Datenschutzregelungen

donum vitae in Baden-Württemberg

Stand 11.6.2021

Inhalt:

Regelungen zur Umsetzung der DS-GVO für *donum vitae* Baden-Württemberg

Stand: 11.4.2021

Seit 25. Mai 2018 gilt die neue EU-Datenschutzgrundverordnung. Auf der Grundlage der Informationen des Datenschutzbeauftragten von BW

https://www.baden-wuerttemberg.datenschutz.de/praxisratgeber-datenschutz-im-verein-nach-der-ds-gvo/

gibt der Vorstand des Landesverbandes von donum vitae in BW für die Umsetzung der DS-GVO in den Regionalverbänden und im Landesverband folgende Empfehlungen:

1. Benennung eines Datenschutzbeauftragten

Der Landesvorstand BW ist der Auffassung, dass die Bestellung eines DSB **nicht notwendig** ist (Begründung S. 4).

Alle **Mitarbeiter/innen** sowie Honorarkräfte **müssen** eine **Information** über die einzuhaltenden Datenschutzregeln ggf. zusammen mit einer Verschwiegenheitserklärung **unterschreiben**. (Muster einer Arbeitsanweisung IT-Sicherheit und einer Verschwiegenheitserklärung auf S.15 und S.22). Auf S. 11 finden Sie die Empfehlungen des Landesverbandes zur IT-Sicherheit im Home-Office.

2. Einwilligungserklärung zum Erheben von personenbezogenen Daten

2.1 Klienten/innen: Eine Einwilligungserklärung im normalen Alltagsgeschäft ist **nicht notwendig**, da wir einen gesetzlichen Auftrag erfüllen. Die Beratenen sollen über ein **Plakat in der Beratungsstelle** über Datenschutz informiert werden. (Muster Aushang für Beratungsstellen auf S.9).
2.2 Mitglieder: Eine Einwilligungserklärung ist **nicht notwendig**, da die von uns erhobenen Daten zur Vertragserfüllung mit dem Verein notwendig sind und nicht veröffentlicht werden.
Vorhandene Mitglieder sollen **schriftlich** über die Datenschutzmaßnahmen **informiert** werden. Neumitglieder werden in der **Beitrittserklärung** über den Datenschutz informiert. (Beispiel S.10)
2.3 Spender/innen: Eine Einwilligungserklärung ist **nicht notwendig**, da die Erhebung der Daten in unserem „berechtigten Interesse“ liegt, weil wir ohne diese Spenden unsere Aufgabe nicht wahrnehmen können. Namen der Spender werden nicht veröffentlicht. Auf die Möglichkeit der Löschung soll bei erneuten Anschreiben hingewiesen werden. Potentielle Neuspender sollen über die Verwendung ihrer Daten **informiert** werden.
2.4 Mitarbeiter/innen: Eine Einwilligungserklärung ist **nicht notwendig**, da die Daten zur Vertragserfüllung notwendig sind und nicht veröffentlicht werden. Allerdings ist eine Einwilligungserklärung für die Veröffentlichung von Bildern der Mitarbeiter/innen auf der Homepage **notwendig** (Formulierungsmuster hinten).
2.5 Honorarkräfte/Referentinnen: Eine Einwilligungserklärung ist **nicht notwendig**, da die Daten zur Vertragserfüllung notwendig sind und nicht veröffentlicht werden. Allerdings ist eine Einwilligungserklärung für die Veröffentlichung von Bildern oder Vorträgen auf der Homepage und anderen Publikationen **notwendig** (Muster auf S.8).

3. Verarbeitungsverzeichnis

Ein Verzeichnis für Verarbeitungstätigkeiten **muss erstellt werden.** (Verzeichnis des LV → S.6 und Vorlage für die RV auf S.7)

4. Datenschutz-Folgenabschätzung

Eine Datenschutzfolgenabschätzung ist **nicht notwendig**.
Sie wäre nur dann erforderlich, wenn die Verarbeitung ein hohes Risiko für die Rechte und Freiheiten für die betroffene Person zur Folge hat. Dies ist insbesondere dann der Fall, wenn eine umfangreiche Verarbeitung besonderer Kategorien von Daten erfolgt (z.B. Verarbeitung von Gesundheitsdaten) oder wenn systematische und umfassende Bewertungen persönlicher Aspekte vorgenommen werden. Das ist bei *donum vitae* nicht der Fall.

5. Information zum Datenschutz auf der Homepage

Neben dem Impressum muss eine **Datenschutzerklärung sichtbar** auf der Homepage sein. (Als Muster kann die Formulierung auf den Seiten des Landesverbandes dienen.)

6. Technische und organisatorisch Maßnahmen – Sicherheitsmanagement (TOM)

Es sind Maßnahmen **zum sicheren Umgang mit Daten auf den Rechnern und in Papierform** zu ergreifen und zu **dokumentieren**. (Die getroffenen Maßnahmen im Landesverband finden sich auf S. 4.)

7. Dienstleister-Vereinbarung zur Auftragsverarbeitung

Mit allen Dienstleistern, die Aufgaben für *donum vitae* erfüllen, bei denen sie mit personenbezogenen Daten umgehen bzw. Einblick in diese haben (z.B. Adressverwaltung, externe Lohnabrechnung, Steuerberater, IT-Dienstleister, Druckerei) muss ein **Auftragsverarbeitungsvertrag (AVV)** abgeschlossen werden. Es dürfen nur Auftragsverarbeiter eingesetzt werden, die eine hinreichende Garantie für eine datenschutzkonforme Datenverarbeitung gewährleisten.
Eine Formulierungshilfe für einen Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO findet sich im „Praxisratgeber Datenschutz für Vereine“ des Landesdatenschutzbeauftragten (siehe o.a. Link) und im internen Bereich des Bundesverbandes.

8. Bußgeld bei Nichteinhalten

Mit den hier gegeben Empfehlungen setzt donum vitae in Baden-Württemberg die DSGVO nach bestem Wissen um. Gegebenenfalls steht vor einer Strafe die Beratung durch den Landesdatenschutz-beauftragten.

9. Informationspflicht bei Datenpannen

Die Verletzung des Schutzes personenbezogener Daten („Datenpanne“) muss schnellstmöglich - innerhalb von 72 Stunden - gemeldet werden. Diese Meldung bei der Landesdatenschutzbehörde geschieht am einfachsten unter folgendem Link:

https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/

10. Vereinbarung innerhalb des Verbandes:

Jeder Regionalverband bestimmt eine Person, die für die Einhaltung der Datenschutzbestimmungen zuständig ist und dem Landesverband als Ansprechpartner für Datenschutz zur Verfügung steht.

Donum vitae in Baden-Württemberg muss keine Datenschutzbeauftragte benennen

Im Blick auf die Bestellung eines Datenschutzbeauftragten empfiehlt der Datenschutzbeauftragte von Baden-Württemberg in seinem Praxisratgeber „Datenschutz im Verein“ (https://www.baden-wuerttemberg.datenschutz.de/praxisratgeber-datenschutz-im-verein-nach-der-ds-gvo/) die Klärung folgender 4 Fragen:

1. **Sind mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt?**

   Das ist weder im Landesverband noch in einem Regionalverband der Fall.

2. **Nimmt der Verein Verarbeitungen vor, die einer Datenschutzfolgenabschätzung unterliegen?**

   Eine Datenschutzfolgenabschätzung ist nur erforderlich, wenn die Verarbeitung personenbezogener Daten ein hohes Risiko für die Betroffenen darstellen würde. Das ist bei unseren Klienten nicht der Fall.

3. **Liegt die Kerntätigkeit des Vereins in Verarbeitungsprozessen, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person erforderlich macht?**

   Die Kerntätigkeit von *donum vitae* liegt in der Schwangerschafts(konflikt)beratung. Die dabei in einer Beratungsstelle (mit in der Regel zwei Beraterinnen auf einer Vollzeitstelle) erhobenen Daten sind entweder anonymisiert (Konfliktberatung) oder vom Gesetz her erforderlich (z.B. Anträge bei Stiftungen). Im letzten Fall erfordern sie keine umfangreiche, regelmäßige Überwachung.
   Die Verwaltung von Daten der Beschäftigten sowie Mitglieder- und Spenderverwaltung sind nicht Teil der Kerntätigkeit sondern notwendig anfallende Nebentätigkeiten.

4. **Besteht die Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten?**

   Zur besonderen Kategorie von Daten gehören personenbezogene Daten, aus denen die rassische, ethnische Herkunft oder politische, religiöse und weltanschauliche Überzeugungen hervorgehen, sowie Daten zur Gesundheit oder zum Sexualleben.
   Die Erhebung solcher Daten in besonderen Beratungsfällen gehört allerdings nicht zur Kerntätigkeit von *donum vitae*, ohne die der Vereinszweck nicht erreicht werden könnte. Eine umfangreiche Bearbeitung oder gar systematische Bewertung solcher Daten findet nicht statt.

Die Bestellung eines **Datenschutzbeauftragten** ist bei *donum vitae* folglich **nicht notwendig** – weder für die Regionalverbände noch für den Landesverband

Dokumentation der Technischen und Organisatorischen Maßnahmen bei *donum vitae* im Landesverband Baden-Württemberg (Sicherheitskonzept)

(Stand Januar 2021)

1. **IT-Sicherheit:**
   - Überprüfung unseres IT-Systems geschah Anfang 2018 durch einen IT-Fachmann (Der Bericht von Herrn Greulich liegt in der Geschäftsstelle.)
   - Alle PC's sind mit einem Passwort geschützt
   - In der Geschäftsstelle wurde ein neuer Server angeschafft.
   - Zu den Anforderungen der IT-Sicherheit und des Datenschutzes im Homeoffice gibt es im Anhang eine separate Empfehlung (Erstellt im Jan 2021)

2. **Papierakten:**
   - Akten mit personenbezogenen Daten werden zur dauerhaften Aufbewahrung in einem abgeschlossenen Stahlschrank gelagert.
   - Die Schlüssel der Stahlschränke werden in einem verschlossenen Schlüsselkasten aufbewahrt.
   - Mitarbeiterinnen und Vorstände des RV haben Schlüssel zu diesem Schlüsselkasten und zur Beratungsstelle/Geschäftsstelle.

3. **Schlüsselliste:**
   - Die Schlüsselliste ist im Dokumentationsordner hinterlegt

4. **Telefonate:**
   - Gespräche am Telefon werde in den Geschäftsräumen ohne anderer Personen geführt

5. **E-Mails:**
   - E-Mails werden über ein gesichertes System verschickt.

6. **Mitglieder**
   - Unterlagen werden bei der Verwaltungskraft und in der Geschäftsstelle in abschließbaren Schränken aufbewahrt.

7. **Spender**
   - Unterlagen werden bei der Verwaltungskraft und in der Geschäftsstelle in abschließbaren Schränken aufbewahrt.

8. **Beschäftigte**
   - Die Personalakten werden bei der Verwaltungskraft und in der Geschäftsstelle in abschließbaren Schränken aufbewahrt.

9. **Schweigepflicht:**
   - Alle Beschäftigten werden über ihre Schweigepflicht und die Datenschutzordnung informiert und müssen die Einhaltung mit ihrer Unterschrift bestätigen. (Vorlage wird erstellt)

10. **Löschung:**
    - Löschung der Personaldaten nach 10 Jahren
    - Löschung der Mitgliederdaten nach 2 Jahren nach Beendigung der Mitgliedschaft
    - Löschung der Spenderdaten nach 2 Jahren
    - Löschung der Referentendaten nach 2 Jahren
    - Löschung der Fotos auf der Webseite unverzüglich nach dem Widerruf der Einwilligung

Verzeichnis von Verarbeitungstätigkeiten

donum vitae Landesverband Baden-Württemberg e.V.
Friedrichstraße 3
69117 Heidelberg

Tel: 06221-4340282
E-Mail: info@donumvitae-bw.de
WEB: www.donumvitae-bw.de

donum vitae
Baden-Württemberg

Verantwortlich: 1. Vorsitzende Gitta Grimm

Verarbeitungs-tätigkeit	Ansprechpartner	Datum der Einführung	Zweck der Verarbeitung	Betroffene	personen-bezogene Daten	Empfänger	Löschfristen	TOM's	Dritt-land
Lohnabrechnung Geschäftsführerin	Herr Trautmann bernhard.f.trautmann@t-online	01.10.2014	Gehaltsauszahlung	Beschäftigte	Name Adresse Rel.	ZGASt Vereinbarung zur auftragsverarbeitung	10 Jahre	siehe Anlage TOMs (Sicherheits konzept)	-
Lohnabrechnung Verwaltungskraft u. Honorarkräfte	Frau Grimm grimm@donumvitae-bw.de	2015	Gehaltsauszahlung	Beschäftigte	Name, Adresse Rel.	Minijob-Zentrale	10 Jahre	siehe Anlage TOMs (Sicherheits konzept)	-
Mitgliedschaft	Fr. Lux info@donumvitae-bw.de	2000	Verwaltung Vereinstätigkeit	Mitglieder	Name Adresse Eintrittsdatum	keine	2 J.nach Kündigung	siehe Anlage TOMs (Sicherheits konzept)	-
Spenderakquise	Frau Lux info@donumvitae-bw.de	2000	Vereinsfinanzierung	Spender	Name Adresse	keine	unverzüglich auf Wunsch	siehe Anlage TOMs (Sicherheits konzept)	-
Referenten	Fr.Traschütz-Hartmann m.traschuetz@donumvitae-hd.de	2014	Vertragserfüllung	Referent/in	Name Adresse	keine	unverzüglich auf Wunsch	siehe Anlage TOMs (Sicherheits konzept)	-
Betrieb der Webseite	Frau Grimm grimm@donumvitae-bw.de	Neu ab 2018/19	Außendarstellung	Webseiten-besucher	IP-Adresse	keine	30 Tage	siehe Anlage TOMs (Sicherheits konzept)	-
Veröffentl. Fotos	Fr.Traschütz-Hartmann m.traschuetz@donumvitae-hd.de	2018	Außendarstellung	Vorstände Geschäftsführerin Beraterinnen	Foto Name	keine	unverzüglich auf Wunsch	siehe Anlage TOMs (Sicherheits konzept)	-
Spendenverwaltung	Frau Lux info@donumvitae-bw.de	2000	Vereinsfinanzierung	Spender	Bankverbindung	Rechnungs-prüfer	10 Jahre	siehe Anlage TOMs (Sicherheits konzept)	-

Verzeichnis von Verarbeitungstätigkeiten

Vorlage für die RV zum Bearbeiten

donum vitae Regionalverband NN e.V.

Tel:
E-Mail
WEB:

Verantwortlich: 1. Vorsitzende NN

Verarbeitungs-tätigkeit	Ansprechpartner	Datum der Einführung	Zweck der Verarbeitung	Betroffene	personen-bezogene Daten	Empfänger	Löschfristen	TOM's	Dritt-land
Beratung von Klientinnen									
Lohnabrechnung Beraterinnen			Gehaltsauszahlung	Beschäftigte	Name Adresse Rel. Bankverbindung	ZGASt Vereinbarung zur Auftragsverarbeitung	10 Jahre	siehe Anlage TOMs (Sicherheits-konzept)	-
Lohnabrechnung Verwaltungskraft u. Honorarkräfte			Gehaltsauszahlung	Beschäftigte	Name, Adresse Rel. Bankverbindung	Minijob-Zentrale	10 Jahre	siehe Anlage TOMs (Sicherheits-konzept)	-
Mitgliedschaft			Verwaltung Vereinstätigkeit	Mitglieder	Name Adresse Eintrittsdatum	keine	2 J. nach Kündigung	siehe Anlage TOMs	-
Spenderakquise			Vereinsfinanzierung	Spender	Name Adresse	keine	unverzüglich auf Wunsch	siehe Anlage TOMs	-
Referenten			Vertragserfüllung	Referent/in	Name Adresse Bankverbindung	keine	unverzüglich auf Wunsch	siehe Anlage TOMs	-
Betrieb der Webseite			Außendarstellung	Webseiten-besucher	IP-Adresse	keine	30 Tage	siehe Anlage TOMs	-
Veröffentl. Fotos			Außendarstellung	Vorstände Beraterinnen	Foto Name	keine	unverzüglich auf Wunsch	siehe Anlage TOMs	-
Spendenverwaltung			Vereinsfinanzierung	Spender	Bankverbindung	Rechnungs-prüfer	10 Jahre	siehe Anlage TOMs	-

Einwilligungserklärung

für die Veröffentlichung von Fotos im Internet

Der Vorstand von donum vitae weist hiermit darauf hin, dass ausreichende technische Maßnahmen zur Gewährleistung des Datenschutzes getroffen wurden. Dennoch kann bei einer Veröffentlichung von Bildern und Daten im Internet ein umfassender Datenschutz nicht garantiert werden. Daher nimmt der/die Unterzeichnende die Risiken für eine eventuelle Persönlichkeits-rechtsverletzung zur Kenntnis und ist sich bewusst, dass:

- die personenbezogenen Daten auch in Staaten abrufbar sind, die keine der Bundesrepublik Deutschland vergleichbaren Datenschutzbestimmungen kennen,
- die Vertraulichkeit, die Integrität (Unverletzlichkeit), die Authentizität (Echtheit) und die Verfügbarkeit der personenbezogenen Daten nicht garantiert ist.

Der/die Unterzeichnende trifft die Entscheidung zur Veröffentlichung von persönlichen Fotos im Internet freiwillig und kann diese Einwilligung gegenüber dem Vorstand jederzeit widerrufen.

……

Erklärung

Ich habe das Vorstehende zur Kenntnis genommen und willige ein, dass der Verein

donum vitae

Bilder von mir zusammen mit meinem Namen auf seiner Internetseite veröffentlichen darf.

Name: …….. Vorname: ……..

Datum: …… Unterschrift: …….

INFORMATIONEN ZUM DATENSCHUTZ

Nach der EU-Datenschutz-Grundverordnung (DS-GVO) sind wir verpflichtet, Sie darüber zu informieren, zu welchem Zweck unsere Beratungsstelle Daten erhebt, speichert oder weiterleitet.

1. WAS BEDEUTET DIE SCHWEIGEPFLICHT UNSERER BERATERINNEN?

Unsere Beraterinnen haben über das, was Sie ihnen im Beratungsgespräch anvertrauen, zu schweigen. Diese Schweigepflicht zählt zum Kernbereich der Berufsethik einer Beraterin. Sie gilt grundsätzlich gegenüber Dritten, auch gegenüber Ihren Familienangehörigen.

2. WELCHE DATEN WERDEN VON UNS ERHOBEN?

Je nach Beratungsanlass erheben wir folgende Daten: Name, Vorname, Anschrift, Telefonnummer, Alter, Geschlecht, Familienstand, Beruf, Schwangerschaftsdaten (Schwangerschaftswoche, Entbindungstermin). Weitere personenbezogene Daten sind im Einzelfall notwendig und deren Angabe ist freiwillig.

3. WARUM ERHEBEN WIR DIESE DATEN?

Die Datenverarbeitung erfolgt aufgrund gesetzlicher Vorgaben (SchKG), um Ihre Situation analysieren zu können und Sie bei der Durchsetzung Ihrer Rechte zu unterstützen.

4. AN WEN GEHEN DIESE DATEN?

Wir übermitteln Ihre personenbezogenen Daten nur dann an Dritte, wenn dies gesetzlich erlaubt ist oder wenn Sie eingewilligt haben. Empfänger dieser Daten können z.B. Stiftungen, Familienkassen, Ämter sein. In anonymisierter Form erfassen wir die erhobenen Daten auch in verschiedenen Statistiken, z.B. für das Regierungspräsidium oder zu vereinsinternen Auswertungen.

5. WERDEN DIE DATEN GESPEICHERT?

Wir bewahren Ihre personenbezogenen Daten nur solange auf, wie dies durch die Verwaltungsvorschrift des Ministeriums vorgegeben ist.

Aufgrund rechtlicher Vorgaben sind wir dazu verpflichtet, diese Daten nach fünf Jahren zu löschen.

6. WELCHE RECHTE HABEN SIE ALS BETROFFENE?

Sie haben das Recht, über die Sie betreffenden Daten Auskunft zu erhalten. Auch können Sie die Berichtigung unrichtiger Daten verlangen.

Darüber hinaus steht Ihnen das Recht auf Löschung von Daten, das Recht auf Einschränkung der Datenverarbeitung sowie das Recht auf Datenübertragbarkeit zu.

Die Verarbeitung Ihrer Daten erfolgt auf Basis von gesetzlichen Regelungen (SchKG). Nur in Ausnahmefällen benötigen wir Ihr Einverständnis. In diesen Fällen haben Sie das Recht, die Einwilligung für die zukünftige Verarbeitung zu widerrufen.

Sollten Sie den Eindruck haben, dass die Verarbeitung Ihrer personenbezogenen Daten nicht rechtmäßig erfolgt, haben Sie das Recht, sich an die zuständige Aufsichtsbehörde für den Datenschutz zu wenden.

7. VERANTWORTLICH FÜR DIE DATENVERARBEITUNG in unserer Beratungsstelle ist:

Name:

Adresse:

Mail:

Beitrittserklärung

Hiermit erkläre ich meinen Beitritt als Mitglied im Landesverband
„*donum vitae* in Baden-Württemberg e.V.“

Bitte in Druckbuchstaben ausfüllen:

Name: ……

Vorname: ……

Titel ……

Adresse: ……

PLZ, Ort: ……

Email: ……

Tel. ……

Wir freuen uns, dass Sie die Arbeit von *donum vitae* mit Ihrer Mitgliedschaft unterstützen. Vielen Dank!
donum vitae nutzt die in dieser Beitrittserklärung erhobenen Daten zum Zwecke der Mitgliederverwaltung, des Beitragseinzuges und zur Übermittlung von Vereinsinformationen. Eine Weitergabe an Dritte außerhalb des Vereins findet nicht statt. Bei Beendigung der Mitgliedschaft werden Ihre Daten gelöscht, soweit sie nicht entsprechend der gesetzlichen Vorgaben aufbewahrt werden müssen. Selbstverständlich geben wir Ihnen jederzeit Auskunft über Ihre bei *donum vitae* gespeicherten personenbezogenen Daten.

Die Mitgliedschaft bei *donum vitae* ist kostenlos. Ihre Spende hilft uns natürlich sehr.

☐ Bitte buchen Sie eine jährliche / monatliche Spende in Höhe von …… € von folgendem Konto ab:

Inhaber ……

Kreditinstitut ……

IBAN

BIC (falls bekannt) ……

Ort ……

Datum …… Unterschrift ……

Datenschutz im Homeoffice

1. Arbeitsumgebung

- Bei der Arbeit zu Hause ist die Umgebung so zu wählen, dass vom Grundsatz her die Vertraulichkeit, Verfügbarkeit und Sicherheit der Daten wie im Büro sichergestellt ist.
- Der Arbeitsplatz ist so gewählt, dass Familienmitglieder oder Besucher keinen Blick auf das Notebook oder in die Papierunterlagen werfen können.
- Es werden Sichtschutzfolien für den PC angeboten.
- Papierunterlagen werden in Dokumentenmappen oder Schränken verschlossen.
- Fenster in Erdgeschosswohnungen werden bei Verlassen des Arbeitsplatzes immer geschlossen.
- Bei Verlassen des Arbeitsplatzes muss der Zugriff durch Andere (z. B. Kinder, Katze) ausgeschlossen werden. (Sperrung des Notebooks).
- Es wird darauf geachtet, dass Telefongespräche nicht von unbefugten Personen mitgehört werden (z. B. Familienangehörige, offenes Fenster, laufende andere Videokonferenz, …)
- Es gilt eine Clean-Desk-Policy am Ende des Arbeitstages.

2. Genutzte Hardware

- Die Bereitstellung von dienstlichen Geräten (Notebook und Smartphone) wird empfohlen. Privatgeräte können nur ausnahmsweise und nur mit einem kostenpflichtigen Antivirenprogramm eingesetzt werden.
- Drucken von Dokumenten ist auf/über private Geräte nicht erlaubt.
- Dienstlich zur Verfügung gestellte Geräte werden nicht für private Zwecke genutzt.

3. Umgang mit Papierdokumenten

- Papierunterlagen werden in geeigneten Mappen (mit Namen der Einrichtung im Falle eines Verlusts und möglichst verschließbar) mit nach Hause genommen.
- Beim Transport von Papierunterlagen werden erhöhte Risikosituationen (z. B. Rücksitz beim Einkaufen, Rucksack im Restaurant, …) vermieden.
- Die Entsorgung erfolgt nicht über den Hausmüll, sondern entweder im Büro oder zu Hause durch einen Aktenvernichter mit mind. Sicherheitsstufe 5 (nach DIN 66399)
- Um die Risiken der Schädigung von wichtigen Papierdokumenten (z. B. Kinder bemalen ein Originaldokument) zu vermeiden, wird bei solchen Dokumenten sofern möglich mit Kopien gearbeitet.
- Empfohlen wird die Nutzung von eAkten, auf die über einen VPN-Zugang auf dem Server der Einrichtung zugegriffen werden kann.

4. **Sicherheit**

- Die Sicherheitsrisiken im Homeoffice erhöhen sich durch die Anbindung an das Internet.
- Die Anbindung an das Netzwerk in der Beratungsstelle geschieht nur mit verschlüsselten VPN-Verbindungen nach Stand der Technik
- Der Zugriff wird nur auf für das Homeoffice erforderliche Server, Dateiablagen und Anwendungen durch die VPN-Verbindung erlaubt.
- Das heimischen Wi-Fi ist mit einem starken Passwort geschützt.
  Öffentliche Wi-Fi-Hotspots werden nicht genutzt.
- Die Softwareaktualisierung, insbesondere des Antivirenprogramms, geschieht automatisch.
- Dienstlichen Smartphones sind durch eine Pin-Sperre geschützt.

Im Folgenden noch einige Stichworte zur Nutzung von Video-Tools:

5. **Video-Beratungs-Tools**

- Ausschließlich über CGM-ELVI gesicherte Beratung
- Am besten über Kopfhörer/Head-Set
- Im ungestörten Raum ohne Einsicht Dritter oder Zuhörer*innen
- Neutraler Hintergrund

6. **Videokonferenzsystemen**

- Zugangsschutz zu Konferenzräumen über Passwörter oder individuelle Einladungslinks
- Keine Aufzeichnung oder sonstige Auswertung der Inhalte durch den Anbieter (z.B. zum Zweck der Qualitätsverbesserung)
- Konfigurationsmöglichkeiten bei Erhebung von Telemetriedaten durch den Anbieter (Empfehlung: Deaktivierung)
- Keine Aufzeichnung der Videokonferenz durch die Einrichtung
- Neutraler oder unscharfer Hintergrund der Nutzer
- Nutzung eines virtuellen Warteraumes, in dem Teilnehmer bis zu Beginn der Konferenz ohne Audio-/Video-übertragung warten können

Quelle zu großen Teilen: Datenschutzrechtliche Regelungen bei Homeoffice, Best-Practice-Prüfkriterien, Bayerisches Landesamt für Datenschutzaufsicht

Versicherung im Homeoffice

Weiterführende Informationen findet man in einem Flyer „10 Tipps zur Pandemieplanung“ der Deutschen Gesetzlichen Unfallversicherung: https://publikationen.dguv.de/widgets/pdf/download/article/2054 .

Auf der Seite der **Bundeszentrale für gesundheitliche Aufklärung** gibt es folgende Anregungen für die Mitarbeiterinnen: https://www.infektionsschutz.de/coronavirus/verhaltensregeln.html#c12132

- Arbeiten Sie – in Abstimmung mit dem Arbeitgeber – wenn möglich, von zu Hause aus.
- Treffen Sie Absprachen möglichst per E-Mail oder Telefon. Nutzen Sie nach Möglichkeit Telefon- oder Videokonferenzen für den Austausch in der Gruppe. Zwingend erforderliche Treffen sollten möglichst kurz und mit wenigen Personen in einem gut belüfteten Raum abgehalten werden. Halten Sie einen Abstand von mindestens 1,5 Metern ein und verzichten Sie auf Berührungen wie z. B. Begrüßung durch Händeschütteln.
- Organisieren Sie Ihre Arbeitsabläufe so, dass Sie möglichst wenig direkten Kontakt zu Ihren Kolleginnen und Kollegen haben, auch in den Pausen.
- Arbeiten Sie, wenn möglich, einzeln oder in kleinen festen Teams (z. B. im Büro oder auf Baustellen).
- Teilen Sie Arbeitsplätze oder Gegenstände (z. B. Tastaturen, Werkzeuge) möglichst nicht mit anderen Personen. Ist dies nicht möglich, reinigen Sie Ihren Arbeitsplatz gründlich und insbesondere beim Verlassen oder bei Dienstantritt. Außerhalb des Gesundheitswesens und der häuslichen Pflege genügt hierzu die Verwendung handelsüblicher Haushaltsreiniger. Im Einzelfall kann eine Desinfektion erforderlich sein, wenn z. B. der Arbeitsplatz von einer erkrankten Person genutzt wurde.
- Nehmen Sie Ihre Mahlzeiten möglichst allein (z. B. im Büro) ein. Wenn Sie Pausenräume oder die Kantine nutzen, halten Sie ausreichenden Abstand zu Kolleginnen und Kollegen.
- Bleiben Sie zu Hause, wenn Sie krank sind, und kurieren Sie sich aus!

Heidelberg, 28.01.2021 Tra/Gm

donum vitae

Datenerhebung zur **Nachverfolgung**
im Falle einer
Erkrankung an Covid-19

Termin am: **um:**

Beraterin: **Dolmetscherin:**

	KlientIn	**Begleitung**
Name		
Vorname		
Telefon/ Handy		
e-mail		

Ich/wir sind damit einverstanden, dass im Falle einer Erkrankung einer Mitarbeiterin der Beratungsstelle an Covid-19 meine Daten zur Nachverfolgung an das Gesundheitsamt weitergegeben werden dürfen. Diese Einverständniserklärung wird nach 2 Wochen vernichtet.

……

Datum Ort Unterschrift

……

Datum Ort Unterschrift

Arbeitsanweisung IT-Sicherheit, Mitwirkung der Anwender
donum vitae NN e.V.

Vorbemerkung: Da die bei donum vitae Beschäftigten überwiegend weiblich sind, verwenden wir hier die weibliche Formulierung und schließen die männliche mit ein.

1. Ziel/Zweck

„Sicherheit kann man nicht einfach mal installieren, Sicherheit muss von uns allen praktiziert werden.“ Dieses Grundprinzip der IT-Sicherheit zielt direkt auf die Mitwirkung der Anwenderinnen von Informations- und Kommunikationstechnik.

Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit. Um dies zu verhindern, ist der sorgfältigen Umgang mit der IT unabdingbar. Es ist die persönliche Verpflichtung jeder Einzelnen, die im Folgenden beschriebenen Grundlagen zu berücksichtigen und bei der täglichen Arbeit im eigenen Verantwortungsbereich umzusetzen.

Der Mitarbeiter muss über den Wert und die Bedeutung von Informationen in seinem Arbeitsgebiet informiert sein.

Der Mitarbeiter muss Informationen so schützen, dass

- die Vertraulichkeit in angemessener Form gewahrt ist,
- die Integrität, d.h. die Korrektheit, Manipulationsfreiheit und Unversehrtheit der Informationen sichergestellt ist,
- Informationen bei Bedarf verfügbar sind,
- die Beteiligung an einer Transaktion nachvollziehbar ist und
- gesetzliche, vertragliche oder aufsichtsrechtliche Verpflichtungen erfüllt werden.

Die Anwenderin ist als Erzeugerin von Daten für die ordnungsgemäße Einstufung der Daten hinsichtlich ihrer Schutzwürdigkeit verantwortlich.

2. Anwendungsbereich und Zuständigkeit

Für die Einhaltung dieser Arbeitsanweisung sind alle Mitarbeiterinnen von *donum vitae* NN. verantwortlich. Dies wird durch die Leitung der Beratungsstelle sichergestellt und durch die einmal jährliche Unterweisung dieser Inhalte mit Bestätigung der Teilnehmerinnen durch Unterschrift und Ablage in der Personalakte dokumentiert.

Diese Arbeitsanweisung ist Teil der allgemeinen arbeitsvertraglichen Sorgfalts- und Datenschutzpflicht und präzisiert diese im Umgang mit IT-Daten und anderem.

Es wird ausdrücklich darauf hingewiesen, dass Mitarbeiterinnen, welche gegen diese Regeln verstoßen, in Regress genommen werden können, arbeitsrechtliche Schritte gegen sie eingeleitet werden können oder auch, je nach Schwere des Falls, strafrechtlich vorgegangen werden kann.

3. Anmeldung am System / Zugang zum System

Der Zugang zum System ist durch Passwort zu schützen. Das System ist nur dann zu aktivieren, wenn damit gearbeitet wird. Das System ist unmittelbar nach Gebrauch vor unberechtigtem Zugriff zu schützen, insbesondere auch beim Verlassen des Raumes. Ein geeigneter Bildschirmschoner mit Passwort ist einzurichten. Die Passwörter sind gemäß der Vorgaben für sichere Passwörter (mind. 8 Stellen, Groß- und Kleinschreibung, Ziffern, Buchstaben und Sonderzeichen) von den Mitarbeitern festzulegen und dürfen weder irgendwo hinterlegt noch jemand anderem (auch keinen KollegInnen oder jemandem vom Vorstand) ausgehändigt werden.

4. Speicherung und Aufbewahrung

Als Dateneigner ist die Mitarbeiterin für die Speicherung der von ihr verarbeiteten Daten und deren Aufbewahrung verantwortlich. Dabei muss folgendes beachtet werden:

- Unbefugte Kenntnisnahme gespeicherter Daten muss vermieden werden (welche Daten in Gemeinschafts-Laufwerk, welche Daten in persönliches Laufwerk speichern, Bildschirmschoner).
- Unautorisierte Veränderung von gespeicherten Daten darf nicht ermöglicht werden (keine Weitergabe Passwort).
- Vom Speicherort (Server) müssen regelmäßig Sicherungskopien erstellt, sicher verwahrt und abwechselnd außerhalb der Beratungsstelle gelagert werden.
- Es ist nicht erlaubt Daten auf lokale oder externe Datenträger zu speichern, außer auf den eingerichteten Laufwerken.
- Wegen der Gefahr des Eintrags von Viren, ist es nicht erlaubt externe Datenträger (Datenstick, externe Festplatten, etc.) an die Rechner von *donum vitae* anzuschließen.
- Gesetzliche Aufbewahrungsfristen müssen eingehalten werden.

5. Umgang mit personenbezogenen Daten

Personenbezogene Daten unterliegen u.a. den Sicherheits- und Schutzvorschriften des Bundesdatenschutzgesetzes (BGSG) und des Telekommunikationsgesetzes (TKG). Bei *donum vitae* NN. e.V. gibt es folgende Kategorien von personenbezogenen Daten:

a. Klientendaten
b. Mitarbeiterdaten
c. Mitglieder bzw. Spenderdaten

Die Verarbeitung, Speicherung und Übermittlung bzw. Nutzung dieser personenbezogenen Daten ist in der Datenschutz-Richtlinie von *donum vitae* NN. geregelt.

6. Nutzung der IT-Ausstattung von *donum vitae* für private Zwecke

Aus Sicherheitsgründen ist es untersagt, Hard- oder Software oder die E-Mail-Adresse oder den Internetzugang etc. von *donum vitae* NN. e.V. für private Zwecke zu nutzen – weder während noch außerhalb der Arbeitszeit.

Im Umkehrschluss dürfen Beratungsstellen-Belange ausschließlich über die dienstliche E-Mailadresse von donum vitae und die Beratungsstellen-Hardware bearbeitet werden. Eine Weiterleitung von E-Mail-mails auf andere Adressen, ein Abruf der E-Mails auf anderer Hardware oder ähnliches ist verboten.

7. Weiterleitung/Übertragung von Informationen

Eine Weiterleitung von Informationen von Berechtigten an Unberechtigte ist untersagt. Dies betrifft sowohl die direkte Weitergabe per Datenträger, E-Mail oder die Bereitstellung in Datenverzeichnissen als auch die Ermöglichung eines unberechtigten Zugriffs. Die Mitarbeiterin hat die Wahl der geeigneten, autorisierten Übertragungseinrichtung gemäß Schutzbedarfsanforderung sicherzustellen.

Insbesondere für die Übertragung von personenbezogenen Daten gilt, dass diese nur verschlüsselt erfolgen darf (siehe IT-Sicherheitskonzept Nr. 5).

Dienstleister bzw. Kooperationspartner, sowie Ehrenamtliche/Vorstandsmitglieder, die Einblick in personenbezogene Daten bekommen, müssen eine Vertraulichkeitsvereinbarung unterzeichnen, bevor Informationen übermittelt bzw. Zugriffe eingeräumt werden.

8. Zugriff auf Informationen

Jede Mitarbeiterin hat bei den Vorkehrungen gegen unbefugte Kenntnisnahme erzeugter Daten mitzuwirken. Es gelten folgende Sicherheitsgrundsätze:

a. Kenntnis nur wenn nötig.
b. Schutzwürdiges mindestens wie persönliches Gut sichern.
c. Keine unnötigen Gespräche über Beratungsstellen-Belange mit Externen.
d. Hinreichender Verschluss von Unterlagen und Gegenständen.
e. Keine Überlassung von Unterlagen, Daten oder Gegenständen an Unbefugte.
f. Kein unbefugtes Vervielfältigen.
g. Nicht mehr benötigte Daten und Informationen müssen so vernichtet werden, dass deren Inhalt nicht mehr rekonstruierbar ist.
h. Keine Ausdrucke am Papierkorb oder Kopiergerät zurücklassen.
i. E-Mails mit zweifelhaftem Inhalt oder von zweifelhaftem Absender dürfen nicht geöffnet werden bzw. müssen umgehend gelöscht werden.
j. Am Telefon dürfen gegenüber nicht bekannten Personen keine Auskünfte erteilt werden (social engineering).

9. Hard- und Softwarekonfiguration

Für die Übertragung von Daten nutzt jede Mitarbeiterin nur zugelassene Übertragungsverfahren, die von autorisierten Personen implementiert sind. Es ist verboten, Systemeinstellungen zu verändern oder Software zu installieren. Veränderungen der Hard- oder Softwarekonfiguration ist nur den vom Vorstand dazu autorisierten Personen/Firmen erlaubt.

Nur lizenzierte Software darf verwendet werden. Die Lizenzen sind zum jederzeitigen Nachweis in einem dafür bestimmten Ordner aufzubewahren.

10. Meldepflicht

Jede Mitarbeiterin hat die Pflicht, sicherheitsrelevante Zwischenfälle unverzüglich an den/die 1. bzw. 2. Vorsitzende/n zu melden. Jeder Verdacht der Datenmanipulation, des Datendiebstahls, einer Infizierung oder anderer Unregelmäßigkeiten ist unverzüglich zu melden.

Anlagen

IT-Sicherheitskonzept *donum vitae* NN. e.V.
Datenschutz-Richtlinie *donum vitae* NN. e.V.

Stand: Februar 2021

Schweigepflichtsentbindung

Hiermit beauftrage ich Frau……., Beraterin bei der Schwangerschafts-beratungsstelle *donum vitae* Regionalverband ……e.V., mich bei meinen sozialen Angelegenheiten zu unterstützen und zu vertreten bei folgender Einrichtung:

Einrichtung	**Angelegenheit**
Jugendamt	
Sozialamt	
Familienkasse	
BAföG-Amt	
Agentur für Arbeit/Jobcenter	
Arbeitgeber/Ausbildungsplatz/Schule	
Rechtsanwalt/-anwältin	
Arzt/Ärztin	
Sonstige	

Ich entbinde Frau ……..von der Schweigepflicht. Sie ist berechtigt, bei den entsprechenden Einrichtungen Auskünfte über meine Angelegenheiten einzuholen und Einsicht in diesbezügliche Akten zu nehmen.

Ich entbinde das Amt/die Einrichtung von den datenschutzrechtlichen Bestimmungen der Geheimhaltung von personenbezogenen Daten.

Ich bin darüber informiert, dass ich diese Erklärung jederzeit widerrufen oder beschränken kann.

Name (Druckschrift): geboren am:

Ort, Datum: Unterschrift:

donum vitae
beraten – schützen – weiterhelfen
staatlich anerkannte Schwangerschaftskonfliktberatungsstelle

Schweigepflichtentbindung

Release from confidentiality / Dégagement de l'obligation de garder le secrect / Mahremiyet Kuralından Feragat / Lirimi nga detyra për mbajtjen e sekretit / Освобождение от запрета на разглашение конфиденциальной информации

Ich / I / Je soussigné(e) / Ben / Unë / Я

Name / Name / Nom / Soyadı / Mbiemri / Фамилия .....

Vorname / First Name / Prénom / Adı / Emri / Имя .....

Geburtsdatum / Date of birth / Date de naissance / Doğum tarihi / Datëlindja / Дата рождения .....

Adresse / Address / Adresse / Adres / Adresa / **Адрес** .....

entbinde die Beraterin, Frau / hereby release counsellor, Mrs / délie la conseillière Mme./ Danışman… Hanım'ın / e liroj konsultenten, znj. / освобождаю консультанта, госпожу

.....

von der Schweigepflicht gegenüber folgender Person /Institution / from her duty of confidentiality in relation to the following person/institution / de son obligation de garder le secrect envers la personne/institution suivante / uymakla yükümlü olduğu mahremiyet kuralının aşağıdaki kişiyle/ kurumla olan görüşmelerinde kaldırılmasını talep ediyorum / nga detyra për mbajtjen e sekretit në lidhje me këtë person/institucion / от запрета на разглашение конфиденциальной информации в отношении следующего лица /учреждения

.....

und stimme zu, dass sich die o. g. Personen über meine persönliche, familiäre und finanzielle Situation in folgender Fragestellung austauschen dürfen / and consent to the above-named persons exchanging information regarding my personal, family and financial situation in the following matter / et j'approuve que les personnes mentionnées ci-dessus peuvent s'échanger sur les sujets actuels suivants concernant ma situation personnelle, famillliale et financière / ve yukarıda adı geçen kişilerle aşağıdaki konuları görüşürken şahsi, ailevi ve maddi durumuma dair bilgileri paylaşmasına izin veriyorum / dhe jam dakord, që personat e lartshënuar të shkëmbejnë informacione rreth situatës sime personale, familjare dhe financiare lidhur me temën si vijon / и соглашаюсь с тем, что вышеупомянутые лица имеют право на обмен информацией относительно моей личной, семейной и финансовой ситуации в связи с данной проблематикой

.....

.....

um die bestmögliche Unterstützung für mich und meine Familie zu ermitteln / in order to identify the best-possible support for me and for my family / afin de trouver le soutien optimal pour moi et ma famille / Bunu bana ve aileme en iyi desteği sağlayabilmek için yaptıklarını biliyorum / për të gjetur përkrahjen më të mirë për mua dhe familjen time / с целью предоставления наилучшей поддержки мне и моей семье.

Diese Einwilligungserklärung zu Weitergabe von Informationen und zum Austausch der Fachkräfte kann ich jederzeit mit Wirkung für die Zukunft widerrufen / I can revoke at any time for the future this declaration of consent to the disclosure and exchange of information between qualified personnel / Je peux, à tout moment pour l'avenir, révoquer cette déclaration de consentement pour la divulgation de renseignements et pour l'échange des professionnels qualifiés sur ma situation / Uzmanların kendi aralarında durumumu görüşebilmeleri için verdiğim bu izni istediğim zaman geri alabilirim / Unë mund ta anulojë në çdo kohë këtë deklaratë miratimi për dhënie dhe shkëmbim informacionesh të specialistëve me efekt për të ardhmen / Данное заявление о согласии относительно передачи и обмена информацией специалистами я могу отозвать в любое время, с этого момента разглашение конфиденциальной информации не допускается.

.....

Datum, Unterschrift / Date, signature / Date, Signature / Tarih, imza / Data, nënshkrimi / Дата, подпись

Verpflichtung zur Wahrung der Vertraulichkeit, zur Beachtung des Datenschutzes sowie ggf. zur Wahrung von Berufs- bzw. Privatgeheimnissen

Im Rahmen Ihrer Tätigkeit für *donum vitae* kommen Sie möglicherweise mit personenbezogenen Daten in Kontakt und sind deshalb zur **Beachtung des Datenschutzes**, insbesondere zur **Wahrung der Vertraulichkeit** verpflichtet.

Personenbezogene Daten dürfen Sie nur auf Anweisung und unter Beachtung der datenschutzrechtlichen Vorgaben und Weisungen von *donum vitae* verarbeiten.

> Unter einer **Verarbeitung** versteht die EU-Datenschutz-Grundverordnung (DSGVO) jeden Vorgang 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 - unabhängig davon, ob die Verarbeitung mit oder ohne Hilfe automatisierter Verfahren ausgeführt wird.
>
> **„Personenbezogene Daten“** im Sinne der DSGVO sind alle Informationen, die sich auf einen identifizierbaren Menschen beziehen; als identifizierbar wird ein Mensch angesehen, der 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 seiner physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Über **interne Angelegenheiten** von *donum vitae,* beispielsweise Personalvorgänge, Geschäftsvorgänge, Zahlen des internen Rechnungswesens und alle weiteren als Geschäftsgeheimnisse zu definierenden Vorgänge ist von Ihnen **Verschwiegenheit** zu wahren. Alle elektronischen oder schriftlichen Unterlagen über solche internen Vorgänge, die Ihnen überlassen oder von Ihnen angefertigt werden, sind vor Einsichtnahme Unbefugter zu schützen.

Im Rahmen Ihrer Tätigkeiten kommen Sie möglicherweise auch mit „**Privatgeheimnissen**“ in Kontakt.

> Dies sind Informationen, die uns im Rahmen unserer Beratungstätigkeit anvertraut werden und an deren Geheimhaltung der Betroffene ein sachliches Interesse hat.

Unabhängig von der vorgenannten datenschutzrechtlichen Verpflichtung haben Sie über diese Informationen strikte **Verschwiegenheit** zu wahren.

Ihre Verpflichtung besteht ohne zeitliche Begrenzung und **auch nach Beendigung Ihrer Tätigkeit** fort.

Über die Verpflichtung auf das Datengeheimnis und die sich daraus ergebenden Verhaltensweisen wurde ich unterrichtet. Das Merkblatt zur Verschwiegenheitserklärung mit dem Abdruck der hier genannten Vorschriften habe ich erhalten.

Ort, Datum Unterschrift des Verpflichtetetn

Art. 4 DSGVO Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

1. „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;
2. „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;

Vorschriften zum GeschGehG

§ 2 GeschGehG - Begriffsbestimmungen

Im Sinne dieses Gesetzes ist Geschäftsgeheimnis eine Information

a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht;

(…)

§ 4 GeschGehG - Handlungsverbote

(1) Ein Geschäftsgeheimnis darf nicht erlangt werden durch

1. unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, oder
2. jedes sonstige Verhalten, dass unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht.

(2) Ein Geschäftsgeheimnis darf nicht nutzen oder offenlegen, wer

1. das Geschäftsgeheimnis durch eine eigene Handlung nach Absatz 1
   a) Nummer 1 oder
   b) Nummer 2

   erlangt hat,
2. gegen eine Verpflichtung zur Beschränkung der Nutzung des Geschäftsgeheimnisses verstößt oder
3. gegen eine Verpflichtung verstößt, das Geschäftsgeheimnis nicht offenzulegen.

(3) Ein Geschäftsgeheimnis darf nicht erlangen, nutzen oder offenlegen, wer das Geschäftsgeheimnis über eine andere Person erlangt hat und zum Zeitpunkt der Erlangung, Nutzung oder Offenlegung weiß oder wissen müsste, dass diese das Geschäftsgeheimnis entgegen Absatz 2 genutzt oder offengelegt hat. Das gilt insbesondere, wenn die Nutzung in der Herstellung, dem Anbieten, dem Inverkehrbringen oder der Einfuhr, der Ausfuhr oder der Lagerung für diese Zwecke von rechtsverletzenden Produkten besteht.

§ 23 GeschGehG - Verletzung von Geschäftsgeheimnissen

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen,

1. entgegen § 4 Absatz 1 Nummer 1 ein Geschäftsgeheimnis erlangt,
2. entgegen § 4 Absatz 2 Nummer 1 Buchstabe a ein Geschäftsgeheimnis nutzt oder offenlegt oder
3. entgegen § 4 Absatz 2 Nummer 3 als eine bei einem Unternehmen beschäftigte Person ein Geschäftsgeheimnis, das ihr im Rahmen des Beschäftigungsverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Beschäftigungsverhältnisses offenlegt

(2) Ebenso wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, ein Geschäftsgeheimnis nutzt oder offenlegt, das er durch eine fremde Handlung nach Absatz 1 Nummer 2 oder Nummer 3 erlangt hat.

(3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz entgegen § 4 Absatz 2 Nummer 2 oder Nummer 3 ein Geschäftsgeheimnis, das eine ihm im geschäftlichen Verkehr anvertraute geheime Vorlage oder Vorschrift technischer Art ist, nutzt oder offenlegt.

(4) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer

1. in den Fällen des Ansatzes 1 oder des Absatzes 2 gewerbsmäßig handelt,
2. in den Fällen des Absatzes 1 Nummer 2 oder Nummer 3oder des Absatzes 2 bei der Offenlegung weiß, dass das Geschäftsgeheimnis im Ausland genutzt werden soll, oder
3. in den Fällen des Absatzes 1 Nummer 2 oder des Absatzes 2 das Geschäftsgeheimnis im Ausland nutzt.

(5) Der Versuch ist strafbar.

(6) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geschäftsgeheimnisses beschränken.

(7) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend. Die §§ 30 und 31 des Strafgesetzbuches gelten entsprechend, wenn der Täter zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz handelt.

(8) 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.

Strafvorschriften des § 42 BDSG

(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 allgemein zugänglich sind,

3. ohne hierzu berechtigt zu sein, verarbeitet oder
4. 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.

Strafgesetzbuch (StGB) § 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlussprüfung,
3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten oder Organ oder Mitglied eines Organs einer Rechtsanwalts-, Patentanwalts-, Wirtschaftsprüfungs-, Buchprüfungs- oder Steuerberatungsgesellschaft,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,
5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes,
6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder
7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,
4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,
5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder
6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufgaben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) (weggefallen)

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Beauftragter für den Datenschutz bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,
2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.