TSG Schwäbisch Hall 1844 e.V.

Leitlinie Datenschutz

für die

TSG Schwäbisch Hall 1844 e.V

Ansprechpartner: TSG Geschäftsstelle

Datum: 2. Mai 2018

Inhaltsverzeichnis

Zweck des Dokuments

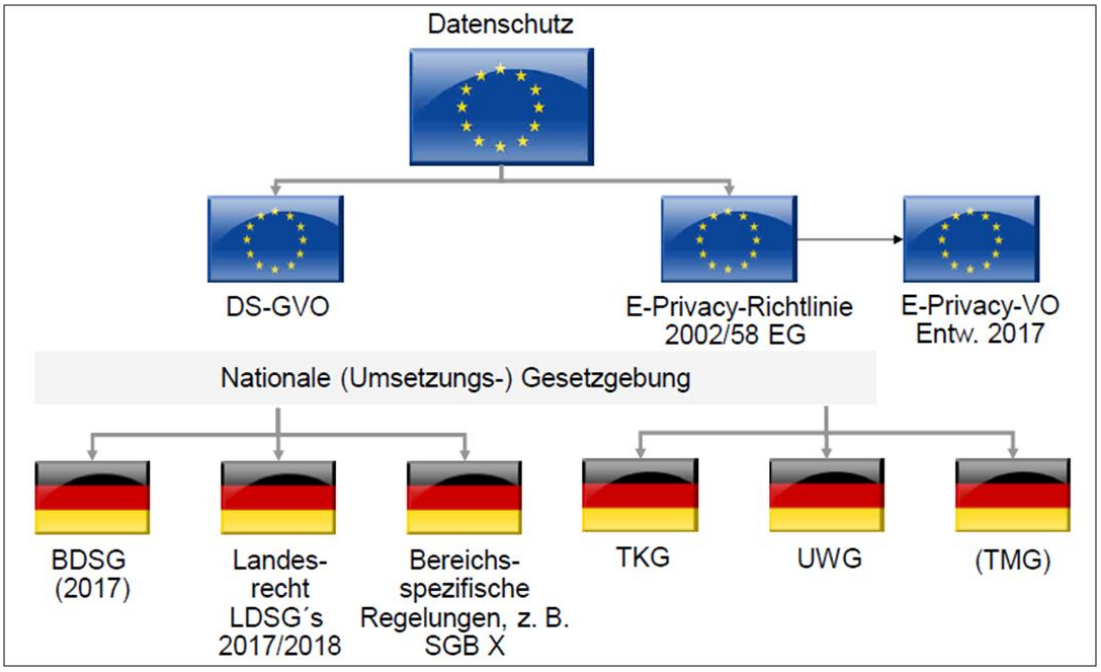
1. Die Leitlinie Datenschutz legt als Grundlagendokument auf Basis der EU-Datenschutzgrundverordnung[1] den Rahmen für die risikogerechte und wirtschaftlich angemessene Datenschutzkonzeption in der TSG Schwäbisch Hall fest.

[1] Im Folgenden EU-DSGVO oder kurz DSGVO genannt

2. Einleitung / Vorwort

Für die TSG Schwäbisch Hall ist die Gewährleistung des Datenschutzes von zentraler Bedeutung.
Datenschutz im Sinne dieser Leitlinie sind alle Maßnahmen, die darauf ausgerichtet sind, den Schutz von personenbezogenen Daten von natürlichen Personen im erforderlichen Umfang zu gewährleisten.
Der Datenschutz in der TSG Schwäbisch Hall zielt einerseits darauf ab, die gesetzlichen Anforderungen des Datenschutzes zu erfüllen, und andererseits Transparenz beim Betroffenen und beim Verein zu schaffen, damit die Entwicklung und der Betrieb von automatisierten Verfahren zweckbestimmt und nutzbringend für alle Beteiligten erfolgt.

3. Gesetzliche Rahmenbedingungen



4. Begriffsbestimmung

Im Sinne der DSGVO bezeichnet der Ausdruck:

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

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

„Einschränkung der Verarbeitung“ die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

„Dateisystem“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

„Verantwortlicher“ 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 können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

„Auftragsverarbeiter“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

„Empfänger“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

„Dritter“ 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 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.

„Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

„biometrische Daten“ mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltens-typischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

„Gesundheitsdaten“ personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

„Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt.

„Unternehmen“ eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen.

„verbindliche interne Datenschutzvorschriften“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben TSG Schwäbisch Hall oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern.

„Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle.

„betroffene Aufsichtsbehörde“ eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

- der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,

- diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder

- eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde.

„grenzüberschreitende Verarbeitung“ entweder

- eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder

- eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.

„maßgeblicher und begründeter Einspruch“ einen Einspruch im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder nicht oder ob die beabsichtigte Maßnahme gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen.

„Dienst der Informationsgesellschaft“ eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates.

„internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

5. Verfahrensablauf

Die datenschutzrechtlichen Verpflichtungen aus gesetzlichen und sonstigen Regelungen sind von den Mitarbeitern der verantwortliche Stelle einzuhalten.

Die Geschäftsstelle hat ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO zu führen und aktuell zu halten.
Wird ein Mangel bezüglich des Datenschutzes erkannt, werden mit dem Präsidium geeignete Maßnahmen erarbeitet, mit denen der Datenschutz hinreichend gewährleistet wird. Wesentliche Grundlagen aus der DSGVO und dem BDSG neu

Die rechtlichen Vorgaben zum Datenschutz und die Interessen der Vereinsmitglieder, Interessenten und Mitarbeiter verlangen einen sicheren und datenschutzkonformen Umgang mit allen personenbezogenen Daten.
Alle Mitarbeiter und das Präsidium sind sich ihrer Verantwortung beim Umgang mit personenbezogenen Daten bewusst.
Wesentliche Rahmenbedingungen zum Datenschutz in der TSG Schwäbisch Hall sind nachfolgend aufgeführt.

5.1. Datenvermeidung, Datensparsamkeit (vgl. Artikel 5 EU-DSGVO)

Der Grundsatz der Datenvermeidung und –sparsamkeit bedeutet, dass Anwendungssysteme sich an dem Ziel auszurichten haben, keine oder so wenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen.

5.2. Einwilligung (vgl. Artikel 4 Nr. 11 EU-DSGVO)

Der Ausdruck „Einwilligung der betroffenen Person“ bezeichnet 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. Formale Anforderungen an die Einwilligung enthält § 7 DS-GVO. Die Einwilligungserklärung muss in verständlicher, leicht zugänglicher Form, in klarer und einfacher Sprache sein. Sie darf nicht in den AGB’s oder in der Datenschutzerklärung „versteckt“ werden, sondern ist getrennt von anderen Inhalten darzustellen.

5.3. Informationspflichten (Art. 13, 14 EU-DSGVO)

Ein Grundpfeiler der EU-DSGVO ist der Grundsatz der Transparenz. Nach diesem Grundsatz soll jede betroffene Person Kenntnis davon haben, welches Unternehmen, welche personenbezogenen Daten, auf welche Art und Weise verarbeitet.
In den Artikeln 13 und 14 ist katalogartig geregelt, welche Informationen konkret mitzuteilen sind, wobei der Umfang der bereitzustellenden Informationen in den beiden Vorschriften variiert. Werden personenbezogene Daten „beim Betroffenen erhoben“ (sog. Direkterhebung), greift Art. 13 DSGVO. Verarbeitet ein Unternehmen hingegen personenbezogene Daten, die nicht „beim Betroffenen erhoben“ wurden, richten sich die Informationspflichten nach Art. 14 DSGVO. Hier kann es sich etwa um Fälle handeln, in denen ein Unternehmen personenbezogene Daten von einem Dritten erhält und zu eigenen Zwecken weiterverarbeitet. Da die betroffene Person in einem solchen Fall oftmals keine Kenntnis von einer solchen Verarbeitung hat, muss das Unternehmen den Betroffenen entsprechend unterrichten. Insbesondere muss es zusätzlich über die Herkunft der empfangenen Daten aufklären (vgl. Art. 14 Abs. 2 lit. f) DSGVO).
worden, die bei der Datenerhebung, -verarbeitung und -nutzung zu beachten sind.

5.4. Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses – § 26 BDSG-neu

Der Beschäftigtendatenschutz ist in der DSGVO nicht ausdrücklich geregelt. Vielmehr eröffnet Artikel 88 DSGVO den Mitgliedstaaten die Möglichkeit, für die Verarbeitung personenbezogener Daten im Beschäftigtenkontext spezifischere Regelungen vorzusehen.
Dem ist der nationale Gesetzgeber nunmehr mit § 26 BDSG-neu nachgekommen, der im Wesentlichen an den Regelungen in § 32 BDSG-alt festhält, sodass sich Banken als Arbeitgeber an den bisher zu § 32 BDSG-alt richterrechtlich entwickelten Anforderungen orientieren können.

5.5. Aufsichtsbehörden der Länder – § 40 BDSG-neu

Für die Überwachung der Einhaltung der DSGVO sowie der Bestimmungen des BDSG-neu durch nicht öffentliche Stellen sind die jeweils nach geltendem Landesrecht benannten Behörden zuständig.

5.6. Recht auf Löschen, Löschkonzept

Um der Anforderung an die Datenlöschung gerecht zu werden, wird empfohlen – fachbereichsspezifisch – Löschkonzepte nach der DIN 66398 zu erstellen und umzusetzen. Dabei sind über die zweckgebundenen Datenspeicherungen und –Verarbeitungen hinaus weitergehende gesetzliche Aufbewahrungsfristen zu berücksichtigen. Durch die jeweiligen Fachexperten muss definiert werden, zu welchem Zeitpunkt eine physische Löschung von Daten erfolgen darf bzw. erfolgen muss, sofern der Zweck für das Vorhalten von Daten nicht mehr gegeben ist und keine gesetzlich notwendigen Aufbewahrungsfristen mehr gegeben sind.
In Bezug auf die Aufbewahrungsfristen sind in jedem Fall immer die Rechtsabteilung (weitere rechtlich bedingte Aufbewahrungsgründe) sowie das Rechnungswesen zur Abstimmung steuerrelevanter Belange einzubinden*.*

5.7. Meldung von Datenschutzverletzungen („Datenschutzpannen“) – Artikel 33, 34 DSGVO

Die Datenschutzgrundverordnung enthält Regelungen zu Informationspflichten bei „Datenschutzpannen“. Die Artikel 33 und 34 DSGVO unterscheiden insofern eine Benachrichtigung der Aufsichtsbehörde und eine Benachrichtigung des Betroffenen. Die Aufsichtsbehörde ist bei einer Beeinträchtigung der Rechte der Betroffenen innerhalb von 72 Stunden zu informieren. Dabei sind der Behörde u.a. die Art der Verletzung, die Anzahl der Betroffenen, die Zahl der betroffenen Datensätze sowie Maßnahmen- und Folgenbeschreibungen zu präsentieren. Eine Benachrichtigung der Betroffenen hat hingegen erst bei einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen zu erfolgen. Eine verbindliche Verfahrensbeschreibung ist in der schriftlich fixierten Ordnung dokumentiert.

5.8. Datensicherheit / Technische und organisatorische Maßnahmen – Artikel 32, 24 DSGVO

Aus Artikel 32 Abs. 1 DSGVO ergibt sich das Erfordernis, Verarbeitungsvorgänge, die personenbezogene Daten zur Grundlage haben, in Abhängigkeit von Risiko und Eintrittswahrscheinlichkeit einzeln zu bewerten („Datenschutzmanagementsystem“). Aufgrund der gleichgerichteten Schutzziele wird für das Datenschutzmanagement auf die in der TSG Schwäbisch Hall etablierten Prozesse zum Risiko- und Informationssicherheitsmanagement (ISMS) zurückgegriffen.
Alle Geschäftsprozesse, die die Verarbeitung personenbezogener Daten zum Gegenstand haben, sind unter Zugrundelegung eines „hohen Schutzbedarfs“ einer Risikoanalyse zu unterwerfen. Die Schutzmaßnahmen sind regelmäßig bzw. anlassbezogen zu überprüfen und anzupassen (PDCA-Zyklus).

5.9. Dokumentationspflichten, Verzeichnis von Verarbeitungstätigkeiten – Artikel 5 Abs. 2, Artikel 30 DSGVO

Artikel 5 Abs. 2 DSGVO fordert vom Verein den mittelbaren Nachweis der Einhaltung der gesetzlichen Bestimmungen. Darüber hinaus sind in einzelnen Artikeln der Datenschutzgrundverordnung auch unmittelbare Dokumentationsanforderungen definiert, beispielsweise zur Datenschutzfolgen-abschätzung, für die Verzeichnisse für Verarbeitungstätigkeiten und für die Meldung der Datenschutzverstöße.

5.10. Sonderbestimmungen zur Auftragsverarbeitung (vgl. Artikel 28 EU-DSGVO)

Werden personenbezogene Daten im Auftrag des Verantwortlichen durch andere – Externe - verarbeitet, ist sowohl der Auftraggeber für die Einhaltung der Vorschriften des Datenschutzes verantwortlich, als auch der Auftragnehmer. So hat z.B. der Auftragnehmer gleichfalls ein Verzeichnis von Verarbeitungstätigkeiten zu führen und auf Anforderung vorzulegen.
Es sind besondere Anforderungen hinsichtlich der Auswahl, Prüfung (vgl. Anlage 3) und Dokumentation (Dokumentationsvorlage siehe Anlage 4) des Auftragnehmers zu beachten. Der Auftragnehmer ist sorgfältig auszuwählen, besonders unter Berücksichtigung der Eignung der von ihm getroffenen Schutzmaßnahmen im Sinne des Datenschutzes. Der Auftrag ist schriftlich zu erteilen mit teilweise vorgeschriebenem Inhalt (Standardvertrag ist im Abschnitt "Dokumente zur Auftragsverarbeitung im Zusammenhang mit dem Bestellprozess" zu finden oder über den Bereich EL erhältlich).
Auftragsverarbeitung im Sinne des Gesetzes liegt vor, wenn eine, mehrere oder alle der nachfolgenden Arbeitsarten vergeben werden:

- Erheben (Aufnehmen von Daten z. B. über Aufnahmeantrag)
- Speichern (Erfassen, Aufbewahren von Daten)
- Verändern (inhaltliches Umgestalten von Daten, Erstellen von Arbeitsergebnissen)
- Übermitteln (Bekanntgeben gespeicherter oder durch DV gewonnener Daten)
- Sperren (Kennzeichnen von Daten zur Einschränkung ihrer Verarbeitung oder Nutzung)

- Löschen
- Nutzen (Verwendung von Daten außerhalb der fünf zuletzt genannten Arbeiten, z. B. der Postversand von Datenträgern wie Listen, Kontoauszügen, Briefen, etc.).

5.11. Aufsichtsbehörde (vgl. Artikel 77 EU-DSGVO).

Die jeweils im Bundesland des Verantwortlichen zuständige Aufsichtsbehörde kontrolliert die Einhaltung des Datenschutzes. Betroffene können bei jeder Aufsichtsbehörde Beschwerde gegen den Verantwortlichen führen.

5.12. Sanktionen bei Verstößen (vgl. Artikel 83 und 84 EU-DSGVO)

Die Nichtbeachtung der Datenschutzbestimmungen ist bußgeldbewehrt (bis zu 20 Mio. € oder 4% des Vorjahres-Konzernumsatzes – davon jeweils der höhere Bußgeldbetrag). In besonders gelagerten Fällen finden Strafvorschriften (bis zu 2 Jahren Freiheitsstrafe) Anwendung.

6. Datenschutzmanagement: Aufgaben, Kompetenzen, Verantwortlichkeiten

6.1. Das Präsidium

trägt als „Verantwortlicher“ im Sinne der DSGVO die Verantwortung nach innen und nach außen. Sie erlässt die internen Regelungen zur Umsetzung des Datenschutzrechts im Unternehmen und hat Weisungsbefugnisse gegenüber Führungskräften und Mitarbeitern. Die Geschäftsleitung entscheidet über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten.
tragen die Verantwortung für die Einhaltung aller Maßnahmen zur Wahrung des Datenschutzes auf der Führungsebene für ihre Mitarbeiter. Im Einzelnen sind dies:

- Beachtung aller datenschutzrechtlichen Verpflichtungen. Darin eingeschlossen sind auch die Pflichten aus der Sicherheitsleitlinie, die auf den Datenschutz hinwirken.
- Jährliche Unterweisung aller Mitarbeiter zum Datenschutz, unverzügliche Unterweisung neuer Mitarbeiter. Gegenstand der Unterweisung ist der Inhalt dieser Richtlinie, sowie das im Personal Self Service Portal zur Verfügung stehende und nach Durchführung vom Mitarbeiter zu bestätigende Webinar.

Sporadische Kontrollen des clean-desk-Verhaltens und anderer Pflichten

6.2. Die Geschäftsstelle

trägt die Verantwortung für die Einhaltung aller Maßnahmen zur Wahrung des Datenschutzes auf der operativen Ebene. Im Einzelnen sind dies:

- Jeder Mitarbeiter hat das Datengeheimnis zu wahren. Mitarbeiter sind auf das Fernmeldegeheimnis (§ 88 TKG) zu verpflichten;
- Verwendung aller betrieblichen DV-Einrichtungen (Großrechner, PC, IIV, mobile Endgeräte, DV im Netz etc.) nur im Rahmen der dienstlichen Aufgaben;
- Beachtung aller datenschutzrechtlichen Verpflichtungen;
- Erkannte Sicherheitsrisiken sind unverzüglich der Führungskraft zu melden, der sich bei Bedarf mit dem DSB in Verbindung setzt.

6.3. Die Abteilungsvorsitzenden und deren Beauftragten

Dateneigner ist stets der Abteilungsvorsitzende für alle in seinen Bereich fallenden Daten und Geschäftsprozesse. Der Dateneigner ist verantwortlich für die Einhaltung aller Belange des Datenschutzes bei Konzeption, Änderung und laufendem Betrieb aller Geschäftsprozesse seines Bereiches.
Die Aufgaben und Verantwortung im Einzelnen sind:

- Verantwortung für Datenschutz in den zugeordneten Geschäftsprozessen im Hinblick auf folgende Belange
- Definition und Aktualisierung von Zugriffsanforderungen (Zugriffsrechte)
- Festlegung Aufbewahrungsfristen
- Festlegung Datensicherungserfordernisse (für Aufbewahrung)
- Abnahme neuer Anwendungssysteme zur Kontrolle der Einhaltung der Vorgaben