



Erklärung zum Einhalten der Datenschutzbestimmungen im Rahmen der Aus- und Weiterbildung an der Berliner FortbildungsAkademie (BFA)

I. Gesetzliche Bestimmungen bei personenbezogenen Daten

Folgende Gesetze und Verordnungen regeln, was im Umgang mit Daten von Patient*innen beachtet werden muss:

- Europäische Datenschutzgrundverordnung (EU-DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- Berliner Datenschutzgesetz (BlnDSG)
- Berufsordnung (BerufsO), insbesondere § 10 der PTK Berlin

Relevante Auszüge für Ihre ambulante Tätigkeit:

Schweigepflicht

„Psychotherapeutinnen und Psychotherapeuten sind zur Verschwiegenheit über Behandlungsverhältnisse verpflichtet und über das, was Ihnen im Zusammenhang ihrer beruflichen Tätigkeit über Patientinnen und Patienten oder Dritte anvertraut und bekannt geworden ist.“
Berufsordnung § 8 Absatz 1

„Im Rahmen kollegialer Beratung, Intervention, Supervision oder zum Zwecke der wissenschaftlichen Forschung und Lehre dürfen Informationen über Patientinnen und Patienten oder Dritte nur in anonymisierter Form im Sinne des Bundesdatenschutzgesetzes verwendet werden. Die Anonymisierung muss sicherstellen, dass keine Rückschlüsse auf die Person möglich sind [...].“ *Berufsordnung § 8 Abs. 6*

Datensicherheit

„Psychotherapeutinnen und Psychotherapeuten haben in ihrem Verantwortungsbereich sicherzustellen, dass erhobene Daten und persönliche Aufzeichnungen sicher verwahrt werden und gegenüber Zugriffen Dritter umfassend geschützt sind [...].“ *Berufsordnung § 10, Absatz 1*

Die vollständigen Datenschutzbestimmungen sowie die Berufsordnung finden Sie unter

- <https://dsgvo-gesetz.de>
- www.gesetze-im-internet.de/bdsg
- www.gesetze.berlin.de
- www.psychotherapeutenkammer-berlin.de

II. Verbindliche Regelungen für den Umgang mit Daten

Auf Grundlage der gesetzlichen Regelungen ist verbindlich einzuhalten:

1. Keine Weitergabe von Informationen, die eine Person eindeutig identifizieren

- a. Jede Weitergabe von Informationen, die eine Person identifizieren, ist ohne Schweigepflichtentbindung für diesen Zweck untersagt. Solche Informationen können auch sein „Leiterin von Firma XY“ oder „Schauspieler bei Serie Z“. Die Schweigepflicht gilt über den Tod des/der Patient*in hinaus.

2. Dokumentationen werden konsequent anonymisiert

- a. In Stundenprotokolle werden keine Nachnamen oder sonstige Hinweise verwendet, die eine einfache Zuordnung zu einer Person erlauben. Stundenprotokolle werden nur unter der sog. "Laufenden Nummer" (LfdNr.) abgelegt bzw. gespeichert.
- b. Punkt a) gilt auch für Fallberichte, Supervisionsprotokolle.
- c. Bei Berichten an den Gutachter gilt ebenfalls das unter a) Geschriebene. Die Chiffre (1. Buchstabe Nachname und Geburtsdatum), die grundsätzlich einen Hinweis auf die Identifikation einer Person darstellt, wird vor dem Versenden an die Krankenkasse von den Mitarbeiter*innen der BFA dem Formular zugefügt.

3. Keine offen einsehbaren Akten im Therapieraum

- a. Weil Therapieräume nicht abgeschlossen werden können, dürfen Akten nicht offen im Therapieraum liegen. Sie sind zu schützen vor der Einsichtnahme Dritter, also auch vor Kolleg*innen oder anderen Patient*innen.

4. Schweigepflichtsentbindung einholen

- a. Schriftliche Schweigepflichtsentbindungen sind einzuholen, sofern eine Kommunikation mit Dritten erforderlich ist. Dies gilt auch, wenn der/die Patient*in ausdrücklich eine Kommunikation mit Dritten wünscht (z.B. Ärzt*innen, Rentenversicherung etc.).

5. Keine unbefugte Einsichtnahme in Akten Dritter

- a. Untersagt ist eine unbefugte Einsichtnahme in Dokumente, Akten und EDV von Patient*innen Dritter, für die keine Schweigepflichtentbindung oder eine Behandlungsbeteiligung besteht. Damit eingeschlossen ist die vorsätzliche Einsicht in Akten anderer Therapeut*innen oder Einträge anderer Therapeut*innen in der Elefant-Software.

6. Entsorgung von sensiblen Daten nur über entsprechende Container

- a. Die Entsorgung von Testunterlagen und Berichten darf ausschließlich über einen Container erfolgen, dessen Inhalt von einer zertifizierten Firma regelmäßig datensicher geschreddert wird. Ein solcher Container steht in unmittelbarer Nähe des Kopierers in der Schloßstraße. Unsere Mitarbeiter*innen nehmen ebenfalls zu schreddernde Akten an.

7. Keine Mitnahme von Akten

- a. Grundsätzlich dürfen keine Unterlagen die BFA verlassen, die Patient*innen identifizieren. Akten dürfen demnach nicht zu Hause aufbewahrt werden.

8. Kommunikation mit Patient*innen außerhalb des Therapieraumes begrenzen

- a. Den Erstkontakt nehmen Sie telefonisch auf. Vergewissern Sie sich, dass Sie mit der Person sprechen, mit der Sie sprechen wollen, bevor Sie „Psychotherapie“ erwähnen. Sprechen Sie nur das Nötigste ab.
- b. Kontakt per E-Mail ist nur erlaubt, wenn Sie die schriftliche Einwilligung des/der Patient*in einholen.

9. Online-Therapie nur über zertifizierte Anbieter

- a. Für die Durchführung von Online-Therapiesitzungen gibt es eine Reihe zertifizierter Anbieter. Nur diese sind zulässig. Die Verwendung von nicht zertifizierten Diensten wie Zoom ist untersagt.
- b. Untersagt sind telefonische Therapiesitzungen.

10. Verschlüsselte Kommunikation über E-Mail mit Supervisor*innen

- a. E-Mails mit personensensiblen Daten wie Gutachter*innen- und Fallberichte an Supervisor*innen dürfen keine Klarnamen oder Chiffre, die sich aus dem Geburtsdatum zusammensetzt, enthalten. Die Chiffre soll nach der Korrektur und Unterschrift handschriftlich nachgetragen werden.
- b. Selbst wenn Berichte keine Chiffre enthalten, lassen sie u.U. Rückschlüsse auf die Person zu und sind im E-Mail Verkehr leicht abzugreifen. Daher dürfen E-Mails ausschließlich verschlüsselt verschickt werden.¹ Ggf. bietet sich an, zu Beginn der Supervision gemeinsam ein Passwort festzulegen.

11. Verschlüsselte Speicherung elektronischer Daten

- a. Sie sind verpflichtet, einen verschlüsselten Ordner für elektronische sensible Daten zu verwenden, z.B. Gutachter*innen- und Fallberichte oder Supervisionsprotokolle. Entweder Sie nutzen dafür einen von uns ausgegebenen USB-Stick, auf dem ein solch verschlüsselter Ordner installiert wurde oder Sie müssen entsprechende Dateien in einen verschlüsselten Ordner auf Ihrem Rechner ablegen². Die unverschlüsselte Ablage von personenbezogenen Daten ist nicht zulässig. Das Passwort als Zugang zu einem Rechner schützt nicht den Zugriff auf die sich auf der Festplatte befindenden Daten.

12. Löschen von verschlüsselten Ordnern vor Entsorgung des Laptops/PCs

- a. Vor der Entsorgung von Hardware müssen sämtliche sensible Daten gelöscht werden (selbst, wenn sie verschlüsselt wurden) oder die Festplatte professionell zerstört werden.

¹ Für alle Betriebssysteme (Windows, Apple und Linux u. a.) kann eine open source Verschlüsselungssoftware, AESCrypt (www.aescrypt.com) verwendet werden. Unterstützung erhalten Sie durch den Systemadministrator der BFA, Tel. 030 7978 76 80. Für verschlüsselte Anhänge ausschließlich zwischen Rechnern mit dem Betriebssystem Windows ist nach wie vor die open source Software AxCrypt (AxCrypt bspw. über www.heise.de) sehr gut geeignet.

² Die hierfür geeignete Freeware unter einer Open Source Lizenz lautet VeraCrypt und ist für Windows, Linux und MacOSX verfügbar. Wir empfehlen, alle privaten Dokumente in bspw. einen VeraCrypt-Ordner abzulegen und den Ordner während des Transports zu schließen. Geht der PC verloren, ist der Fremdzugriff bei einem ausreichend langen Passwort praktisch nicht möglich. Um Datenverluste zu vermeiden, was auch eine Forderung des Datenschutzgesetzes ist, sollten Sie den geschlossenen Safeordner (sowohl den safe auf dem USBStick als auch den auf ihrem PC angelegten Ordner) regelmäßig auf eine andere Festplatte speichern bzw. kopieren. Diese Festplatte sollte sich nach Möglichkeit an einem anderen Ort als ihr PC bzw. USB-Stick befinden.

13. Umgehende Meldung von Datenschutzverstößen

- a. Nach dem Datenschutzgesetz muss ein Verlust eines Datenträgers, auf dem sich personensensible Daten befinden, dem Landesdatenschutzbeauftragten innerhalb von 72 Stunden gemeldet werden, wobei ausreichend verschlüsselte Daten relativ unproblematisch sind. Im Fall eines Verlustes informieren Sie bitte umgehend die Institutsleitung, ggf. parallel den Landesdatenschutzbeauftragten Berlin.

14. Daten sparsam erheben

- a. Sowohl im BDSG, als auch in der EU-DSGVO und der Berufsordnung gilt der Grundsatz der Datensparsamkeit. Dem gegenüber steht die Dokumentationspflicht, die sich jedoch nach dem Zweck richtet. Die Dokumentation soll eine ordnungsgemäße Behandlung sicherstellen sowie ihre Fortführung hinsichtlich Diagnose und Therapie. Inhalt und Umfang der Dokumentation müssen sich hiernach richten.
- b. Für die ordnungsgemäße Behandlung kann im Rahmen der Ausbildung u.U. notwendig sein, einzelne Sitzungen elektronisch aufzuzeichnen, um sie in der Supervision zu thematisieren, wobei zwingend eine Zustimmung zur Datenerhebung und –verarbeitung seitens des/der Patient*in erforderlich ist und die Datei ebenfalls verschlüsselt gespeichert werden muss. Sie darf zudem nur zweckentsprechend lange aufbewahrt werden und muss nach der Supervision ordnungsgemäß gelöscht werden (inkl. Leeren des elektronischen Papierkorbes).

15. Ordnungsgemäße Übergabe von Akten nach Abschluss der Ausbildung

- a. Alle Therapieunterlagen müssen nach der Beendigung einer Therapie von eigenen Geräten gelöscht und der BFA vollständig übergeben werden, die ihrerseits zu einer 10-jährigen Aufbewahrung verpflichtet ist. Patient*innen haben ein Einsichtsrecht in alle Teile ihrer Patient*innen-Akte und nehmen dieses Recht mitunter Jahre nach Ende einer Therapie in Anspruch. Stellen Sie sicher, dass Sie ordnungsgemäß dokumentiert haben. Einer formell und materiell ordnungsgemäßen Dokumentation kann bis zum Gegenbeweis Glauben geschenkt werden.

III. Verantwortliche für Datenverarbeitung und Datenschutz an der BFA

1. Verantwortlich für die Datenverarbeitung der BFA:

Andreas Bartz und Klaus Conrads, Schloßstraße 107/108, 12163 Berlin.

Andreas Bartz: Tel: 030 / 797 45 420, bartz@b-f-a.de, Fax: 030 / 79 78 68 29

Klaus Conrads: Tel: 030 / 70 09 66 55, conrads@b-f-a.de, Fax: 030 / 79 78 68 29

2. Für die BFA zuständiger Datenschutzbeauftragter:

Herr Dr. Thomas Pudelko, Grunewaldstraße 15, 10823 Berlin.

Tel: 0152 / 34 23 94 01, datenschutz@t-pudelko.de

IV. Anhänge

1) Ausgewählte Bestimmungen der Datenschutzgrundverordnung (DSGVO)

Artikel 5 DSGVO

(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“); 4.5.2016 L 119/35 Amtsblatt der Europäischen Union DE (1 Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).
- 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“);

Art. 9 DSGVO Verarbeitung besonderer Kategorien personenbezogener Daten

- (1) 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 ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

- h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich.

Art. 32 Abs. 4 DSGVO

(4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Art. 83 Abs. 4 DSGVO

(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.

2) Ausgewählte Bestimmungen des Bundesdatenschutzgesetzes (BDSG)

§ 24 BDSG Verarbeitung zu anderen Zwecken durch nichtöffentliche Stellen

(1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nichtöffentliche Stellen ist zulässig, wenn

- 1. sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder
- 2. sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

(2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen des Absatzes 1 und ein Ausnahmetatbestand nach Artikel 9 Absatz 2 der Verordnung (EU) 2016/679 oder nach § 22 vorliegen.

§ 27 BDSG (Forschungszwecke)

(1) 1Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 679/2016 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 679/2016 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. 2Der Verantwortliche sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 vor.

§ 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 allgemein 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.

§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.

§ 53 BDSG Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

3) Ausgewählte Bestimmungen des Strafgesetzbuches (StGB)

§ 202a 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.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 202d Datenhehlerei

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie

2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

§ 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.

Erklärung zur Einhaltung des Datenschutzes und der Schweigepflicht

Mir wurde erläutert, dass ein Verstoß gegen das ärztliche Berufsgeheimnis nicht nur eine Berufspflichtverletzung darstellt, sondern auch eine strafrechtliche Verantwortlichkeit begründen kann.

Mir ist bekannt, dass

- sich meine Schweigepflicht auf alles, was mir in Ausübung oder aus Anlass meiner Tätigkeit anvertraut oder bekannt geworden ist, erstreckt;
- sich die Verschwiegenheitspflicht auch auf schriftliche Mitteilungen von Patient*innen, Aufzeichnungen über Patient*innen, und sonstige Befunde bezieht;
- die Verschwiegenheitspflicht gegenüber jedermann besteht (für den/die nicht explizit eine Schweigeverpflichtung vorliegt), so auch gegenüber meinen eigenen Familienangehörigen, gegenüber Familienangehörigen der Patient*innen, gegenüber Ärzt*innen, Arbeitskolleg*innen soweit eine Mitteilung nicht aus dienstlichen Gründen erfolgt, gegenüber demjenigen/derjenigen, der/die von der betreffenden Tatsache bereits Kenntnis erlangt hat;
- meine Verschwiegenheitspflicht auch nach dem Tod von Patient*innen fortbesteht;
- meine Verschwiegenheitspflicht auch nach Beendigung meines Ausbildungsverhältnisses fortbesteht.

Mit der Unterzeichnung dieser Datenschutzerklärung verpflichte ich mich

- patientenbezogene Berichte, die ich auf meinem eigenen PC schreibe, grundsätzlich in einem Safe³ abzuspeichern, der mit einem sicheren und nur mir bekannten Passwort⁴ gesichert ist. Ich verpflichte mich, dieses Passwort entweder auswendig zu lernen oder aber an einem anderen, sichereren Ort als meinen PC aufzubewahren und nicht als "Passwort" zu kennzeichnen.
- Darüber hinaus verpflichte ich mich, patientenbezogene Daten am Ende der Aus- bzw. Weiterbildung vollständig von meinem PC zu löschen.

Ich verpflichte mich zum Einhalten der weiteren Datenschutzbestimmungen, d.h. zur ordnungsgemäßen Aufzeichnung, Verarbeitung, Aufbewahrung und Löschung von personenbezogenen Patient*innen-Daten.

Weiter erstreckt sich meine Verschwiegenheitspflicht auch auf die mir bei meiner Tätigkeit bekannt werdenden persönlichen, wirtschaftlichen und sonstigen Verhältnisse der Mitarbeiter*innen der Berliner FortbildungsAkademie.

Eine Kopie dieser Verpflichtungserklärung zum Datenschutz ist mir ausgehändigt worden.

³ Beispiel für ein Safe ist "VeraCrypt" (open source software s. homepage bfa). Alternativ gibt die BFA einen USB-Stick heraus, auf dem ein Safe installiert ist.

⁴ Mindestens 8 Zeichen, darunter Groß- u. Kleinbuchstaben, Zahlen und Sonderzeichen

....., den
Ort Datum Vor- und Nachname in Druckbuchstaben/Ausbildungskurs

.....
(Unterschrift Psychotherapeut*in in Aus- o. Weiterbildung)

Bestätigung über den Erhalt eines USB-Stick

Hiermit bestätige ich den Erhalt eines USB-Sticks⁵ zur Verschlüsselung von Daten, der mir leihweise von meinem Ausbildungsinstitut zur Verfügung gestellt wird*. Nach Beendigung der Ausbildung (spätestens bei Erhalt Fachkundezeugnis) ist der Stick in einwandfreiem Zustand unaufgefordert herauszugeben.

....., den
Ort Datum Vor- und Nachname in Druckbuchstaben/Ausbildungskurs

.....
(Unterschrift Psychotherapeut*in in Aus- o. Weiterbildung)

* bei Verlust muss die BFA den Psychotherapeut*innen in Ausbildung 10,00 € in Rechnung stellen

⁵ Es gibt sowohl einen Stick für das Windows- sowie für das Mac- Betriebssystem