem Anbieter zu einem anderen wechseln können, ohne den Verlust ihrer Daten befürchten zu müssen.

6. Widerspruchsrecht

Der Betroffene kann gegen die Verarbeitung seiner personenbezogenen Daten Widerspruch erheben, der eine Weiterverarbeitung der Daten, abgesehen von einigen definierten Ausnahmen, für unzulässig erklärt. Zusätzlich hat er auch ein gesondertes ausdrückliches Widerspruchsrecht gegen die Verarbeitung von personenbezogenen Daten zum Zweck der Direktwerbung.

Soweit ein Kunde Widerspruch gegen die Verarbeitung seiner personenbezogenen Daten erhebt, ist der Datenschutzbeauftragte oder dessen Vertretung zu informieren und vor einer Verarbeitung der Daten eine sorgfältige Prüfung in Abstimmung mit dem Datenschutzbeauftragten oder dessen Vertretung vorzunehmen. Dies gilt nicht, wenn eine Rechtsvorschrift zur Verarbeitung verpflichtet oder die Verarbeitung der personenbezogenen Daten für die Durchführung des Vertrages notwendig ist.

7. Beschwerderecht

Betroffenen wird das Recht zuerkannt, sich bei der zuständigen Aufsichtsbehörde zu beschweren, wenn sie der Ansicht sind, dass eine Verarbeitung der sie betreffenden personenbezogenen Daten gegen die DSGVO oder ein nationales Gesetz verstößt.

8. Folgen einer Verletzung von Rechten Betroffener

Zu beachten ist, dass dem Betroffenen bei rechtswidriger Verarbeitung seiner personenbezogenen Daten Unterlassungs- und Schadensersatzansprüche zustehen können.
Weitere Einzelheiten zum Datenschutzbeauftragten finden sich in § 15 dieses Datenschutz-Handbuches.

§ 9 Vertraulichkeit der Verarbeitung

Nur Befugte und auf die Einhaltung des Datengeheimnisses sensibilisierte Mitarbeiter dürfen personenbezogene Daten verarbeiten. Insbesondere ist es untersagt, solche Daten für eigene private Zwecke zu nutzen, an Unbefugte zu übermitteln oder diesen auf andere Weise zugänglich zu machen. Unbefugt in diesem Sinne sind z. B. auch Arbeitskollegen, sofern sich nicht aufgrund des Tätigkeitsfeldes und der konkreten Aufgaben dieser Kollegen etwas anderes ergibt.
Diese Vertraulichkeit besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

§ 10 Grundsätze der Datensicherheit

Das Unternehmen hat als verantwortliche Stelle sicherzustellen, dass personenbezogene Daten in einer Weise verarbeitet werden, die dem Stand der Technik entsprechen und ein angemessenes Schutzniveau aufweisen. Dies beinhaltet auch den Schutz gegen unberechtigte oder ungesetzliche Verarbeitung. Darüber hinaus haben wir unter Berücksichtigung des Risikos angemessene technische und organisatorische Maßnahmen getroffen, die einen Verlust, die Zerstörung oder eine Schädigung von personenbezogenen Daten sowie die Beeinträchtigung von Persönlichkeits- und Freiheitsrechten verhindern sollen.
Um beurteilen zu können, was ein angemessenes Schutzniveau ist, muss im Vorfeld der Verarbeitung durch das Unternehmen geklärt werden, welchen Schutzbedarf die relevanten personenbezogenen Daten besitzen. Die Schutzbedarfsfeststellung ist als ein erster Schritt essentiell, wenn es später darum geht, geeignete und organisatorische Maßnahmen auszuwählen.

Im Datenschutzrecht sind vier Schutzziele aufgelistet, die bei der Verarbeitung personenbezogener Daten sicherzustellen sind.

Die Schutzziele sind:

1. Vertraulichkeit, d. h. Daten sind für unberechtigte nicht zugänglich
2. Integrität, d. h. Daten können nicht verfälscht werden
3. Verfügbarkeit, d. h. Daten stehen zur Verfügung, wenn sie gebraucht werden
4. Belastbarkeit, d. h. die Widerstandsfähigkeit des Systems

Folgende Schritte sind zu beachten:

1. Schutzbedarf feststellen
2. Risiken bewerten / falls erforderlich Datenschutz-Folgenabschätzung durchführen
3. Maßnahmen treffen
4. Nachweise erbringen

Die zur Datensicherheit erforderlichen technisch-organisatorischen Maßnahmen beziehen sich auf:

- Rechner (Server und Arbeitsplatzrechner)
- Netze bzw. Kommunikationsverbindungen
- Applikationen

Hinsichtlich der Server sind physische und infrastrukturelle Sicherheitsmaßnahmen installiert, die Zutrittskontrollen (mit differenzierten Berechtigungen), Schließsysteme und Brandschutzmaßnahmen umfassen. Alle Arbeitsplatzrechner sind mit einem Passwortschutz ausgestattet. Das unternehmenseigene Netzwerk ist durch Firewall-Systeme vor unberechtigtem, externem Zugang und Zugriff aus dem Internet geschützt. Die Übertragung von Daten mit Personenbezug außerhalb des Netzwerks erfolgt verschlüsselt. Sofern hiervon abgewichen wird, ist dies dem Bereich Datenschutz gegenüber zu begründen. Zum Schutz der personenbezogenen Daten in den Datenbanken ist ein personen- und applikationsbezogener Zugangs- und Zugriffsschutz eingerichtet. Diese technisch-organisatorischen Maßnahmen sind in ein die Verantwortlichkeiten regelndes Datenschutz- und Sicherheitsmanagement einzubetten.

§ 11 Telekommunikation und Internet

Die Verarbeitung personenbezogener Daten, die bei der Telekommunikation mit dem Betroffenen einschließlich der Internet-Kommunikation anfallen, richtet sich nach den vorhandenen Arbeitsanweisungen bzw. nach dem jeweils geltenden Recht.

§ 12 Meldungen von Datenschutzverletzungen

Die Meldung einer Datenschutzverletzung an die Aufsichtsbehörde muss unverzüglich und möglichst binnen 72 Stunden nachdem dem Verantwortlichen diese Verletzung bekannt wurde, erfolgen. Erfolgt die Meldung erst nach Ablauf von 72 Stunden, so ist diese Verzögerung zu begründen.

Die Meldung hat zumindest folgende Informationen zu enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (wenn möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der personenbezogenen Datensätze),
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,

- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Datenschutzverletzung und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Der Verantwortliche muss alle Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten (Auswirkungen, ergriffene Abhilfemaßnahmen) dokumentieren. Diese Dokumentation dient der Aufsichtsbehörde zur Überprüfung der korrekten Einhaltung der Meldepflicht.
Die betroffene Person ist im Falle eines voraussichtlich hohen Risikos unverzüglich von der Datenschutzverletzung zu benachrichtigen.

Diese Benachrichtigung muss zumindest Folgendes beinhalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten in klarer und einfacher Sprache,
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen,
- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung,
- eine Beschreibung der vom Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Eine Benachrichtigung der betroffenen Person ist nicht erforderlich, wenn

- auf die von der Verletzung betroffenen personenbezogenen Daten geeignete technische und organisatorische Sicherheitsvorkehrungen angewandt wurden (insbesondere, wenn dadurch unbefugte Personen keinen Zugang zu diesen Daten haben, etwa durch Verschlüsselung),
- der Verantwortliche durch nachträgliche Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Person aller Wahrscheinlichkeit nach nicht mehr besteht, oder
- die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. In diesem Fall muss jedoch eine öffentliche Bekanntmachung erfolgen, oder eine ähnliche Maßnahme ergriffen werden, damit die betroffenen Personen vergleichbar wirksam informiert werden.

§ 13 Abhilfe/Sanktionen/Verantwortlichkeiten

Die Geschäftsführung des Unternehmens ist verantwortlich für die Datenverarbeitung. Damit sind sie verpflichtet sicherzustellen, dass die gesetzlichen und die in diesem Handbuch enthaltenen Anforderungen des Datenschutzes berücksichtigt werden. Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen.
Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter.
Bei Datenschutzkontrollen durch Behörden ist der Datenschutzbeauftragte umgehen zu informieren.

Die Geschäftsführung muss dem Datenschutzbeauftragten einen Datenschutzkoordinator benennen. Ein Datenschutzkoordinator kann in Abstimmung mit dem Datenschutzbeauftragten diese Aufgabe auch für mehrere Gesellschaften wahrnehmen.
Die Datenschutzkoordinatoren sind vor Ort Ansprechpartner für den Datenschutz. Sie können Kontrollen durchführen und haben die Mitarbeiter mit den Inhalten des Datenschutz-Handbuches vertraut zu machen.
Die Geschäftsführung ist verpflichtet, dem Datenschutzbeauftragten sowie den Datenschutzkoordinatoren umgehend Verletzungen der sich aus diesem Handbuch ergebenden Verpflichtungen und Beschwerden zu melden und sie bei ihrer Tätigkeit, der Umsetzung des Datenschutzrechts, zu unterstützen.
Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen die Datenschutzkoordinatoren rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren.
Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für die Verarbeitung besonderer Kategorien personenbezogener Daten. Die Führungskräfte müssen sicherstellen, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden.
Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht können strafrechtlich verfolgt werden und Schadensersatzansprüche nach sich ziehen.
Die DSGVO sieht zudem die Verhängung von erheblichen Bußgeldern gegenüber Unternehmen als Verantwortlichen vor. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich gemacht werden können, ziehen grundsätzlich arbeitsrechtliche Sanktionen entsprechend dem jeweils geltenden nationalen Recht nach sich.

§ 14 Der Datenschutzbeauftragte

Der Datenschutzbeauftragte als externes weisungsunabhängiges Organ überwacht die Einhaltung der DSGVO sowie aller weiteren nationalen Gesetzen und des Datenschutz-Handbuches und überprüft dies in regelmäßigen Abständen stichprobenartig. Die jeweiligen Geschäftsführungen sind für die Bestellungen der Datenschutzbeauftragten verantwortlich.
Die jeweiligen Geschäftsführungen sind verpflichtet, den Datenschutzbeauftragten in seiner Tätigkeit zu unterstützen. Um Verstößen schon im Vorfeld entgegenzuwirken, ist der Bereich Datenschutz frühzeitig zu beteiligen (vgl. § 5 Ziffer 12).
Bei Verletzungen der sich aus diesem Handbuch ergebenden Verpflichtungen und Beschwerden sind die verantwortlichen Führungskräfte verpflichtet, umgehend den zuständigen Datenschutzbeauftragten oder dessen Vertreter zu unterrichten.
Mitarbeiter, Kunden oder sonstige Vertragspartner haben jederzeit die Möglichkeit, sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten zu wenden. Anfragen und Beschwerden werden vertraulich behandelt.

Kann der zuständige Datenschutzkoordinator einer Beschwerde nicht abhelfen oder einen Verstoß gegen dieses Handbuch nicht abstellen, muss er den Datenschutzbeauftragten einschalten. Die Entscheidungen des Datenschutzbeauftragten zur Abhilfe der Datenschutzverletzung sind von der jeweiligen Geschäftsführung zu berücksichtigen.
Anfragen von Aufsichtsbehörden sind immer auch dem Datenschutzbeauftragten mitzuteilen.

Der Datenschutzbeauftragte kann wie folgt erreicht werden:

coseco GmbH
Stephan Hartinger
Datenschutzbeauftragter (TÜV)
D-86836 Graben
Tel 08232-80988-70
Fax 08232-80988-99
E-Mail: s.hartinger@coseco.de

Als Ansprechpartner auf Seiten der GreenGate AG fungieren:

Name:	Christiane Lagemann
Tel:	+49 2243 92307-23
E-Mail:	c.lagemann@greengate.de

Der Ansprechpartner übernimmt die Koordinierung zwischen der GreenGate AG und dem Datenschutzbeauftragten, indem er insbesondere mögliche Anfragen und/oder Beschwerden zum Thema Datenschutz an den Datenschutzbeauftragten weiterleitet und die ggf. erforderliche weitere Umsetzung koordiniert.

§ 15 Relevante Gesetzesauszüge

Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a. auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b. für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“)

d. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 7 DSGVO Bedingungen für die Einwilligung

(1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

(2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.

(3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

(4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrages, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.

Art. 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

(2) Geldbußen werden je nach den Umständen des Einzelfalls zusätzlich zu oder anstelle von Maßnahmen nach Artikel 58 Absatz 2 Buchstaben a bis h und i verhängt. Bei der Entscheidung über die Verhängung einer Geldbuße und über deren Betrag wird in jedem Einzelfall Folgendes gebührend berücksichtigt:

a. Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
b. Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
c. jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;
d. Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;
e. etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;
f. Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;
g. Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;
h. Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;
i. Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;
j. Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und
k. jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

(3) Verstößt ein Verantwortlicher oder ein Auftragsverarbeiter bei gleichen oder miteinander verbundenen Verarbeitungsvorgängen vorsätzlich oder fahrlässig gegen mehrere Bestimmungen dieser Verordnung, so übersteigt der Gesamtbetrag der Geldbuße nicht den Betrag für den schwerwiegendsten Verstoß.

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a. die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;
b. die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;
c. die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

(5) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a. die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;
b. die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;
c. die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;
d. alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;
e. Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1.

(6) Bei Nichtbefolgung einer Anweisung der Aufsichtsbehörde gemäß Artikel 58 Absatz 2 werden im Einklang mit Absatz 2 des vorliegenden Artikels Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

(7) Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können.

(8) Die Ausübung der eigenen Befugnisse durch eine Aufsichtsbehörde gemäß diesem Artikel muss angemessenen Verfahrensgarantien gemäß dem Unionsrecht und dem Recht der Mitgliedstaaten, einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren, unterliegen.

(9) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, kann dieser Artikel so angewandt werden, dass die Geldbuße von der zuständigen Aufsichtsbehörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von Aufsichtsbehörden verhängten

Geldbußen haben. In jeden Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Die betreffenden Mitgliedstaaten teilen der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften mit, die sie aufgrund dieses Absatzes erlassen, sowie unverzüglich alle späteren Änderungsgesetze oder Änderungen dieser Vorschriften.

Art. 84 DSGVO Sanktionen

(1) Die Mitgliedstaaten legen die Vorschriften über andere Sanktionen für Verstöße gegen diese Verordnung — insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen — fest und treffen alle zu deren Anwendung erforderlichen Maßnahmen. Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

(2) Jeder Mitgliedstaat teilt der Kommission bis zum 25. Mai 2018 die Rechtsvorschriften, die er aufgrund von Absatz 1 erlässt, sowie unverzüglich alle späteren Änderungen dieser Vorschriften mit.

§ 41 BDSG Anwendung der Vorschriften über das Bußgeld- und Strafverfahren

(1) Für Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. § 68 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass das Landgericht entscheidet, wenn die festgesetzte Geldbuße den Betrag von einhunderttausend Euro übersteigt.

(2) Für Verfahren wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 2016/679 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten und der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung und des Gerichtsverfassungsgesetzes, entsprechend. Die §§ 56 bis 58, 87, 88, 99 und 100 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung. § 69 Absatz 4 Satz 2 des Gesetzes über Ordnungswidrigkeiten findet mit der Maßgabe Anwendung, dass die Staatsanwaltschaft das Verfahren nur mit Zustimmung der Aufsichtsbehörde, die den Bußgeldbescheid erlassen hat, einstellen kann.

§ 42 BDSG Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,
   1. einem Dritten übermittelt oder
   2. auf andere Art und Weise zugänglich macht

   und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemeine zugänglich sind,
   1. ohne hierzu berechtigt zu sein, verarbeitet oder
   2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 43 BDSG Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder

2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 202a StGB Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 206 StGB Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in den Nummern 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die
   1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
   2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
   3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 263a StGB Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 Abs. 2 bis 7 gilt entsprechend.

(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.

§ 269 StGB Fälschung beweiserheblicher Daten

(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) § 267 Abs. 3 und 4 gilt entsprechend.

§ 303 StGB Sachbeschädigung

(1) Wer rechtswidrig eine fremde Sache beschädigt oder zerstört, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Ebenso wird bestraft, wer unbefugt das Erscheinungsbild einer fremden Sache nicht nur unerheblich und nicht nur vorübergehend verändert.
(3) Der Versuch ist strafbar.

§ 303 a StGB Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
(2) Der Versuch ist strafbar.
(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 88 TKG Fernmeldegeheimnis

(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.
(2) Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.
(3) Den nach Absatz 2 Verpflichteten ist es untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis von Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach § 138 des Strafgesetzbuches hat Vorrang.
(4) Befindet sich die Telekommunikationsanlage an Bord eines Wasser- oder Luftfahrzeugs, so besteht die Pflicht zur Wahrung des Geheimnisses nicht gegenüber der Person, die das Fahrzeug führt oder gegenüber Stellvertreter.

§ 17 UWG Verrat von Geschäfts- und Betriebsgeheimnissen

(1) Wer als eine bei einem Unternehmen beschäftigte Person ein Geschäfts- oder Betriebsgeheimnis, das ihr im Rahmen des Dienstverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Dienstverhältnisses unbefugt an jemand zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen, mitteilt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer zu Zwecken des Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber des Unternehmens Schaden zuzufügen,

1. sich ein Geschäfts- oder Betriebsgeheimnis durch
   a) Anwendung technischer Mittel,
   b) Herstellung einer verkörperten Wiedergabe des Geheimnisses oder
   c) Wegnahme einer Sache, in der das Geheimnis verkörpert ist,

   unbefugt verschafft oder sichert oder
2. ein Geschäfts- oder Betriebsgeheimnis, das er durch eine der in Absatz 1 bezeichneten Mitteilungen oder durch eine eigene oder fremde Handlung nach Nummer 1 erlangt oder sich sonst unbefugt verschafft oder gesichert hat, unbefugt verwertet oder jemandem mitteilt.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. gewerbsmäßig handelt,
2. bei der Mitteilung weiß, dass das Geheimnis im Ausland verwertet werden soll, oder
3. eine Verwertung nach Absatz 2 Nr. 2 im Ausland selbst vornimmt.

(5) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

(6) § 5 Nr. 7 des Strafgesetzbuches gilt entsprechend.

§ 106 UrhG Unerlaubte Verwertung urheberrechtlich geschützter Werke

(1) Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

Anlageverzeichnis

DS VE 011	Belehrung und Erklärung zum Datenschutz
DS RI 012	Richtlinie zur dienstlichen und privaten Nutzung der EDV-Ausstattung und von TK-Anlagen
DS RI 013	Richtlinie zur Nutzung mobiler Datenendgeräte
DS RI 014	Richtlinie zum Umgang mit Wartungsfirmen und Serviceleistern
DS RI 015	Richtlinie zum Löschen personenbezogener Daten
DS RI 016	Richtlinie zur Vernichtung von Datenträgern mit personenbezogenen Daten
DS AA 011	Arbeitsanweisung für die Benutzung des Internets

Belehrung und Erklärung zum Datenschutz

Diese Belehrung und Erklärung ersetzt die derzeit geltenden Regelungen im jeweiligen Arbeitsvertrag und versteht sich als Nachtrag.

Die Sicherheit und der Fortbestand unseres Unternehmens sind in hohem Maße vom fehlerfreien Funktionieren der technischen Einrichtungen, speziell auch der informationstechnischen Einrichtungen, abhängig. Dazu gehören die elektronische Datenverarbeitung (EDV) und die Telefonanlage.
Unsachgemäße Nutzung und Missbrauch der informationstechnischen Einrichtungen erhöhen unter anderem das Gefährdungspotential. Sie verursachen auch erhebliche Mehrkosten für Wartung und Reparatur, für die Speicherung der anfallenden digitalen Daten, deren tägliche Sicherung und Archivierung und für die ausfallsichere Auslegung der informationstechnischen Komponenten.
Außerdem müssen laut Datenschutzgrundverordnung (DSGVO) und Bundesdatenschutzgesetz (BDSG-neu) personenbezogene Daten von Mitarbeiterinnen und Mitarbeitern, Kunden und Dritten besonders geschützt werden.

1. Datenschutz

Die Speicherung, Verarbeitung und Weitergabe von personenbezogenen Daten ist nur mit Zustimmung des Betroffenen oder unter bestimmten Bedingungen erlaubt. Diese Daten sind zu Zwecken der rechtmäßigen Aufgabenerfüllung und im Rahmen der Tätigkeit im Unternehmen zu erheben, zu verarbeiten, bekanntzugeben, zugänglich zu machen, weiterzugeben oder in sonstiger Weise zu nutzen. Personenbezogene Daten sind alle zu einer Person gehörenden Einzelangaben über persönliche und sachliche Verhältnisse. Diese Verpflichtung besteht grundsätzlich gegenüber allen Personen (auch anderen Mitarbeitern des Unternehmens), Firmen, Behörden und Organisationen mit welchem Mitarbeiter bei der Erfüllung ihrer Tätigkeit Kontakt haben.
Diese Verpflichtung bleibt auch nach Beendigung des Arbeitsverhältnisses bestehen.
Verstöße gegen die Datenschutzgrundverordnung oder das Bundesdatenschutzgesetz können arbeitsrechtliche Konsequenzen wie beispielsweise Abmahnung und Kündigung, Schadensersatzansprüche oder eine Bestrafung gemäß §§ 42, 43 BDSG-neu nach sich ziehen.
Mängel beim Datenschutz bzw. der Datensicherung sind schnellstmöglich einem Vorgesetzten oder den im Datenschutzhandbuch genannten Ansprechpartnern zu melden.
Bestehende Vorschriften hinsichtlich Meldung, Umgang, Unterrichtungspflicht an den Betroffenen und Sicherung personenbezogener Daten sind zu beachten. Zum Schutz personenbezogener Daten ist im Rahmen der zugewiesenen Aufgaben die notwendige Sorgfalt anzuwenden.
Weitere Informationen zum Datenschutz sowie Gesetzesauszüge sind für alle Mitarbeiter zugänglich im Datenschutz-Handbuch. Hierauf wird ausdrücklich verwiesen.

2. Verantwortungsvolle Nutzung der informationstechnischen Einrichtungen des Unternehmens

Um die Sicherheit und den Schutz der informationstechnischen Einrichtungen und der gespeicherten Daten zu gewährleisten, ist es notwendig, dass alle Mitarbeiter unseres Unternehmens mit den informationstechnischen Einrichtungen verantwortungsbewusst umgehen.

Die nachfolgend aufgeführten Regelungen sind von den Mitarbeitern einzuhalten:

1. Im EDV-Netzwerk des Unternehmens und besonders auf allen Servern, Computern und Laptops werden nur Softwareprodukte installiert und genutzt, die von der Geschäftsleitung genehmigt und rechtmäßig lizenziert wurden. Zur Erfüllung der jeweiligen Aufgaben, darf der entsprechende Mitarbeiter Softwareprodukte auf dem Ihm überlassen Computer (Laptop) installieren. Fehlen die benötigten Berechtigungen werden die Softwareprodukte von der IT-Abteilung installiert.
2. Mitarbeiter dürfen ohne Befugnis keine fremde Software aus dem Internet herunterladen. Dazu gehören speziell Demoprogramme, Computerspiele oder Utilities. Datenbestände, die von außerhalb (z.B. auf externen Datenträgern wie externen Festplatten, Disketten, CDs, DVDs, Memory-Sticks etc.) in das Unternehmen eingebracht werden, dürfen nicht ohne Erlaubnis der Geschäftsleitung verwendet werden.
3. Unbefugte Personen dürfen, weder von zugekaufter noch von im Unternehmen selbst entwickelter Software, Kopien erstellen. Die Mitarbeiter sollen innerhalb ihres Wirkungskreises dafür Sorge tragen, den Zugriff unbefugter Personen auf ihre Arbeitsmittel (beispielsweise durch Sperren ihres Bildschirms beim Verlassen des Arbeitsplatzes), zu verhindern.
4. Bei Abwesenheit der Mitarbeiter (z.B. wegen Urlaub) ist eine automatische Abwesenheitsnotiz im E-Mailprogramm einzurichten.
5. Passwörter sollen nicht offen einsehbar hinterlegt werden, weder als Notiz in den jeweiligen Büros, noch als Datei auf Computern oder Datenträgern. Passwörter sollen in regelmäßigen Abständen geändert werden. Hierzu erfolgt bei Zeiten eine Aufforderung durch das System. Wichtige administrative Passwörter sind in einem versiegelten Umschlag im Tresor des Unternehmens zu hinterlegen. Passwörter dürfen nicht an Dritte weitergegeben werden.
6. Unternehmensinterne Daten dürfen nur mit Genehmigung der Geschäftsleitung das Firmengelände verlassen oder außerhalb des Firmengeländes verwendet werden. Dies gilt insbesondere für Geschäftsgeheimnisse, Kunden- und interne Produktdaten.
7. Die Mitarbeiter sichern zu, dass sie alle im Rahmen des Vertragsverhältnisses und ihrer Tätigkeit bekannt gewordenen Daten, Informationen und Dokumente über die Angelegenheiten des Unternehmens, Mitarbeiter, Lieferanten, Kunden und sonstigen Kontakte zeitlich unbegrenzt, insbesondere auch über die Dauer des Vertragsverhältnisses hinaus, streng vertraulich behandeln und geheim halten. Sie versichern, dass sie derartige Informationen Dritten, außer im Rahmen der Erfüllung ihrer Pflichten, nicht zugänglich machen oder sonst zum eigenen oder fremden Nutzen preisgeben werden. Ziehen Mitarbeiter im Auftrag des Unternehmens Dritte zur Mitarbeit hinzu, ist diesen die gleiche Verschwiegenheitspflicht aufzuerlegen.

9. Sollten Fehler, Störungen oder Sicherheitslücken bei der Nutzung der EDV-Einrichtungen des Unternehmens festgestellt werden, ist die IT-Abteilung schnellstmöglich darüber in Kenntnis zu setzten. Bei Verdacht auf Virengefahr, Datenspionage oder andere Umstände, die die Sicherheit der Informationstechnologie des Unternehmens betreffen, ist schnellstmöglich die IT-Abteilung zu informieren.
10. Jeder Mitarbeiter hat die technischen Einrichtungen pfleglich zu behandeln und mit den informationstechnischen Ressourcen und Verbrauchsmaterialien sparsam umzugehen.
11. Betriebsdaten sollen generell so gespeichert werden, dass bei Ausfall einer Mitarbeiterin/eines Mitarbeiters deren/dessen Vertretung oder der Vorgesetzte auf diese Daten zugreifen kann. Für die Speicherung von Betriebsdaten ist das persönliche Verzeichnis, auf das nur der einzelne Mitarbeiter über ihr/sein Passwort zugreifen kann, nicht geeignet. Betriebsdaten (z.B. Word- oder Excel-Dateien) sollten in Gruppenverzeichnissen abgelegt werden.
12. Verlässt eine Mitarbeiterin/ein Mitarbeiter befristet (Mutterschutz, Kur, Elternzeit) oder unbefristet (Kündigung, Rente) das Unternehmen, so hat sie/er die Datenbestände an eine Kollegin/einen Kollegen zu übergeben. Vorgesetzte sollen die ordnungsgemäße Übergabe von Datenbeständen sicherstellen.
13. Die informationstechnischen Einrichtungen, besonders der Zugriff auf das Internet, sollten innerhalb der Arbeitszeit möglichst nicht für private Zwecke gebraucht werden.
14. Die Nutzung der geschäftlichen E-Mail-Adresse für private Zwecke soll stets unterlassen werden.
15. Eine Speicherung von privaten Daten auf den unternehmenseigenen Arbeitsmitteln ist generell verboten. Sollte eine Speicherung von privaten Daten dennoch dringend erforderlich sein, sind diese auf dem lokalen Laufwerk C zu speichern. Es soll keine Speicherung im Netzwerk oder der unternehmensinternen Cloud erfolgen.
16. Der Zugriff auf pornografische, politisch radikale, verfassungsfeindliche, jugendgefährdende, rassistische oder gewaltverherrlichende Internetinhalte ist grundsätzlich nicht gestattet.

3. Betriebsgeheimnis

Es ist den Mitarbeitern untersagt, im Rahmen des Arbeitsverhältnisses bekannt gewordene Betriebs- oder Geschäftsgeheimnisse weiterzugeben oder in sonstiger Form für eigene Zwecke zu verwerten oder zu nutzen. Ein Verstoß gegen diese Geheimhaltungsverpflichtung kann unterschiedliche Konsequenzen nach sich ziehen. Zu den von der Geheimhaltungsverpflichtung erfassten Geschäfts- und Betriebsgeheimnissen gehören insbesondere Informationen, Kenntnisse, Know-how aus den Bereichen Management, Finanzen, Konzeption, Entwicklung, Vertrieb, sowie alle die Datenverarbeitung betreffenden Einzelheiten. Die Geheimhaltungsverpflichtung erstreckt sich nicht auf nachweislich offenkundige Informationen und Kenntnisse.

4. Erklärung

Die Mitarbeiterin/der Mitarbeiter erklärt, dass die ihr/ihm im Rahmen ihrer/seiner Tätigkeit für den Arbeitgeber bekannt gewordenen Geschäftsgeheimnisse und Daten Eigentum des Arbeitgebers sind und dass sie/er diese bei Ausscheiden aus dem Unternehmen unaufgefordert an ihren/seinen Vorgesetzten herausgeben wird und keine Abschriften, auch nicht zu privaten Zwecken, anfertigen wird. Die Mitarbeiterin/der Mitarbeiter erklärt hiermit, hinreichend über die bestehenden, oben beschriebenen Pflichten und das ihr/ihm auferlegte Datengeheimnis, über die Folgen ihrer Verletzung unterrichtet zu sein sowie diese verstanden zu haben und verpflichtet sich zu ihrer Einhaltung. Der Inhalt des Datenschutz-Handbuches ist Ihr/ihm bekannt.
Diese Erklärung bleibt auch über die Beendigung des Arbeitsverhältnisses hinaus bestehen.

Ort, den _____

_____
Name des Arbeitnehmers in Druckschrift

_____
Unterschrift des Arbeitnehmers

Richtlinie zur dienstlichen und privaten Nutzung der EDV-Ausstattung und von TK-Anlagen

Die Sicherheit und der Fortbestand unseres Unternehmens sind in hohem Maße vom fehlerfreien Funktionieren der technischen Einrichtungen, speziell auch der informationstechnischen Einrichtungen abhängig. Dazu gehören die elektronische Datenverarbeitung (EDV) und die Telefonanlage. Durch Computerviren, Spionage und Sabotage sind diese Einrichtungen besonders gefährdet.
Unsachgemäße Nutzung sowie bewusster und unbewusster Missbrauch der informationstechnischen Einrichtungen erhöhen nicht nur das Gefährdungspotential. Sie verursachen erhebliche Mehrkosten für Wartung und Reparatur, für die Speicherung der anfallenden digitalen Daten, deren tägliche Sicherung und Archivierung und für die ausfallsichere Auslegung der informationstechnischen Komponenten.
Zur Erfüllung der jeweiligen Aufgaben stellt die GreenGate AG ihren Mitarbeitern jeweils eine PC-Ausstattung zur Verfügung. Die Systeme werden in einem funktionsfähigen Zustand von einem IT-Mitarbeiter vor Ort installiert. Alle zur Verfügung stehenden Softwareprodukte oder technischen Komponenten werden ausschließlich von der IT-Abteilung installiert und verteilt.
Um die Sicherheit und den Schutz der informationstechnischen Einrichtungen und der gespeicherten Daten zu gewährleisten und die Kosten der Informationstechnologie in akzeptablen Grenzen zu halten, ist es notwendig, dass alle Mitarbeiter unseres Unternehmens mit den informationstechnischen Einrichtungen verantwortungsbewusst und kostenbewusst umgehen. Die nachfolgend aufgeführten Regelungen sind von allen Mitarbeitern einzuhalten:

1. Softwareprodukte können und dürfen lediglich von der IT-Abteilung auf den Servern des Unternehmens installiert werden. Zur Erfüllung der jeweiligen Aufgaben, darf der entsprechende Mitarbeiter Softwareprodukte auf dem Ihm überlassen Computer (Laptop) installieren. Fehlen die benötigten Berechtigungen werden die Softwareprodukte von der IT-Abteilung installiert. Es werden lediglich lizensierte Produkte verwendet. Das Kopieren der in unserem Haus eingesetzten, urheberrechtlich geschützten Software oder der durch die Firma erstellten Programme ist ein Verstoß gegen das Urheberrechtsgesetz. Die nicht genehmigte Vervielfältigung (das sog. Raubkopieren) urheberrechtlich geschützter Werke (beispielsweise Software, Bilder, Musik, Videos, etc.) verpflichtet unser Unternehmen unter Umständen zum Schadensersatz und hat daneben strafrechtliche Folgen für den Raubkopierer. Ein solches Verhalten kann unser Unternehmen nicht tolerieren, da es widerrechtlich ist und gegen die Unternehmensphilosophie unseres Hauses verstößt.
2. Im Umgang mit der EDV-Ausstattung und den TK-Anlagen gelten insbesondere folgende Regelungen:
   - Betriebssysteme, Anwendungsprogramme, Updates und Hotfixes dürfen nur von Beauftragten der Geschäftsleitung installiert werden.
   - Mitarbeiter dürfen ohne Befugnis keine fremde Software aus dem Internet herunterladen oder auf anderem Weg auf Computern des Unternehmens installieren. Dazu gehören auch Bildschirmschoner, Demoprogramme, Computerspiele oder Utilities.
   - Alle Datenbestände, die von außerhalb des Firmengeländes (z.B. auf externen Datenträgern wie externen Festplatten, Disketten, CDs, DVDs, Memory-Sticks etc.) kommen, müssen durch das aktuelle Antivirenprogramm des Unternehmens überprüft werden, bevor sie verwendet werden.

3. Unternehmenseigene Laptops (keine PC-Workstations o. ä.) können zu Hause oder auf Dienstreisen eingesetzt werden. Die Mitarbeiter sind selbst dafür verantwortlich, die Firmendaten, wie Präsentationen, Reiseberichte, Protokolle etc., nach deren Rückkehr auf dem Server zu sichern. Alle Programme, Dokumentationen oder sonstige schützenswerte Daten unterliegen dem Datenschutz und dürfen Dritten nicht zugänglich gemacht werden.
4. Unbefugte Personen dürfen weder von zugekaufter noch von im Unternehmen selbst erstellter Software Kopien erstellen. Die Lizenzbedingungen von Softwareherstellern sind einzuhalten.
5. Passwörter dürfen nicht offen einsehbar hinterlegt werden, weder als Notiz in den Büros der Mitarbeiter noch als Datei auf Computern oder Datenträgern. Wichtige administrative Passwörter müssen in einem versiegelten Umschlag im Tresor des Unternehmens hinterlegt werden.
   Passwörter sind absolut vertraulich und dürfen unter keinen Umständen an Dritte weitergegeben werden. Das Passwort sollte aus mindestens sechs Zeichen und einer Buchstaben-, Zahlen-, Sonderzeichenkombination bestehen.
6. Unternehmensinterne Daten dürfen nur mit Genehmigung der Geschäftsleitung das Firmengelände verlassen oder außerhalb des Firmengeländes verwendet werden. Insbesondere dürfen ohne Zustimmung der Geschäftsleitung firmeninterne Datenbestände, speziell Adressbestände, Kundendaten oder Produktdaten, weder mittels E-Mail oder Fax noch mittels anderer Datenträger (Laptop, Diskette, CD, DVD, Memory-Stick, externe Festplatte etc.) oder in ausgedruckter Form außer Haus gebracht werden.
7. Mitarbeiter dürfen nicht versuchen, auf Bereiche des LANs oder WANs vorzudringen, die nicht für den jeweiligen Mitarbeiter und sein Aufgabengebiet freigegeben oder vorgesehen sind, auch dann nicht, wenn es durch unzureichende Rechtevergabe oder technische Mängel möglich ist. Über derartige fehlerhafte Rechtevergabe oder technische Mängel ist der Vorgesetzte oder die IT-Abteilung umgehend zu informieren.
8. Bei Verdacht auf Virengefahr, Datenspionage oder anderer Umstände, die die Sicherheit der Informationstechnologie des Unternehmens betreffen, ist unverzüglich ein Vorgesetzter oder ein IT-Mitarbeiter des Unternehmens zu informieren.
9. Störungen und Defekte bei informationstechnischen Einrichtungen und auftretende Fehler in der Software sind unverzüglich den dafür verantwortlichen Personen, in der Regel der IT-Abteilung, zu berichten.
10. Die Datensicherung wird von der IT-Abteilung durchgeführt. Diese wendet hierbei besondere Sorgfalt an.
11. Den Mitarbeitern stehen ein Internetzugang, eine E-Mail-Adresse, ein Telefon und ein Fax-Dienst zur Verfügung. Diese sind für die Bewältigung der Aufgaben am Arbeitsplatz und zur Kommunikation mit Kollegen, Kunden oder Lieferanten vorgesehen. Jeder Mitarbeiter ist angehalten, die technischen Einrichtungen pfleglich zu behandeln und mit den informationstechnischen Ressourcen sparsam umzugehen. Das betrifft auch den Verbrauch von Speicherplatz auf den Servern und von Verbrauchsmaterialien wie Druckerpapier, Druckfolien, Druckerpatronen usw.

12. Verlässt ein Mitarbeiter kurzzeitig seinen Arbeitsplatz, ist der Benutzeraccount zu sperren. Am Ende eines Arbeitstages müssen sich alle Mitarbeiter von ihrem PC abmelden und diesen, sowie sämtliche angeschlossenen Geräte, ausschalten.
13. Sollte der eigene Arbeitsplatz eines Mitarbeiters belegt oder defekt sein, können sich Mitarbeiter im Firmennetzwerk an einem beliebigen freien Arbeitsplatz anmelden, um ihren Aufgaben nachzukommen. Der Defekt wird schnellstmöglich von der IT-Abteilung behoben. Sollte dies nicht möglich sein, wird der vom Unternehmen beauftragte IT-Dienstleister mit der Reparatur beauftragt.
14. Betriebsdaten müssen generell so gespeichert werden, dass bei Ausfall eines Mitarbeiters dessen Vertretung oder der Vorgesetzte auf diese Daten zugreifen kann. Für die Speicherung von Betriebsdaten ist das persönliche Verzeichnis, auf das nur der einzelne Mitarbeiter über sein Passwort zugreifen kann, nicht geeignet. Betriebsdaten wie Word- oder Exceldateien sollten vielmehr in Gruppenverzeichnissen abgelegt werden. Damit bei Ausfall eines Mitarbeiters diese Daten von anderen Mitarbeitern gefunden werden, muss die Ordnerstruktur im Gruppenverzeichnis auf dem/den Servern ständig mit den zuständigen Kollegen abgesprochen werden. Namen für Ordner oder Dokumente sollen eindeutig gewählt werden, damit Dokumente auch von Kollegen schnell geortet werden können.
15. Während einer vorübergehenden Abwesenheit (beispielsweise Urlaub) sollen alle Mitarbeiter eine automatische Antwort in ihrem E-Mail-Postfach schalten, um dadurch die Absender der eingehenden E-Mails zu informieren, über welchen Zeitraum der adressierte Mitarbeiter nicht erreichbar ist, dass E-Mails und ggf. Faxe nicht weitergeleitet werden und welche Mitarbeiter für dringende Fälle (Aufgaben oder Kundenanfragen etc.) zur Verfügung stehen, um Anliegen zu bearbeiten. Ist der Mitarbeiter selbst nicht in der Lage (z. B. durch schwere Krankheit), eine solche Abwesenheitsnotiz einzurichten, kann die IT-Abteilung oder die Geschäftsleitung dies übernehmen.
16. Verlässt ein Mitarbeiter befristet (Mutterschutz, Elternzeit, Kur) oder unbefristet (Kündigung, Rente) das Unternehmen, so ist er/sie angehalten die Datenbestände an einen Kollegen/eine Kollegin zu übergeben. Vorgesetzte sind angehalten, die ordnungsgemäße Übergabe von Datenbeständen sicherzustellen.
17. Werden informationstechnische Einrichtungen, speziell der Zugriff auf das Internet privat genutzt, sollte dies grundsätzlich außerhalb der regulären Arbeitszeit geschehen.
18. Die Nutzung der geschäftlichen E-Mail-Adresse für private Zwecke ist zu unterlassen.
19. Das Abonnieren von Newslettern zum privaten Gebrauch ist ebenfalls zu unterlassen.
20. Es ist untersagt über externe E-Mail-Accounts firmeninterne Nachrichten zu versenden.
21. Die Mitarbeiter sind angehalten, keine privaten Daten (Dokumente, digitale Fotos etc.) auf den Computern zu speichern.
22. Der Zugriff auf pornografische, politisch radikale, verfassungsfeindliche, jugendgefährdende, rassistische oder gewaltverherrlichende Internetinhalte ist generell verboten.
23. Bei Mehrfachempfängern z. B. beim Versand von Newslettern, ist immer die Bcc-Adressierung zu verwenden: Die Mehrfach-E-Mail wird an den Absender (An) gerichtet und alle Empfänger unter Bcc aufgelistet. Hierbei ist mit großer Sorgfalt zu arbeiten.

24. Das Speichern betrieblicher Daten beispielsweise in Dropbox, Google Cloud oder ähnlichen ist verboten. Diese dürfen nur in der firmeninternen Cloud oder im Netzwerk gespeichert werden. Bei Fragen können sich Mitarbeiter gerne an die IT-Abteilung wenden.
25. Bei Einschränkungen der Funktionstüchtigkeit der überlassenen Arbeitsmittel, die nicht durch eigene zulässige Maßnahmen behoben werden können, ist schnellstmöglich die IT-Abteilung zu kontaktieren.

Beim Aufruf von Seiten, die aktive Komponenten (Videostreams, mp3 u. a.) enthalten, werden diese protokolliert.
Internet-Nutzungsdaten werden zwischengespeichert, d. h. der allgemeine Internetverkehr wird ebenfalls protokolliert.
Die Mitarbeiter haften in gesetzlichem Umfang für Verhaltensweisen, die gegen diese Richtlinie verstoßen. Dies betrifft im besonderen Maße die Datensicherheit auf allen im Zugriff befindlichen Systemen.
Weiteres ist der „Arbeitsanweisung für die Benutzung des Internets DS AA 011“ zu entnehmen.

Richtlinie zur Nutzung mobiler Datenendgeräte

Diese Richtlinie ist ergänzend zu der „Richtlinie zur dienstlichen und privaten Nutzung der EDV-Ausstattung und von TK-Anlagen“

1. Hardware

Der Mitarbeiter wird mit zusätzlicher Hardware, z.B. Tablet, Notebook, Smartphone, etc. ausgestattet oder es wird für die Dauer einer Dienstreise zusätzlich Hardware zur Verfügung gestellt.
Der Mitarbeiter hat alle diese Geräte mit Sorgfalt zu behandeln und diese im funktionsfähigen Zustand zu halten bzw. am Ende der Dienstreise unaufgefordert wieder in der IT-Abteilung abzugeben.

2. Nutzung von mobilen Datenendgeräten (Tablet PC, Notebook, Smartphones)

Geschäftsdaten wie E-Mail, Kontakte und Kalender sind auf dem Server gespeichert und benötigen keine zusätzliche Sicherung.
Das Erstellen einer Sicherung aller weiteren geschäftsrelevanten Daten, welche sich auf dem mobilen Datenendgerät befinden liegen in der Verantwortung des Nutzers.
Nicht geschäftsrelevanten Daten können temporär auf einem lokalen Laufwerk abgespeichert werden.
Bitte beachten Sie dabei Folgendes:

- Daten auf dem lokalen Laufwerk werden bei einer Datensicherung nicht berücksichtigt.
- Bei einem Absturz der Festplatte gehen diese Daten unwiderruflich verloren.
- Sind auf dem lokalen Laufwerk zu große Datenmengen abgespeichert, hat dies negativen Einfluss auf die Leistung des Rechners.

Private Multimediadaten (Bilder, Musik, Filme, usw.) dürfen nicht im Firmennetzwerk oder der firmeninternen bzw. dezentralen Server-Cloud gespeichert werden.

Weiter sind folgende Regeln einzuhalten:

- Die Gerätesoftware der mobilen Datenendgeräte darf nicht verändert werden.
- Das Synchronisieren von geschäftsrelevanten Daten mit dem privaten Rechner ist untersagt.
- Jegliches Laden/Installieren von kostenpflichtigen Applikationen (‚Apps‘) zu Lasten des Arbeitgebers ist untersagt, es sei denn, diese Applikation wurde seitens des Arbeitgebers zur Nutzung empfohlen und freigegeben.
- Überprüfen Sie vor Ihrer Auslandsreise, ob Sie Ihren Tarif im Reiseland nutzen können.
- Innerhalb der Europäischen Union (EU) kann in der Regel Ihre Datenflatrate unbesorgt genutzt werden.
- Außerhalb der EU sollte Datenroaming nur in absoluten Ausnahmesituationen aktiviert werden, da es unter Umständen unverhältnismäßig hohe Kosten verursachen kann.
- Die hohen Kosten außerhalb der EU lassen sich mit einer passenden Auslandsoption reduzieren. Bei längeren Aufenthalten außerhalb der EU lohnt sich, der Kauf einer Sim-Karte vor Ort.

3. Nutzung von privaten mobilen Datenendgeräten

Geschäftsdaten wie E-Mail, Kontakte und Kalender sind auf dem Server gespeichert und benötigen keine zusätzliche Sicherung auf Ihrem privaten Geräten.

Zur eigenen Sicherheit, sollte auf Ihren mobilen Datenendgeräten, immer eine aktuelle Version eines Virenscanners vorhanden und aktiv sein.

Da sich bei der Nutzung von privaten mobilen Datenendgeräten geschäftsrelevante Daten auf diesen Geräten befinden, ist ein entsprechender Passwortschutz einzurichten, um die Nutzung durch Dritte zu verhindern.

Ohne entsprechende Sicherheitsvorkehrungen ist der Zugriff mit privaten mobilen Datengeräten auf geschäftsrelevante Daten nicht gestattet.

Im Verlustfall ist umgehend die Geschäftsleitung oder IT-Abteilung zu benachrichtigen.

4. Physischer Schutz mobiler Geräte

Die Geräte können stationär oder auch unterwegs betrieben und mitgeführt werden.

Mobile Datenendgeräte wie Tablet PCs, Notebooks, Smartphones, sind vorrangig für geschäftliche Zwecke zu verwenden. Soweit sie außerhalb des Firmengeländes zum Einsatz kommen, sind sie durch die jeweiligen Nutzer angemessen gegen Missbrauch und Diebstahl zu schützen. Es ist daher u.a. unzulässig

(a) mobile Datenendgeräte unbeaufsichtigt in nicht verschlossenen Räumen zu lassen.

(b) mobile Datenendgeräte in Fahrzeugen zu lassen, auch wenn diese abgeschlossen sind.

(c) mobile Datenendgeräte Dritten (auch Familienangehörigen) zu überlassen.

Mobile Datenendgeräte sind stets sicher aufzubewahren und sollten nicht unbeaufsichtigt gelassen werden.

Mobile Datenendgeräte dürfen nie extremen Temperaturen ausgesetzt werden. Insbesondere der Akku, aber auch das Display können dadurch beschädigt werden.

Geräte, die in sehr kalten Räumen aufbewahrt wurden, dürfen nicht sofort eingeschalten werden, sondern müssen erst der normalen Umgebungstemperatur angepasst sein, damit das Gerät nicht durch sich bildendes Kondenswasser beschädigt wird.

Ebenso müssen diese Geräte vor Umwelteinflüssen wie beispielsweise vor Feuchtigkeit durch Regen oder Spritzwasser geschützt werden.

Im Übrigen gelten die Ausführungen in den Bedienungsanleitungen.

5. Software

Die IT-Abteilung ist berechtigt, nicht erlaubte Programme vom Client (PC, Notebook) zu deinstallieren. Dies betrifft ebenfalls diverse Browser-Plug-ins.

Es sollten keine eigenen Programme, Spiele, Bilder, Filme, Musik oder andere Tools auf firmeneigenen mobilen Datenendgeräten installiert werden.

6. Mängel/Schäden

Bei Einschränkungen der Funktionstüchtigkeit, die nicht durch eigene zulässige Maßnahmen behoben werden können, ist unverzüglich Verbindung mit einem IT-Mitarbeiter aufzunehmen. Mit diesem IT-Mitarbeiter wird das weitere Vorgehen abgestimmt. Der Einsatz fremder IT-Firmen oder Werkstätten ist untersagt, da evtl. Garantievereinbarungen erlöschen könnten.

Bei Verlust oder grober Beschädigung durch Dritte ist die Polizei einzuschalten. Gleichzeitig ist der Verlust/ Schaden bei der IT-Abteilung anzuzeigen.

7. Haftung

Die Mitarbeiter haften in gesetzlichem Umfang für Verhaltensweisen, die gegen diese Richtlinie verstoßen. Dies betrifft im besonderen Maße die Datensicherheit auf allen im Zugriff befindlichen Systemen.

Richtlinie zum Umgang mit Wartungsfirmen und Serviceleistern

Um ein möglichst störungsfreies Arbeiten mit Hard- und Softwarekomponenten sicherzustellen, müssen diese ordnungsgemäß verwaltet und gewartet werden.
Wartungs- und Pflegearbeiten werden von der internen IT-Abteilung ausgeführt. Sollte dies nicht möglich sein, wird ein IT-Dienstleister damit beauftragt. Im Falle der Beauftragung, wird eine Vereinbarung zur Auftragsverarbeitung geschlossen.

1. Interne Pflege- und Wartungsarbeiten von einer externen Firma

Sind Wartungs- und Pflegearbeiten von einer externen Firma im Hause durchzuführen, so sind Maßnahmen zu definieren, die die Einhaltung der Datenschutzbestimmungen sicherstellen, wie z. B.:

- Bei der Fernwartung muss der Verbindungsaufbau stets durch uns erfolgen, so dass Wartungsarbeiten nur mit unserem Wissen und Willen beginnen können.
- Wir müssen das Wartungspersonal als autorisiert identifizieren können. Alle Aktivitäten eines Wartungsvorgangs, die in einer Protokolldatei festgehalten werden, sind zu überprüfen und zur Beweissicherung entsprechend den gesetzlichen Aufbewahrungsfristen aufzubewahren.
- Datenträger dürfen den Bereich der speichernden Stelle niemals unkontrolliert verlassen können.

2. Externe Pflege- und Wartungsarbeiten

- Werden IT-Systeme zur Wartung oder Reparatur außer Haus gegeben, sind in der Regel alle besonderen Kategorien personenbezogener Daten, die sich auf den Datenträgern befinden, vorher physikalisch zu löschen.
- Ist dies nicht möglich, weil aufgrund eines Defektes nicht mehr auf Datenträger zugegriffen werden kann, sind die mit der Reparatur beauftragten Unternehmen auf die Einhaltung der Verschwiegenheit zu verpflichten.
- Die Durchführung externer Wartungsarbeiten ist zu protokollieren; es ist anzugeben, welche IT-Systeme oder Komponenten wann und an wen zur Reparatur gegeben wurden, wer dies veranlasst hat, zu welchem Zeitpunkt die Reparatur abgeschlossen sein sollte und wann das Gerät wieder zurückgebracht wurde.
- Bei Versand oder Transport sind die zu reparierenden IT-Komponenten vor Beschädigungen und Diebstahl zu schützen.
- IT-Systeme, die durch Passwörter geschützt sind, müssen je nach Umfang der Reparaturarbeiten den Wartungstechnikern bekannt gegeben werden, damit diese auf die Geräte zugreifen können.
- IT-Systeme oder Komponenten sind nach Rückgabe auf Vollständigkeit zu überprüfen. Alle Passwörter sind zu ändern. PC-Datenträger sind nach Rückgabe mittels eines aktuellen Viren-Suchprogramms auf Computerviren zu überprüfen.

3. Verträge mit Dritten

Der Vertrag muss folgende Inhalte enthalten:

1. Gegenstand und Dauer der Verarbeitung;
2. Art und Zweck der Verarbeitung;
3. Art der personenbezogenen Daten & Kategorien von betroffenen Personen;
4. Umfang der Weisungsbefugnisse;
5. Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit;
6. Sicherstellung von technischen & organisatorischen Maßnahmen;
7. Hinzuziehung von Subunternehmern;
8. Unterstützung des für die Verarbeitung Verantwortlichen bei Anfragen und Ansprüchen Betroffener;
9. Unterstützung des für die Verarbeitung Verantwortlichen bei der Meldepflicht bei Datenschutzverletzungen;
10. Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung;
11. Kontrollrechte des für die Verarbeitung Verantwortlichen und Duldungspflichten des Auftragsverarbeiters;
12. Pflicht des Auftragsverarbeiters, den Verantwortlichen zu informieren, falls eine Weisung gegen Datenschutzrecht verstößt.

Ferner hat der Auftragnehmer eine Verpflichtungserklärung zur Geheimhaltung und zum Datenschutz abzugeben.

4. Entsorgung von Datenträgern durch Dritte

Datenträger, die schützenswerte Daten enthalten (Papier, Festplatten etc.) und nicht mehr gebraucht werden oder aufgrund eines Defektes ausgesondert werden sollen, sind durch den Benutzer selbst oder die Fachabteilung so zu entsorgen, dass keine Rückschlüsse auf vorher gespeicherte Daten möglich sind. Bei funktionstüchtigen Datenträgern ist dies durch physikalisches Löschen der Daten zu erreichen, bei nicht funktionierenden Datenträgern durch mechanische Zerstörung.

Sofern durch das eigene Unternehmen keine sichere Entsorgung durchgeführt werden kann, ist mit der Entsorgung ein Dienstleistungsunternehmen zu beauftragen. Der damit betraute externe Dienstleister hat vertraglich die Einhaltung der Datenschutz- und Sicherheitsbestimmungen zuzusichern und eine Geheimhaltungsverpflichtung abzugeben, wie bereits oben dargestellt.

Da auch Informationen durch unbedachte Entsorgung oder Wiederverwendung von Geräten kompromittiert werden können, sind anstatt der herkömmlichen Löschfunktion Speichergeräte mit sensiblen Informationen physisch zu vernichten oder auf sichere Weise zu überschreiben.

Alle Geräte, die Speichermedien enthalten, z. B. Festplatten, sind zu überprüfen, um sicherzustellen, dass sensible Daten und lizenzierte Software vor der Übergabe beseitigt oder überschrieben werden.

Jedes Gerät, das entsorgt werden soll, ist daraufhin zu überprüfen, ob noch Speichermedien enthalten sind. Ist dies der Fall, sind die Speichermedien physisch zu vernichten oder auf sichere Weise zu überschreiben.

Richtlinie zum Löschen personenbezogener Daten

Um die datenschutzrechtlichen Bestimmungen der Datenschutzgrundverordnung (im Folgenden DSGVO) sowie des neuen Bundesdatenschutzgesetzes (BDSG-neu) einzuhalten und die Löschung der Daten der verschiedenen Betroffenen zu gewährleisten, wurde das nachfolgende Löschkonzept entwickelt.

Nach den geltenden rechtlichen Bestimmungen der DSGVO sind Daten gemäß Art. 17 DSGVO zu löschen, sofern deren Verarbeitung und Speicherung nicht erlaubt ist.

Auch können Betroffene gemäß Art. 18 DSGVO unter bestimmten Voraussetzungen eine Einschränkung der Verarbeitung verlangen. Daher sind personenbezogene Daten nicht nur zufällig zu löschen, sondern es bedarf sinnvoller Regelungen, welche die gesetzlichen Aufbewahrungspflichten und andere Vorschriften berücksichtigen.

1. Begriffsdefinitionen

(1) Anonymisieren ist der Prozess durch den die personenbezogenen Daten so verändert werden, dass der Betroffene nicht mehr direkt oder indirekt identifiziert werden kann.

(2) Aufbewahrungsfrist ist die Frist für die eine Datenart nach rechtlichen Vorgaben beim Verantwortlichen verfügbar sein muss.

(3) Betroffener ist eine identifizierte oder identifizierbare natürliche Person.

(4) Einschränkung der Verarbeitung gemäß Art. 4 Nr. 3 DSGVO. Werden im Sinne der DSGVO bereits gespeicherte personenbezogene Daten „markiert“, bedeutet dies, dass durch diese Einschränkung derartige Daten für Benutzer nicht verfügbar sind bzw. verwendet werden dürfen.

(5) Löschen bedeutet das Behandeln von personenbezogenen Daten in der Art, dass diese nach dem Vorgang nicht mehr vorhanden oder unkenntlich sind bzw. nicht mehr verwendet oder rekonstruiert werden können.

(6) Löschfrist ist die Frist nach der eine Datenart bei regulärer Verwendung in den Prozessen des Verantwortlichen spätestens zu löschen ist.

(7) Löschklasse ist die Kombination aus Löschfrist und abstraktem Startzeitpunkt für den Fristlauf.

(8) Löschkonzept sind die Festlegungen mit denen ein Verantwortlicher sicherstellt, dass die personenbezogenen Datenbestände rechtskonform gelöscht werden.

(9) Löschregel ist die Kombination aus Löschfrist und Bedingung für den Startzeitpunkt des Fristlaufs.

(10) Personenbezogene Daten gemäß Art. 4 Nr. 1 DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie dem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, psychologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

(11) Pseudonymisierung nach Art. 4 Nr. 5 DSGVO ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technisch-organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

(12) Sperren von Datenbeständen bedeutet eine Zugriffsbeschränkung in den Prozessen des Verarbeiters.

(13) Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder Verantwortlicher, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedsstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedsstaaten vorgesehen werden.

(14) Vorhaltefrist ist die Frist, für die eine Datenart zu Verwendung vom Verantwortlichen aufgrund fachlicher Anforderungen oder gesetzlicher Bestimmungen mindestens verfügbar sein muss.

2. Datenarten

(1) Je nach Datenart ist zu entscheiden, wann personenbezogene Daten zu löschen sind. Daten müssen gelöscht werden, wenn sie nicht mehr erforderlich sind und eine rechtliche Vorschrift die Speicherung nicht erlaubt.

(2) Die Datenart richtet sich nach einem fachlichen Zweck, unabhängig davon wo diese Daten gespeichert werden und den einschlägigen rechtlichen Vorschriften. Jede abgegrenzte Datenart wird einer sog Löschregel zugeordnet. Jede Datenart orientiert sich an einem fachlichen Verwendungszweck innerhalb der Organisation des Verantwortlichen.

(3) Wenn ein Datenbestand für unterschiedliche Zwecke verwendet wird, können sich unterschiedliche Regelungen für die Löschung ergeben.

(4) Eine Datenart wird durch Datenobjekte gebildet, die zu einem gemeinsamen Zweck verarbeitet werden und einen Personenbezug herstellen. Die Zuordnung von Datenobjekten zu Datenarten ist organisationsintern festzulegen und kann sich überschneiden, wenn bspw. mehrere Datenarten das gleich Datenobjekt verwenden.

(5) Sollten für eine Datenart unterschiedliche Archivierungsdauern vorgeschrieben sein, so ist wegen der unterschiedlichen Löschfristen eine eigene Datenart zu bilden.

(6) Hinsichtlich der verschiedenen Datenarten wird sowohl auf die gesetzlichen als auch auf die von der GreenGate AG festgelegten Aufbewahrungsfristen verwiesen.

3. Regelprozess und Standardlöschfristen

(1) Jede Löschregel muss datenschutzkonform definiert werden. Es bedarf einer Löschfrist und einem Starzeitpunkt ab welchem die Frist zu laufen beginnt.

(2) Die Vorhaltefrist für eine bestimmte Datenart beinhaltet, dass diese Datenart durch mindestens ein System bis zum Ablauf der Aufbewahrungsfrist zur Verfügung stehen muss. Die Aufbewahrungsfrist bildet das Minimum der Vorhaltefrist. Eine darüberhinausgehende Speicherung ist nur dann möglich, wenn dies rechtlich erlaubt ist.

(3) Nach dem Ende dieser Vorhaltefrist werden die Daten beim Verantwortlichen nicht mehr benötigt.

(4) Nach dem Ende der Vorhaltefrist muss aus datenschutzrechtlichen Gesichtspunkten gelöscht werden, sofern keine Regelung die Aufbewahrung erlaubt. Die Summe aus der Vorhaltefrist und der datenschutzrechtlich erlaubten Aufbewahrungsfrist bestimmt die längst mögliche Löschfrist im Bereich der Datenverarbeitung im Regelprozess (Regellöschfrist). Nach Ablauf dieser Regellöschfrist müssen alle Datenarten von allen Verantwortlichen gelöscht werden. Diese Regelung betrifft auch die Löschung bei Auftragnehmern des Verantwortlichen.

(5) Für den Fall, dass die Rechtslage einen Spielraum für die Verwendung von Datenarten einräumt, kann der Verwendungs- und Löschprozess innerhalb der gesetzlich festgelegten Grenzen gestaltet werden. Hier hat der Verantwortliche abzuwägen wie ob und wie lange nach Ende der Vorhaltefrist eine Löschung erfolgen soll.

(6) Wenn durch einschlägige Rechtsvorschriften Fristen für die Löschung von Datenarten vorgegeben sind, stellen diese Fristen die Obergrenze für die Festlegung einer Löschfrist dar.

(7) In Ausnahmefällen ist es möglich Daten in einem vom Regelprozess abweichenden Prozess zu verwenden, wenn die Daten für diese Verarbeitung einer anderen Datenart zugeordnet werden und dies rechtlich zulässig ist.

(8) Die Aufbewahrungsfristen sind aus dem jeweiligen Verzeichnis von Verarbeitungstätigkeiten zu entnehmen. Nach Ablauf dieses Zeitraums sind die Daten zu löschen, sofern die Speicherung nicht weiterhin erlaubt ist. Diese Aufbewahrungsfristen legen somit die Standardlöschfrist fest, ab wann Daten gelöscht werden sollen.

4. Löschen in Sondersituationen und Abweichungen von den Standardlöschfristen

(1) Sollte eine Löschfrist von einer Standardlöschfrist abweichen, so sind die Prinzipien der Erforderlichkeit und Datensparsamkeit anzuwenden.

(2) In manchen Situationen und unter manchen Bedingungen kann es notwendig werden, außerhalb der Leitlinien dieses Löschkonzepts zu löschen.

(3) Hierunter fallen die Sondersituationen, dass vor der Regellöschfrist gelöscht werden muss aber auch die Alternative, dass länger als die Regellöschfrist aufbewahrt werden soll. Beiden Fällen liegt ein überwiegendes Interesse zu Grunde.

(4) Hierzu zählen bspw. das Löschen von unberechtigt erhobenen personenbezogenen Daten und das Löschen im Fall eines berechtigten Löschbegehrens des Betroffenen.

(5) Es ist somit möglich einzelne Daten von Betroffenen nach Bedarf zu löschen.

(6) Im Fall von bspw. Rechtsstreitigkeiten oder außergerichtlichen Streitigkeiten kann es angebracht sein, die Regellöschfristen zu verlängern solange der Rechtsstreit noch nicht abgeschlossen ist und die Unterlagen noch benötigt werden. In diesem Fall sollten die Daten der Datenart mit einer längeren Löschfrist zugeordnet werden.

(7) Für den Fall, dass sich der Verwendungszweck der personenbezogenen Daten ändert und dies mit den einschlägigen rechtlichen Vorschriften vereinbar ist, hat auch hier eine Anpassung der Löschregelung an den Verwendungszweck zu erfolgen.

(8) Für Restbestände von personenbezogenen Daten, welche keinem Regelprozess oder einer Sondersituation zugeordnet werden können, sind im Einzelfall zu beurteilen. Die Beurteilung solcher Einzelfälle erfolgt unter Abwägung der jeweiligen Interessen unter Beachtung des Grundsatzes der Datensparsamkeit und wird vom Datenschutzbeauftragten ggf. in Zusammenarbeit mit dem zuständigen Leiter der Abteilung ermittelt.

5. Archivierung und Sicherungskopien

(1) Archive sollen Daten langfristig vorhalten. Daten werden archiviert, wenn keine Veränderungen mehr an diesen vorgenommen werden.

(2) In Archiven unterliegen die personenbezogenen Daten damit einer Löschfrist je nach entsprechender Datenart.

(3) Sicherungskopien (Backups) werden nicht als Archive verwendet. Backups dienen der Wiederherstellung von Systemen und Datenbeständen nach bspw. Störungen und dürfen daher nicht verändert werden. Backups bestehen meist aus verschiedenen Versionen oder Versionsketten. Die einzelnen Daten erreichen damit die Löschfrist zu sehr unterschiedlichen Zeiten.

(4) In Sicherungskopien sind oft personenbezogene Daten enthalten, die frühzeitig gelöscht werden müssen. Allerdings ist es notwendig für die Wiederherstellung in einem potentiellen Störfall die Sicherungskopien für einen gewissen Zeitraum vorzuhalten, wodurch die Löschfrist für manche der Daten überschritten wird. Die Löschfristen dürfen lediglich um das datenschutzrechtlich vertretbare Maß überschritten werden, weshalb sich die Löschfrist der Sicherungskopie an der kürzesten Löschfrist der jeweils enthaltenen Datenart orientieren muss. Hinsichtlich der personenbezogenen Daten in Sicherungskopien muss gewährleistet sein, dass die Backups lediglich zu Systemwiederherstellungen genutzt werden.

(5) Für die Löschung von Backups ist somit eine eigene Frist festzulegen.

(6) Es muss folglich eine Trennung zwischen Archiven und Backups vorgenommen werden.

6. Gesperrte Daten

(1) Diese Datenbestände unterliegen besonderen Zugriffsbeschränkungen und werden nicht mehr in den Prozessen des Verarbeiters benötigt oder dürfen nicht mehr in den Prozessen des Verarbeiters verwendet werden.

(2) Die Zugriffsrechte auf diese Daten sind auf die Mitarbeiter einzuschränken, die die notwendigen verbliebenen Arbeiten an bzw. mit diesen Daten vornehmen.

(3) Die Daten sind mit erhöhter Sorgfalt zu behandeln.

(4) Daten sind insbesondere dann zu sperren, wenn keine Geschäftsbeziehung mehr besteht, die Geschäftsbeziehung beendet wurde, keine Erklärung des Betroffenen vorliegt, dass die personenbezogenen Daten weiter genutzt werden können oder der Betroffene eine Sperrung der Daten verlangt und dieses Verlangen rechtmäßig ist. Es ist ferner möglich Daten aus unternehmensinternen Gründen zu sperren.

7. Unzulässige Datenbestände

(1) Sollte sich herausstellen, dass personenbezogene Daten nach den geltenden Vorschriften in unzulässiger Weise gespeichert wurden, sind diese unverzüglich zu löschen.

(2) Wenn ein Betroffener ein Löschbegehren an den Verantwortlichen für ein bestimmtes Datenobjekt stellt, welches sich auf ihn bezieht und dieses noch gespeichert ist, ist dieses unverzüglich zu löschen. Dem Betroffenen ist die Löschung der Datenobjekte mitzuteilen.

8. Löschregeln, Löschklassen

(1) Die Löschfrist und ein Starzeitpunkt ab dem der Lauf der Löschfrist beginnt ergeben die sog. Löschregel. Eine sog. abstrakte Löschregel stellt auf einen abstrakten Startzeitpunkt ab.

(2) Der Startzeitpunkt basiert auf einer konkreten Bedingung welche im Lebenszyklus einer Datenart auftritt.

(3) Bedingungen können solche sein, die bei Erhebung der Daten, während des Lebenszyklusses oder bei Beendigung der Beziehung zum Betroffenen auftreten. Der mögliche Startzeitpunkt der Löschfrist ist damit auf einen der folgenden drei Zeitpunkte festzulegen: die Erhebung der Daten, den Abschluss eines Vorgangs oder das Ende einer Beziehung zum Betroffenen.

(4) Eine Löschklasse wird gebildet, indem eine Standardlöschfrist und ein abstrakter Starzeitpunkt zusammengeführt werden.

9. Fristberechnung der Löschfrist

(1) Erheblich für den Beginn der Löschfrist sind die in § 7 Abs. 3 beschriebenen Bedingungen:
   a. Zeitpunkt der Entstehung der Daten (Datenerhebung),
   b. Zeitpunkt der Beendung des Vorgangs,
   c. Zeitpunkt der Beendung der Beziehung zum Betroffenen.

(2) Die Löschfrist beginnt mit dem Ablauf des Kalenderjahres in welchem eine der in Abs. 1 aufgeführten Bedingungen eingetreten ist.

(3) Die Frist endet nach Ablauf der jeweiligen Frist mit dem Ende des Kalenderjahres.

10. Entsorgung der personenbezogenen Daten und Verantwortliche für die Löschung innerhalb des Unternehmens

(1) Hinsichtlich der Art der Löschung und Entsorgung personenbezogener Daten wird auf die Richtlinie des Datenschutzhandbuchs *„DS RI 016: Richtlinie über die Vernichtung von Datenträgern“* verwiesen.

(2) Verantwortlich für die Entsorgung der Papierunterlagen innerhalb der GreenGate AG ist die jeweilige Abteilung.

(3) Verantwortlich für die Entsorgung von digitalen Unterlagen innerhalb der GreenGate AG, sofern die jeweilige Abteilung keinen Zugriff auf diese hat, ist die IT-Abteilung.

(4) Die Verantwortlichen innerhalb der GreenGate AG haben dafür Sorge zu tragen, dass die Löschregelungen eingehalten werden.

Richtlinie über die Vernichtung von Datenträgern mit personenbezogenen Daten

Bei der Auswahl geeigneter Verfahren zum Vernichten von Datenträgern mit personenbezogenen Daten sind sowohl analoge Datenträger wie z.B. Papier aber auch digitale Datenträger (elektronisch, magnetisch, optisch) zu berücksichtigen. Die Vernichtung von Datenträgern kann sowohl intern aber auch durch externe Dienstleister mit geeigneten Vernichtungsverfahren erfolgen.

1. Vernichten von analogen Datenträgern

Mit Aktenvernichtern können Papier-Dokumente, aber auch Chipkarten und CD‘s so vernichtet werden, dass die ursprünglichen Informationen nicht mehr ohne Weiteres rekonstruiert werden können. Je nach Art und Umfang der Daten muss zwingend der Schutzbedarf ermittelt werden. Dieser wird in drei Schutzklassen eingeteilt. Abhängig davon, um welche Art von Daten es sich handelt, ergibt sich die Schutzklasse die wiederum ausschlaggebend für die Wahl der Sicherheitsstufe ist.

- **Schutzklasse 1 – normaler Schutzbedarf für interne Daten:**
  Telefonlisten, Produktlisten, Lieferantendaten, Korrespondenz, die kein besonderes Wissen des Unternehmens beinhaltet, Werbung, Postwurfsendungen, einfache Notizen
- **Schutzklasse 2 – hoher Schutzbedarf für vertrauliche Daten:**
  Betriebswirtschaftliche Auswertungen, interne Berichte, Daten aus der Finanzbuchhaltung, Jahresabschlüsse, Angebote, Anfragen, Kundenadressen, Personaldaten, Computerdaten
- **Schutzklasse 3 – sehr hoher Schutzbedarf für besonders vertrauliche und geheime Daten:**
  Zeugenschutzprogramme, Informationen aller Geheimhaltungsgrade des Bundes und der Länder, geheime und streng geheime Unterlagen aus Forschung und Entwicklung von Wirtschaftsunternehmen, Gutachten, Verträge, Patente, Daten aus Krankenhäusern, Gesundheitsdaten von Mitarbeitern, Patientenakten

Für jede Schutzklasse werden die zugehörigen Sicherheitsstufen und damit die Größe der von den Aktenvernichtern erzeugten Partikel definiert.

- **Sicherheitsstufe 1:** Allgemeine Daten - Reproduktion mit einfachem Aufwand
- **Sicherheitsstufe 2:** Interne Daten - Reproduktion mit besonderem Aufwand
- **Sicherheitsstufe 3:** Sensible Daten - Reproduktion mit erheblichem Aufwand
- **Sicherheitsstufe 4:** Besonders sensible Daten - Reproduktion mit außergewöhnlichem Aufwand
- **Sicherheitsstufe 5:** Geheim zu haltende Daten - Reproduktion mit zweifelhaften Methoden
- **Sicherheitsstufe 6:** Geheime Hochsicherheitsdaten - Reproduktion technisch nicht möglich
- **Sicherheitsstufe 7:** Top-Secret-Hochsicherheitsdaten - Reproduktion ausgeschlossen

Für die Vernichtung von Datenträgern mit normalem Schutzbedarf sollten Vernichtungsgeräte der Sicherheitsstufen 3 oder höher verwendet werden. Bei höherem Schutzbedarf sollten Geräte der Sicherheitsstufen 4, 5 oder höher eingesetzt werden.

Vernichtungsgeräte unterliegen durch die Nutzung einem normalen Verschleiß. Durch Vernichtung von Material, für dass das Vernichtungsgerät nicht geeignet ist, können Schäden entstehen. In beiden Fällen wird die Schneidqualität beeinträchtigt, sodass in regelmäßigen Abständen eine Prüfung des Vernichtungsgutes notwendig ist. Hier reicht zumeist ein Vergleich des Vernichtungsgutes mittels Sichtkontrolle gegen die Angaben aus der Gerätedokumentation.

2. Vernichten von digitalen Datenträgern

Um die sichere Vernichtung vertraulicher Daten zu gewährleisten, müssen diese so vernichtet werden, dass eine Rekonstruktion mit hoher Wahrscheinlichkeit ausgeschlossen werden kann.
Für Datenträger, die nicht weiterverwendet werden oder defekt sind, müssen geeignete Verfahren festgelegt aber auch geeignete Geräte, Anwendungen oder Dienstleistungen zur Verfügung stehen.
Welche Verfahren geeignet sind, um die bei der GreenGate AG vorkommenden Daten oder Datenträger zu vernichten, hängt vom Grad der Schutzbedürftigkeit der Informationen ab. Daher wird von uns eine Anforderungsanalyse vor der Auswahl durchgeführt, um das geeignete Vernichtungsverfahren zu ermitteln.

Hierbei sollten unter anderem folgende Fragen beantwortet werden:

- Welche Datenträgertypen (z. B. optisch oder magnetisch) sollen vernichtet werden?
- Wie groß ist der Datenträger (Datenvolumen) selbst?
- Wie hoch ist der Schutzbedarf der auf den Datenträgern gespeicherten Daten?
- Wurden bzw. werden die Datenträger in einem geschützten Bereich verwendet?
- Wird das Ergebnis der Vernichtung dem Schutzbedarf gerecht?
- Welche Geräte, Anwendungen oder Dienstleistungen stehen für die Vernichtung zur Verfügung und sind diese für den identifizierten Schutzbedarf und die Datenträger-Arten geeignet?
- Wie groß ist die voraussichtliche Menge von Datenträgern eines Typs, der gelöscht bzw. vernichtet werden soll?

Wenn möglich, sollte die Vernichtung von Datenträgern arbeitsplatz- und zeitnah durchgeführt werden, damit die Datenträger möglichst nicht zwischengelagert werden müssen. Damit wird in der Regel auch der Personenkreis, der mit den Datenträgern umgeht, eingeschränkt und die Sicherheit im Umgang mit personenbezogenen Daten erhöht.

3. Vernichtung durch Dienstleister

Je nach Schutzbedarf der Informationen und der verwendeten Datenträger kommen unterschiedliche Vernichtungsarten zum Einsatz. Daher kann es sinnvoll sein, sich für die Vernichtung externer Dienstleister zu bedienen. In vielen Fällen wird der Dienstleister mit dem Abtransport und der Verwertung bereits vernichteter Datenträger beauftragt.
Im Falle des Abtransportes nicht vernichteter Datenträger mit dem Ziel der Vernichtung und Verwertung ist folgendes zu beachten.

3.1 Absicherung beim Auftraggeber

- Es muss dokumentiert werden, welche Verfahren zum Vernichten für die verschiedenen Datenarten und den jeweiligen Schutzbedarf ausgewählt wurden und wie diese anzuwenden sind.
- Zu vernichtende Datenträger müssen bis zur Abholung innerhalb der GreenGate AG vor unbefugtem Zugriff gesichert aufbewahrt werden. Hierfür werden Container aufgestellt, die so abgesichert sind, dass Datenträger nicht wieder entnommen werden können.
- Die Standorte der Sammelcontainer sollten arbeitsplatznah gewählt werden, damit zu vernichtende Datenträger zwischenzeitlich nicht ungesichert aufbewahrt werden.
- Trotz Outsourcing sind interne Regelungen notwendig, um beispielsweise festzulegen, wie Datenträger eingesammelt und bis zur Abholung durch den Dienstleister verwahrt werden.
- Außerdem müssen Transport und Vernichtung angemessen abgesichert werden. Dazu sind mit der Dienstleistungsfirma detaillierte vertragliche Vereinbarungen zu treffen. Es muss regelmäßig überprüft werden, dass diese Vereinbarungen eingehalten werden.

3.2 Absicherung beim Transport

- Es muss sichergestellt sein, dass nur die mit dem Transport beauftragten Personen die zu vernichtenden Datenträger ausgehändigt bekommen. Dafür sind zunächst beim Auftraggeber Personen zu benennen, die in den Entsorgungsprozess eingewiesen sind und die die korrekte Ausführung der Abläufe überwachen können. Die beauftragten Transportboten müssen sich als solche ausweisen können, damit die gesammelten vertraulichen Daten nicht an einen Unbefugten herausgegeben werden.
- Die Übergabe der Datenträger ist sowohl bei der Ein- und Ablieferung schriftlich zu bestätigen.
- Auf der gesamten Transportstrecke muss gewährleistet sein, dass nur berechtigte Personen das Material transportieren.
- Auf der gesamten Transportstrecke sollten weder die Mitarbeiter der Transportfirma noch andere Personen auf das Material Zugriff nehmen können. Dies kann z. B. durch verschlossene oder verplombte Behälter gewährleistet werden.

3.3 Absicherung beim Dienstleister

- Der Entsorgungsdienstleister muss einen funktionierenden Sicherheitsprozess aufgesetzt haben, so dass die zu vernichtenden Datenträger zuverlässig unlesbar gemacht werden und keine unbefugten Personen Informationen daraus gewinnen können.
- Der Dienstleister muss ein aktuelles, nachvollziehbares Datenschutz- und Sicherheitskonzept vorweisen.
- Bei der Anlieferung ist die Vollständigkeit des Transportguts zu überprüfen; So ist also z. B. die Anzahl der Behälter und deren Gewicht zu kontrollieren.
- Beim Dienstleister wird das zu entsorgende Material typischerweise zunächst zwischengelagert. Hier muss sichergestellt sein, dass es eine funktionierende Zutrittskontrolle gibt, damit Unbefugte keinen Zugriff auf die zu vernichtenden Datenträger oder Geräte erhalten.
- Die Geräte und Werkzeuge zur Vernichtung von Datenträgern dürfen nur von Mitarbeitern bedient werden, die in deren Handhabung eingewiesen wurden.

Arbeitsanweisung für die Benutzung des Internets

1. Ziel und Zweck

Ziel und Zweck dieses Dokumentes ist es, allen (internen und externen) Mitarbeitern einen Leitfaden an die Hand zu geben, damit sie sich bei der Benutzung des Internets verantwortungsbewusst im Sinne des Unternehmens verhalten können.

2. Geltungsbereich

Diese Arbeitsanweisung gilt für alle internen und externen Mitarbeiter des Unternehmens. Dazu gehören alle beschäftigten Arbeitnehmer, Aushilfen, Werkstudenten, Volontäre sowie Drittunternehmen, mit denen Verträge zur Leistungserbringung vereinbart werden. Neue Versionen ersetzen die alten Versionen dieses Dokuments vollständig, sofern dies nicht anders ausgewiesen ist.

3. Hintergrund dieser Sicherheitsmaßnahmen

Das Internet ist ein rasant wachsendes Kommunikationsnetz mit allen Vor- und Nachteilen eines offenen weltweiten Netzes. Nützliche wie auch unwichtige, sogar kriminelle Informationen sind verfügbar.
Die erste Priorität der unternehmensweiten Sicherheit beim Internet hat zum Ziel, Mitarbeitern ein Höchstmaß an Transparenz für das Internet bei gleichzeitigem Schutz unternehmensinterner Systeme und Informationen zu bieten.

4. Gefahrenpotential

Es ist wichtig, sich der Tatsache bewusst zu sein, dass

- das Internet auch von Personen benutzt wird, die nicht immer das Wohl des Unternehmens im Sinne haben;
- alle über das Internet ausgetauschten Informationen von einer Vielzahl unbekannter Personen (Kriminelle, Spione, Saboteure, Geheimdienste etc.) gelesen und missbraucht werden können;
- die Computer-Viren, Computer-Würmer, Trojanische Pferde oder sonstige schädliche Programme über das Internet unkontrolliert verbreitet und große materielle und immaterielle Schäden verursachen können.

5. Sicherheitsmaßnahmen des Unternehmens

Ein Schutz vor den möglichen Gefahrenpotentialen in unserem Unternehmen kann nur dann gewährleistet werden, wenn alle betroffenen Mitarbeiter des Unternehmens diese Arbeitsanweisung beachten und danach handeln.

6. Verantwortlichkeit für den Computer-Arbeitsplatz

Jeder Computer-Arbeitsplatz ist einem Benutzer bzw. einer Benutzergruppe zugeordnet. Für jeden Arbeitsplatz gibt es mindestens einen Verantwortlichen, in der Regel ist das der Besitzer. Der Besitzer ist für die Einhaltung der Vorschriften und Arbeitsanweisungen des Unternehmens verantwortlich.

7. Nutzung von zugelassener Hard- und Software

Jeder Computer-Arbeitsplatz darf grundsätzlich nur die vom Unternehmen zugelassene bzw. genehmigte Hard- und Software beinhalten. Diese sind alle offiziell erworbenen, lizenzierten, überlassenen bzw. selbstentwickelten Hard- und Softwareprodukte. Erweiterungen, die Fremdanschlüsse schaffen, sind genehmigungspflichtig.

8. Schutz vor unbefugtem Zugriff

Jeder Mitarbeiter hat seinen Computer-Arbeitsplatz vor unbefugtem Zugriff zu schützen.

9. Internet-Zulassung

Aufgrund der schnell verändernden Internet-Technologien muss jeder neue Dienst durch die Netzwerk-Betreiber auf Sicherheitsrelevanz überprüft werden, bevor er zum Einsatz kommt.
Für die Internet-Zulassung ist hiermit vereinbart, dass

- der Benutzer im Sinne und im Interesse des Unternehmens handelt,
- die Benutzung grundsätzlich während der Arbeitszeit nur im Zusammenhang mit dem Aufgabenumfeld stehen sollte und
- der Benutzer sich über die Gefahren und Risiken im Internet bewusst ist.

10. Berechtigung für Internet-Dienste

Zum Internet gehören verschiedene Internet-Dienste, z. B.:

- **WWW**
  (World Wide Web) - Leicht bedienbare Anwenderprogramme, die den Zugriff auf Informationen mit Hilfe des Protokolls HTTP (Hyper Text Transfer Protocol) und HTTPS (Hyper Text Transfer Protocol Secure) ermöglicht
- **E-Mail**
  (Electronic Mail) - Ein Internet-Dienst zum Versenden und Empfangen von elektronischen Nachrichten.
- **FTP**
  (File Transfer Protocol) - Ein Internet-Dienst zur Übertragung von Dateien von und zu entfernten Rechnern.
- **Social Media**
  (Soziale Medien) findet Verwendung als Überbegriff für Medien, in denen Internetnutzer Erfahrungen, Meinungen, Eindrücke oder Informationen austauschen und Wissen sammeln können. Zu diesen Medien zählen Foren, Weblogs, Wikis, Facebook, Twitter und Auskunftsportale.
- **Remote Access Service**
  Ein Dienst zum Einloggen und Arbeiten auf einem entfernten Rechner.

Mitarbeiter sind nach Anerkennung der „Belehrung und Erklärung zum Datenschutz DS VE 011“ berechtigt, die zugelassenen Dienste entsprechend in Anspruch zu nehmen.

11. Speicherung von Internet-Zugriffen

- Jede Benutzeraktivität bzw. Transaktion im Internet wird gespeichert (protokolliert) und für einen durch das Löschkonzept definierten Zeitraum aufbewahrt. Somit ist eine Nutzung, das Speichern/ Herunterladen von Software, Dateien und Internet-Seiten nachweisbar. Dieses Logging-Verfahren ist notwendig, um potentielle Angriffe (Hacking, Spionage, Sabotage, etc.) festzustellen und an die zuständigen Strafverfolgungsbehörden weiterleiten zu können (siehe Auswertung).
- Die E-Mail-Header werden im Zuge der Spam- und Virenprüfung von E-Mails protokolliert.
- Bei einer systemgefährdenden Auffälligkeit sind die zuständigen Stellen im Unternehmen berechtigt, den jeweiligen PC zu überprüfen und ggf. Änderungen vorzunehmen.

12. Auswertung von Internet-Zugriffen

Die gespeicherten Internet-Zugriffe (Protokollierung) dürfen laut

- Datenschutzgrundverordnung (DSGVO),
- Bundesdatenschutzgesetz (BDSG-neu) sowie
- Betriebsverfassungsgesetz (div. Mitbestimmungsrechte)

nicht zur Auswertung personenbezogener/personenbeziehbarer Daten verwendet werden.
Im Hinblick auf die Wahrung der Interessen der Mitarbeiter und im Sinne des Datenschutzes werden folgende Maßnahmen ergriffen:

- **Zugriff auf gespeicherte Daten**
  Es wird gewährleistet, dass nur autorisierte Personen in begründeten Fällen die gespeicherten Daten einsehen und auswerten. Die Auswertung der gespeicherten Daten erfolgt unter Einbindung der IT-Abteilung, und der Geschäftsleitung bzw. einer von ihr beauftragten Person. Über die Auswertung wird der betroffene Mitarbeiter informiert. Es wird ein ausführliches Protokoll über die Auswertung erstellt. Der betroffene Mitarbeiter erhält eine Kopie dieses Protokolls.
- **Speicherungsdauer der Daten**
  Die gespeicherten Daten werden vor dem Zugriff nicht autorisierter Personen geschützt aufbewahrt. Sofern aufgrund allgemeiner Vorgaben (z.B. gesetzliche Auflagen) eine vorgeschriebene Aufbewahrungsfrist erforderlich ist, wird diese der Geschäftsführung rechtzeitig vorher unter Angabe der Gründe mitgeteilt. Nach Ablauf der Aufbewahrungsfrist werden die gespeicherten Daten im Sinne der Datenschutzgrundverordnung gelöscht.
- **Leistungs- und Verhaltenskontrolle**
  Eine Verhaltens- oder Leistungskontrolle der Mitarbeiter durch Auswertung der gespeicherten Daten erfolgt nicht.

13. Maßnahmen bei Verstößen gegen die Arbeitsanweisung

Die Zugangsberechtigung erlischt, wenn das Internet fahrlässig oder unzulässig für solche Zwecke eingesetzt wird, die das Unternehmen materiell bzw. immateriell schädigen, und damit gegen diese Arbeitsanweisung verstoßen. Bei schweren Verstößen oder Missbrauchsfällen können neben dem Internet-Zulassungsentzug weitere disziplinäre und arbeitsrechtliche Maßnahmen eingeleitet werden.

Zum schweren Verstoß gehört die grobe Fahrlässigkeit bzw. Missbrauch bezogen auf die Nutzung, die Speicherung und die Weitergabe der folgenden Daten:

- sittenwidrige, obszöne und respektlose Angebote,
- menschenverachtende und rassistische Propagandadaten,
- Sekten-Propaganda bzw. -Mitgliederwerbung jeder Art,
- Unbefugtes Software-Herunterladen für Privatzwecke, wenn dadurch grob fahrlässig Lizenzrechte verletzt werden

14. Kontrolle über die Einhaltung von Arbeitsanweisungen

Die IT-Abteilung ist zuständig für die Überprüfung/Kontrolle der Einhaltung von Arbeitsanweisungen zum Thema Internet.

15. Definitionen der Begriffe

- Die **autorisierten Personen** für die Auswertung im Sinne dieser Arbeitsanweisung ist die IT-Abteilung.
- Eine **Auswertung** im Sinne dieser Arbeitsanweisung ist notwendig, sofern die gespeicherten Internet-Zugriffe zur Feststellung der potentiellen Angriffe (z.B. Hacking, Spionage, Sabotage) bzw. der schweren Verstöße gegen diese Arbeitsanweisung es erforderlich machen, grobe Fahrlässigkeit bzw. den Missbrauchsfall unter Einbindung der IT-Abteilung, der Geschäftsleitung bzw. einer von ihr beauftragten Person zu überprüfen bzw. nachzuweisen.
- **Besitzer** eines Computer-Arbeitsplatzes ist in der Regel ein Mitarbeiter, der an diesem Arbeitsplatz arbeitet.
- **Computer-Arbeitsplatz** sind Systeme im Sinne dieser Arbeitsanweisung, wenn sie in festen bzw. mobilen Arbeitsumgebungen Zugriff auf das Internet haben (PC, Notebook, Laptop, NC, usw.).
- **Computer-Viren** gehören zu den Programmen mit Schadensfunktionen. Ein Computer-Virus ist eine nicht selbständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Ein Virus infiziert andere Programme mit einer Kopie von sich selbst. Bösartige Viren beschädigen andere Programme oder Daten, löschen die Plattenverzeichnisstruktur oder richten andere Schäden an.
- Bei **Computer-Würmern** handelt es sich um Störprogramme, die sich selbständig in einem Computer-Netzwerk ausbreiten. Diese Störprogramme können sich reproduzieren und mit Hilfe von Netzwerkfunktionen selbst auf andere Computer kopieren. Die Programm-Kopien können sogar andere Funktionen übernehmen als das Ursprungsprogramm.
- **Trojanische Pferde** sind Sabotage-Programme, die unter falschem Namen bzw. falscher Identität ins Computersystem gelangen. Der Name eines "Trojanischen Pferdes" suggeriert häufig eine nützliche Funktion oder ist sogar identisch mit dem Namen eines bekannten Software-Programms. Den wahren Charakter zeigen die Trojanischen Pferde bei der Ausführung, indem sie zerstörerische Funktionen ausführen.

- **Datenträgermedium** ist das Speichermedium für Daten und Programme (Festplatte, CD, DVD, USB-Stick usw.).
- **Datenträgerlaufwerk** ist das jeweilige Steuerungsinstrument des Datenträgers zum Lesen und Speichern von Daten und Programmen.
- Eine **Firewall** als zentraler Übergang zum Internet ist eine Kombination von Hardware- und Software-Komponenten, der eine sichere Verbindung zwischen dem Netzwerk des Unternehmens und Netzwerken erlaubt, die nicht unter der Kontrolle des Unternehmens sind. Die Systemkonfiguration und die Filterregeln müssen gewährleisten, dass nur die erlaubten Verbindungen zugelassen werden.
- Die **Protokollierung** im Sinne dieser Arbeitsanweisung liegt vor, sofern die Daten über die Internet-Zugriffe gespeichert und verwendet werden, um diese später auswerten zu können.