REFUGEE LAW CLINICS DEUTSCHLAND

Datenschutzrecht für Refugee Law Clinics

Broschüre mit Rechtsgrundlagen und Mustervorlagen

Ein Kooperationsprojekt
der
AG Datenschutz

Editorial

Diese Broschüre wurde als Kooperationsprojekt verschiedener RLCs im Rahmen der AG Datenschutz des Refugee Law Clinics Deutschland e.V. erstellt.

Verantwortliche Bearbeiter:

Daniel Kamiab Hesari (RLC Deutschland) und Simon Schulze (RLC Deutschland und RLC Munich)

Bearbeiter*innen:

Gilbert Bär (Law & Legal Bayreuth), Sven Bleckmann (RLC Hannover), Sofie Eich (RLC Saarbrücken), Christoph Halder (SRB Passau), Paul König (RLC Berlin), Bettina Trittmann (Goethe-Uni LC), Paul Weimann (RLC Berlin) und Simon Herker (RLC Deutschland)

Layout

Stefanie Sommer

Inhaltliche Anmerkungen werden über <datenschutz[at]rlc-deutschland.de> gerne entgegengenommen. Bei Interesse an der zukünftigen Mitarbeit in der AG Datenschutz kann gerne dieselbe Adresse verwendet werden.

Mit freundlicher Unterstützung von:

Die Beauftragte der Bundesregierung für Migration, Flüchtlinge und Integration

Robert Bosch Stiftung

Wir danken allen Beteiligten für ihr Engagement während der Erstellung dieser Broschüre!

REFUGEE LAW CLINICS DEUTSCHLAND

Kontaktinformationen

Refugee Law Clinics Deutschland e.V.
c/o Wigwam eG
Prinzenallee 74
13357 Berlin
Online: www.lawclinics.de

V.i.S.d.P.
Katrin Sass,
Co-Vorsitzende des Vorstands
Jan Haas,
Co-Vorsitzender des Vorstands

© Refugee Law Clinics Deutschland e.V.

Inhaltsverzeichnis

A. Einleitung 4

B. Die rechtlichen Vorgaben der DS-GVO für RLCs 5

I. Rechtliche Einordnung der ehrenamtlichen Rechtsberatung 5

II. Anwendungsbereich und Definitionen der DS-GVO 5

III. Gewährleistungsziele der DS-GVO 7

IV. Zulässigkeit der Datenverarbeitung 7

1. Die sechs Tatbestände des Art. 6 Abs. 1 DS-GVO 7
   - *a) Einwilligung 8*
   - *b) Erfüllung eines Vertrages 10*
   - *c) Wahrnehmung berechtigter Interessen 11*
   - *d) Erfüllung von Rechtspflichten 13*
2. Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DS-GVO) 14
3. Auftragsverarbeitung (Art. 28 DS-GVO) und Drittländer (Art. 44 ff. DS-GVO) 16
   - *a) Weitergabe an Dritte 16*
   - *b) Auftragsverarbeitung 16*
   - *c) Übermittlung in Drittländer 17*

V. Pflichten des Verantwortlichen 19

1. Verarbeitungsverzeichnis (Art. 30 DS-GVO) 19
2. Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) 20
3. Datensicherheit (Art. 32 DS-GVO) 21
4. Datenschutzbeauftragte*r (§ 38 BDSG/ Art. 37 – 39 DS-GVO) 22
5. Löschung personenbezogener Daten (Art. 17 DS-GVO) 24
6. Meldungen bei Verletzung des Datenschutzes (Art. 33 und 34 DS-GVO) 27
7. Informationspflichten (Art. 13 und 14 DS-GVO) 28
   - *a) Direkterhebung bei den Betroffenen (Art. 13 DS-GVO) 28*
   - *b) Erhebung über Dritte (Art. 14 DS-GVO) 29*
8. Satzungsanpassung und Datenschutzordnung 31

VI. Rechte der Betroffenen 33

1. Formale und inhaltliche Anforderungen (für alle Betroffenenrechte) 33
2. Auskunftsrecht (Art. 15 DS-GVO) 33
3. Recht auf Löschung / „Recht auf Vergessenwerden“ (Art. 17 Abs. 1 DS-GVO) 36
4. Widerspruchsrecht (Art. 21 DS-GVO) 36
5. Recht auf Berichtigung (Art. 16 DS-GVO) 37
6. Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO) 37
7. Recht auf Datenübertragbarkeit/Datenportabilität (Art. 20 DS-GVO) 37

VII. Befugnisse der Aufsichtsbehörde (insb. Sanktionsbefugnis) 38

C. Hinweise zur Datenschutzkonformität von Internetauftritten 39

I. Betrieb einer Website (Datenschutzerklärung) 39

II. Betrieb von Social-Media (insb. Facebook-Fanpages) 42

1. Informationspflichten bei Social Media 43
2. Exkurs: (Mit-)Verantwortlichkeit von Fanpagebetreibern 46

D. Weiterführende Informations- und Literaturhinweise 48

I. Ausgewählte Kommentare und Ratgeber 48

II. Sonstige Informationsquellen im Internet 49

E. Vorlagenverzeichnis 50

I. Anhang 1: Beratungsvertrag (inkl. Vollmacht, Hinweisen zur Datenverarbeitung und der datenschutzrechtlichen Einwilligung) 51

1. Beratungsvertrag (mit Klient*innen) 51
2. Vollmacht 54
3. Hinweise zur Datenverarbeitung für Klient*innen 55
4. Einwilligung für Klient*innen 57

*II. Anhang 2: Verpflichtung der studentischen Berater*innen (inkl. Hinweisen zur Datenverarbeitung und einem Auszug der gesetzl. Vorschriften) 58*

1. Verpflichtung der studentischen Berater*innen 58
2. Hinweise zur Datenverarbeitung für Berater*innen 61
3. Gesetzliche Vorschriften zur Vertraulichkeit 63

III. Anhang 3: Einwilligung für Drittbetroffene (inkl. Hinweisen zur Datenverarbeitung) 66

1. Einwilligung für Drittbetroffene 66
2. Hinweise zur Datenverabreitung für Drittbetroffene 67

*IV. Anhang 4: Einwilligung Supervisor*innen/Beirät*innen (inkl. Hinweisen zur Datenverarbeitung) 69*

1. Einwilligung für Supervisor*innen/Beirät*innen 69
2. Hinweise zur Datenverabeitung für Supervisor*innen/Beirät*innen 70

*V. Anhang 5: Einwilligung Dolmetscher*innen (inkl. Hinweise zur Datenverarbeitung) 72*

1. Einwilligung für Dolmetscher*innen 72
2. Hinweise zur Datenverarbeitung für Dolmetscher*innen 73

*VI. Anhang 6: Einwilligung Sozialarbeiter*innen (inkl. Hinweise zur Datenverarbeitung) ... 75*

1. Einwilligung für Sozialarbeiter*innen 75
2. Hinweise zur Datenverarbeitung für Sozialarbeiter*innen 76

VII. Anhang 7: Verarbeitungsverzeichnis (inkl. TOM) 78

1. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 Abs. 1 DS-GVO 78

2. Anleitung zur Erarbeitung technischer und organisatorischer Maßnahmen (TOM, Art. 32 DS-GVO) 89

*VIII. Anhang 8: Vertraulichkeitsverpflichtung RLC-Angehörige & Supervisor*innen/Beirät*innen 92*

1. Vertraulichkeitsverpflichtung 92
2. Anlage zur Verpflichtung auf die Vertraulichkeit 93

*IX. Anhang 9: Vertraulichkeitsverpflichtung Dolmetscher*innen 96*

1. Vertraulichkeitsverpflichtung 96
2. Anlage zur Vertraulichkeitsverpflichtung 97

X. Anhang 10: Bestellung eines/einer Datenschutzbeauftragten 98

XI. Anhang 11: Vorschlag für einen Satzungspassus für Vereins-(R)LCs 99

XII. Anhang 12: Vorschlag für eine Datenschutzordnung für Vereins-(R)LCs 100

XIII. Anhang 13: Datenschutzerklärung für die Website 104

XIV. Anhang 14: Datenschutzerklärung für Facebook 111

XV. Anhang 15: Abwägungshilfe für berechtigte Interessen (3x5 Matrix) 113

F. Urheberrechtliche Hinweise 115

A. Einleitung

Liebe RLCs,

ihr leistet eine ganz tolle und wichtige Arbeit, aber das wisst ihr ja sicherlich. Damit ihr euch auf eure Kernaufgabe(n) konzentrieren könnt, haben wir für euch diese Broschüre zum Thema Datenschutz zusammengestellt. Wir, das sind hauptsächlich die RLCs aus Bayreuth, Frankfurt, Hannover, München, Saarbrücken sowie der Dachverband. Diese Broschüre soll euch die Arbeit und den Umgang mit dem Thema Datenschutz erleichtern und euch Hilfestellungen zu den einzelnen Punkten bieten. Die Broschüre ist als Praxisleitfaden für Euch gedacht und konzipiert. Wir freuen uns, wenn er darüber hinaus auch anderen Rechtsberatungsstellen wertvolle Impulse liefern kann.

Diese Broschüre besteht im Wesentlichen aus zwei Teilen. In den Kapiteln *B* und *C* werden zunächst die rechtlichen Grundlagen der Datenverarbeitung im Hinblick auf die Tätigkeiten der Refugee Law Clinics dargestellt. Um die teilweise rechtlich sehr abstrakten Inhalte im direkten Bezug zur RLC-Arbeit zu setzten, finden sich häufig Praxishinweise, die durch einen gestrichelten Kasten (wie der untenstehende Haftungsausschluss) gekennzeichnet wurden. Dort werden meist konkrete Beispiele aus unserer RLC-Arbeit mit den rechtlichen Anforderungen verbunden, um die Umsetzung zu erleichtern. In Kapitel *D* findet sich eine knappe Zusammenstellung von weiterführenden Informations- und Literaturhinweisen, die besonders für die über diese Broschüre hinausgehende Recherche geeignet sind. Am Ende in Kapitel *E* haben wir für euch Vorlagen zusammengestellt, welche ihr gerne eins-zu-eins verwenden dürft. Beachtet dabei aber bitte, dass in vielen Dokumenten für eure RLC individuelle Anpassungen notwendig sind. Auf die jeweils einschlägigen Vorlagen wird im Rahmen der inhaltlichen Darstellung *B* und *C* durch die die bereits angesprochenen gestrichelten Kasten aufmerksam gemacht.

Grundsätzlich hatten wir bei Erstellung den Anspruch eine praxisnahe Broschüre und keine wissenschaftliche Abhandlung zu schreiben. Deshalb finden sich nur vereinzelt Verweise auf Literatur und sonstige Quellen, wenn eine Frage besonders strittig ist oder wir den Verweis für besonders wertvoll gehalten haben.

Wir hoffen, euch hiermit eine Hilfestellung an die Hand geben zu können, welche euch die Arbeit mit dem Datenschutz erleichtert. Wir freuen uns über Anregungen, Verbesserungsvorschläge, aber auch mögliche Kritik. Sendet uns diese bitte an <datenschutz[at]rlc-deutschland.de>.

Haftungsausschluss

Der Refugee Law Clinics Deutschland e.V. und die Verfasser*innen übernehmen keine Haftung für die Informationen, Auskünfte, Risikoeinschätzungen und Vorlagen dieser Broschüre. Sie dient als Hilfestellung, die die Subsumtion und Anwendung des Datenschutzrechts auf die individuelle Rechtsberatungsstelle nicht ersetzen kann.

B. Die rechtlichen Vorgaben der DS-GVO für RLCs

I. *Rechtliche Einordnung der ehrenamtlichen Rechtsberatung*

Vorab: Anders als für Rechtsanwälte und Rechtsanwältinnen gelten für die Arbeit von RLCs **keine rechtlichen Privilegien**. Die Rechtsberater*innen unterliegen keiner beruflichen Schweigepflicht nach § 203 StGB. Sie haben auch kein Zeugnisverweigerungsrecht auf § 53 Abs. 1 StPO. Somit greift für sie auch kein Beschlagnahmeverbot nach § 97 Abs. 1 StPO. Die Befugnisse der Aufsichtsbehörden sind - anders als nach § 29 Abs. 3 BDSG gegenüber Berufsgeheimnisträgern - auch nicht eingeschränkt. RLCs, unabhängig ob *Vereins-RLC* oder *Uni-RLC*, unterliegen somit uneingeschränkt den datenschutzrechtlichen Vorgaben. Welches Regelungsregime im Einzelnen gilt, ist abhängig von der Einstufung als öffentliche oder nicht-öffentliche Stelle im Sinne des Datenschutzrechts.

Uni-RLCs ohne eigene Rechtspersönlichkeit unterliegen als öffentliche Stellen dem Landesdatenschutzrecht, welches im Regelfall umfassend auf die DS-GVO verweist, indes in Einzelheiten davon abweicht. Da die Universität bereits selbst die datenschutzrechtlichen Vorgaben erfüllen muss, gibt es bereits ein Verarbeitungsverzeichnis, einen Datenschutzbeauftragten etc., woran anzuknüpfen ist. Im Zweifel ist mit dem Datenschutzbeauftragten der Universität Rücksprache zu halten, da die Rechtsberatung in vielen Punkten von der üblichen Verarbeitungstätigkeit einer Universität abweicht.

Vereins-RLCs mit eigener Rechtspersönlichkeit sind verpflichtet die datenschutzrechtlichen Vorgaben selbst umzusetzen. Im Folgenden wird grundsätzlich nicht zwischen den beiden Organisationsformen von RLCs unterschieden. In den Bereichen, wo sich relevante Unterschiede ergeben, wird darauf explizit hingewiesen

II. *Anwendungsbereich und Definitionen der DS-GVO*

Regelungsgegenstand der DS-GVO ist die automatisierte – und nichtautomatisierte, wenn in einem Dateisystem gespeicherte – **Verarbeitung personenbezogener Daten**, Art. 2 Abs. 1 DS-GVO. Räumlich beschränkt ist sie auf Verantwortliche, die entweder selbst in der EU niedergelassen sind oder deren Angebot sich an Personen richtet, die sich in der EU befinden, Art. 3 Abs. 1 und 2 DS-GVO. Für die **RLCs** ist von der Anwendbarkeit der Verordnung auszugehen.

Was sind personenbezogene Daten?

Personenbezogene Daten (Art. 4 Nr. 1 DS-GVO) sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Ein personenbezogenes Datum setzt sich also aus drei Elementen zusammen: **Information, natürliche Person** und Identifiziertheit bzw. **Identifizierbarkeit**.

- **Information** ist jede Art von Aussage über eine Person. Auch *subjektive* Informationen, wie Meinungen, Einschätzungen oder Beurteilungen sind erfasst. Ob eine derartige Aussage der Wahrheit entspricht, ist nicht relevant. Und auch die Art der Daten, ihr Format und Speichermedium spielen keine Rolle: die Informationen können alphabetisch, numerisch, grafisch, fotografisch, akustisch „oder in sonstiger Weise" vorliegen.
- Diese Information muss sich auf eine **natürliche Person** beziehen. Juristische Personen genießen dagegen keinen Schutz. Der Bezug auf die natürliche Person kann sich direkt aus dem Inhalt der Information ergeben (Name, Alter, Herkunft etc.). Es genügt aber auch ein indirekter Personenbezug: Aussagen über eine Sache oder ein anderes Verhältnis können mittelbar Rückschlüsse auf eine natürliche Person zu lassen. So bezieht sich eine Aussage über den Wert einer Immobilie formal auf das Objekt, gleichzeitig aber auch auf die Eigentümer des Objekts. Ein anderes Beispiel: Informationen über eine Kapitalgesellschaft mit nur einem Gesellschafter.
- Die Information muss sich schließlich einer bestimmten Person zuordnen lassen. Die Identität der Person kann sich unmittelbar aus der Information selbst ergeben (**Identifiziertheit**). Es genügt aber auch, wenn sie sich erst durch Verknüpfung mit weiteren Informationen einer Person zuordnen lässt (**Identifizierbarkeit**). Hier ist eine Risikoabwägung vorzunehmen: Die Person gilt als identifizierbar, wenn die Identifizierung mit den vernünftigerweise in Betracht kommenden Mitteln wahrscheinlich ist. Zu berücksichtigen sind also nur verhältnismäßige Mittel. Umstritten ist, ob es allein auf die Mittel ankommt, die dem Verantwortlichen zur Verfügung stehen oder ob auch Mittel Dritter einzubeziehen sind.[1] Diese Streitigkeit spielt jedoch in der täglichen Arbeit der RLCs eine untergeordnete Rolle.

Praxistipp

In der **RLC-Arbeit** fallen regelmäßig personenbezogene Daten an. Typischerweise sind dies:

Daten aus der **Rechtsberatung**

- Daten der **Klient*innen**
- Daten von fallrelevanten **Dritten**
- Daten von **Sozialarbeiter*innen**/Kontaktpersonen der Klient*innen
- Daten von **behördlichen Ansprechpartner*innen**

Daten aus der **RLC-Verwaltung**

- Daten der **Berater*innen** bzw. Vereins-Mitglieder
- Daten von **Supervisor*innen/Beirät*innen**
- Daten von **Dolmetscher*innen**

Daten der Besucher*innen der **RLC-Internetauftritte**

[1] Zum Streitstand: *Klar/Kühling*, in: Kühling/Buchner, DS-GVO/BDSG, Art. 4 DS-GVO Rn. 25 ff.

Was ist eine Datenverarbeitung?

Verarbeitung (Art. 4 Abs. 2 DS-GVO) ist schlicht ***jeder Vorgang*** im Zusammenhang mit personenbezogenen Daten (zum Beispiel 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). Dieser Vorgang kann automatisiert, also **rechnergestützt**, sein. Auch die nicht-automatisierte Verarbeitung ist jedoch erfasst, wenn die Daten in einem Dateisystem gespeichert werden. Dateisystem ist jede strukturierte Datensammlung, die nicht digital ist (z.B. ein alphabetisch geordneter **Handaktenschrank**).

Diese Einschränkung ist für Uni-RLCs nicht von Bedeutung, da das Landesdatenschutzrecht eine Erstreckung der datenschutzrechtlichen Vorgaben auf derartig verarbeitete personenbezogene Daten anordnet.

Wer ist Verantwortlicher?

Verantwortlicher (Art. 4 Nr. 7 DS-GVO) ist die natürliche oder juristische Person, welche allein oder gemeinsam mit anderen, über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Bei **Vereins-RLCs** ist dies also der **Verein als juristische Person** bzw. letztlich über § 26 Abs. 1 S. 2 BGB der Vereinsvorstand. Bei **Uni-RLCs** ist Verantwortlicher die **Universität**.

III. *Gewährleistungsziele der DS-GVO*

Die nach Art. 5 Abs. 1 DS-GVO vorgesehenen Gewährleistungsziele (Grundsätze) für die Datenverarbeitung sind: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. Diese Gewährleistungsziele sind in den Vorschriften der DS-GVO ausgestaltet und werden teilweise für deren Auslegung herangezogen. Der Verantwortliche muss deren Einhaltung nachweisen können (sog. Rechenschaftspflicht), Art. 5 Abs. 2 DS-GVO.

IV. *Zulässigkeit der Datenverarbeitung*

1. Die sechs Tatbestände des Art. 6 Abs. 1 DS-GVO

Die Verarbeitung personenbezogener Daten steht generell unter einem Verbot mit Erlaubnisvorbehalt. Bei jedem einzelnen Datenverarbeitungsvorgang muss also begründet werden, dass er rechtmäßig ist.

Von den im Folgenden dargestellten Bedingungen muss **mindestens eine erfüllt sein**, **damit** die Datenverarbeitung **zulässig** ist. Die Darstellung konzentriert sich auf die hier typischerweise einschlägigen Erlaubnistatbestände und deren entsprechende Anwendungsbereiche. Die Erlaubnistatbestände sind nach Relevanz für die RLC-Arbeit aufgelistet, nicht nach der Reihenfolge in Art. 6 DS-GVO.

a) Einwilligung

Die im Beratungsalltag wichtigste Möglichkeit, die Datenverarbeitung zu legalisieren, ist die **Einwilligung** (Art. 6 Abs. 1 S. 1 lit. a DS-GVO). Sie wird legaldefiniert in Art. 4 Nr. 11 DS-GVO. Weitere Anforderungen an die Einwilligung ergeben sich aus Art. 7 und 8 DS-GVO.
Eine Einwilligung muss **eindeutig, zweckgebunden, freiwillig, informiert**, nicht notwendigerweise schriftlich, aber in allen Punkten **nachweisbar** sein.

In **materieller** Hinsicht muss die Einwilligung also die folgenden Voraussetzungen erfüllen:

- **Eindeutigkeit**:
  Die Einwilligung muss „unmissverständlich" sein, Art. 4 Nr. 11 DS-GVO. Der Wille der betroffenen Person muss sich also eindeutig ergeben; aus ihrer Erklärung oder Handlung. Die Einwilligung kann nämlich bei hinreichender Eindeutigkeit – anders als im Rahmen des Art. 9 DS-GVO (siehe hierzu sogleich ***B.IV.2***) – auch konkludent erfolgen.
- **Zweckbindung**:
  Die Einwilligung muss für einen oder mehrere bestimmte Zwecke mit Bezug auf die konkrete Verarbeitung erfolgen, Art. 6 Abs. 1 S. 1 lit. a DS-GVO. Im Zuge der Einwilligungserteilung muss der Verarbeitungszweck also so präzise wie möglich festgelegt werden.
- **Freiwilligkeit**:
  Die Einwilligung ist nur wirksam, wenn sie ohne jeden Druck und Zwang abgegeben werden konnte. Mehr noch: Die Betroffenen müssen eine echte Wahlfreiheit haben. Dies wird nach – umstrittener – Ansicht verneint, wenn einer Person suggeriert wird, die beabsichtigte Datenverarbeitung hänge von ihrer Einwilligung ab, obwohl ein anderer Erlaubnistatbestand greift. Bestehen Unsicherheiten, ob die Einwilligung schon aus einem anderen Grund rechtmäßig ist, sollte gegenüber der betroffenen Person jedenfalls offengelegt werden, dass es sich um eine Einwilligung zur Absicherung handelt – dann lässt sich die Freiwilligkeit gut begründen.
- **Informiertheit**:
  Die Einwilligung muss „in informierter Weise" erfolgen, Art. 4 Nr. 11 DS-GVO. Als Ausdruck der informationellen Selbstbestimmung kann eine Einwilligung nur wirksam sein, wenn sie in Kenntnis aller entscheidungsrelevanten Informationen abgegeben wird. Nur so können Risiken und Vorteile abgeschätzt und eine sachgerechte Entscheidung getroffen werden. Damit die betroffene Person weiß, was mit ihren Daten geschehen soll, muss sie – **vor der Einwilligung** – zumindest die folgenden Informationen erhalten:
  - Die Identität des Verantwortlichen
  - Eine Umschreibung der betroffenen Daten
  - Die beabsichtigten Verarbeitungszwecke
  - Die potenziellen Datenempfänger
  - Die beabsichtigte Verarbeitungs- und Speicherdauer
  - Der Hinweis auf die Betroffenenrechte, insbesondere die Widerruflichkeit der Einwilligung

  Der Umfang der Informationspflicht orientiert sich an Art. 13 und 14 DS-GVO (hierzu ausführlich ***B.V.7.a***)), ein Verstoß gegen diese weitergehende Vorschrift hat aber nicht automatisch die Unwirksamkeit der Einwilligung zufolge.

In **formeller** Hinsicht ist Folgendes zu beachten:

- Die Einwilligung unterliegt **keinem Schriftformerfordernis**. Sie kann z.B. auch elektronisch erfolgen. Der Verantwortliche trägt aber nach Art. 7 Abs. 1 DS-GVO die Beweislast dafür, dass eingewilligt wurde. Die Einwilligung ist deshalb in jedem Fall gut zu dokumentieren. Bei schriftlichen

Einwilligungsklauseln ist auf gestalterische und inhaltliche Transparenz zu achten – insbesondere muss sie von anderen Vertragsteilen klar zu unterscheiden sein, Art. 7 Abs. 2 S. 1 DS-GVO.

- Einwilligung bedeutet auch im Datenschutzrecht vorherige Zustimmung: Sie muss also zu einem Zeitpunkt **vor der Datenverarbeitung** erklärt worden sein. Eine nachträgliche Zustimmung hat dagegen keine Legalisierungswirkung.
- Die betroffene Person muss **einsichtsfähig** sein, d.h. die Konsequenzen ihrer Handlung abschätzen können. Dies entspricht nicht der zivilrechtlichen Geschäftsfähigkeit: Auch Minderjährige können einsichtsfähig sein, was jeweils im Einzelfall zu beurteilen ist. Entscheidend ist hierbei die Fähigkeit des Minderjährigen zu selbständigem und verantwortungsbewusstem Verhalten, sowie Art und Zweck der Datenverarbeitung. Fehlt die erforderliche Einsichtsfähigkeit, müssen die Eltern für den Minderjährigen einwilligen.

Die Einwilligung stellt einen für die Praxis gut handhabbaren Erlaubnistatbestand dar. Von ihr sollte allerdings nur dann Gebrauch gemacht werden, wenn die **Datenverarbeitung auf keine andere Rechtsgrundlage gestützt werden kann.** Dies liegt zum einen an den soeben beschriebenen Zweifeln an der Freiwilligkeit, falls die Verarbeitung auch ohne Einwilligung zulässig wäre. Zudem ist die Einwilligung jederzeit **widerruflich**, Art. 7 Abs. 3 S. 1 DS-GVO. Widerruft die betroffene Person ihre Einwilligung, wird die weitere Verarbeitung der Daten unzulässig.

Vor diesem Hintergrund sollte die Reichweite der Einwilligung gestaltet werden: Kann die Verarbeitung etwa bereits durch Vertragserfüllung legalisiert werden (Art. 6 Abs. 1 S. 1 lit. b DS-GVO, dazu gleich ausführlich *B.IV.1.b)*), sollte **von einer zusätzlichen Einwilligung Abstand genommen** werden. Geht die Verarbeitung jedoch darüber hinaus und greift kein anderer Erlaubnistatbestand, muss auf eine Einwilligung zurückgegriffen werden. **Aber Achtung**: Werden besonders **sensible Daten** nach Art. 9 DS-GVO verarbeitet, gelten besondere Erlaubnistatbestände. Unter Umständen braucht es dann dennoch eine Einwilligung, obwohl die Datenverarbeitung nicht über das für die Vertragserfüllung erforderliche Maß hinausgeht. So ist es beim **Beratungsvertrag** (dazu ausführlich unter *B.IV.2*).

Praxistipp

Für die **Beratungstätigkeit** der RLCs ist die **Einwilligung** der **wichtigste Erlaubnistatbestand**. Auch wenn diese nicht zwingend schriftlich erfolgen muss, empfehlen wir zu Dokumentationszwecken die Verwendung unserer Vorlage in Anhang 1. Neben einem Beratungsvertrag und einer Vollmacht findet ihr dort auch eine datenschutzrechtliche Einwilligung für Klient*innen (*E.I.4*). Damit die Einwilligung auch in informierter Weise erfolgt, sollten zuvor die Hinweise zur Datenverarbeitung (*E.I.3*) ausgehändigt werden.

Für die übrigen in der RLC-Arbeit anfallenden Daten ist stets zu prüfen, ob die Verarbeitung auf einen anderen der im Folgenden dargestellten Erlaubnistatbestände gestützt werden kann. Nur **subsidiär** sollte auf die Einwilligung zurückgegriffen werden. Ist keine andere Rechtsgrundlage einschlägig, findet ihr Vorlagen für die Einwilligung von **Drittbetroffenen, Supervisor*innen, Dolmetscher*innen und Sozialarbeiter*innen** in den Anhängen 3 bis 6. Auch hier ist zuvor die Informationspflicht durch Aushändigung der jeweiligen Hinweise zur Datenverarbeitung zu erfüllen.

Vorlagen

Anhang 1: Beratungsvertrag *(inkl. Vollmacht, Hinweisen zur Datenverarbeitung und der datenschutzrechtlichen Einwilligung)*

Anhang 2: Verpflichtung der studentischen Berater*innen *(inkl. Hinweisen zur Datenverarbeitung und einem Auszug der gesetzl. Vorschriften)*

Anhang 3: Einwilligung für Drittbetroffene *(inkl. Hinweisen zur Datenverarbeitung)*

Anhang 4: Einwilligung Supervisor*innen/Beirät*innen *(inkl. Hinweisen zur Datenverarbeitung)*

Anhang 5: Einwilligung Dolmetscher*innen *(inkl. Hinweise zur Datenverarbeitung)*

Anhang 6: Einwilligung Sozialarbeiter*innen *(inkl. Hinweise zur Datenverarbeitung)*

b) Erfüllung eines Vertrages

Die Verarbeitung personenbezogener Daten ist auch dann erlaubt, wenn sie zur **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen, erforderlich ist (Art. 6 Abs. 1 S. 1 lit. b DS-GVO).

Zwischen dem Verantwortlichen und der betroffenen Person muss also ein **vertragliches bzw. vorvertragliches Verhältnis** bestehen. Die Erforderlichkeit der Datenverarbeitung kann sich dabei nicht nur aus den Hauptleistungspflichten, sondern auch aus vertraglichen Nebenpflichten ergeben.

Besonderes Augenmerk liegt hier auf der **Erforderlichkeit**, welche die Reichweite des Erlaubnistatbestands begrenzt: Es muss sich um Daten handeln, deren Verarbeitung objektiv für die Erfüllung des konkreten Vertragszwecks erforderlich ist. Hierzu ein Beispiel: Ein Supervisor*innen-Vertrag erlaubt es grundsätzlich, deren Namen und Kontaktdaten für die RLC-Administration zu verarbeiten. Soll den Supervisor*innen jedoch Werbung (wobei der weite Begriff der „Werbung“ zu beachten ist) zugeschickt werden, ist dies nicht mehr für die Durchführung der Supervisionen erforderlich. Ein anderer Rechtfertigungstatbestand ist hier nicht einschlägig, weshalb eine Einwilligung nötig wäre. Ein weiteres Beispiel ist die Weitergabe der Daten an Dritte (siehe hierzu auch ***B.IV.3.a)***). Auch hier sollte stets sorgfältig geprüft werden, ob nicht eine Einwilligung notwendig ist.

Auch wenn die Datenverarbeitung auf diesen Erlaubnistatbestand gestützt werden kann, besteht – wie bei allen Erlaubnistatbeständen – **vor der Datenverarbeitung** die **Informationspflicht** nach Art. 13 f. DS-GVO. Näheres dazu unter ***B.V.7.a).***

Praxistipp

Noch einmal: Allein der **Beratungsvertrag** ist als Grundlage für die Verarbeitung der Daten aus der Beratung **nicht ausreichend**, da dort in der Regel auch sensible Daten nach Art. 9 DS-GVO betroffen sind (hierzu gleich ausführlich unter ***B.IV.2***).

Werden in eurer RLC vertragliche **Vereinbarungen mit den Berater*innen, Supervisor*innen, Dolmetscher*innen** geschlossen, kann dies als Grundlage für die jeweilige Datenverarbeitung jedoch genügen. Das ist der Fall, wenn keine sensiblen Daten anfallen und die Datenverarbeitung nicht weitergeht als zur Vertragsdurchführung erforderlich. Wichtig ist, dass die betroffenen Personen auch in diesen Fällen vor der Datenverarbeitung nach Art. 13 und 14 DS-GVO zu informieren sind (siehe hierzu ***B.V.7***).

Ein entsprechendes Beispiel findet ihr in der **Vorlage in Anhang 2**: Die Verarbeitung der Daten der Berater*innen stützt sich in diesem Fall allein auf die „Verpflichtung der studentischen Berater*innen“ (***E.II.1***). Der Informationspflicht wird durch vorherige Aushändigung der „Hinweise zur Datenverarbeitung“ (***E.II.2***) Genüge getan. Entsprechend könnte auch bei Supervisor*innen und Dolmetscher*innen vorgegangen werden.

Erfolgt deren Arbeit hingegen ohne vertragliche Grundlage könnt ihr euch an unseren **Vorlagen in Anhang 3 und 4** orientieren: Die Datenverarbeitung stützt sich dann jeweils auf eine eigenständige **datenschutzrechtliche Einwilligung** nach Art. 6 Abs. 1 lit. a DS-GVO. Zuvor sind auch hier zu Informationszwecken die Hinweise zur Datenverarbeitung auszuhändigen.

c) Wahrnehmung berechtigter Interessen

Eine Datenverarbeitung ist auch dann rechtmäßig, wenn sie zur Wahrnehmung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Allerdings nur, sofern nicht die Interessen der betroffenen Person überwiegen, Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

Der Verantwortliche oder ein Dritter muss also zunächst ein berechtigtes Interesse an der Verarbeitung haben. Zu den berechtigten Interessen zählen rechtliche, aber auch tatsächliche, wirtschaftliche oder ideelle Interessen. Sodann ist eine **Abwägung** erforderlich: Wenn die Interessen als gleichwertig einzustufen sind, darf die Verarbeitung stattfinden.

In der Praxis ist dieser Erlaubnistatbestand recht schwer handhabbar. Die Darlegungslast, dass die Betroffeneninteressen nicht überwiegen, liegt beim Verantwortlichen. Es sollte also dokumentiert werden, warum die Betroffeneninteressen im Einzelfall als nicht überwiegend angesehen wurden. In **Vorlage 15** findet ihr eine Abwägungshilfe mit weiterführenden Hinweisen, die zugleich der Dokumentation des Abwägungsvorgangs dienen kann.

Auch bei diesem Erlaubnistatbestand müssen die Betroffenen vor der Datenverarbeitung nach Art. 13 und 14 DS-GVO **informiert** werden (ausführlich unter ***B.V.7***).

Praxistipp

Für RLCs ist dieser Erlaubnistatbestand von Bedeutung für **Daten über fallrelevante Dritte**, die bei Klient*innen erhoben werden (z.B. Informationen über Familienangehörige etc.).

Dann stellen sich **zwei Fragen**:

1) Kann die Verarbeitung der Daten der Dritten über die **Wahrnehmung berechtigter Interessen** gerechtfertigt werden **oder** bedarf es einer **Einwilligung**?
   - Eine Rechtmäßigkeit der Datenverarbeitung über die Wahrnehmung berechtigter Interessen scheidet aus, wenn besonders sensible Daten nach Art. 9 DS-GVO betroffen sind. Dann muss einer der Ausnahmetatbestände des Art. 9 Abs. 2 DS-GVO greifen, in der Regel also eine Einwilligung eingeholt werden (hierzu ausführlich *B.IV.2*)
   - Falls keine besonders sensiblen Daten verarbeitet werden, sind die Interessen im Einzelfall abzuwägen. Dazu kann die **Vorlage in Anhang 15** herangezogen werden.
2) Ist der Dritte nach Art. 14 DS-GVO über die Datenverarbeitung zu **informieren**?
   - Grundsätzlich ja. Abgesehen werden kann davon nur, wenn einer der Ausnahmetatbestände greift. Dazu später mehr unter *B.V.7.b)*.

Ein typisches Beispiel der RLC-Arbeit für die Wahrnehmung berechtigter Interessen ist die Verarbeitung von Daten (typischerweise Name, Telefonnummer und E-Mail-Adresse) von **behördlichen Ansprechpartner*innen.** Im konkreten Fall wäre das berechtigte Interesse die Durchsetzung von Rechtsansprüchen für die Klient*innen, welches gegenüber dem Interesse des*r betroffenen Behördenmitarbeiter*in überwiegt. Für den Abwägungsvorgang siehe Anhang 15 (*E.XV*).

Vorlage

Anhang 15: Abwägungshilfe für berechtigte Interessen (3x5 Matrix)

Wir empfehlen für die Abwägung der Interessen beispielsweise auf die in Anhang 15 aufgeführte 3x5 Matrix mit insgesamt 15 Kriterien in den drei Kategorien „**Daten**", „**Akteure**" und „**Verarbeitung**" zurückzugreifen. Für jedes Kriterium wird festgestellt, ob aus diesem eine geringe, normale oder schwere Belastung für die betroffene Person resultiert. Zu beachten ist, dass bei manchen Kriterien eine geringe oder eine schwere Belastung von vornherein ausscheiden, sodass nur die Entscheidung „gering/normal" oder „normal/schwer" verbleibt. In diesem Fall sind die entsprechenden Felder in der Matrix „ausgegraut".

Für Verarbeitungsvorgänge, die auf berechtigte Interessen gestützt werden sollen, bietet es sich an die Matrix einmal durchzukreuzen. Wenn sich die Verantwortlichen einer RLC dazu entscheiden, einen Verarbeitungsvorgang auf berechtigte Interessen zu stützen, sollte die ausgefüllte Matrix gespeichert werden, um den Abwägungsvorgang später nachweisen zu können.

d) Erfüllung von Rechtspflichten

Das Datenschutzrecht ist gegenüber der Erfüllung unions- oder mitgliedstaatlicher **Rechtspflichten** subsidiär; diese können also eine **Datenverarbeitung rechtfertigen** (Art. 6 Abs. 1 S. 1 lit. c DS-GVO). Art. 6 Abs. 1 S. 1 lit. c DS-GVO ist für sich genommen kein Erlaubnistatbestand für eine Datenverarbeitung.

Die Rechtsgrundlage hierfür ergibt sich vielmehr aus Gebots- oder Verbotsnormen in Gestalt von Gesetzen, Rechtsverordnungen und Satzungen sowie Verwaltungsakten und Urteilen. Die entsprechende Rechtsnorm muss den Zweck der Verarbeitung selbst festlegen, ein im öffentlichen Interesse liegendes Ziel verfolgen und in Bezug auf den verfolgten Zweck verhältnismäßig sein.

Von diesem Erlaubnistatbestand werden typischerweise Aufzeichnungs- und **Aufbewahrungspflichten** sowie Melde-, Vorlage-, Aussage- und Transparenzpflichten umfasst. Die nachfolgenden Erlaubnistatbestände sind der Vollständigkeit halber aufgenommen worden und haben in der RLC-Arbeit **keine besondere Praxisrelevanz**:

- **Wahrung lebenswichtiger Interessen der Betroffenen:**
  Erlaubt ist jedermann die Verarbeitung personenbezogener Daten zur Wahrung lebenswichtiger Interessen der betroffenen Person (Art. 6 Abs. 1 S. 1 lit. d DS-GVO): der Datenschutz weicht dem Schutz des Lebens.
- **Erfüllung einer Aufgabe im öffentlichen Interesse:**
  Die Verarbeitung personenbezogener Daten ist zulässig, wenn sie zur Erfüllung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt (Art. 6 Abs. 1 S. 1 lit. e DS-GVO). Dieser Buchstabe betrifft in erster Linie staatliche Datenverarbeitung und betrifft RLCs in der Regel nicht.

Praxistipp

Für die RLCs kommt insbesondere die **Aufbewahrungspflicht nach § 147 Abs. 3 Abgabenordnung (AO)** in Betracht. Sämtliche von dieser Norm umfassten Unterlagen (§ 147 Abs. 1 AO) müssen zur Ermöglichung von Steuerprüfungen zehn bzw. sechs Jahre aufbewahrt werden. Im Folgenden werden nun die verschiedenen Dokumente aufgelistet, wobei besonders die für die RLC-Arbeit praxisrelevanten Dokumente fett markiert sind.

Zehn Jahre müssen folgende Dokumente aufbewahrt werden:

- Bücher und Aufzeichnungen, **Inventare**, **Jahresabschlüsse (wie z.B. der jährliche Bericht der Kassenprüfer*innen)**, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen (§ 147 Abs. 1 Nr. 1);
- **Buchungsbelege (wie z.B. Bankbelege, Rechnungen, Fahrtkostenabrechnungen, Kopien von Spendenbescheinigungen, Lohnabrechnungen für SHKs oder Dozent*innen oder sonstige Mitarbeiter*innen, Mietbelege, Versicherungspolicen)** (§ 147 Abs. 1 Nr. 4);
- Unterlagen nach Art. 15 Abs. 1 und Art. 163 des Zollkodex der Union (§ 147 Abs. 1 Nr. 4a).

Sechs Jahre müssen folgende Dokumente aufbewahrt werden:

- die empfangenen Handels- oder Geschäftsbriefe (§ 147 Abs. 1 Nr. 2);
- Wiedergaben der abgesandten Handels- oder Geschäftsbriefe (§ 147 Abs. 1 Nr. 3);
- **sonstige Unterlagen, soweit sie für die Besteuerung von Bedeutung sind (wie z.B. steuerrelevante E-Mail-Korrespondenz, Kalkulationen des Jahresbudgets)** (§ 147 Abs. 1 Nr. 5).

Für die einschlägigen Dokumentengruppen sollten die jeweils zutreffenden Aufbewahrungspflichten in das Löschkonzept bzw. das Verarbeitungsverzeichnis aufgenommen werden. In dem von uns als **Anhang 7** zur Verfügung gestellten Beispiel eines Verarbeitungsverzeichnisses (siehe *E.VII.1*) müssten die einschlägigen Aufbewahrungspflichten unter Nr. 9 ergänzt werden. Eine umfangreiche Erläuterung zum Verarbeitungsverzeichnis ist unter *B.V.1* abrufbar.

Hinweis für Unterscheidung zwischen Uni-RLCs und Vereins-RLCs

Die Aufbewahrungspflicht des § 147 AO **gelten in jedem Fall für Vereins-RLCs**. Bei Uni-RLCs können auch andere gesetzlichen Aufbewahrungspflichten einschlägig sein. Dies muss im **Einzelfall für der zuständigen Stelle der Universität abgeklärt** werden.

2. Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DS-GVO)

Für besonders sensible Daten stellt die DS-GVO in Art. 9 erhöhte Rechtsmäßigkeitsvoraussetzungen auf.[2] Dadurch soll für Daten mit besonderer Grundrechtsrelevanz ein stärkerer Schutz gewährleistet werden. Nach Art. 9 Abs. 1 DS-GVO zählen hierzu etwa Daten zur **ethnischen Herkunft, politischen Meinung, religiösen Überzeugung, sexuellen Orientierung und Gesundheitsdaten**. Es handelt sich also um Informationen, die in der RLC-Praxis regelmäßig im Rahmen der Beratungstätigkeit relevant werden.

Die Verarbeitung dieser Art von Daten ist **grundsätzlich verboten**, es sei denn es greift einer der **Ausnahmetatbestände** des Art. 9 Abs. 2 DS-GVO. Die praxisrelevantesten sind:

[2] Die „**sensiblen Daten**" werden teilweise in der Literatur auch als „**sensitive Daten**" bezeichnet, so etwa bei *Weichert*, in: Kühling/Buchner, DS-GVO, Art. 9, Rn. 13. Aus Gründen der Einheitlichkeit wird hier am Begriff „sensible Daten" festgehalten.

- Das Verarbeitungsverbot gilt nicht, wenn die betroffene Person **ausdrücklich eingewilligt** hat, Art. 9 Abs. 2 lit. a DS-GVO. Hinsichtlich der Einwilligung gilt das zu Art. 6, 7 und 8 gesagte umfassend (siehe *B.IV.1.a)*). „Ausdrücklich" bedeutet darüber hinaus, dass sich die Einwilligung explizit auf die Verarbeitung sensibler Daten beziehen muss. Zudem ist eine konkludente Einwilligung hier nicht möglich.
- Art. 9 Abs. 2 lit. d DS-GVO erlaubt die Verarbeitung sensibler Daten für sog. **Tendenzbetriebe**, also politisch, religiös oder gewerkschaftlich ausgerichteter Organisationen. Die Vorschrift gilt jedoch nur für die **interne** Datenverarbeitung und auch nur hinsichtlich der eigenen Mitglieder oder anderer regelmäßiger Kontakte. Grund ist, dass Daten zur politischen Überzeugung oder gewerkschaftlichen Mitgliedschaft der eigenen Mitglieder für das Funktionieren dieser Organisationen unabdingbar sind. **Unseres Erachtens findet die Privilegierung für Tendenzbetriebe auf RLCs keine Anwendung.** In jedem Fall würde die Vorschrift aber auch nur für die interne Mitglieder- und Supervisor*innen-Verwaltung greifen.
- Art. 9 Abs. 2 lit. f DS-GVO erlaubt die Datenverarbeitung sensibler Daten, soweit dies zur **Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen** erforderlich ist. Die Durchsetzung eines Anspruchs soll nicht allein daran scheitern, dass sensible Daten verarbeitet werden müssten. Es geht hier aber um Rechtsansprüche des (bzw. gegen den) Verantwortlichen, also **der RLC**, nicht etwa der Klient*innen. Damit die Verarbeitung auch „erforderlich" ist, sollte zumindest plausibel gemacht werden können, dass die entsprechenden Daten als Beweismittel benötigt werden. Werden Daten für diese Zwecke benötigt, sind die Daten auch später nicht zu löschen (siehe *B.V.5* und *B.VI.3*). Zu Beginn der Beratung werden Anhaltspunkte für spätere Rechtsstreitigkeiten in aller Regel nicht vorliegen, so dass die Beratungstätigkeit nicht auf diesen Erlaubnistatbestand gestützt werden kann.
- Schließlich ist die Verarbeitung sensibler Daten auch zulässig, wenn die Daten zum Schutz der lebenswichtigen Interessen der betroffenen Person oder eines*r Dritten erforderlich ist, diese*r aber nicht selbst einwilligen kann. Es geht hier also um **Notstandskonstellationen**, in denen auf den hypothetischen Willen des*r Betroffenen abgestellt wird. Gibt es aber einen gesetzlichen Vertreter, darf nicht auf Art. 9 Abs. 2 lit. c DS-GVO abgestellt werden, sondern es ist dessen Einwilligung einzuholen. Die Vorschrift wird im RLC-Alltag nur in seltenen Ausnahmefällen relevant werden.

Praxistipp

Für die RLCs ist vor allem die Einwilligung wichtig. Da es in der Beratung regelmäßig um sensible **Daten der Klient*innen** geht, ist deren **ausdrückliche Einwilligung** einzuholen. Diese sollte dokumentiert werden. Hierzu kann die „**Datenschutzrechtliche Einwilligung für Klient*innen**" aus **Vorlage 1** (siehe *E.I*)benutzt werden. Zuvor ist der Informationspflicht nachzukommen, z.B. durch Aushändigung der „Hinweise zur Datenverarbeitung" aus der Vorlage.

3. Auftragsverarbeitung (Art. 28 DS-GVO) und Drittländer (Art. 44 ff. DS-GVO)

Es kann vorkommen, dass Dritte in die Verarbeitung einbezogen werden oder die personenbezogenen Daten in "Drittländer" übermittelt werden müssen. Hier stellt die DS-GVO einige weitere Voraussetzungen auf, die beachtet werden müssen.

a) Weitergabe an Dritte

Die schlichte **Weitergabe** personenbezogener Daten an Dritte stellt eine **Form der Verarbeitung** im Sinne des Art. 4 Abs. 2 DS-GVO dar. Deren Rechtmäßigkeit bestimmt sich somit nach den allgemeinen Zulässigkeitsvoraussetzungen, die oben dargestellt wurden.

Es sind dabei **zwei Verarbeitungsvorgänge** zu unterscheiden, für welche die rechtliche Zulässigkeit gesondert zu begründen ist: Die Verarbeitung durch den Verantwortlichen und die Weitergabe an den Dritten. Für beide muss einer der Erlaubnistatbestände des Art. 6, 9 DS-GVO erfüllt sein.

b) Auftragsverarbeitung

Von der schlichten Übermittlung zu unterscheiden ist die **Auftragsverarbeitung** im Sinne der Art. 28 f. DS-GVO, bei dem der Verantwortliche die Verarbeitung personenbezogener Daten durch eine andere juristische Person oder Stelle vornehmen lässt. Wesensmerkmal der Auftragsverarbeitung ist die **Weisungsabhängigkeit** des Dritten. Der Verantwortliche bleibt somit Herr*in der Verarbeitung. Die Auftragsverarbeitung ist – anders als die Weitergabe – kein eigener Verarbeitungsvorgang, sondern ein bloßes Mittel der Verarbeitung.[3] Die Verarbeitung durch den Verantwortlichen muss also eine der in Art. 6 Abs. 1 DS-GVO genannten Bedingungen erfüllen. Ist das der Fall, darf der Verantwortliche dann auch unter den Voraussetzungen der Art. 28 DS-GVO einen oder mehrere Auftragsverarbeiter einsetzen. Grundlage der Auftragsverarbeitung muss ein entsprechender Vertrag (**AV-Vertrag**) sein, dessen Mindestinhalt sich aus Art. 28 Abs. 3 DS-GVO ergibt.

[3] Diese Privilegierungswirkung ist unter der DS-GVO nicht mehr unumstritten, wird aber überwiegend angenommen, siehe etwa *Hartung*, in: Kühling/Buchner, DS-GVO/BDSG, Art. 28 DS-GVO Rn. 15 und *Bertermann*, in: Ehmann/Selmayr, DS-GVO, Art. 28 Rn. 7.

Praxistipp

Die meisten der typischen Auftragsverarbeiter (Cloud-Dienste etc.) haben sich auf die Vorgaben der DS-GVO eingestellt: Gleichzeitig mit dem Vertragsschluss schließen die Kunden automatisch auch den AV-Vertrag ab. Aber Achtung: Bei manchen Anbietern muss man selbst aktiv werden und einen entsprechenden Vertrag abschließen. Die RLCs sollten deshalb alle externen Stellen, an die Daten übermittelt werden, einmal durchgehen und sich fragen:

1. Zunächst: Handelt es sich um eine **Weitergabe** oder eine **Auftragsverarbeitung**?

2. Anschließend:
   a. Bei einer Weitergabe: Ist ein **Erlaubnistatbestand** im Sinne der Art. 6, 9 DS-GVO gerade auch für die Weitergabe der Daten erfüllt?
   b. Bei einer Auftragsverarbeitung: Liegt ein **AV-Vertrag** mit dem Anbieter vor? Dieser sollte zu Dokumentationszwecken aufbewahrt werden.

c) Übermittlung in Drittländer

Werden Daten an Dritte außerhalb der EU bzw. des EWR weitergegeben oder dort eine Auftragsverarbeitung vorgenommen, kommt zu den obigen Anforderungen an die Weitergabe bzw. Auftragsverarbeitung jeweils eine **weitere Rechtmäßigkeitsvoraussetzung** hinzu.

Art. 44 ff. DS-GVO enthalten Sonderregelungen für die **Übermittlung personenbezogener Daten an Empfänger in Drittländer**. Übermittlung umfasst insofern jede Form der Offenlegung von personenbezogenen Daten an eine Stelle außerhalb des Geltungsbereichs der DS-GVO. Hierzu gehört die physische Übertragung von Daten, aber auch das bloße Zugänglichmachen solcher Daten, etwa durch Einräumen von Zugriffsrechten an außerhalb der EU gelegene Dritte. Auch die Auftragsverarbeitung wird von der Vorschrift erfasst.

Übermittlungen in Drittländer sind nur zulässig, wenn neben den allgemeinen Zulässigkeitsvoraussetzungen der DS-GVO (die Datenverarbeitung also auch innerhalb der EU erfolgen dürfte), auch einer der besonderen **Erlaubnistatbestände der Art. 45ff.** DS-GVO erfüllt ist:

- Nach Art. 45 Abs. 1 DS-GVO dürfen Daten übermittelt werden, wenn das Drittland ein angemessenes Datenschutzniveau bietet. Dies wird durch einen sog. **Angemessenheitsbeschluss** der Kommission festgelegt. Ein solcher liegt vor für die **USA** (Privacy Shield; Wirksamkeit wird allerdings von EuGH gerade geprüft), die **Schweiz** (aufgrund der noch fehlenden Anpassung deren Datenschutzrechts an die DS-GVO ebenfalls kritisch), **Kanada** und **Australien**.

- Liegt kein Angemessenheitsbeschluss vor, stellt die DS-GVO in Art. 46 die Möglichkeit zur Verfügung, durch vertragliche oder vertragsähnliche Vereinbarungen zwischen dem Datenübermittler in der EU und dem Datenempfänger im Drittland einen Schutz herzustellen, der den Mangel an ausreichenden gesetzlichen Datenschutzvorschriften kompensiert. Dies kann insbesondere durch den Abschluss sog. **Standarddatenschutzklauseln** (auch: Standardvertragsklauseln) geschehen, Art. 46 Abs. 2 lit. c DS-GVO.
- Liegt kein Fall von Art. 45 oder 46 DS-GVO vor, muss davon ausgegangen werden, dass die Daten nach ihrer Übermittlung nicht mehr in einer Art und Weise geschützt sind, wie es im Geltungsbereich der DS-GVO der Fall wäre. Dennoch erlaubt Art. 49 Abs. 1 S. 1 lit. a DS-GVO die Übermittlung in ein Drittland, wenn die betroffene Person **ausdrücklich** in die Übermittlung **eingewilligt** hat, nachdem sie über die für sie bestehenden möglichen Risiken ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien unterrichtet wurde. Die Vorschrift eignet sich wegen ihres Ausnahmecharakters aber wohl nicht für Verarbeitungen, die massenhaft, wiederholt oder routinemäßig erfolgen sollen.[4]

Praxistipp

Für die Nutzung von **Cloudangeboten** gilt für die RLCs somit Folgendes: Wenn es sich um einen Anbieter handelt, dessen Server ausschließlich im **EU/EWR-Raum** stehen, genügt der Abschluss eines AV-Vertrags. Das ist die in der Praxis einfachste Variante.

Die Auftragsverarbeitung in **Drittländern** ist bei Vorliegen eines AV-Vertrags dann zulässig, wenn für das Land ein Angemessenheitsbeschluss besteht; zum Beispiel also wenn das Angebot eines US-Unternehmens genutzt wird, welches auf der privacy shield list geführt wird (einsehbar unter https://www.privacyshield.gov/list). Allerdings ist zu bedenken, dass die Rechenzentren vieler US-Unternehmen nicht nur in den USA liegen, so dass eine Übermittlung in andere Drittländer jedenfalls nicht ausgeschlossen werden kann. In diesen Fällen müssen dann Standarddatenschutzklauseln mit dem Cloud-Anbieter abgeschlossen werden.

[4] So jedenfalls *Zerdick*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung 2. Aufl. 2018, Art. 49 Rn. 4.

Praxistipp

Bei Redaktionsschluss (30.01.2019) war noch nicht absehbar, ob und wie **Großbritannien** die EU am 30.03.2019 verlassen wird. Der am 05.12.2018 vorgestellte (aber inzwischen vom britischen Unterhaus abgelehnte) Vorschlag für einen Austrittvertrag enthält in Art. 67 eine Fortgeltungsklausel für die DS-GVO. Datenschutzrechtlich relevant wären vor allem das Szenario eines ungeregelten Austritts (sog. *Hard Brexit*) oder die Einigung auf einen Austrittsvertrags, der die Fortgeltung der DS-GVO in Großbritannien nicht vorsieht. In dessen Folge wäre ab dem Austrittstag jeder Datentransfer dorthin (z.B. bei Webhostern, Cloudservices etc.) eine Übermittlung in ein Drittland. **Alle vorgenannten Hinweise zur Drittstaatenübermittlung wären dann auch für Großbritannien einschlägig**. Die Handhabe würde erst durch einen (bald zu erwartenden) Angemessenheitsbeschluss der Kommission vereinfacht.

V. *Pflichten des Verantwortlichen*

1. Verarbeitungsverzeichnis (Art. 30 DS-GVO)

Der Verantwortliche ist verpflichtet, alle Verarbeitungstätigkeit in seinem Zuständigkeitsbereich in einem Verzeichnis zu führen, Art. 30 Abs. 1 DS-GVO. Dieses Verzeichnis dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft den Verantwortlichen ihrer **Rechenschaftspflicht** aus Art. 5 Abs. 2 DS-GVO zu entsprechen und nachzuweisen, dass die Vorgaben aus der DS-GVO eingehalten werden.

Grundsätzlich muss jeder Verantwortliche ein Verarbeitungsverzeichnis führen. Ausgenommen sind nach Art. 30 Abs. 5 DS-GVO nur Verantwortliche mit weniger als 250 Mitarbeiter*innen. Diese Ausnahme gilt jedoch wiederum dann nicht, wenn die Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, wenn die **Verarbeitung nicht nur gelegentlich** erfolgt oder eine **Verarbeitung sensibler Daten** i.S. von Art. 9 oder Art. 10 DS-GVO erfolgt. Da jedoch RLCs, wie nahezu jeder Verein, personenbezogener Daten nicht nur gelegentlich verarbeiten, und in der Beratung zudem regelmäßig auch sensible Daten anfallen, haben RLCs ein Verarbeitungsverzeichnis zu führen.

Das Verarbeitungsverzeichnis muss schriftlich oder in einem elektronischen Format geführt werden, Art. 30 Abs. 3 DS-GVO. Sein Mindestinhalt ergibt sich aus Art. 30 Abs. 1 DS-GVO. Das Verzeichnis muss nicht von sich aus an die Datenschutzbehörde übermittelt werden, die bloße Existenz genügt also; die Behörden haben aber ein Einsichtsrecht, Art. 30 Abs. 4 DS-GVO.

Vorlage

Anhang 7: Verarbeitungsverzeichnis (inkl. TOM)

In Anhang 7 befindet sich ein beispielhaftes Verarbeitungsverzeichnis, welches gleichzeitig als Vorlage zum Entwurf eines eigenen Verzeichnisses und als Orientierung für die korrekte Eintragung dienen soll. Daher sollte hier ganz besonders darauf geachtet werden, dass die Vorlage eine beispielhafte Verarbeitung der Goethe-Uni LC darstellt. Diese kann sich stark von Ort zu Ort unterscheiden und **muss daher unbedingt an die örtlichen Gegebenheiten angepasst werden**.

2. Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)

Die DS-GVO schreibt vor, dass **besonders riskante Verarbeitungsvorgänge präventiv** – also bereits vor der jeweiligen Verarbeitung – auf ihre möglichen Folgen **überprüft** werden, damit der Verantwortliche die Risiken ggf. durch entsprechende Abhilfemaßnahmen eindämmen kann. Dafür sieht Art. 35 DS-GVO die sogenannte Datenschutz-Folgenabschätzung (DSFA) vor.

Ob eine solche durchzuführen ist, bestimmt sich nach folgendem Prüfungsschema:

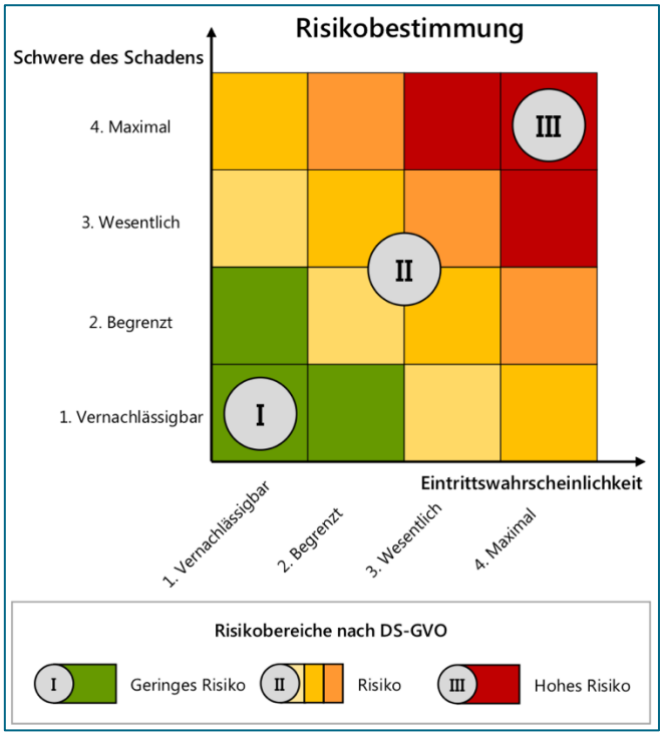
Eine DSFA ist zunächst dann zwingend erforderlich, wenn **besonders sensible Daten „umfangreich" verarbeitet** werden. Wir denken, dass RLCs davon nicht erfasst sind. Die Verarbeitung von Mandantendaten durch einen Einzelanwalt soll nach Erwägungsgrund 91 der DS-GVO nicht unter die Vorschrift fallen. Die DSK sieht eine umfangreiche Verarbeitung von Daten typischerweise erst bei großen Anwaltssozietäten gegeben.[5] Eine RLC, bei der (neben den Administratoren) in der Regel nur zwei Berater*innen Zugang zu Daten haben, dürfte eher einem Einzelanwalt als einer Großkanzlei entsprechen. Das wird schon durch einen Vergleich der Fallzahlen deutlich. Zudem wird die Erhebung der von Art. 9 DS-GVO erfassten Daten in RLCs zumeist auf das für die Beratung notwendige Mindestmaß beschränkt und der Kreis der zugriffsberechtigten Personen klein gehalten.

Nach Art. 35 Abs. 1 DS-GVO ist eine DSFA zudem dann durchzuführen, wenn eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dieser Tatbestand wird zunächst durch die "Liste der Verarbeitungstätigkeiten,

[5] Im Rahmen der Blacklist nach Art. 35 Abs. 4 DS-GVO, https://www.datenschutzkonferenz-online.de/media/ah/20181017_ah_DSK_DSFA_Muss-Liste_Version_1.1_Deutsch.pdf.

für die eine DSFA durchzuführen ist" (sog. **Blacklist**) verbindlich konkretisiert.[6] Für RLCs ist derzeit jedoch keine der genannten Verarbeitungstätigkeiten einschlägig.

Schließlich ist eine DSFA auch immer dann durchzuführen, wenn die Verarbeitung **voraussichtlich ein hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge hat, Art. 35 Abs. 1 DS-GVO. Ob das Risiko als „hoch" einzuschätzen ist, bedarf einer **individuellen Prüfung in der RLC**. Dabei kann sich an nebenstehendem Modell des BayLDA orientiert werden.[7] Wegen des besonderen Schutzbedarfs der in der Beratung verarbeiteten Daten ist die potentielle Schadensschwere regelmäßig als "wesentlich" einzuordnen. Die Eintrittswahrscheinlichkeit hängt hingegen entscheidend von den technischen und organisatorischen Maßnahmen zur Datensicherheit ab, die in der jeweiligen RLC angewendet werden. Wird den im nächsten Abschnitt vorgeschlagenen Maßnahmen zur Datensicherheit im Wesentlichen gefolgt, wird die Eintrittswahrscheinlichkeit in der Regel als "begrenzt" einzustufen sein. Dann ist nicht von einem hohen Risiko im Sinne des Art. 35 Abs. 1 DS-GVO auszugehen und eine DSFA jedenfalls nicht zwingend durchzuführen.
Solltet ihr eine DSFA dennoch für erforderlich halten, könnt ihr euch bei deren Umsetzung an dem Leitfaden von *bitkom* orientieren.[8]



3. Datensicherheit (Art. 32 DS-GVO)

Art. 32 DS-GVO enthält eine umfassende Verpflichtung für den Verantwortlichen, geeignete technische und organisatorische Maßnahmen (TOM) zur Gewährleistung der Sicherheit der Datenverarbeitung zu ergreifen.

Die DS-GVO folgt hinsichtlich der Datensicherheit einem relativen Ansatz: Das Schutzniveau muss unter Berücksichtigung des Stands der Technik und der Implementierungskosten in einem angemessenen Verhältnis zu den von der Verarbeitung ausgehenden Risiken stehen (vgl. Art. 32 Abs. 2 DS-GVO). Je sensibler beispielsweise die verarbeiteten Daten sind, desto größer ist die mögliche Schadenshöhe und umso umfassendere Maßnahmen der Datensicherheit verlangt Art. 32 DS-GVO den

[6] Die jeweils aktuelle Liste kann gefunden werden unter: https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_VerarbeitungsvorgaengeDSK.html?nn=9937868 – sie wird voraussichtlich zweimal im Jahr aktualisiert.
[7] https://www.lda.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf.
[8] https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/FirstSpirit-1496129138918170529-LF-Risk-Assessment-online.pdf.

Normadressaten im Einzelfall ab. Grundlage der Risikoabschätzung kann eine DSFA nach Art. 35 DS-GVO sein.

Welche konkreten Maßnahmen der Verantwortliche zur Erreichung eines angemessenen Schutzniveaus trifft, steht in seinem Ermessen. Art. 32 Abs. 1 Hs. 2 DS-GVO enthält einen kurzen, nicht abschließenden Katalog verschiedener technischer und organisatorischer Maßnahmen, die zum Teil eher Zielvorgaben ähneln.

Praxistipp

Die RLCs müssen Maßnahmen ergreifen, um ihre Daten angemessen zu sichern. Eine Anleitung zur Erarbeitung geeigneter TOM findet sich unter *E.VII.2*. Ein Anwendungsbeispiel könnt ihr unter Nr. 7 des Verarbeitungsverzeichnisses einsehen *(E.VII.1)*.

Auf jeden Fall sind Maßnahmen zu ergreifen, die mit minimalem Aufwand die Sicherheit stark erhöhen. In technischer Hinsicht gehören hierzu Updates von Software (insb. Browser, Flash, Java) und Betriebssystem. In organisatorischer Hinsicht sind Berater*innen und Dolmetscher*innen auf die Vertraulichkeit zu verpflichten. Hierzu können die Vorlagen in Anhang 8 und 9 genutzt werden.

Vorlagen

Anhang 7.2: *Anleitung zur Erarbeitung technischer und organisatorischer Maßnahmen (TOM, Art. 32 DS-GVO)*

*Anhang 8: Vertraulichkeitsverpflichtung RLC-Angehörige & Supervisor*innen/Beirät*innen*

*Anhang 9: Vertraulichkeitsverpflichtung Dolmetscher*innen*

4. Datenschutzbeauftragte*r (§ 38 BDSG/ Art. 37 – 39 DS-GVO)

Als Maßnahme der Selbstkontrolle sieht das Datenschutzrecht die Bestellung eines*r Datenschutzbeauftragten (DSB) vor. Diese*r soll den Verantwortlichen intern kontrollieren, entscheidet jedoch nicht über die Datenverarbeitung – verantwortlich bleibt der Verantwortliche. Die Ansprüche der betroffenen

Personen und etwaige Maßnahmen der Aufsichtsbehörden richten sich deshalb allein gegen den Verantwortlichen.[9]

Ein*e DSB ist nach Art. 37 Abs. 1 lit. c DS-GVO zwingend zu benennen, wenn die Kerntätigkeit in der **umfangreichen Verarbeitung** besonders **sensibler Daten** nach Art. 9 DS-GVO besteht. Zwar zählt die Beratung und die damit notwendigerweise verbundene Verarbeitung sensibler Daten zur Kerntätigkeit der RLCs.[10] Der Umfang der Verarbeitung ist jedoch – wie schon bei Art. 35 DS-GVO (*B.V.2*) – eher nicht als umfangreich anzusehen.
Die Pflicht zur Benennung eines*r DSB ergibt sich für RLCs in aller Regel aber aus § 38 BDSG. Ein*e DSB ist danach auch dann zwingend, wenn der Verantwortliche in der Regel **mindestens zehn Personen** ständig mit der automatisierten Datenverarbeitung beschäftigt. Das Tatbestandsmerkmal "ständig" ist bereits dann erfüllt, wenn die computergestützte Datenverarbeitung (worunter schon das Versenden einer E-Mail oder Eingabe und Speichern von personenbezogenen Daten zählt) nur gelegentlich (Richtwert: einmal im Monat) anfällt. Ob auch ehrenamtliche Mitarbeiter*innen „beschäftigt" werden, ist zwar umstritten, mehrere Aufsichtsbehörden nehmen dies jedoch an.[11] Wir empfehlen deshalb für RLCs mit mehr als 10 Berater*innen die Benennung eines*r DSB.

DSB kann grundsätzlich jede*r werden, er/sie sollte jedoch über **grundlegende Datenschutzkenntnisse** verfügen. In Anbetracht des in Erwägungsgrund 13 DS-GVO implizit geäußerten Verhältnismäßigkeitsprinzips halten wir es für die fachliche Expertise für ausreichend, wenn die/der DSB sich z.B. mithilfe dieser Broschüre sowie der Lektüre der einschlägigen Rechtsnormen mit dem Datenschutzrecht für RLCs sowie mit den **Grundlagen technischer Datensicherheit** beschäftigt. Daneben sind die **aktuellen Entwicklungen sorgfältig zu verfolgen**, um auf Veränderungen reagieren zu können. Es bedarf in jedem Fall **keiner formalen Qualifikation** etc. Die kostenpflichtige Beschäftigung eines/einer DSB ist jedenfalls für die meisten RLCs finanziell nicht leistbar und unverhältnismäßig. Wir vertreten daher die Auffassung, dass überwiegend ehrenamtlich getragene Vereine auch eine*n ehrenamtliche*n DSB aus den eigenen Reihen benennen dürfen, was beispielsweise von der saarländischen Datenschutzbehörde als ausdrücklich zulässig betrachtet wurde.

Der DSB darf nicht weisungsgebunden sein; dies ist vom Verein sicherzustellen. Er/sie darf keine Nachteile wegen seiner/ihrer Stellung als DSB erfahren. Dass der DSB andere Aufgaben wahrnimmt, ist nach Art. 38 Abs. 6 DS-GVO zulässig, das darf aber nicht zu Interessenkonflikten führen. Beispielsweise kann der DSB nicht gleichzeitig noch Aufgaben der Mitglieder- oder Personalverwaltung übernehmen. In Vereins-RLCs darf **kein Vorstandsmitglied** als DSB benannt werden,

[9] Denkbar ist allein eine deliktische Haftung des Datenschutzbeauftragen gegenüber den Betroffenen, siehe *Bergt*, in: Kühling/Buchner, DS-GVO/BDSG, Art. 37 DS-GVO Rn. 54.
[10] Fraglich ist, ob es sich bei der Datenverarbeitung nicht um eine bloße Hilfsfunktion für den eigentlichen Zweck der RLCs handelt. Bei Anwälten wird die Verarbeitung der Mandantendaten aber zur Kerntätigkeit gezählt, *Heberlein*, in: Ehmann/Selmayr, DS-GVO, Art. 37 Rn. 27.
[11] Landesbeauftrage für Datenschutz und Informationsfreiheit **NRW**, Datenschutz im Verein, S. 6, https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Datenschutz-im-Verein/Datenschutz-Verein.pdf; Der Landesbeauftragte für den Datenschutz **Baden-Württemberg**, Datenschutz im Verein nach der DS-GVO, S. 32, https://www.lda.bayern.de/media/info_bw_verein.pdf, hierauf bezieht sich das BayLDA für **Bayern** (unter weitere Datenschutzthemen), https://www.lda.bayern.de/de/infoblaetter.html.

damit der DSB seiner Kontroll- und Beratungsfunktion effektiv nachkommen kann. Die Kontaktdaten des DSB müssen vom Verarbeitungsverantwortlichen der RLC veröffentlicht und der zuständigen Aufsichtsbehörde gemeldet werden, Art. 37 Abs. 7 DS-GVO.

Praxistipp

RLC müssen **im Regelfall** eine*n **DSB bestellen**. Diese*r muss hinreichend fachlich qualifiziert sein – sie/er muss aber nicht zwingend eine formale Qualifikation (also etwa einen Lehrgang für DSBs) in diesem Bereich nachweisen können. Es empfiehlt sich jedoch eine*n DSB zu bestellen, die/der **grundlegenden Kenntnis im Datenschutzrecht** nachweisen kann.

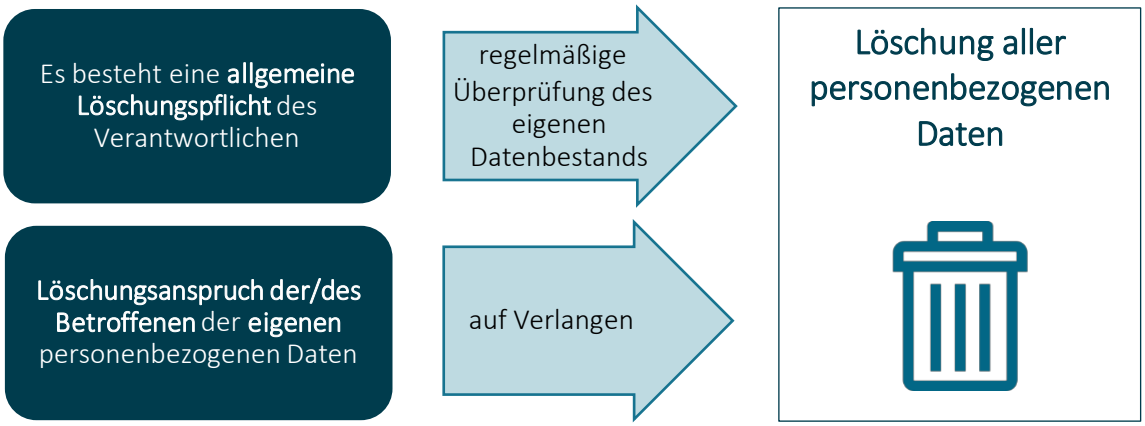
In jedem Fall müssen Interessenskonflikte der/des DSB verhindert werden. Er/sie sollte daher **nicht** dem Leitungsgremium (bei Uni-RLCs) oder dem **Vorstand** (bei Vereins-RLCs) angehören, da man so Gefahr läuft sich selbst zu kontrollieren. Eine solche Selbstkontrolle ist unzulässig und muss verhindert werden.

Vorlage

Anhang 10: Bestellung eines/einer Datenschutzbeauftragten

5. Löschung personenbezogener Daten (Art. 17 DS-GVO)

Entgegen seiner Überschrift normiert Art. 17 DS-GVO nicht nur das „Recht auf Vergessenwerden“, sondern auch die antragsunabhängige Pflicht des Verantwortlichen zur Löschung personenbezogener Daten:



Die Löschpflicht tritt u.a. ein, wenn

- die betroffene Person ihre **Einwilligung widerruft** (Art. 17 Abs. 1 lit. b DS-GVO),
- die betroffene Person **Widerspruch** (nach Art. 21 DS-GVO) gegen die Verarbeitung einlegt und keine vorrangigen berechtigten Gründe vorliegen (Art. 17 Abs. 1 lit. c DS-GVO) oder
- die Daten **unrechtmäßig verarbeitet** wurden (Art. 17 Abs. 1 lit. d DS-GVO).

Und für die RLC-Praxis am wichtigsten: wenn die Daten für die Zwecke, für die sie erhoben bzw. verarbeitet wurden, nicht mehr notwendig sind (**Zweckfortfall**), Art. 17 Abs. 1 lit. a DS-GVO. Die Vorschrift schließt an den Grundsatz der Zweckbindung aus Art. 5 Abs. 1 lit. b DS-GVO an, wonach Daten nur für festgelegte, eindeutige und legitime Zwecke erhoben bzw. verarbeitet werden dürfen. Wann Daten zur Zweckerfüllung nicht mehr notwendig sind, lässt sich nicht immer pauschal festlegen und erfordert eigentlich eine Prüfung in jedem Einzelfall. Soweit sich aber für bestimmte Arten von Daten im Vorhinein absehen lässt, dass der Erhebungs- oder Verarbeitungszweck nach einer bestimmten Zeit nicht mehr bestehen wird, empfiehlt es sich mit einem (ggf. automatisierten) **Löschkonzept mit Löschfristen** zu arbeiten. Dieses Löschkonzept kann auch in das Verarbeitungsverzeichnis integriert werden. So lässt sich leicht überprüfen, ob für jede Verarbeitungstätigkeit ein entsprechendes Konzept besteht.

Für die typischerweise in RLCs anfallenden Datenkategorien kann zu den folgenden Zeitpunkten von einem Zweckfortfall ausgegangen werden:

Art der Daten	Zweckfortfall
Daten der Klient*innen, von fallrelevanten Dritten, Sozialarbeiter*innen/Kontaktpersonen der Klient*innen	Abschluss der Beratung
Daten von Supervisor*innen, Dolmetscher*innen etc.	Ende der Tätigkeit für die RLC
Daten der Berater*innen	Ende der Beratungstätigkeit bzw. Austritt aus dem Verein

Wann der jeweilige Zeitpunkt genau eingetreten ist, lässt sich in der Praxis freilich nicht immer ohne Weiteres bestimmen. Oft verlaufen etwa Beratungen im Sande, ohne dass es einen klaren Abschlusstermin gäbe. Wir empfehlen daher, von einem Beratungsabschluss auszugehen, wenn sich in einem Fall seit **6 Monaten** nichts mehr getan hat.

Ist einer der genannten Tatbestände erfüllt, sind die entsprechenden Daten **unverzüglich** zu löschen. Hiervon macht Art. 17 Abs. 3 DS-GVO aber einige **Ausnahmen**: Die Pflicht zur Löschung der erhobenen Daten tritt u.a. nicht ein, soweit erforderlich

- für die Erfüllung einer **Rechtspflicht** (Art. 17 Abs. 3 lit. b, 1. Var. DS-GVO).
- Diese **Speicherverpflichtung** kann sich aus Unionsrecht oder nationalem Recht ergeben, insbesondere aus handels- oder steuerrechtlichen Aufbewahrungspflichten. Für die RLCs kommt insbesondere die **Aufbewahrungspflicht nach § 147 Abs. 3 Abgabenordnung (AO)** in Betracht, wonach bestimmte Unterlagen zur Ermöglichung von Steuerprüfungen zehn bzw. sechs Jahre aufbewahrt werden müssen (siehe hierzu schon den Praxistipp bei ***B.IV.1.d)***).für die Ausübung oder **Verteidigung von Rechtsansprüchen** (Art. 17 Abs. 3 lit. e DS-GVO).

Die weitere Speicherung der Daten ist für die Verteidigung von Rechtsansprüchen jedenfalls dann erforderlich, wenn mit dem Betroffenen bereits ein (gerichtliches oder außergerichtliches) Verfahren läuft oder ein solches konkret absehbar ist. Andererseits lässt sich die Gefahr, auch zu einem späteren Zeitpunkt, zivilrechtlich in Anspruch genommen zu werden, meist erst nach dem Ablauf der Verjährungsfrist ausschließen. Die bloße theoretische Möglichkeit zukünftiger Rechtsstreitigkeiten soll die weitere Speicherung jedoch nicht „erforderlich“ machen, so dass die Speicherung bis zur Verjährung nicht automatisch zulässig ist. In diesen Fällen ist vielmehr eine **Interessenabwägung im Einzelfall** maßgeblich: Die Wahrscheinlichkeit der Geltendmachung von Ansprüchen, sowie deren Gewicht, ist dem Ausmaß der Beeinträchtigung der Interessen des Betroffenen durch eine weitere Speicherung gegenüberzustellen. Nur wenn erstere überwiegen, ist die weitere Speicherung zulässig. Dies wird meist nur dann der Fall sein, wenn

Anhaltspunkte für zukünftige Rechtsstreitigkeiten bestehen. Im Einzelfall können die Daten aufgrund der kenntnisunabhängigen Verjährungshöchstfrist aus § 199 Abs. 3 S. 1 Nr. 1 BGB dann bis zu 10 Jahre gespeichert werden, wobei die Interessenabwägung regelmäßig zu überprüfen ist

Praxistipp

In der Praxis sollte der RLC-Datenbestand also **jedenfalls einmal jährlich überprüft** werden: Daten, deren Verarbeitungszweck sich erledigt hat, sind zu löschen. Nur wenn sich in einem Fall begründen lässt, dass die weitere Speicherung erforderlich ist, können die Daten behalten werden. Dies kommt insbesondere bei konkreten Anhaltspunkten für zukünftige Rechtsstreitigkeiten in Betracht.

6. Meldungen bei Verletzung des Datenschutzes (Art. 33 und 34 DS-GVO)

Wenn RLCs von einer Datenschutzverletzung in ihrem Verantwortungsbereich erfahren, sind sie gemäß Art. 33 Abs. 1 DS-GVO verpflichtet, diese der zuständigen **Aufsichtsbehörde** innerhalb von 72 Stunden zu **melden**. Dabei sind nach Art. 33 Abs. 3 DS-GVO die Art der Verletzung, deren wahrscheinlich Folgen und ergriffene Gegenmaßnahmen zu beschreiben, sowie Kontaktdaten des Datenschutzbeauftragten oder einer anderen Ansprechperson mitzuteilen. Die Meldepflicht besteht nur dann nicht, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht, wenn ihnen erhebliche wirtschaftliche oder gesellschaftliche Nachteile drohen (z.B. Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung). Nicht umfasst ist etwa der Fall, dass versehentlich mehrere Empfänger einer E-Mail versehentlich im CC-Feld und nicht BCC-Feld eintragen wurden. Dass ein solches Risiko aufgrund einer sachgerechten Risikoabwägung nicht bestand, wäre von den RLCs gegebenenfalls gegenüber der Aufsichtsbehörde nachzuweisen. Dafür ist es wichtig, der in Art. 33 Abs. 5 DS-GVO statuierten umfassenden **Dokumentationspflicht** nachzukommen.

Im Fall einer Datenschutzverletzung ist nach Art. 34 Abs. 1 DS-GVO zudem auch die **betroffene Person** zu **benachrichtigen**. Allerdings nur, wenn die Verletzung voraussichtlich ein **hohes Risiko** für dessen persönlichen Rechte und Freiheiten zur Folge hat. Die Voraussetzungen sind gegenüber der Meldepflicht aus Art. 33 DS-GVO also deutlich erhöht. Von einem hohen Risiko ist jedoch wohl jedenfalls immer dann auszugehen, wenn besonders sensible Daten im Sinne des Art. 9 DS-GVO Gegenstand der Datenschutzverletzung waren. Das deutsche Recht sieht in § 29 Abs. 1 S. 3 BDSG eine Ausnahme von der Benachrichtigungspflicht bei überwiegendem Geheimhaltungsinteresse eines Dritten vor.

7. Informationspflichten (Art. 13 und 14 DS-GVO)

a) Direkterhebung bei den Betroffenen (Art. 13 DS-GVO)

Werden personenbezogene Daten bei der **betroffenen Person selbst** erhoben, trifft die RLCs vor oder spätestens gleichzeitig mit der Erhebung die Informationspflicht des Art. 13 DS-GVO. Typische Fälle der Verarbeitung personenbezogener Daten durch RLCs sind beispielsweise während der Beratung die Daten von Klient*innen, bei der internen Verwaltung die Daten von Mitgliedern bzw. Berater*innen oder auch durch das Betreiben einer Webseite- und/oder eines Facebook-Auftritt die Daten von sonstigen Dritten (siehe dazu weiter unten ***C.I***).

Die stets zu erteilenden Informationen befinden sich Art. 13 Abs. 1 DS-GVO, situationsabhängig sind nach Abs. 2 weitere Informationen zur Verfügung zu stellen (u.a. Speicherdauer, Betroffenenrechte). Obwohl der Gesetzeswortlaut davon spricht, dass die Informationen nach Art. 13 Abs. 2 DS-GVO nur erteilt werden müssen, wenn „diese notwendig sind, um eine faire und transparente Verarbeitung zu gewährleisten“, sollten diese immer erteilt werden.[12]

Die Informationspflichten sollten mit den sonstigen Pflichten (Verarbeitungsverzeichnis/Löschkonzepte etc.) immer synchron gehalten werden – es sollten sich also unter keinen Umständen Widersprüche ergeben. Zudem sind die Informationen in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln (Art. 12 Abs. 1 DS-GVO).

Mitzuteilen sind dann nach **Art. 13 Abs. 1 DS-GVO**[13]:

- **Name und Kontaktdaten des Verantwortlichen** im Sinne der DS-GVO (= die RLC, daher Vereinsname gem. § 57 BGB bzw. Name der universitären Institution und Adresse/sonstige Erreichbarkeit) sowie ggf. dessen Vertreter im Sinne des Art. 13 DS-GVO (Vereine haben i. d. R. keinen Vertreter im Sinne der Vorschrift, da ein solcher nur zu benennen ist, wenn es keine Niederlassung in der EU gibt.);
- **Kontaktdaten** des ggf. vorhandenen **Datenschutzbeauftragten**;
- **Zwecke**, für die die personenbezogenen Daten verarbeitet werden sollen und Rechtsgrundlage der Verarbeitung (Bsp.: Beratungsleistung, Mitgliedsdatenverwaltung etc.)
- das **berechtigte Interesse**, insofern die Datenerhebung auf einem berechtigten Interesse des Verantwortlichen oder eines Dritten nach Art. 6 Abs. 1 Satz1 lit. f DS-GVO beruht;
- **Empfänger** oder **Kategorien von Empfängern** der personenbezogenen Daten (Bsp.: Gruppe von Berater*innen, Supervisor*innen/Beirät*innen);
- **Absicht des Verantwortlichen**, die personenbezogenen Daten an ein **Drittland oder eine internationale Organisation zu übermitteln** (Bsp.: Möglichkeit von Wartungszugriffen durch IT-Dienstleister wie z.B. Cloud-Anbieter mit Sitz in einem Drittstaat wie etwa den USA).

[12] So gehen z.B. Paal/Hennemann in: Paal/Pauly, DS-GVO/BDSG 2. Aufl., Art. 13 DS-GVO, Rn. 22 von einer unwiderleglichen, gesetzlichen Vermutung aus, dass die Informationen des Abs. 2 immer für die transparente Verarbeitung vonnöten sind.

[13] Die folgende Auflistung der Pflichten nach Art. 13 Abs.1 und Abs. 2 DS-GVO stammt weitestgehend von *LDI NRW*, Datenschutz im Verein nach der DS-GVO (November 2018), S. 12.

Zusätzlich sind nach **Art. 13 Abs. 2 DS-GVO** Informationen über

- die geplante **Speicherdauer**,
- die **Betroffenenrechte**,
- das **Recht zum jederzeitigen Widerruf einer Einwilligung** und die Tatsache, dass die Rechtmäßigkeit der Verarbeitung auf Grundlage der Einwilligung bis zum Widerruf unberührt bleibt (Bsp.: Widerruf der Einwilligung zur Verwendung der personenbezogenen Daten zu Zwecken der Beratung),
- das **Beschwerderecht** bei einer **Aufsichtsbehörde**,
- ggf. die **gesetzliche oder vertragliche Verpflichtung des Verantwortlichen** (z.B. Speicherverpflichtungen wie § 147 AO, siehe *B.IV.1.d)*),
- personenbezogene Daten Dritten bereitzustellen und die möglichen Folgen der Nichtbereitstellung der personenbezogenen Daten (Bsp.: Verpflichtung des Vereins zur Übermittlung von Daten an eine Versicherung aus Versicherungsvertrag bspw. zur Absicherung von Fahrten eines Vereins) und
- im Falle einer automatisierten Entscheidungsfindung (einschließlich *Profiling*) aussagekräftige Informationen über die verwendete Logik, die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung (Anmerkung: Dies dürfte bei RLC regelmäßig nicht der Fall sein)

zur Verfügung zu stellen.

Praxistipp

Der Informationspflicht nach Art. 13 DS-GVO wird durch Verwendung der in den **Anhängen 1 bis 6** jeweils enthaltenen **„Hinweisen zur Datenverarbeitung“** Genüge getan.

b) Erhebung über Dritte (Art. 14 DS-GVO)

Werden Daten über eine Person **bei einem Dritten** erhoben, ist der/die Betroffene grundsätzlich nach Art. 14 DS-GVO zu informieren. Das gilt auch bei Spontanübermittlungen, die auf der eigenen Initiative des Dritten beruhen, wenn die Daten anschließend vom Verantwortlichen zielgerichtet verarbeitet werden. Die Informationspflicht tritt also etwa grundsätzlich ein, wenn ein*e Klient*in Informationen über Dritte in der Beratung kundtut und diese sodann in die Akte aufgenommen und gespeichert werden.

Worüber der Dritte zu informieren ist, ergibt sich aus Art. 14 Abs. 1 und 2 DS-GVO – der **Inhalt** korrespondiert weitgehend mit der soeben behandelnden Informationspflicht aus Art. 13 DS-GVO. Zudem ist aber etwa auch offenzulegen, aus welcher Quelle die Informationen stammen, Art. 14 Abs. 2 lit. f DS-GVO.

Die Informationspflicht ist fristgebunden. Bei rein interner Verarbeitung ist der Dritte **spätestens innerhalb eines Monats** zu

informieren, Art. 14 Abs. 3 lit. a DS-GVO; bei Weitergabe der Informationen spätestens im Zeitpunkt der Weitergabe, Art. 14 Abs. 3 lit. c DS-GVO.

Ausschlusstatbestände befinden sich in Abs. 5 der Vorschrift. Die wichtigsten lauten:

- **Kenntnis (Abs. 5 lit. a):** Der Dritte ist nicht zu informieren, wenn und soweit er schon informiert wurde. Dies kommt insbesondere bei Datenübermittlungen in Betracht, wenn der ursprüngliche Verantwortliche bereits nach Art. 13 DS-GVO informiert hat.
- **Unmöglichkeit (Abs. 5 lit. b Var. 1):** Die Erfüllung der Informationspflicht ist unmöglich, wenn der Verantwortliche die betroffene Person nicht kennt und auch nicht identifizieren kann. Geht es allerdings nur darum, dass er sich – womöglich aufwändig - Kontaktdaten beschaffen müsste, liegt kein Fall der Unmöglichkeit vor.
- **Unverhältnismäßiger Aufwand (Abs. 5 lit. b Var. 2):** Maßgeblich ist hier eine Abwägung zwischen dem voraussichtlichen Aufwand der Mitteilung und dem Informationsinteresse der betroffenen Person. Die Ausnahmevorschrift wird aber äußerst restriktiv gehandhabt: Die Art. 29-Datenschutzgruppe nennt als Beispiel etwa historische Forscher, die eine Datenbank mit 20.000 Betroffenen nutzen möchte, die vor 50 Jahren erstellt und seitdem nicht mehr aktualisiert wurde.[14]
- **Gefährdung der Verarbeitungsziele (Abs. 5 lit b. Var. 4):** Dies ist der Fall, wenn die Tatsache der Datenerhebung vor der betroffenen Person geheim gehalten werden muss, damit die Verarbeitung ihr Ziel erreichen kann. Auch hier ist dieses Geheimhaltungsbedürfnis mit dem Informationsinteresse der betroffenen Person abzuwägen.
- **Berufsgeheimnis (Abs. 5 lit. d):** Anderes als Rechtsanwälte sind RLCs keine Berufsgeheimnisträger im Sinne des § 203 StGB (siehe bereits unter ***B.I***), sodass die Vorschrift keine Anwendung findet.
- **Geheimhaltungspflicht (Abs. 5 lit. d iVm § 29 Abs. 1 S. 1 BDSG):** Der Dritte ist nicht zu informieren, wenn andernfalls Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Es bedarf jeweils einer Interessenabwägung im Einzelfall, im Rahmen derer das berechtigte Geheimhaltungsinteresse des Dritten dem datenschutzrechtlichen Informationsanspruch des Betroffenen gegenüberzustellen ist. Es sind dann auch geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person zu ergreifen. Es ist darüber hinaus schriftlich festzuhalten, aus welchen Gründen von einer Information abgesehen worden ist.
- **Beeinträchtigung zivilrechtlicher Ansprüche (Abs. 5 lit. d iVm § 33 Abs. 1 BDSG):** Die Informationspflicht tritt nicht ein, wenn durch deren Erfüllung die Geltendmachung, Ausübung oder Verteidigung **zivilrechtlicher** Ansprüche beeinträchtigt würde

[14] Artikel-29-Datenschutzgruppe, WP 260, S. 36, https://www.ldi.nrw.de/mainmenu_Service/submenu_Links/Inhalt2/Artikel-29-Gruppe/wp260rev01_de.pdf.

8. Satzungsanpassung und Datenschutzordnung

Ob Vereins-RLCs eine Datenschutzordnung erlassen und/oder Datenschutzbestimmungen in ihre Vereinssatzung aufnehmen müssen, ist aktuell nicht abschließend geklärt. **Eine Rechtsgrundlage gibt es dafür seit Inkrafttreten der DS-GVO nicht mehr.** In jedem Fall sind **Uni-RLCs von dieser Verpflichtung nicht erfasst**, da es sich um spezifische Regelungen für die juristische Person des Vereins handelt.

Für die Vereins-RLCs beurteilten die Aufsichtsbehörden der einzelnen Bundesländer die Frage der Notwendigkeit uns gegenüber unterschiedlich: In **Bayern** etwa wird der Erlass einer **Datenschutzordnung nicht für erforderlich** erachtet, in **Nordrhein-Westfalen** wird es **empfohlen**, im **Saarland** als **verpflichtend** eingestuft. Ob die Vereins-RLCs deshalb eine Datenschutzordnung erlassen wollen und/oder die Satzung ändern, bleibt ihnen deshalb selbst überlassen; hier eine klare Empfehlung für alle Bundesländer zu geben, ist aktuell nicht möglich. Wenn sich die zuständige Aufsichtsbehörde noch nicht positioniert hat, ist eine Anfrage sinnvoll und vermeidet Zweifel.

Im Anhang findet sich aber ein Vorschlag für einen Satzungspassus und eine Datenschutzordnung. Wenn sich die RLC dafür entscheidet, ist es wichtig, dass sich die Datenschutzordnung und die sonstigen datenschutzrechtlichen Unterlagen, insbesondere das Verarbeitungsverzeichnis (siehe ***B.V.1***), **nicht widersprechen.** Die Dokumentationspflichten bleiben neben der Datenschutzordnung trotzdem bestehen und müssen den Anforderungen der DS-GVO genügen.

Die **Datenschutzordnung dient dazu**, für die Betroffenen transparent darzustellen, von wem welche Daten wie verarbeitet werden, wer für die Verarbeitung zuständig ist etc. Es ist empfehlenswert, sich beim Aufbau der Datenschutzregelungen am Weg der Daten von der Erhebung über die Speicherung, Nutzung, Verarbeitung (insbesondere Übermittlung) bis zu ihrer Sperrung und Löschung zu orientieren. Dabei ist jeweils konkret festzulegen, **welche Daten** (z.B. Name, Vorname, Adresse, E-Mail-Adresse usw.) welcher Personen (z.B. Vereinsmitglieder, Teilnehmer an Veranstaltungen oder Lehrgängen, Besucher von Veranstaltungen) für **welche Zwecke** verwendet werden, ggf. auch, ob Vordrucke und Formulare zum Einsatz kommen. Der Verein sollte hier außerdem regeln, **welcher Funktionsträger zu welchen Daten Zugang hat** und zu welchem Zweck er Daten von Mitgliedern und Dritten verarbeiten und nutzen darf. Ferner sollte geregelt werden, welche Daten zu welchem Zweck im Wege der **Auftragsdatenverarbeitung** (z.B. Verlagerung personenbezogener Daten in eine Cloud) verarbeitet werden.

Praxistipp

Die entsprechenden Informationen könnten theoretisch auch in die Vereinssatzung aufgenommen werden. Die Datenschutzordnung hat jedoch den Vorteil, dass sie per Vorstandsbeschluss verabschiedet und geändert werden kann. Im Gegensatz dazu braucht es bei einer Satzungsänderung stets eine Mitgliedervollversammlung und die Satzung muss im Vereinsregister beim zuständigen Registergericht geändert werden. Dafür fallen in der Regel auch zusätzliche Kosten an.

Deshalb bietet sich **folgende Lösung** an: Der Verein beschließt im Rahmen der Mitgliedervollversammlung einmal **eine Satzungsänderung** (Vorlage 11, siehe *E.XI*), die knapp auf die Datenschutzordnung verweist. Danach verabschiedet der Vorstand eine **Datenschutzordnung** (Vorlage 11, siehe *E.XII*), die ggf. auch später einfach geändert werden kann.

Vorlagen

Anhang 11: Vorschlag für einen Satzungspassus für Vereins-(R)LCs

Anhang 12: Vorschlag für eine Datenschutzordnung

VI. *Rechte der Betroffenen*

1. Formale und inhaltliche Anforderungen (für alle Betroffenenrechte)

Bei der Verarbeitung personenbezogener Daten stehen den Betroffenen gem. Art. 12ff. DS-GVO eine Reihe von Rechten zu (sog. Betroffenenrechte). Unter ***B.V.7.a)*** wurde bereits erörtert, dass der Verantwortliche in der Pflicht steht, die Betroffenen über ihre Rechte aufzuklären. Im Folgenden wird nun auf die einzelnen Rechte eingegangen. Zunächst folgen aber einige allgemeine Hinweise, die für sämtlichen Betroffenenrechte gelten.

Für die Geltendmachung der Betroffenenrechte gilt grundsätzlich Formfreiheit (möglich also etwa *in persona*, schriftlich oder auch mündlich via Telefon). Die Rechte sind unentgeltlich zu gewähren, es sei denn, es handelt sich um offensichtlich unbegründete Anträge, exzessiven Missbrauch durch die Betroffenen nach Art. 12 Abs. 5 S. 2 lit. a DS-GVO oder um Datenkopien nach Art. 15 Abs. 3 S. 2 DS-GVO handelt.

Der Verarbeiter, also typischerweise die RLC selbst, hat unverzüglich, spätestens innerhalb eines Monats auf die Geltendmachung von Betroffenenrechten zu reagieren. Wenn es sich um einen sehr komplexen Fall handelt und mehr Zeit für die Bearbeitung benötigt wird, muss der Verarbeiter den/die Betroffene*n kontaktieren und kann die Frist auf bis zu 3 Monate verlängern (Art. 12 Abs. 3 DS-GVO). Um einen solchen komplexen Fall dürfte es sich aber bei den verhältnismäßig kleinen Datenmengen bei RLCs regelmäßig nicht handeln.

2. Auskunftsrecht (Art. 15 DS-GVO)

Betroffenen Personen steht (unabhängig vom Rechtsgrund der Datenerhebung) gem. Art. 15 Abs. 1, 2 DS-GVO das Recht zu, eine Auskunft über sämtliche sie betreffende personenbezogene Daten zu erhalten.
Der Anspruch umfasst die erhobenen Daten an sich, sowie sämtliche zur Kategorisierung erfassten Metadaten. Ein solcher Auskunftsanspruch dürfte in der täglichen Arbeit der RLCs das praxisrelevanteste Betroffenenrecht darstellen.

Die Bearbeitung einer Auskunftsanfrage lässt sich in der Praxis am besten in zwei Schritte unterteilen:

1. Schritt - Verarbeitungsbestätigung

Bevor eine Auskunft erteilt wird, muss stets die Identität des*r Antragsteller*in überprüft werden. Bei begründeten Zweifeln an der Identität muss die RLC die Auskunft einstweilen aussetzen und alle vertretbaren Möglichkeiten nutzen, die beantragende Person zu identifizieren (Art. 12 Abs. 6 DS-GVO). Denn die Auskunftserteilung an einen Dritten wäre ein Verstoß gegen die DS-GVO. Wenn ein*e Betroffen*er beispielsweise eine Anfrage via Telefon oder über eine bisher unbekannte E-Mail-Adresse stellt, sind begründete Zweifel anzunehmen. Man könnte die Person also etwa bitten, die der RLC bereits bekannte E-Mail-Adresse zu verwenden und so ihre/seine Identität durch Übereinstimmung verifizieren. Bei einer Ablehnung der Auskunft infolge der zweifelhaften Identität sind die Vorgaben des Art. 12 Abs. 4 DS-GVO zu beachten.

Sobald die Identität verifiziert ist sollte überprüft werden, **ob** überhaupt personenbezogene Daten erfasst wurden. Wenn keinerlei Daten vorliegen (was jedoch in der Praxis selten auftreten dürfte), muss eine sog. Negativbestätigung erteilt werden. Wenn Daten vorliegen, sollte die betroffene Person informiert werden, dass Daten vorliegen und diese innerhalb der unter ***B.VI.1*** beschriebenen Frist herausgegeben werden.

2. Schritt - Präzisierungsbestätigung

Wenn im ersten Schritt festgestellt wurde, dass Daten über die betreffende Person vorliegen, wird in einem zweiten Schritt die eigentliche Auskunft vorbereitet. Hierbei muss über die personenbezogenen Daten selbst Auskunft erteilt werden, z.B. “Herr Max Mustermann” etc.

Die nachfolgend genannten Punkte sind gem. Art. 15 Abs. 1 DS-GVO bei der Auskunft in jedem Fall ergänzend zu den genannten personenbezogenen Daten zu nennen:

- Konkreter Verarbeitungszweck (Art. 15 Abs. 1 lit. a);
  - Beispiel: *“Fallbearbeitung: Herr Max Mustermann in Sachen Familiennachzug”*

- Kategorisierung der Daten (Art. 15 Abs. 1 lit. b);
  - Beispiel:
    - *“unmittelbare Personendaten” (z.B. Name, Adresse, Geburtsdatum),*
    - *“Gesundheitsdaten” (z.B. Atteste, Gutachten),*
    - *“Fluchtgeschichte” (z.B. Aufzeichnung des Fluchtweges etc.)*

- Empfänger oder Kategorien von Empfängern (Art. 15 Abs. 1 lit. c), gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
  - Beispiel:
    - *“Übermittlung innerhalb der RLC an die Berater*innen”*
    - *“Übermittlung an Auftragsverarbeiter Microsoft Inc.”*
- falls möglich, die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer (Art. 15 Abs. 1 lit. d);
  - Beispiel: *“Die geplante Speicherdauer beträgt XX Jahre, da wir verpflichtet sind die Daten solange zu speichern.” (*zur Speicherdauer siehe ***B.V.5***)
- Verweis auf die weiteren Betroffenenrechte (Art. 15 Abs. 1 lit. e, f)
  - Bei der Bearbeitung einer Anfrage muss explizit auf folgende Betroffenenrechte hingewiesen werden:
    - Recht auf Berichtigung (Art. 16 DS-GVO)
    - Recht auf Löschung (Art. 17 DS-GVO)

        - Recht auf Einschränkung der Datenverarbeitung (Art. 18 DS-GVO)
        - Recht auf Widerspruch gegen die Verarbeitung (Art. 21 DS-GVO)
        - Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 79 DS-GVO)
    - Es reicht jedoch ein Hinweis auf die Rechte, da es nicht um eine Rechtsberatung geht.[15] Es dürfte also ausreichen auf die Rechte in fetter Schrift hinzuweisen und jedes der Rechte in 1-2 Sätzen im Rahmen der Auskunft zu erläutern.
- Herkunft der Daten, sofern diese nicht bei der betroffenen Person erhoben wurden (Art. 15 Abs. 1 lit. g); ein typischer Fall dafür in der RLC-Arbeit wäre eine Mail mit Informationen, die von einem Freund/Familienangehörigen des Klienten nachträglich an eine*n Berater*in geschickt wurden.
    - Beispiel: *"Telefongespräch/E-Mail vom 26.05.2018 mit Frau/Herrn XY"*

Neben der konkreten Auskunft in der Präzisierungsbestätigung besteht für den Verantwortlichen nach Art. 15 Abs. 3, 4 DS-GVO die Pflicht, eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen. Es handelt sich dabei um die "Rohdaten", die nicht verändert werden dürfen. Das kann dazu führen, dass z.B. bei einer Anfrage des Klienten die Kommunikation (z.B. per Mail geführte) mit und über ihn als Kopie herauszugeben ist. Als Ausnahme zu diesem Recht ist Art. 15 Abs. 4 DS-GVO vorgesehen.

Eine Datenkopie ist stets in der Form (digital oder physisch) zur Verfügung zu stellen, in der die Daten auch originär erhoben wurden.

Die Auskunft ist **zwingend abschließend zu formulieren**! Ergibt sich aus der Auskunft nicht, dass dem Verantwortlichen keine weiteren Daten der jeweiligen Person vorliegen, ist die Auskunft unvollständig. Von daher sollte die Auskunft mit einer derartigen Formulierung abschließen.

Praxistipp

Für die Beantwortung von Auskunftsanfragen sollte jede RLC vorbereitet sein. Es macht also Sinn die **interne Aktenstruktur** (und dabei insb. die IT-Struktur) so **umzubauen**, dass man möglichst zu **allen relevanten Bereichen der Präzisierungsbestätigung** klare Auskünfte **innerhalb der gebotenen Frist** geben kann.

Deshalb hier nochmals die relevanten Bereiche der Präzisierungsbestätigung:

- **Verarbeitungszweck**
- **Kategorisierung**
- **Empfänger und Kategorien von Empfängern**
- **Geplante Speicherdauer**
- **Herkunft der Daten**

Für den Hinweis auf die **weiteren Betroffenenrechte** sollten einige standardisierte Sätze für die Auskunft formuliert werden. Darüber hinaus sollte man sich überlegen, wie man die Daten im Rahmen der **Datenkopie unverändert exportiert**. Für elektronisch verarbeitete Daten empfiehlt es sich, sämtliche Daten in einem Ordner oder einer Datei (z.B. PDF) zusammenzufassen. Danach sollte man sämtliche Daten via E-Mail weiterleiten und die Versandbestätigung irgendwo dokumentieren. Wenn Daten physisch erhoben wurden und auch in dieser Form herausgegeben werden müssen, sollte man alle Dokumente kopieren und sich die Übergabe der Daten quittieren

[15] So auch Franck, in: Gola, DS-GVO 2. Aufl. 2018, Art. 15, Rn. 16.

3. Recht auf Löschung / „Recht auf Vergessenwerden“ (Art. 17 Abs. 1 DS-GVO)

Mit der objektiven Pflicht zur Löschung personenbezogener Daten aus Art. 17 Abs. 1 DS-GVO korrespondiert ein subjektives Recht des Betroffenen, von dem Verantwortlichen die Löschung zu verlangen. Liegen die entsprechenden Voraussetzungen vor (siehe hierzu ausführlich ***B.V.5***) haben die Betroffenen also einen **Anspruch auf Löschung**. Dieser kann durch formlosen Antrag beim Verantwortlichen geltend gemacht werden. Zur Verdeutlichung soll das folgende Beispiel[16] dienen:

Praxistipp

Beispiel: Austritt eines Mitglieds aus dem Verein

X tritt aus dem Verein aus. Seine Mitgliedsdaten sind, sofern keine gegenseitigen Ansprüche mehr im Raume stehen, daher nicht mehr für die Zwecke notwendig, für die sie erhoben wurden (z. B. Mitgliederverwaltung, ggf. Beitragsverwaltung). Demnach hat er einen Anspruch auf Löschung, den er sodann auch geltend macht. **Was muss der Verein nun tun?**

Die Daten des X sind grundsätzlich zu löschen. Es besteht bspw. dann eine Ausnahme von diesem Grundsatz, wenn X eine Einwilligung erteilt hat (bspw. Einwilligung zur Aufnahme in eine Ehemaligenliste) oder steuerrechtliche Aufbewahrungspflichten der Löschung entgegenstehen. In letzterem Fall sind die Daten aber dann zu sperren, d. h. sie dürfen nur noch aufbewahrt werden, um die Aufbewahrungspflichten zu erfüllen und nicht etwa dafür, den X zu kontaktieren.

4. Widerspruchsrecht (Art. 21 DS-GVO)

Jeder Betroffene kann grundsätzlich auch jeder richtigen und zulässigen Verarbeitung von personenbezogenen Daten widersprechen. Dies gilt aber nur, wenn die Verarbeitung der entsprechenden Daten auf Art. 6 Abs. 1 lit. e oder f DS-GVO gestützt wurde, also insbesondere wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen erfolgte (siehe hierzu ***B.IV.1.c)***). Findet die Verarbeitung ihre Grundlage dagegen in einem anderen Erlaubnistatbestand, ist ein Widerspruch nicht möglich.

Aber: Im Fall der Einwilligung hat der Betroffene ein Widerrufsrecht aus Art. 7 Abs. 3 DS-GVO (siehe hierzu bereits ***B.IV.1.a***)).

Das Widerspruchsrecht hat die folgenden Voraussetzungen:

- Die betreffenden Daten müssen den/die Widersprechende*n **selbst betreffen** (→ Widerspruch funktioniert nur bei eigenen Daten).
- der/die Betroffene muss erläutern, dass für ihn/sie eine **besondere Situation** vorliegt, die den Widerspruch rechtfertigt.

[16] Beispiel stammt von *LDI NRW*, Datenschutz im Verein nach der DS-GVO (November 2018), S. 17.

- Es dürfen **keine zwingenden, überwiegenden schutzwürdigen Gründe des Verantwortlichen** vorliegen (Bsp.: Relevanz für gerichtliche Verfahren, Daten sind relevant für rechtl. Anspruch gegen den Betroffenen).

5. Recht auf Berichtigung (Art. 16 DS-GVO)

Auf Verlangen der Betroffenen besteht eine **Berichtigungspflicht** der sie/ihn betreffenden personenbezogenen Daten, soweit diese unrichtig sind. Ohnehin unterliegen RLCs gemäß Art. 5 Abs. 1 lit. d DS-GVO der Pflicht, nur sachlich richtige Daten zu verarbeiten. Der betroffenen Person obliegt grundsätzlich die Darlegungs- und Beweislast für das Vorliegen einer Unrichtigkeit.

6. Recht auf Einschränkung der Verarbeitung (Art. 18 DS-GVO)

Auf Verlangen der Betroffenen ist in den in Art. 18 Abs. 1 DS-GVO genannten Fällen die weitere Verarbeitung bereits gespeicherter Daten zu unterlassen. Nach der Definition des Art. 4 Nr. 3 DS-GVO müssen diese Daten dann mit einem **Einschränkungsvermerk gekennzeichnet werden** und dürfen nur in den Fällen des Art. 18 Abs. 2 DS-GVO verarbeitet werden (Einwilligung der betroffenen Person; Schutz der Rechtsansprüche/Rechte des Betroffenen oder einer anderen Person; wichtiges öffentliches Interesse). Die Einschränkung kann verlangt werden, wenn **einer** der folgenden Einschränkungsgründe **vorliegt**:

- Bestreiten der **Richtigkeit der Daten**
- **Unrechtmäßigkeit der Verarbeitung** (und der Verantwortliche verweigert ein Recht auf Löschung)
- Geltendmachung, Ausübung oder Verteidigung von **Rechtsansprüchen**
- Einlegen eines **Widerspruchs** (bei dem noch keine Interessensabwägung stattgefunden hat)

7. Recht auf Datenübertragbarkeit/Datenportabilität (Art. 20 DS-GVO)

Das Recht auf Datenübertragbarkeit bedeutet, dass eine betroffene Person, die zu einer anderen Beratungsstelle oder einem*r Rechtsanwält*in gehen möchte, auf Verlangen alle über sie erhobenen Daten erhalten soll. Dabei müssen die Daten in „maschinenlesbarer" Form, also in der Praxis in einem gängigen Dokumentenformat, zur Verfügung gestellt werden. Es geht demnach um die Möglichkeit der betroffenen Person, ihre Daten „mitzunehmen".

Das Recht auf Datenübertragbarkeit setzt voraus, dass

- die Daten den/die Antragsteller*in selbst betreffen,
- diese dem Verantwortlichen aktiv und willentlich im Wege einer Einwilligung oder aufgrund eines Vertrages bereitgestellt wurden,
- durch die Herausgabe keine Rechte Dritter beeinträchtigt werden (Abs. 3)
- und die Daten mithilfe **automatisierter Verfahren** verarbeitet wurden (z.B.

automatische Erfassung von Fotos durch Social-Media Plattformen[17]).

Der Begriff der Verarbeitung „mithilfe automatisierter Verfahren“ ist dabei gleichbedeutend mit der „automatisierten Verarbeitung“ nach Art. 2 Abs. 1 DS-GVO. Erfasst sind demnach alle rechnergestützten Vorgänge mit personenbezogenen Daten. Ausgenommen vom Recht auf Datenportabilität sind lediglich nicht-automatisierte Verarbeitungsvorgänge, durch welche die Daten in einem Dateisystem erfasst werden, also etwa das händische Erstellen von Akten, die in einen alphabetisch geordneten Aktenschrank einsortiert werden.

Praxistipp

Was muss die RLC bei einer Anfrage auf Datenübertragung tun?

1. Die RLC muss nun zunächst prüfen, **welche Daten von dem Recht auf Datenübertragbarkeit erfasst sind**. Das sind alle personenbezogenen Daten, die die oben aufgelisteten Kriterien erfüllen. Insbesondere kommen also alle Daten der betroffenen Person in Betracht, die digital vorliegen. Nicht erfasst sind etwa handschriftliche Notizen der Berater*innen.

2. Die ermittelten Daten müssen nun in „**maschinenlesbarer Form**“ übermittelt werden. Bei den im Rahmen einer RLC verarbeiteten Daten bedeutet das in der Praxis eines der standardmäßig eingesetzten Datei-Formate wie z.B. XLS (Excel) oder DOCX (Word).

Praxistipp

Relevanz aller Betroffenenrechte in der RLC-Arbeit:

Zusammenfassend lässt sich für die Betroffenenrechte im Zusammenhang mit der RLC-Arbeit sagen, dass vor allem das **Auskunftsrecht (Art. 15 DS-GVO)** und das **Recht auf Löschung (Art. 17 DS-GVO)** eine Rolle spielen dürften.

Insbesondere auf dessen Umsetzung sollte sich jede RLC vorbereiten, wobei als Betroffene sowohl die Klient*innen als auch alle sonstigen in der RLC tätigen Personen in Betracht kommen.

VII. *Befugnisse der Aufsichtsbehörde (insb. Sanktionsbefugnis)*

Die Aufsichtsbehörden, sprich die Datenschutzbeauftragten der Länder und des Bundes, haben die Anwendung der DS-GVO zu überwachen und durchzusetzen, Art. 57 DS-

[17] Dieses Beispiel der Datenübertragbarkeit nannte die Europäische Kommission in einem *working paper* von 2012; Europäische Kommission, SEC (2012) 72 final, vom 25.01.2012, S. 72.

GVO. Zu diesem Zweck stehen ihnen eine Reihe von Untersuchungs- (Art. 58 Abs. 1 DS-GVO) und Abhilfebefugnissen (Art. 58 Abs. 2 DS-GVO), wie die Informationsbeschaffung, Warnung oder **Verwarnung** (Art. 58 Abs. 1 lit. a; Abs. 2 lit. a, b DS-GVO) zu. Die Abhilfebefugnisse der Datenschutz-Aufsichtsbehörden enthalten auch Sanktionsbefugnisse, d.h. die Befugnis, **Geldbußen** wegen Verstößen gegen die DS-GVO zu verhängen (Art. 58 Abs. 2 lit. i iVm Art. 83 DS-GVO). Nach dem Schuldgrundsatz ist insofern ein vorsätzliches oder fahrlässiges Verhalten Voraussetzung.

Dem steht die Verpflichtung der Aufsichtsbehörden zu einer Aufklärungs- und Sensibilisierungsfunktion (Art. 57 Abs. 1 lit b, d) gegenüber. Die Datenschutzbeauftragten können bei Unsicherheiten über die Auslegung des Datenschutzrechts deshalb sehr gerne kontaktiert werden. Einige Datenschutzbeauftragten bieten sogar Beratung über eine "DS-GVO-Hotline" an.

Praxistipp

Für RLCs bedeutet dies, dass Verstöße gegen die in dieser Broschüre aufgeführten datenschutzrechtlichen Vorschriften zum Einschreiten der Aufsichtsbehörde führen können. **Geldbußen sind in der Praxis aber nur als *ultima ratio* zu erwarten.** In der Regel werden die Aufsichtsbehörden einen Verantwortlichen zunächst anschreiben, um den Sachverhallt zu erörtern, und gegebenenfalls Verwarnungen aussprechen.

C. Hinweise zur Datenschutzkonformität von Internetauftritten

I. *Betrieb einer Website (Datenschutzerklärung)*

Als Betreiber*in einer Website muss man, wie auch in jedem anderen Bereich, über die Verarbeitung personenbezogener Daten aufklären und es muss für bestimmte Verarbeitungsvorgänge eine Einwilligung eingeholt werden. Für die Information der Betroffenen hat sich das Modell der Datenschutzerklärung auf der Website etabliert.

Bei dem Betrieb einer Website ist es praktisch unmöglich keine personenbezogenen Daten zu erheben. Deswegen muss die Website stets über eine Datenschutzerklärung verfügen, um alle Informationspflichten (insb. aus Art. 13 DS-GVO, siehe ***B.V.7.a)***) zu erfüllen. Es bietet sich an in der Datenschutzerklärung nicht nur auf die Verarbeitung hinzuweisen, die direkt auf der Website stattfindet, sondern dort z.B. auch über die Datenverarbeitung im Rahmen einer Beratungsanfrage oder einer Spende an die RLC aufzuklären.

Wie erstelle ich eine Datenschutzerklärung für unserer RLC?

Vorlage

Anhang 13: Datenschutzerklärung für die Website

Hinweis:

Bitte beachtet, dass eine Datenschutzerklärung immer der aktuellen Datenverarbeitung auf der Website entsprechen muss. Zudem erfordern Gesetzesänderungen, Erklärungen der Datenschutzbehörden und Gerichtsentscheidungen etc. häufiger kleinere Anpassungen, weswegen die Datenschutzerklärung **regelmäßig überprüft** werden sollte. Die AG Datenschutz wird versuchen bei relevanten Änderungen eine aktualisierte Version der Vorlage zu veröffentlichen.

Praxistipp

Wie verwenden wir die Vorlage (Anhang 13) richtig?

Die Vorlage der Datenschutzerklärung ist, vereinfacht gesagt, in zwei Teile aufgeteilt:

- Der **allgemeine Teil** befindet sich am Anfang und am Ende der Erklärung. Dieser ist farblich nicht eingefärbt und enthält allgemeine Angaben zu den Verantwortlichen der Verarbeitung, die Betroffenenrechte, zur Datensicherheit und zu den richtigen Ansprechpartnern. **Alle diese Teilbereiche werden auf jeden Fall benötigt** und sollten nur in den gelb markierten Bereichen entsprechend für die jeweilige (R)LC angepasst werden.

- Der **besondere Teil** ist der gesamte mittlere Bereich und ist grün markiert. Diese Teilbereiche beschreiben die verschiedensten Verarbeitungsvorgänge, sowie Tools und Webanwendungen wie z.B. Youtube, Google Ads, Jetpack (Wordpress), diverse Social-Media Plattformen (wie z.B. Facebook, Twitter). Jede dieser Webanwendungen verarbeitet personenbezogene Daten, weshalb über deren Einsatz aufgeklärt werden muss. Die RLC muss also in einem ersten Schritt identifizieren, welche der in §§ 4-12 genannten Dienste eingesetzt werden. Im zweiten Schritt sollten dann alle Anwendungen aus der DS-Erklärung entfernt werden, die nicht verwendet werden.
  Auch die grünen Bereiche enthalten teilweise gelb markierte Felder. Diese müssen entsprechend angepasst werden, wenn dieser Teilbereich beibehalten wird.

Als **Alternative zu der von uns erstellten Vorlage** gibt es im Internet inzwischen eine ganze Reihe von Generatoren, mit denen man sich recht schnell und kostenfrei selbst eine individuell zugeschnittene Datenschutzerklärung generieren lassen kann.

Praxistipp

Beispiele für die beschriebenen **Datenschutzerklärungs-Generatoren** :

1. https://DS-GVO-muster-datenschutzerklaerung.dg-datenschutz.de/
- https://www.activemind.de/datenschutz/datenschutzhinweis-generator/
- https://www.wbs-law.de/it-recht/datenschutzrecht/datenschutzerklaerung-generator/
- https://datenschutz-generator.de/

Eine so erzeugte Datenschutzerklärung sollte vor der Einbindung aber kritisch gegengelesen werden. Insbesondere muss darauf geachtet werden, dass alle Verarbeitungsvorgänge in der Datenschutzerklärung aufgenommen wurden. Werden z.B. PlugIns von Drittanbietern, Google Fonts oder sonstige Dienste eingebunden, müssen diese darin enthalten sein. Teilweise werden die Verlinkung und Namensnennung des Urhebers verlangt. Wird das nicht gemacht, liegt unter Umständen ein urheberrechtlicher Verstoß vor.

Hinweis: Da die von uns erarbeitete Vorlage schon weitestgehend auf die Verarbeitungsvorgänge einer RLC heruntergebrochen wurde, empfehlen wir – wenig überraschend – die Verwendung der oben genannten Vorlage.

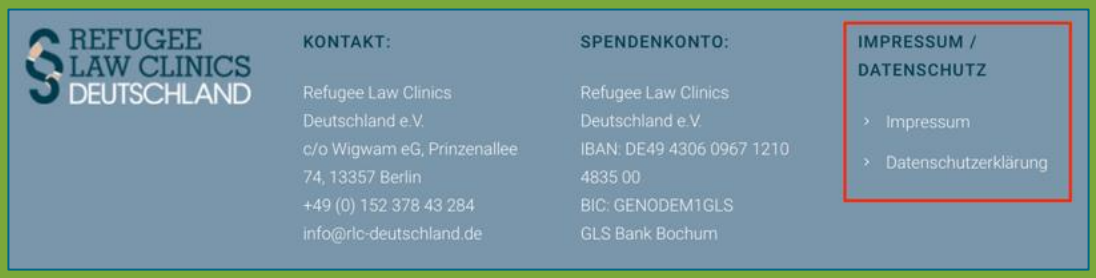
Wo füge ich die DS-Erklärung auf der Website ein?

Die Datenschutzerklärung muss für die Betroffenen auf der Website einfach auffindbar sein. In Anlehnung an die vom BGH (Urt. v. 20.06.2006, Az. I ZR 228/03) entwickelte 2-Klick-Regel bei der Impressumspflicht (§ 5 TMG), wird häufig auch die einfache Auffindbarkeit der Datenschutzerklärung so interpretiert. Das bedeutet, dass man die DS-Erklärung beim Aufrufen der Website durch maximal zwei Klicks aufrufen können sollte.

Um gar nicht erst über die Menge an Klicks nachdenken zu müssen, platziert man die Datenschutzerklärung am besten im sog. „Footer“ der Website, also dem untersten Bereich einer Website, der von jeder Seite erreichbar ist.

Praxistipp

Beim RLC-Dachverband auf der Website sieht das z.B. so aus (der rote Kasten dient hier nur der Verdeutlichung):



Im Sinne der Übersichtlichkeit sollte zwischen Impressum und Datenschutzerklärung unterschieden werden, wobei eine gemeinsame Überschrift (wie in der Abbildung) eher der Übersichtlichkeit verhilft und daher sogar anzuraten ist.

Mit einem Klick auf die Verlinkung im Footer sollte man dann zu einer eigenen Seite geleitet werden, wo die Datenschutzerklärung komplett aufgeführt wird. Da die Übersichtlichkeit und Nachvollziehbarkeit ein wichtiger Bestandteil der Erklärung ist, sollte man in jedem Fall eine gut lesbare Schriftart und -größe wählen. Zudem sollte man vor dem Upload auch nochmals die richtige Nummerierung der einzelnen Unterpunkte überprüfen.

II. *Betrieb von Social-Media (insb. Facebook-Fanpages)*

Eigentlich unterscheidet sich die Nutzung von Social Media im Großen und Ganzen nicht von jeder anderen Verarbeitung personenbezogener Daten. Aufgrund der technischen Komplexität und der teilweise undurchsichtigen Datenverarbeitung im Hintergrund durch die Social-Media-Dienste (Facebook, Twitter, Instagram etc.) stellen sich aber doch einige spezielle Fragen. Deshalb schon mal vorab: Es reicht sicher nicht aus, sich auf eine datenschutzkonforme Verarbeitung und Information der Betroffenen vonseiten der Dienste zu verlassen. Im Folgenden werden wir uns vor allem auf die Nutzung sog. „Fanpages" konzentrieren, die wohl den Regelfall von RLC-Social-Media bildet. Fanpages sind alle von einem Dritten betriebenen Seiten auf einer Social-Media-Plattform (wie z.B. die Facebook-Fanpage des Dachverbands).

Hinweis für den Betrieb von Facebook-Fanpages

Bitte beachtet, dass es nach Einschätzung der DSK vom 05. September 2018 aktuell praktisch nicht möglich ist, eine rechtssichere Facebook-Fanpage zu betreiben. Der Betrieb erfolgt auf eure eigene Gefahr hin. Details zum möglichen **Haftungsrisiko** finden sich unter *C.II.2*.

1. Informationspflichten bei Social Media

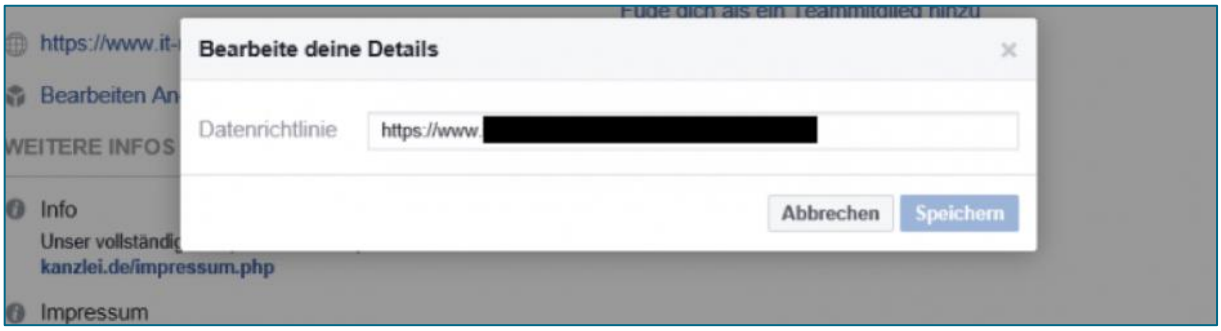
Auch für Social Media gelten dieselben Informationspflichten wie für jede andere Datenverarbeitung. Deshalb muss über sämtliche Verarbeitungen auf der Plattform aufgeklärt werden. Da man den Aufbau von Fanpages meist nur sehr eingeschränkt verändern und daher die Informationen nicht optimal platzieren kann, bietet es sich an auf die **Datenschutzerklärung auf der eigenen Homepage zu verlinken**. Daher sollte in die Datenschutzerklärung auf der eigenen Homepage auch die Verarbeitung der personenbezogenen Daten durch die RLC auf den verwendeten Fanpages mit aufgenommen werden.

Da niemand so richtig weiß, was Facebook & Co. tatsächlich mit den Daten der Nutzer machen, bietet es sich hier an, für jede Plattform auf gängige und anerkannte Standardformulierungen zurückzugreifen. Diese sind in unserer unter *C.I* genannten Datenschutzerklärungs-Vorlage und in den durch Generatoren erzeugten Datenschutzerklärungen in der Regel enthalten.

Wie verlinke ich auch die Datenschutzerklärung meiner Website auf Facebook?

Gehe auf eure Facebook-Page und klicke in der linken Leiste auf „Info“. Scroll runter bis du den Punkt „Datenrichtlinie“ siehst.

Geh nun auf "Bearbeiten" - dann erscheint folgendes Fenster:



Hier fügst Du nun den Link eurer DS-Erklärung der Website ein und klickst auf "speichern". Fertig. Bitte kontrolliere jetzt noch, ob die Speicherung auch angenommen wurde und bei Betätigung der Verlinkung "Datenschutzrichtlinie" auf der Fanpage die DS-Erklärung auch richtig angezeigt wird.

Alternative: Meine RLC hat aktuell gar keine Website, auf der man eine Datenschutzerklärung positionieren könnte und auf die man verlinken könnte. Allerdings betreiben wir eine Facebook-Fanpage. Gibt es eine Möglichkeit trotzdem eine Datenschutzerklärung auf der Website zu positionieren?

Ja. Es gibt die Möglichkeit dafür die **Notizen-Funktion** bei Facebook zu nutzen. Da dies einiger Einrichtungsschritte bei Facebook bedarf, haben wir dafür eine eigene Vorlage erstellt. Diese Vorlage enthält sowohl die Anleitung als auch eine Vorlage für eine spezielle Datenschutzerklärung.

Vorlage

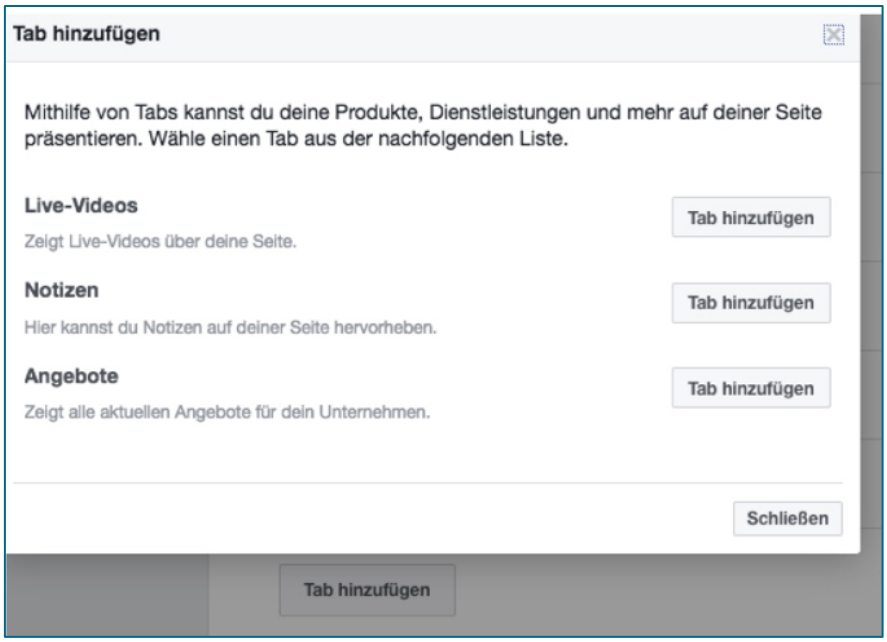
Anhang 14: Datenschutzerklärung für Facebook

Hinweis:

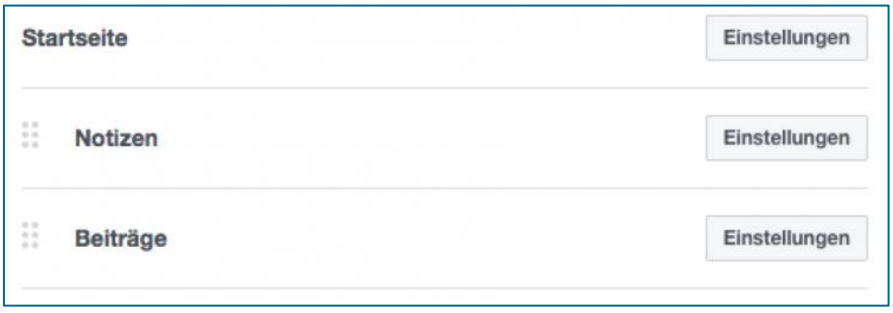
Diese Vorlage ist nur für solche (R)LCs sinnvoll, die **keine eigene Website haben auf dessen Datenschutzerklärung sie verlinken könnten**. Alle (R)LCs mit eigener Website sollten auf **die Vorlage in Anhang 13** zurückgreifen, da sonst zwei Datenschutzerklärungen aktuell gehalten werden müssen und die hier beschriebene Lösung über die Notizen-Funktion einige Nachteile bietet (z.B. Personen mit Zugriff auf den Facebook-Account können diese – unbeabsichtigt - recht leicht deaktivieren).

Wo füge ich die spezielle Datenschutzerklärung bei Facebook ein?[18]

In einigen Fällen fehlt der Tab „Notizen“ auf Facebook-Seiten, sodass dieser erst hinzugefügt werden muss. Dazu geht ihr auf euer Facebook-Seite unter > Einstellungen > Seite bearbeiten. Am Ende der Seite klickt ihr auf „Tab hinzufügen“. Es öffnet sich folgendes Fenster, in dem Sie erneut die Notizen mit „Tab hinzufügen“ bestätigen.

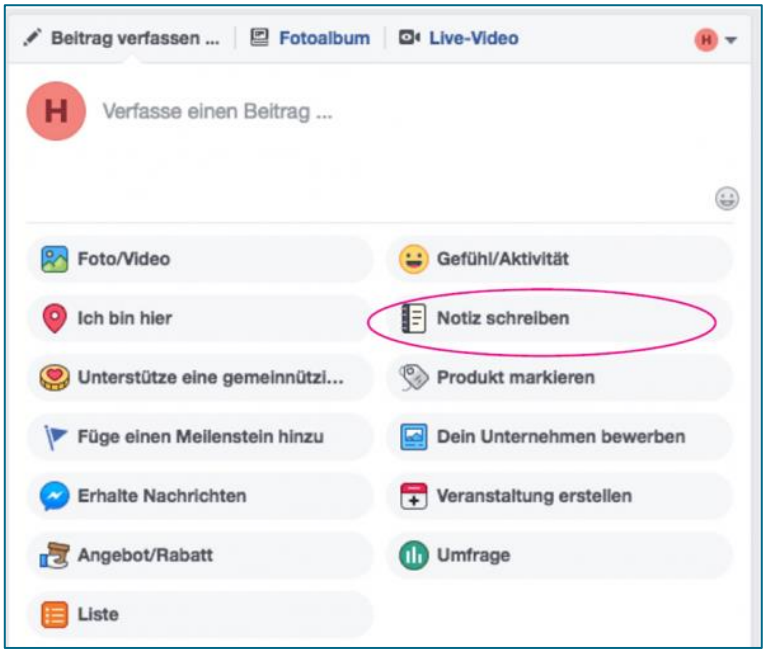


Damit die Notizen auf Ihrer Seiten-Pinnwand ganz oben erscheinen, ist es notwendig, dass ihr diese per Drag&Drop durch einen Klick auf die 6 grauen Punkte nach oben holt und zwar direkt unter die Startseite:



So weit zu den Vorbereitungen. Nun könnt ihr auf eure Startseite wechseln und dort beginnen die Notiz zu schreiben. Die Überschrift nennt ihr am besten „Datenschutzerklärung“. Im Textfeld könnt ihr dann einfach die für eure RLC angepasste DS-Erklärung einfügen.

[18] Diese Anleitung stammt in weiten Teilen von https://www.it-recht-kanzlei.de/datenschutzerklaerung-facebook-darstellung.html.



So sieht die fertige Datenschutzerklärung dann auf Ihrer Facebook-Seite aus:

2. Exkurs: (Mit-)Verantwortlichkeit von Fanpagebetreibern

Die jüngste Rechtsprechung des EuGH (Urt. vom 05.06.2018, Az. C-210/16) hat die Situation für Betreiber von Fanpages (also i.d.R. die RLC) nochmals erschwert. Demnach sind auch Betreiber von Fanpages (im konkreten Fall bei Facebook; dies lässt sich aber auf andere Plattformen übertragen) zumindest zum Teil **mit für die Datenerhebung durch Facebook verantwortlich**. Dies begründet das Gericht mit der von Facebook standardmäßig zur Verfügung gestellten und nicht abdingbaren Funktion *Facebook Insight*, die es dem Betreiber erlaubt, die gewünschte Zielgruppe anhand von Parametern (z.B. Alter, Beruf oder Geschlecht) zu bestimmen und daher zu beeinflussen, wessen Daten verarbeitet werden.

Im Ergebnis führt dies zu einer gemeinsamen Entscheidung über Zweck und Mittel der Verarbeitung („Joint Control") gem. Art. 4 Nr. 7 DS-GVO für die eine **Vereinbarung zwischen den Verantwortlichen gem. Art 26 DS-GVO**

erforderlich ist. In der Theorie bedeutet dies also, die RLC müsste einen Vertrag über die verschiedenen Verantwortlichkeiten mit Facebook schließen - ansonsten stellt dies einen gravierenden Verstoß gegen geltendes Recht dar.
Dass dies natürlich die Mitarbeit von Facebook voraussetzt, ist der Konferenz der unabhängigen Datenschutzbehörden (DSK) bereits einen Tag nach Urteilsverkündung aufgefallen (Entschließung vom 6.6.2018). Kurz darauf hat Facebook reagiert und nun standardmäßig mit den Betreibern der Fanpages diese Vereinbarung geschlossen.

Sollte jede RLC deswegen vorübergehend ihre Facebook-Fanpage schließen?

Diese Entscheidung müssen die Verantwortlichen einer jeden RLC für sich selbst treffen. Da unseres Wissens bisher für den Betrieb von Fanpages noch keine Bußgelder verhängt wurden, kann das Risiko des weiteren Betreibens einer nicht sonderlich hoch frequentierten Fanpage als sehr gering eingeschätzt werden. Allerdings muss man sich darüber im Klaren sein, dass Facebook-Fanpages aktuell nicht datenschutzkonform betrieben werden können.

Deswegen sollte man in jedem Fall die Neuerungen bei Facebook und die Erklärungen der DSK auf den Websites der Landesdatenschutzbehörden der Länder zu diesem Thema aufmerksam verfolgen Im November 2018 wurde bekannt, dass die Berliner Datenschutzbeauftragte einen Fragebogen an Unternehmen verschickt hat mit Fragen, die die Facebook-Fanpage betrafen. Es zeichnet sich also ab, dass die Aufsichtsbehörden Druck auf Facebook und Fanpage-Betreiber aufbauen wollen.

D. Weiterführende Informations- und Literaturhinweise

I. *Ausgewählte Kommentare und Ratgeber*

Ehmann/Selmayr, Datenschutz-Grundverordnung, 2. Aufl. 2018.

→ Seit der überarbeiteten 2. Auflage von 2018 hat der *Ehmann/Selmayr* erheblich in seinem Umfang zugenommen. Jetzt handelt es sich eher um einen sehr ausführlichen Kommentar zum Nachschlagen von Detailfragen.

Gola, DS-GVO, 2. Aufl. 2018

→ Ein kompakter Kommentar, der sich zum schnellen Nachschlagen anbietet.

Koreng/Lachenmann, Formularhandbuch Datenschutzrecht, 2. Aufl. 2018.

→ Eine sehr umfangreiche Sammlung an Vorlagen und Formularen, auf die wir in dieser Broschüre mehrfach zurückgegriffen haben.

Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018.

→ Ein sehr guter und umfangreicher Kommentar, der sich – ähnlich wie der *Ehmann/Selmayr* - eher für das Nachschlagen von Detailfragen anbietet.

Kranig/Ehmann, Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine, 1. Aufl. 2017.

→ Ein einfach zu lesender Ratgeber von zwei Mitarbeitern des BayLDA mit vielen guten Hinweisen, die teilweise auch den Weg in diese Broschüre gefunden haben.

LDI NRW, Datenschutz im Verein nach der Datenschutz-Grundverordnung, Stand: November 2018.

→ Eine Broschüre der nordrhein-westfälische Datenschutzbehörde, die explizit für Vereine konzipiert wurde und eine Vielzahl guter Beispiele enthält. Die Broschüre ist hier abrufbar.

Paal/Pauly, Datenschutz-Grundverordnung Bundesdatenschutzgesetz (Beck'sche Kompakt-Kommentare), 2. Aufl. 2018.

→ Ein kompakter Kommentar im ähnlichen Format wie der *Gola*, der sich zum schnellen Nachschlagen anbietet.

II. *Sonstige Informationsquellen im Internet*

Datenschutz Notizen

→ Eine von dem privaten Unternehmen *Datenschutz Nord* betriebene Plattform, die über alle aktuellen Entwicklungen im Datenschutz berichtet. Dort kann man die Beiträge (durch den Themen-Reiter) auch z.B. nach "Aufsichtsbehörden" sortieren und die aktuellsten Beiträge der Behörden auf einen Blick sehen.

Datenschutz-Praxis

→ Eine von dem privaten Verlag *WEKA Media* betriebene Plattform, die zu praktisch allen neuen Entwicklungen im Datenschutzrecht etwas veröffentlicht.

Die Website der DSK

→ Die Datenschutzkonferenz (DSK) ist der *Zusammenschluss aller Datenschutzbehörden des Bundes und der Länder* und veröffentlicht regelmäßig Kurzpapiere, Entschließungen und Beschlüsse zu aktuellen Themen. Diese sind über die Website abrufbar.

Die Website des ULD

→ Das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein (ULD) gehört zu den aktivsten Datenschutzbehörden in Deutschland und hat auf ihrer Website einen "Ticker" auf dem ca. 1-2 Mal im Monat die relevantesten Infos aufgeführt sind.

E. Vorlagenverzeichnis

Hinweise zur Verwendung der Vorlagen

Die nachfolgenden Vorlagen wurden entweder von Mitgliedern der AG Datenschutz selbst erstellt oder es wurde die Weiterverbreitung explizit durch Dritte (wie z.B. Kanzleien) genehmigt.

Es kann **keine Haftung für die Richtigkeit und Aktualität der Vorlagen** übernommen werden. Eine individuelle Prüfung für die konkreten Einsatzzwecke im Rahmen einer jeden RLC ist zwingend notwendig. Wir werden jedoch versuchen die Vorlagen möglichst aktuell zu halten.

Die Vorlagen setzen sich zum Teil aus mehreren Dokumenten wie z.B. einem allgemeinen Hinweis (als Handreichung) und einer Einwilligungserklärung zusammen. Falls es mehrere Teildokumente für einen Zweck gibt, wurden diese unter einer Überschrift (I., II. etc.) zusammengefasst aber getrennt aufgeführt (1., 2. etc.).

Sämtliche Vorlagen dürfen im Rahmen der RLC-Arbeit frei verwendet und abgeändert werden. Eine kommerzielle Nutzung dieser Vorlagen (insb. gegenüber Dritten) ist nicht zulässig.

Die Vorlagen sind zur einfacheren Anpassung für die Zwecke einer jeden RLC im Format *docx* separat hier abrufbar. Falls eure (R)LC noch keinen Zugang zu der Plattform Confluence hat, könnt ihr euch gerne jederzeit an <wissensmanagement[at]rlc-deutschland.de> wenden.

I. *Anhang 1: Beratungsvertrag (inkl. Vollmacht, Hinweisen zur Datenverarbeitung und der datenschutzrechtlichen Einwilligung)*

1. Beratungsvertrag (mit Klient*innen)

Beratungsvertrag

zwischen

(1) der **XY Law Clinic**, Postanschrift

(im Folgenden „**XY-LC**“)

und

---

(2) [*Vor-, Nachname und Anschrift Klient*in*]

(im Folgenden „**d. Klient*in**“)

(zusammen die „**Parteien**“)

Vorbemerkungen

Die XY-LC ist eine Einrichtung der XY-Universität, die gemäß dem Rechtsdienstleistungsgesetz (§ 6 Abs. 2 RDG)

- Ratsuchenden unentgeltliche Beratung auf dem Gebiet des Asyl-, Aufenthalts- und Sozialrechts anbietet,
- Jura-Studierenden der XY-Universität ermöglicht, ihre im Studium erworbenen Rechtskenntnisse praktisch anzuwenden und ihre Beratungskompetenz zu erweitern,
- und so zugleich die Ausbildung und das soziale Engagement der XY-Universität im Fachbereich Rechtswissenschaft unterstützt.

Vor diesem Hintergrund vereinbaren die Parteien eine Beratung unter den folgenden Bedingungen:

§ 1 Vertragsgegenstand

1.) D. Klient*in beauftragt die XY-LC, sie/ihn zu beraten und zu unterstützen, und zwar bei der Klärung und rechtlichen Begutachtung von Anliegen im Bereich des XY-Rechts und damit verbundener Rechtsgebiete (die „**Beratung**“). D. Klient*in kann die XY-LC mit dem beiliegenden Formular („**Vollmacht**“) bevollmächtigen.

2.) Bei der Beratung werden Studierende („**Studentische Berater*innen**“) sowie studentische Hilfskräfte und wissenschaftliche Mitarbeiter*innen der XY-Universität im Auftrag der XY-LC tätig (gemeinsam „**XY-LC-Angehörige**“ genannt). D. Klient*in gestattet hiermit ausdrücklich die Übertragung der Beratung auf XY-LC-Angehörige.

3.) Die XY-LC ist im Einzelfall berechtigt Dolmetscher*innen zur Verständigung in der Beratung zu beauftragen.

4.) Die XY-LC berät nur außergerichtlich; in gerichtlichen Verfahren dürfen Studentische Berater*innen nur beim Entwurf von Schriftsätzen oder Anträgen oder bei der Vorbereitung auf Gerichtsverhandlungen unterstützen.

5.) Die XY-LC berät nur in nicht eilbedürftigen oder existenzbedrohlichen Fällen.

6.) Das Beratungsverhältnis kommt erst mit und ab wirksamer Unterzeichnung dieses Vertrages zustande. Die Kontaktaufnahme und vorherige Gespräche begründen noch kein Auftragsverhältnis.

§ 2. Maßstab der Beratung

1.) D. Klient*in ist sich bewusst und wird ausdrücklich darauf hingewiesen, dass die Studentischen Berater*innen ohne abgeschlossenes Jura-Studium als juristische Laien tätig werden. Die Studentischen Berater*innen sind nicht als Rechtsanwält*innen zugelassen. Die Beratung kann nicht das Niveau einer Rechtsberatung durch eine*n Rechtsanwalt/anwältin erreichen und ersetzt nicht die Beratung durch eine*n Rechtsanwalt/anwältin.

2.) Besondere Regelungen für Rechtsanwält*innen finden keine Anwendung (z.B. kein Zeugnisverweigerungsrecht, kein Schutz vor Beschlagnahme von Informationen, keine Berufshaftpflichtversicherung, Anzeigepflicht bei besonders schweren Straftaten).

3.) Die Studentischen Berater*innen beraten unter Anleitung („Supervision“) einer Person, die entgeltlich beraten darf oder die Befähigung zum Richteramt hat (d. „**Supervisor*in**“) (§ 6 Abs. 2 RDG).

§ 3. Unentgeltlichkeit der Beratung

Die Beratung ist unentgeltlich.

§ 4. Beendigung

Das Beratungsverhältnis kann durch beide Parteien jederzeit durch Kündigung beendet werden. Die XY-LC darf aber nur zur Unzeit kündigen, wenn ein wichtiger Grund vorliegt. Ein wichtiger Grund liegt insbesondere vor, wenn die XY-LC die Beratungstätigkeit nicht erbringen kann, weil

a) sie für den betreffenden Sachverhalt keine*n Supervisor*in findet;

b) der Sachverhalt die Fähigkeiten der Studentische Berater*innen übersteigt;

c) d. Klient*in sich vorsätzlich und schwerwiegend rechtswidrig verhält; oder

d) d. Klient*in auch nach Fristsetzung ihrer Mitwirkungspflicht (§ 5) nicht nachkommt.

§ 5. Mitwirkungspflichten d. Klient*in

1.) D. Klient*in wird der XY-LC und den Studentischen Berater*innen alle für die Beratung relevanten Informationen zur Verfügung stellen und Dokumente vorlegen.

2.) Insbesondere ist d. Klient*in verpflichtet, Protokolle von Beratungsgesprächen kritisch zu überprüfen. Er/Sie muss auf Unvollständigkeiten oder Fehler in der Sachverhaltsdarstellung hinweisen.

§ 6. Haftung

1.) Die XY-LC haftet gegenüber d. Klient*in nur für Vorsatz und grobe Fahrlässigkeit und orientiert sich am Verkehrskreis juristischer Laien.

2.) Diese Haftungsbeschränkung gilt nicht für Schäden aus der Verletzung des Lebens, des Körpers oder der Gesundheit oder Verstöße gegen datenschutzrechtliche Vorschriften.

3.) Die Haftungsbeschränkung gilt auch nicht bei Verletzung wesentlicher Vertragspflichten. Wesentliche Vertragspflichten sind solche,

a) die die XY-LC erfüllen muss, um den Vertrag ordnungsgemäß durchzuführen;

b) auf deren Erfüllung d. Klient*in vertraut und auch vertrauen darf und

c) deren schuldhafte Nichterfüllung die Erreichung des Vertragszwecks gefährdet.

Wenn die XY-LC eine wesentliche Vertragspflicht verletzt, haftet sie nur für den Schaden, der bei Vertragsabschluss vorhersehbar war und typischerweise eintritt.

4.) D. Klient*in verzichtet darauf, direkte Ansprüche gegen XY-LC-Angehörige und Supervisor*innen gerichtlich geltend zu machen, außer bei Vorsatz und grober Fahrlässigkeit; Absätze 2 –3 gelten entsprechend.

§ 7. Vertraulichkeit

1.) Die XY-LC verpflichtet sich zur Verschwiegenheit über alle Informationen d. Klient*in, die sie im Rahmen der Beratung erlangt („**Beratungsinformationen**“).

2.) Die XY-LC darf die Beratungsinformationen aber an XY-LC-Angehörige weitergeben. Die XY-LC und die XY-LC-Angehörigen dürfen die Beratungsinformationen an andere XY-LC-Angehörige und an die von der XY-LC beauftragten Dolmetscher*innen weitergeben. Die XY-LC und die XY-LC-Angehörigen dürfen die Beratungsinformationen auch an d. Supervisor*innen weitergeben, aber nur in anonymisierter oder im Einzelfall pseudonymisierter Form und nur soweit für die Supervision erforderlich.

3.) Die XY-LC bemüht sich darum, dass XY-LC-Angehörige, Supervisor*innen und von der XY-LC beauftragte Dolmetscher*innen die Beratungsinformationen ebenfalls vertraulich behandeln.

4.) Die XY-LC verpflichtet sich insbesondere, alle im Zusammenhang mit der Beratung erhaltenen personenbezogenen Daten vertraulich zu behandeln und dabei die gesetzlichen Datenschutzvorschriften und die beiliegenden Datenschutzhinweise einzuhalten.

§ 8. Schlussbestimmungen

1.) Abweichende Vereinbarungen zu diesem Vertrag sind auch wirksam, wenn sie mündlich getroffen werden. Zu Beweis- und Dokumentationszwecken werden beide Parteien auf eine textliche Erfassung solcher abweichenden Vereinbarungen hinwirken.

2.) Sind oder werden einzelne Bestimmungen dieses Beratungsvertrages nichtig oder unwirksam oder enthält dieser Beratungsvertrag eine Lücke, so bleiben die übrigen Bestimmungen dieses Beratungsvertrages gültig. Die Parteien vereinbaren, die Gültigkeit der verbleibenden Bestimmungen dieses Beratungsvertrages in jedem Fall zu erhalten, und schließen § 139 BGB und eine etwaig darin liegende Beweislastumkehr insgesamt aus.

3.) Als Gerichtsstand wird XYStadt vereinbart,

a) falls d. Klient*in keinen allgemeinen Gerichtsstand im Inland hat,

b) für Klagen gegen d. Klient*in, falls d. Klient*in nach Abschluss dieses Vertrages seinen/ihren Wohnsitz ins Ausland verlegt oder der Wohnsitz oder der gewöhnliche Aufenthalt d. Klient*in zum Zeitpunkt der Klageerhebung nicht bekannt ist

.

Mit dem Beratungsvertrag sind wir einverstanden:

Ort, Datum	Unterschrift/en
	für die XY-LC
Ort, Datum	Unterschrift/en
	*Klient*in*

2. Vollmacht

Vollmacht

Der/die Unterzeichnende

Vor-, Nachname, Anschrift

_____

(„**Vollmachtgeber*in**“)

bevollmächtigt hiermit mit der Befugnis zur Erteilung von Untervollmachten im gleichen Umfang wie diese Vollmacht die

XY-Universität / XY-Uni Law Clinic (XY-LC),
Postanschrift,

d. Vollmachtgeber*in bei allen außergerichtlichen Angelegenheiten im Zusammenhang mit der Klärung und rechtlichen Begutachtung ihres/seines Anliegens im Bereich des XY-Rechts und damit verbundener Rechtsgebiete gemäß dem Beratungsvertrag zwischen d. Vollmachtgeber*in und der XY-Universität / XY-LC vom

[_____] (die „**Beratung**“)

soweit rechtlich zulässig zu vertreten, insbesondere (aber nicht nur) in folgenden Angelegenheiten:

a) außergerichtliche Interessenvertretung, insbesondere Geltendmachung von Ansprüchen gegen Dritte, Behörden und sonstige Stellen,

b) Einsicht in und Einholung oder Beantragung von Auskünften und Abschriften aus behördlichen Akten oder Registern im Zusammenhang mit der Beratung (insbesondere Akten bei Ausländer-, Asyl- und Sozialbehörden, Melde-, Ausländer- oder Schuldnerregister, polizeiliche und staatsanwaltliche Ermittlungsakten),

c) Abgabe von (auch einseitigen) Erklärungen,

d) Vorbereitung und Stellung von außergerichtlichen Anträgen in XY-rechtlichen Angelegenheiten und damit zusammenhängenden Rechtsangelegenheiten bei Behörden und privaten Stellen,

e) Vertretung in XY-rechtlichen sowie damit zusammenhängenden Angelegenheiten und bei außergerichtlichen Verhandlungen gegenüber privaten und öffentlichen Stellen, insbesondere gegenüber Sozial-, Ausländer- und anderen Verwaltungsbehörden sowie gegenüber Finanzbehörden,

e) Begründung und Aufhebung von Vertragsverhältnissen im Zusammenhang mit der Beratung.

Der/die Vollmachtgeber*in stellt hiermit die Bevollmächtigte von sämtlichen Ansprüchen, Kosten und Schäden frei, die diesem/r infolge der Ausübung dieser Vollmacht entstehen und die nicht das Ergebnis eines vorsätzlichen oder grob fahrlässigen Verhaltens der Bevollmächtigten oder ihrer Unterbevollmächtigten sind. Es gelten § 6 2) und 3) des Beratungsvertrages für die Freistellung entsprechend.

Ort, Datum **Vor-, Nachname** **Unterschrift/en**

_____

*Vollmachtgeber*in*

3. Hinweise zur Datenverarbeitung für Klient*innen

Hinweise zur Datenverarbeitung (für Klient*innen) nach Art. 13, 14 DS-GVO

1. Wer verarbeitet Ihre Daten?

Wir, die

XY-Universität / XY Law Clinic („XY-LC")

Postanschrift

http://www.XY-LC.de

(Telefonnummer und Kontaktdaten siehe Homepage)

informieren Sie hier darüber, was wir im Rahmen unserer studentischen Rechtsberatung mit Ihren personenbezogenen Daten tun und welche Rechte Ihnen nach dem Datenschutzrecht zustehen. Wir sind **Verantwortliche** für die Verarbeitung Ihrer personenbezogenen Daten (Art. 4 Nr. 7 DS-GVO[19]). Wenn Sie Fragen oder Sorgen wegen der Verarbeitung Ihrer Daten haben, sprechen Sie uns an!

Sie können sich auch an unseren [**behördlichen] Datenschutzbeauftragten** [der XY-Universität] wenden:

Name, Postanschrift, Telefon, Fax, E-Mail

2. Welche Daten erheben wir von wem und für welchen Zweck?

Wenn Sie mit uns einen Beratungsvertrag abschließen, bitten wir Sie um folgende **personenbezogenen Daten**, soweit das für die Beratung notwendig ist:

- Ihr Name, Vorname, Geschlecht, Geburtsdatum/ -ort und Staatsangehörigkeit
- Angaben zum Familienstand und zur Verwandtschaft (insb. Kinder)
- Wohn-/Meldeanschrift, Telefonnummer, E-Mail-Adresse
- Ihr ausländerrechtlicher bzw. aufenthaltsrechtlicher Status, Aktenzeichen und andere Ordnungsmerkmale von Behörden
- die wirtschaftlichen Verhältnisse (Vermögen, Einkommen, Verbindlichkeiten) von Ihnen und Angehörigen Ihrer sozialrechtlichen Bedarfsgemeinschaft (§ 7 III, IIIa SGB[20] II)
- wie wir uns mit Ihnen verständigen können (also Ihre Sprachkenntnisse)
- Ihre Auszüge aus dem Ausländerzentralregister
- Unterlagen, auch eingescannt, (z.B. Ausweise, Bescheide etc.) die Sie uns zur Prüfung und Beratung überlassen, und Ihre Korrespondenz mit Dritten (Behörden, gemeinnützige Einrichtungen, Rechtsanwält*innen) in der Beratungsangelegenheit.

Wir erheben diese Daten **bei Ihnen**. Auf Ihre Anweisung holen wir soweit nötig auch bei einer Sie überweisenden **Einrichtung** (etwa Ihrer Flüchtlingsunterkunft) oder bei Ihrem zuvor von Ihnen mandatierten Anwalt Daten ein.

Wir erheben, speichern und verarbeiten diese Daten, um Sie **identifizieren, kontaktieren, sachgerecht beraten und vertreten zu können,** und zwar nur mit Ihrer Einwilligung (Art. 6 I S. 1 lit. a DS-GVO). Sensible Daten (i.S.d. Art. 9 I DS-GVO), wie z.B. Daten bzgl. Ihrer ethnischen Herkunft oder religiösen Überzeugung, verarbeiten wir nur soweit notwendig und nur mit **Ihrer Einwilligung** (Art. 6 I S. 1 lit. a, 7, 9 II lit. a DS-GVO). Für **Ihre Einwilligung** können Sie das beiliegende Muster („Datenschutzrechtliche Einwilligung") benutzen.

Die Datenverarbeitung kann auch dazu dienen, **Haftungsansprüche abzuwickeln**, die Sie gegen uns erheben, dann auf Basis von berechtigtem Interesse (Art. 6 I S. 1 lit. f DS-GVO).

3. Wie lange speichern wir Ihre Daten?

Wir löschen Ihre personenbezogenen Daten bei uns, wenn die Beratung endet oder Sie Ihre Einwilligung widerrufen. Falls gesetzliche Aufbewahrungsfristen bestehen, löschen wir die Daten erst, wenn diese Fristen abgelaufen sind. Wir prüfen regelmäßig zum Ende eines jeden Kalenderjahres, ob es erforderlich ist, Ihre Daten weiter zu speichern.

Wir können im begründeten Einzelfall Daten, die wir für eine Beweisführung brauchen, bis zu 10 Jahre aufbewahren, wenn wir annehmen dürfen, dass Sie Haftungsansprüche gegen uns geltend machen wollen.

4. An wen übermitteln wir Ihre Daten?

Wir übermitteln Ihre Daten nur an wenige Dritte außerhalb der XY-LC, nämlich an die Beratungsstelle, die Ihren Fall an die XY-LC weiterverwiesen hat, und an alle öffentlichen Stellen, gegen deren Vorgehen Sie sich mit unserer Unterstützung wenden oder von denen Sie Leistungen beanspruchen möchten.

Innerhalb der XY-LC erhalten nur die XY-LC-Angehörigen Zugriff, die Sie beraten oder mit der Administration Ihrer Beratung betraut sind.

An die Supervisor*innen übermitteln wir Ihre Daten grundsätzlich nur in anonymisierter Form[21].Im Einzelfall und nur soweit für die Rechtsberatung erforderlich

[19] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („**DS-GVO**").

[20] Sozialgesetzbuch.

[21] Die Informationen werden derart verändert, dass nicht mehr auf Sie geschlossen werden kann.

übermitteln wir Ihre Daten ggf. in pseudonymisierter Form[22].

Nur mit Ihrer ausdrücklichen Einwilligung geben wir im Einzelfall nicht anonymisierte/pseudonymisierte Daten an Supervisor*innen; insbesondere, wenn diese*r eine Mandatierung für Ihren Fall prüfen soll.

5. Warum sind Ihre Daten für uns wichtig?

Für eine **sachgerechte und erfolgreiche Rechtsberatung** und die damit verbundenen vertraglichen Pflichten, ist es wichtig, dass wir Ihre Daten verarbeiten können. Wenn wir diese Daten nicht oder nur teilweise bekommen oder verarbeiten, können wir den Beratungsvertrag mit Ihnen nicht vollständig erfüllen.

6. Welche Rechte haben Sie?

Sie können

- Ihre **Einwilligung** jederzeit uns gegenüber **widerrufen** (Art. 7 Abs. III DS-GVO); wir werden dann die Datenverarbeitung, die auf dieser Einwilligung beruhte, in der Zukunft nicht mehr vornehmen;
- **Auskunft** über Ihre von uns verarbeiteten personenbezogenen Daten erhalten (Art. 15 DS-GVO);
- verlangen, dass wir Ihre von uns verarbeiteten personenbezogenen Daten **berichtigen** oder **vervollständigen** (Art. 16 DS-GVO);
- verlangen, dass wir Ihre bei uns verarbeiteten personenbezogenen Daten **löschen** (Art. 17 DS-GVO), wenn
  - Ihre personenbezogenen Daten für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind,
  - Sie Ihre Einwilligung widerrufen,
  - Sie gemäß Art. 21 DS-GVO erfolgreich Widerspruch gegen die Verarbeitung eingelegt haben,
  - Ihre personenbezogenen Daten unrechtmäßig verarbeitet wurden, oder
  - die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

  Dies gilt jedoch nicht, falls die Verarbeitung erforderlich ist (Art. 17 III DS-GVO)
  - zur Ausübung des Rechts auf freie Meinungsäußerung und Information
  - zur Erfüllung einer rechtlichen Verpflichtung,
  - aus Gründen des öffentlichen Interesses,
  - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

  oder die Verarbeitung im Einzelfall nach anderen gesetzlichen Vorschriften weiterhin zulässig ist.

verlangen, dass wir **die Verarbeitung** Ihrer bei uns verarbeiteten personenbezogenen Daten **einschränken** (Art. 18 DS-GVO), soweit

- Sie die Richtigkeit der Daten bestreiten,
- wir die Daten nicht verarbeiten dürfen, Sie aber deren Löschung ablehnen,
- wir die Daten nicht länger benötigen, Sie die Daten aber benötigen, um Rechtsansprüche geltend zu machen, auszuüben oder zu verteidigen, oder
- sie gemäß Art. 21 DS-GVO Widerspruch gegen die Verarbeitung eingelegt haben,

- Ihre uns bereitgestellten personenbezogenen Daten in einem **strukturierten, gängigen und maschinenlesbaren Format** von uns **erhalten** oder **einem anderen Verantwortlichen übermitteln** lassen (Art. 20 DS-GVO) oder

Nach Art. 21 DS-GVO haben Sie grds. ein **Widerspruchsrecht** gegen die Verarbeitung Ihrer personenbezogenen Daten, wenn Sie aufgrund Ihrer besonderen Situation dafür Gründe haben und soweit wir die Verarbeitung für einen Verarbeitungszweck lediglich auf berechtigtes Interesse stützen (Art. 6 IS. 1 **lit. f** DS-GVO).

Wir weisen aber darauf hin, dass wir Ihre personenbezogenen Daten trotzdem weiterverarbeiten dürfen, soweit die Verarbeitung Ihrer Daten lediglich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erfolgt.

Es genügt jeweils eine formlose Mitteilung (Mail) an:

mail@XY-LC.de

Sie können sich außerdem bei einer Aufsichtsbehörde **beschweren**, wenn Sie denken, dass wir bei der Verarbeitung Ihrer Daten gegen die DS-GVO verstoßen (Art. 77 DS-GVO).

Ihre Beschwerde nimmt etwa der

Landesbeauftragte
für Datenschutz und Informationsfreiheit
Postanschrift, Telefon
https://datenschutz.XYLand.de/ entgegen.

7. Schlussbemerkungen

Wir planen keine Übermittlung Ihrer Daten in Drittländer außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums.

Automatisierte Entscheidungsfindung insbesondere Profiling (Art. 22 DS-GVO) gibt es bei uns nicht.

Hinweis: Wenn Daten (Anfragen, Dokumente etc.) auf Basis des Internet unverschlüsselt übertragen werden (etwa per E-Mail), sind sie nur schlecht vor dem Zugriff durch Dritte geschützt.

[22] Ihr Name oder andere Identifikationsmerkmale werden durch ein Pseudonym ersetzt, um die Rückschlüsse auf Ihre Person wesentlich zu erschweren.

4. Einwilligung für Klient*innen

Datenschutzrechtliche Einwilligung (für Klient*innen)

Vor-, Nachname d. Klient*in

Ich, _____,

willige hiermit ein, dass die XY-LC und die XY-LC-Angehörigen für die studentische Rechtsberatung und Fallbearbeitung meine personenbezogenen Daten verarbeiten (Art. 4 Nr. 2 DS-GVO), die in Ziffer 2 der *Hinweise zur Datenverarbeitung* aufgelistet sind und die ich der XY-LC zur Rechtsberatung freiwillig zur Verfügung stelle oder durch meine*n zuvor von mir mandatierte*n Anwalt/Anwältin oder durch eine mich überweisende Einrichtung (etwa Flüchtlingsunterkunft) zur Verfügung stellen lasse.

Ich bin **ausdrücklich damit einverstanden**, dass meine

- Angaben zum Familienstand und Verwandtschaft (insb. Kinder) sowie Staatsangehörigkeit
- Sprachkenntnisse in Wort und/oder Schrift und
- personenbezogenen Angaben in Ausweisdokumenten (z.B. Reisepass) und Korrespondenz mit Dritten (etwa Behörden, Rechtsanwält*innen, gemeinnützigen Einrichtungen),
- meine Auszüge aus dem Ausländerzentralregister

in dem für die Rechtsberatung notwendigen Umfang verarbeitet werden, auch wenn man daraus im Einzelfall auf mein Sexualleben, meine rassische und ethnische Herkunft, meine religiösen Überzeugungen oder meine Gesundheit schließen kann.

Ich bin außerdem einverstanden, dass die von mir freiwillig mitgeteilten oder durch Dritte mit meiner Einwilligung erhobenen und an die XY-LC übermittelten personenbezogenen Daten an folgende Empfänger*innen übermittelt und von diesen verarbeitet werden:

!! Bitte Zutreffendes ankreuzen !!

☐ an alle öffentlichen Stellen, gegen deren Vorgehen ich mich – vertreten durch eine*n XY-LC-Angehörige*n – wende bzw. von denen ich Leistungen beanspruche oder beanspruchen möchte,

☐ an die Beratungsstelle, die meinen Fall an die XY-LC weiterverwiesen hat, zur Information über das Ergebnis und zur weiteren Beratung und Bearbeitung des Anliegens,

☐ an die Supervisor*innen in pseudonymisierter Form, sofern das im Einzelfall erforderlich ist oder wird,

☐ an die Supervisor*innen, sofern das im Einzelfall erforderlich ist oder wird (z.B. zur Anfrage, ob eine Mandatierung möglich ist). ***Hinweis: Bitte das nur ankreuzen, wenn im Einzelfall erforderlich (ggf. nachträglich, falls es notwendig wird)! An Supervisor*innen werden grundsätzlich nur anonymisierte und im Einzelfall pseudonymisierte Daten übermittelt.***

Diese Einwilligung erteile ich freiwillig.

Ich kann meine Einwilligung ohne Angabe von Gründen jederzeit bei der XY-LC

→ schriftlich: XY-,
Postanschrift

→ per E-Mail an: Mail@XY-LC.de

mit Wirkung für die Zukunft ganz oder zum Teil **widerrufen**.

Ich habe verstanden, dass meine Daten nur insoweit erhoben werden, als die XY-LC sie braucht, um den Beratungsvertrag mit mir zu erfüllen und eine sachgerechte und erfolgreiche Rechtsberatung zu ermöglichen.

Ort, Datum

Unterschrift/en der betroffenen Person; bei Kindern, die noch nicht die erforderliche Einsichtsfähigkeit erlangt haben: Unterschrift/en beider Elternteile oder sonstiger gesetzlicher Vertreter

II. *Anhang 2: Verpflichtung der studentischen Berater*innen (inkl. Hinweisen zur Datenverarbeitung und einem Auszug der gesetzl. Vorschriften)*

1. Verpflichtung der studentischen Berater*innen

Verpflichtung der studentischen Berater*innen

Es vereinbaren

_____

- d. studentische Berater*in - **und die Law Clinic XY (im Folgenden: RLC-XY) Folgendes:**

I. Mitwirkung d. studentischen Berater*innen in RLC

1. D. studentische Berater*in wirkt in der RLC-XY auf vielfältige Weise mit:
   a) Sie/Er wird als Berater/in für die RLC-XY tätig mit der Aufgabe, Klient*innen der RLC-XY bei der Klärung und rechtlichen Begutachtung ihrer Anliegen im Bereich des Sozial- und Aufenthaltsrechts und damit verbundener Rechtsgebiete zu beraten und zu unterstützen, wobei sich die Beratung auf die außergerichtliche Unterstützung beschränkt.
   b) Sie/Er erarbeitet und präsentiert Vorträge oder Workshops für Gruppen (z.B. Ehrenamtliche) über sozial- oder aufenthaltsrechtliche Themen.
   c) Sie/Er erarbeitet und erstellt Informationsmaterialien für Berater*innen im RLC-XY-Team oder für Ratsuchende (z.B. Ehrenamtliche, Klient*innen) zu sozial- oder aufenthaltsrechtlichen Themen.
   d) Sie/Er beteiligt sich an den Aktivitäten der RLC-XY (z.B. Vorträge, Ringvorlesungen etc.) und an der Weiterentwicklung des Angebotes und der Organisation der RLC-XY.
2. Die Mitwirkung d. stud. Berater*in erfolgt freiwillig, unentgeltlich und weisungsfrei als Teil der universitären Ausbildung im Rahmen des Studiums.

II. Beginn und Ende der Mitwirkung

1. Die Mitwirkung in der RLC-XY ist Teil der Lehre im Studium am Fachbereich 01 Rechtswissenschaft der J.W. Goethe-Universität Frankfurt. Voraussetzung für die Mitwirkung ist daher, dass d. stud. Berater*in an der XY-Universität im Fachbereich Rechtswissenschaft eingeschrieben ist oder belegt, dass die Mitwirkung Teil eines anderen Studiengangs an der Goethe-Universität ist.
2. Die Mitwirkung beginnt mit Unterzeichnung dieser Vereinbarung.
3. Die Mitwirkung endet in folgenden Fällen:
   a) mit Zugang einer entsprechenden schriftlichen Erklärung d. stud. Berater*in bei der RLC-XY;
   b) mit Zugang eines Ausschlusses aus der RLC-XY gem. Ziffer VII. Nr. 2 dieser Vereinbarung; oder
   c) mit der Exmatrikulation d. stud. Berater*in aus dem Fachbereich 01 Rechtswissenschaft oder dem betreffenden anderen Studiengang, gleich aus welchem Grund (auch bei erfolgreichem Abschluss des Studiums oder Fachwechsel).

III. Beratungsvereinbarung und Vollmacht von Klient*innen

1. Zwischen der RLC-XY und den ratsuchenden Klient*innen wird eine Beratungsvereinbarung geschlossen. D. stud. Berater*in ist nicht Vertragspartner dieser Beratungsvereinbarung, sondern wird von der RLC-XY im Rahmen der Ausbildung für die Beratung eingesetzt.
2. D. stud. Berater*in ist ermächtigt, namens der RLC-XY als Einrichtung der XY-Universität die Beratungsvereinbarung mit d. Klient*in zu unterzeichnen.

IV. Grundpflichten d. stud. Beraters/Beraterin

1. D. stud. Berater*in darf sich bei der Mitwirkung in der RLC-XY, insbesondere bei der Beratung nicht unsachlich verhalten, insb. nicht bewusste Unwahrheiten oder herabsetzende Äußerungen verbreiten, zu denen andere Beteiligte oder der Beratungsverlauf keinen Anlass gegeben haben.
2. D. stud. Berater*in darf keine widerstreitenden Interessen vertreten.
3. D. stud. Berater*in ist bei der Behandlung der ihr/ihm anvertrauten Vermögenswerte (einschließlich der von der RLC-XY zur Verfügung gestellten Materialien, technischen Einrichtungen und Räumlichkeiten) zu der erforderlichen Sorgfalt verpflichtet. Fremdes Eigentum ist unverzüglich an d. Berechtigte/n weiterzuleiten oder bei den koordinierenden Mitarbeiter*innen der RLC-XY abzugeben.
4. D. stud. Berater*in ist verpflichtet, sich im Rahmen des RLC-XY-Angebotes fortzubilden und regelmäßig supervidieren zu lassen.
5. D. stud. Berater*in fühlt sich folgendem **Selbstverständnis** verpflichtet:
   Alle stud. Berater*innen der RLC-XY engagieren sich je nach ihrer Ausbildung im Rahmen ihrer Möglichkeiten freiwillig und unentgeltlich in der RLC-XY. Das

Uni-Team der RLC-XY unterstützt die stud. Berater*innen dabei organisatorisch und inhaltlich und sorgt für die bestmögliche Ausstattung und Rahmenbedingungen. Jede*r stud. Berater*in ist mit gleicher Einsatzbereitschaft dazu bereit, Aufgaben zu übernehmen, und trägt so zu einem positiven, konstruktiven und fairen Arbeitsklima unter den stud. Berater*innen bei. Dadurch können sich die Klient*innen der RLC-XY darauf verlassen, dass regelmäßig eine Sprechstunde stattfindet, dass sich stud. Berater*innen ihrer Fälle annehmen und diese in angemessener Zeit bearbeitet werden. Die stud. Berater*innen unterstützen einander bei ihrem Engagement mit Rat und Tat, z.B. durch kollegiale Beratung bei der Fallbearbeitung, nachvollziehbare Dokumentation und Informationsweitergabe, Verbindlichkeit in ihren Absprachen, Beteiligung an Abstimmungen, kurze Reaktionszeiten auf Fragen oder Nachrichten etc. Aus Gründen der Fairness unter den stud. Berater*innen und der Effektivität der RLC-XY als Ganzer sollte die Arbeitsbelastung aller stud. Berater*innen grundsätzlich vergleichbar sein. Wer seine Beteiligung in der RLC-XY aus nachvollziehbaren Gründen (z.B. Endphase der Examensvorbereitung o.ä.) für längere Zeit erheblich reduziert, gibt das rechtzeitig bekannt.
Konkret bedeutet das: Stud. Berater*innen der RLC-XY sind bereit,

a) mind. einmal pro Monat eine offene RLC-XY-Sprechstunde zu übernehmen,

b) Fälle aus der Sprechstunde nach Möglichkeit selbst zu übernehmen,

c) mind. einmal pro Jahr an Street Law-Workshops aktiv mitzuwirken,

d) regelmäßig an internen Weiterbildungs-Workshops teilzunehmen,

e) regelmäßig zur kollegialen Beratung beizutragen, indem sie am Consilium teilnehmen (oder sich rechtzeitig entschuldigen),

f) die zur internen Planung verwendete App „XY“ zu nutzen und generell aktiv zu einer effizienten Kommunikation innerhalb der RLC-XY beizutragen.

V. Maßstab der Mitwirkung, insb. der Beratung, und Haftung

1. D. stud. Berater*in ist kein* fertig ausgebildete*r Jurist*in, sondern juristischer Laie. Deshalb orientiert sich die Haftung der RLC-XY gegenüber Dritten, insb. zu beratenden Klient*innen am Verkehrskreis juristischer Laien und ist auf Vorsatz und grobe Fahrlässigkeit beschränkt, außer es handelt sich um Schäden an Leib, Leben oder Gesundheit oder um die Verletzung wesentlicher Pflichten aus einer Vereinbarung.
2. D. stud. Berater*in sagt zu, die Mitwirkung, insb. die Beratung gewissenhaft und sorgfältig auszuführen.
3. Da d. stud. Berater*in die Mitwirkung als Teil der universitären Ausbildung leistet, haftet sie/er der RLC-XY im Innenverhältnis nur folgendermaßen:

   a) Für vorsätzliche oder deliktische Handlungen haftet d. stud. Berater*in der RLC-XY persönlich, insbesondere, wenn sie/er bewusst und gewollt falsch berät oder sich bewusst pflichtwidrig über die Supervision hinwegsetzt.

   b) D. stud. Berater*in ist bekannt, dass wer nach § 6 Abs. 2 Satz 1 des Rechtsdienstleistungsgesetzes (RDG) eine unentgeltliche Dienstleistung außerhalb familiärer, nachbarschaftlicher oder ähnlich enger persönlicher Beziehungen erbringt, sicherstellen muss, dass die Rechtsdienstleistung durch eine Person, der die entgeltliche Erbringung dieser Rechtsdienstleistung erlaubt ist, durch eine Person mit Befähigung zum Richteramt oder unter Anleitung einer solchen Person erfolgt. Demnach kommt eine persönliche Haftung d. stud. Berater*in auch in Fällen grober Fahrlässigkeit in Betracht, wenn sich d. stud. Berater*in über die Supervision hinwegsetzt, sie nicht berücksichtigt oder in Zweifelsfällen nicht sucht.

   c) Eine persönliche Haftung d. stud. Berater*in kommt insbesondere auch dann in Betracht, wenn sie/er gegen die Verschwiegenheitspflicht der Ziffer VI. grob fahrlässig oder vorsätzlich verstößt.

VI. Vereinbarung über Verschwiegenheit und Datenschutz zur Erfüllung von Art. 5 Abs. 1 lit. f der Datenschutz-Grundverordnung („DS-GVO“) und zur Einhaltung weiterer Vorschriften zur Wahrung des Sozialgeheimnisses

1. D. stud. Berater*in ist zur Verschwiegenheit verpflichtet und behandelt alle im Zusammenhang mit der Mitwirkung an der RLC-XY, insb. der Beratung bekannt gewordenen Informationen und erhaltenen Unterlagen vertraulich, es sei denn die Tatsachen sind offenkundig oder bedürfen ihrer Bedeutung nach keiner Geheimhaltung. Ein Zeugnisverweigerungsrecht besteht allerdings nicht.

2. Verpflichtung

   a) auf die Vertraulichkeit

   Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daher ist es d. stud. Berater*in nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der ihr/ihm übertragenen Aufgaben erforderlich ist. Dabei ist es grundsätzlich unerheblich, ob diese Daten „digital“ (in IT-Systemen) oder „analog“ (Akten der Ratsuchenden der RLC-XY, behördliche Korrespondenz, Ausweisdokumente, Mitschriften, Kopien etc.) verarbeitet werden.

Diese Verpflichtung besteht umfassend. Nach den einschlägigen gesetzlichen Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zu unbefugtem Zugang führt. Dies gilt für die Tätigkeit d. stud. Berater*in innerhalb und außerhalb der RLC-XY, z.B. gegenüber Ratsuchenden und Interessierten. Die Pflicht zur Wahrung der Vertraulichkeit bleibt auch im Falle einer Änderung oder Beendigung des Engagements für die RLC-XY ohne zeitliche Begrenzung bestehen.

b) zur Wahrung des Sozialgeheimnisses

Die Tätigkeit d. stud. Berater*in in der RLC-XY berührt das Sozialgeheimnis (§§ 35 SGB I, 67, 78 SGB X). Sofern Daten verarbeitet werden, die dem Sozialgeheimnis unterliegen, hat sie/er diese im gleichen Umfang geheim zu halten, wie die ursprünglich übermittelnde Stelle. Insbesondere darf sie/er Sozialdaten Dritter nicht an Unbefugte preisgeben.

3. Daraus ergeben sich u.a. folgende Pflichten:

c) D. stud. Berater*in darf Informationen, Daten bzw. Unterlagen mit Bezug zu Personen nur weitergeben, soweit dies in einer Vereinbarung zwischen RLC-XY und der betroffenen Person vereinbart ist;

d) Personenbezogene Daten, Sozialdaten, Unterlagen sowie weitere zur Fallbearbeitung notwendige Daten dürfen nur innerhalb der RLC-XY mit den dafür vorgesehenen DV-Systemen elektronisch erfasst, gespeichert, ver- und bearbeitet, genutzt und (z.B. per Mail) übermittelt werden.

e) Außerhalb der von der RLC-XY zur Verfügung gestellten EDV-Systeme dürfen personenbezogene Daten nur erfasst, gespeichert, verarbeitet, genutzt oder weitergegeben werden, wenn sie anonymisiert[23] oder pseudonymisiert[24] werden.

VII. Rechtsfolgen bei Verstößen

1. Verstöße gegen die Datenschutzvorschriften bzw. die Vorschriften zum Sozialgeheimnis können nach den gesetzlichen Vorschriften ggf. mit Geldbuße, Geld- oder Freiheitsstrafe geahndet werden (§§ 41 BDSG iVm. 14 OWiG, 85 SGB X iVm. 42 BDSG).
2. Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt zudem einen Verstoß gegen die Pflichten aus dieser Vereinbarung dar. Sollte d. stud. Berater*in fahrlässig gegen eine Verpflichtung aus dieser Vereinbarung verstoßen, erfolgt beim ersten Verstoß eine Abmahnung. Bei trotz Abmahnung wiederholten oder bei vorsätzlichen Verstößen wird d. stud. Berater*in – je nach Schwere des Verstoßes vorübergehend oder dauerhaft - von der Mitwirkung an der RLC-XY ausgeschlossen.
3. Entsteht der von der Datenverarbeitung betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen. Datenschutzverstöße d. stud. Berater*in sind außerdem mit möglicherweise sehr hohen Bußgeldern für die J. W. Goethe Universität Frankfurt bedroht (Art. 83 DS-GVO), die gegebenenfalls zu Ersatzansprüchen gegenüber d. stud. Berater*in führen können.

VIII. Unterrichtung über die vorgenannten Verpflichtungen

Über die Verpflichtungen in Ziffer VI. und VII. und die zu ihrer Erfüllung erforderlichen Verhaltensweisen wird d. Studierende unterrichtet Sie/Er ist sich über die bei einem Verstoß drohenden Sanktionen bewusst.

IX. Einwilligung zur Anfertigung und Verwendung von Fotografien

D. stud. Berater*in ist damit einverstanden, dass Foto- bzw. Filmaufnahmen von ihr/ihm für die Zwecke der RLC-XY gemacht, verarbeitet, gespeichert und veröffentlicht werden

_____	_____
Ort, Datum	Ort, Datum
_____	_____
- studentische*r Berater*in -	- Verantwortliche*r der RLC-XY -

[23] D.h. derart verändert werden, dass Angaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit unverhältnismäßig großem Aufwand einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

[24] D.h. der Name und andere Identifikationsmerkmale durch ein Kennzeichen (Pseudonym) ersetzt werden, um die Bestimmung der betroffenen Person auszuschließen oder wesentlich zu erschweren.

2. Hinweise zur Datenverarbeitung für Berater*innen

Hinweise zur Datenverarbeitung der Daten von XY-LC-Angehörigen (wissenschaftliche Mitarbeiter*innen, studentische Hilfskräfte, studentische Berater*innen) nach Art. 13 DS-GVO

1. Wer verarbeitet Ihre Daten?

Im Folgenden möchten wir, die

XY-Universität / XY-Uni Law Clinic („**XY-LC**“)

Postanschrift

Mail@XY-LC.de

(die aktuelle Telefonnummer sowie weitere Kontaktdaten können Sie der Homepage entnehmen)

über die Verarbeitung Ihrer personenbezogenen Daten im Rahmen unserer studentischen Rechtsberatung und die Ihnen nach dem Datenschutzrecht zustehenden Rechte informieren. Wir sind der für die Verarbeitung Ihrer personenbezogenen Daten **Verantwortliche** gemäß Art. 4 Nr. 7 DS-GVO[25].

Wenn Sie Fragen über die Verarbeitung Ihrer Daten haben, sprechen Sie uns gerne an!

Sie können sich auch an unseren [**behördlichen**] **Datenschutzbeauftragten** [der XY-Universität] wenden:

Name, Postanschrift, Telefon, Fax, E-Mail

2. Welche Daten erheben wir, von wem, für welchen Zweck?

Wir erheben folgende (Kategorien von) **personenbezogenen Daten von Ihnen**, jedoch nur in dem tatsächlich notwendigen Umfang:

- Ihre Kontaktdaten (Name, Vorname, Uni-E-Mail-Adresse, private E-Mail-Adresse, Telefonnummer, Wohnanschrift, Matrikelnummer),
- Ihre zeitliche Verfügbarkeit,
- Protokolldateien (wie Zugrifflogs, Bearbeitungsprotokolle, etc.) hinsichtlich Ihrer Mitarbeit bei der XY-LC,
- falls zutreffend, Ihre Absolvierung eines Praktikums bei einem/r unserer Supervisor*innen.

Die Erhebung dieser Daten erfolgt grundsätzlich **bei Ihnen**. Die Daten können auch Ihren Angaben entnommen werden, die Sie bei Immatrikulation an oder bei Unterschrift eines Arbeitsvertrages mit der XY-Universität gemacht haben.

Wir erheben, speichern und verarbeiten diese Daten, um Sie **kontaktieren zu können, Ihre Beteiligung an der XY-LC zu dokumentieren und um unsere Beratungspraxis administrativ durchführen zu können und die Zusammenarbeit aller Beteiligten zu fördern.** Diese Datenverarbeitung stützen wir grds. auf Art. 6 I S. 1 lit. b DS-GVO.

Die Datenverarbeitung dient ggf. in Einzelfällen auch der **Abwicklung von Haftungsansprüchen**, die Sie gegen uns erheben, auf Basis von berechtigtem Interesse (Art. 6 I S. 1 lit. f DS-GVO).

3. Wie lange speichern wir Ihre Daten?

Ihre von uns erhobenen personenbezogenen Daten werden grundsätzlich nach **Wegfall des Zwecks** bzw. Ablauf der gesetzlichen **Aufbewahrungsfristen** gelöscht. Diese Erforderlichkeit der weiteren Speicherung Ihrer Daten wird in diesem Sinne regelmäßig zum kalendarischen Jahresende geprüft.

Im begründeten **Einzelfall** können sämtliche zur Beweisführung erforderlichen Daten bis zu 10 Jahre aufbewahrt werden, wenn Tatsachen die Annahme rechtfertigen, dass Sie die Geltendmachung von Haftungsansprüchen gegen uns beabsichtigen.

4. An wen übermitteln wir Ihre Daten?

Innerhalb der XY-LC erhalten nur die XY-LC-Angehörigen Zugriff. Eine Übermittlung der Daten findet, allerdings nur im notwendigen Umfang (insb. E-Mail-Adresse) und nur an diejenigen Supervisor*innen statt, die bei einer Beratung, mit der Sie betraut sind, eingesetzt werden.

5. Welche Rechte haben Sie?

Sie können

- **Auskunft** über Ihre von uns verarbeiteten personenbezogenen Daten erhalten (Art. 15 DS-GVO),
- die **Berichtigung** unrichtiger oder **Vervollständigung** Ihrer von uns verarbeiteten personenbezogenen Daten verlangen (Art. 16 DS-GVO),
- die **Löschung** Ihrer bei uns verarbeiteten personenbezogenen Daten verlangen, wenn
  - Ihre personenbezogenen Daten für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind,
  - Sie gemäß Art. 21 DS-GVO erfolgreich Widerspruch gegen die Verarbeitung eingelegt haben,

[25] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („**DS-GVO**“).

- Ihre personenbezogenen Daten unrechtmäßig verarbeitet wurden, oder
- die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (Art. 17 DS-GVO).

Dies gilt jedoch nicht, falls die Verarbeitung erforderlich ist (Art. 17 DS-GVO)

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information
- zur Erfüllung einer rechtlichen Verpflichtung,
- aus Gründen des öffentlichen Interesses,
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

oder die Verarbeitung im Einzelfall nach anderen gesetzlichen Vorschriften weiterhin zulässig ist.

– die **Einschränkung der Verarbeitung** Ihrer bei uns verarbeiteten personenbezogenen Daten verlangen (Art. 18 DS-GVO), soweit
  - die Richtigkeit der Daten von Ihnen bestritten wird,
  - die Verarbeitung unrechtmäßig ist, Sie aber deren Löschung ablehnen,
  - wir diese Daten nicht länger benötigen, Sie jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen, oder
  - gemäß Art. 21 DS-GVO Widerspruch gegen die Verarbeitung eingelegt haben,

Ihre uns bereitgestellten personenbezogenen Daten in einem **strukturierten, gängigen und maschinenlesbaren Format erhalten**, und diese Daten **einem anderen Verantwortlichen** durch uns **übermitteln** lassen (Art. 20 DS-GVO).

Nach Art. 21 DS-GVO haben Sie grds. ein **Widerspruchsrecht** gegen die Verarbeitung Ihrer personenbezogenen Daten einlegen, wenn Sie aufgrund Ihrer besonderen Situation dafür Gründe haben und soweit wir die Verarbeitung lediglich auf berechtigtes Interesse stützen (Art. 6 I S. 1 **lit. f** DS-GVO).

Wir weisen aber darauf hin, dass wir Ihre personenbezogenen Daten trotzdem weiterverarbeiten dürfen, soweit die Verarbeitung Ihrer Daten lediglich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erfolgt.

Es genügt jeweils eine formlose Mitteilung an:

Mail@XY-LC.de

Sie können sich außerdem gemäß Art. 77 DS-GVO bei einer Aufsichtsbehörde **beschweren**, wenn Sie der Ansicht sind, dass unsere Verarbeitung Ihrer personenbezogenen Daten gegen diese Verordnung verstößt.

Ihre Beschwerde nimmt etwa der

Landesbeauftragte für Datenschutz und Informationsfreiheit
Postanschrift

Telefon
Webseite

entgegen.

6. Schlussbemerkungen

Wir beabsichtigen keine Übermittlung Ihrer Daten in Drittländer außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums.

Eine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Art. 22 DS-GVO findet nicht statt.

Wir weisen abschließend darauf hin, dass die internetbasierte, unverschlüsselte Datenübertragung von Anfragen oder Dokumenten (etwa per E-Mail) keinen Schutz vor dem Zugriff durch Dritte bietet.

3. Gesetzliche Vorschriften zur Vertraulichkeit

Gesetzliche Vorschriften zur Vertraulichkeit (für studentische Berater*innen)

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim behördlichen Datenschutzbeauftragten:

Art. 4 DS-GVO[26] – 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;[…]

Art. 5 DS-GVO - Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

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

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

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

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

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

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

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

Art. 29 DS-GVO – Verarbeitung unter der Aufsicht des Verantwortlichen […]

Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen

[26] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („**DS-GVO**“).

verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

§ 67 SGB X – Begriffsbestimmungen

(1) […]

(2) Sozialdaten sind personenbezogene Daten (Artikel 4 Nummer 1 der Verordnung (EU) 2016/679), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden. Betriebs- und Geschäftsgeheimnisse sind alle betriebs- oder geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben. (3)-(5) […]

§ 35 SGB I – Sozialgeheimnis

(1) Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Absatz 2 Zehntes Buch) von den Leistungsträgern nicht unbefugt verarbeitet werden (Sozialgeheimnis). Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. […] (2) […]

(2a) Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt. (3) […]

(4) Betriebs- und Geschäftsgeheimnisse stehen Sozialdaten gleich. (5)-(7)[…]

§ 78 SGB X – Zweckbindung und Geheimhaltungspflicht eines Dritten, an den Daten übermittelt werden

(1) Personen oder Stellen, die nicht in § 35 des Ersten Buches genannt und denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, zu dem sie ihnen befugt übermittelt worden sind. Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. Die Dritten haben die Daten in demselben Umfang geheim zu halten wie die in § 35 des Ersten Buches genannten Stellen. […]

(2) Werden Daten an eine nicht-öffentliche Stelle übermittelt, so sind die dort beschäftigten Personen, welche diese Daten speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, von dieser Stelle vor, spätestens bei der Übermittlung auf die Einhaltung der Pflichten nach Absatz 1 hinzuweisen.

(3)-(4) […]

Art. 83 DS-GVO – Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

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

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;

f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und

k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

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

(4) Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis

zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist:

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

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

a) die Grundsätze für die Verarbeitung, einschließlich der Bedingungen für die Einwilligung, gemäß den Artikeln 5, 6, 7 und 9;

b) die Rechte der betroffenen Person gemäß den Artikeln 12 bis 22;

c) die Übermittlung personenbezogener Daten an einen Empfänger in einem Drittland oder an eine internationale Organisation gemäß den Artikeln 44 bis 49;

d) alle Pflichten gemäß den Rechtsvorschriften der Mitgliedstaaten, die im Rahmen des Kapitels IX erlassen wurden;

e) Nichtbefolgung einer Anweisung oder einer vorübergehenden oder endgültigen Beschränkung oder Aussetzung der Datenübermittlung durch die Aufsichtsbehörde gemäß Artikel 58 Absatz 2 oder Nichtgewährung des Zugangs unter Verstoß gegen Artikel 58 Absatz 1. (6) – (9) […]

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

(1) Für Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 679/2016 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung.

(2) Für Verfahren wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 679/2016 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten und der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung und des Gerichtsverfassungsgesetzes, entsprechend. […]

§ 14 OWiG – Beteiligung

(1) Beteiligen sich mehrere an einer Ordnungswidrigkeit, so handelt jeder von ihnen ordnungswidrig. Dies gilt auch dann, wenn besondere persönliche Merkmale (§ 9 Abs. 1), welche die Möglichkeit der Ahndung begründen, nur bei einem Beteiligten vorliegen. (2) […]

(3) Handelt einer der Beteiligten nicht vorwerfbar, so wird dadurch die Möglichkeit der Ahndung bei den anderen nicht ausgeschlossen. Bestimmt das Gesetz, daß besondere persönliche Merkmale die Möglichkeit der Ahndung ausschließen, so gilt dies nur für den Beteiligten, bei dem sie vorliegen. (4) […]

Art. 82 DS-GVO – Haftung und Recht auf Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. (2)-(6) […]

§ 85 SGB X – Strafvorschriften

(1) Für Sozialdaten gelten die Strafvorschriften des § 42 Absatz 1 und 2 des Bundesdatenschutzgesetzes entsprechend.
(2)-(3) […]

§ 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)-(4) […]

III. *Anhang 3: Einwilligung für Drittbetroffene (inkl. Hinweisen zur Datenverarbeitung)*

1. Einwilligung für Drittbetroffene

Datenschutzrechtliche Einwilligung (für Drittbetroffene)

Vor-, Nachname d. Dritten

Ich, _____,

willige hiermit ein, dass die XY-LC und die XY-LC-Angehörigen meine personenbezogenen Daten (Art. 4 Nr. 2 DS-GVO), die in Ziffer 2 der *Hinweise zur Datenverarbeitung* aufgelistet sind, zum Zwecke der studentischen Rechtsberatung und Fallbearbeitung d. Klient*in, [Name] verarbeitet.

Ich bin **ausdrücklich damit einverstanden**, dass meine

- Angaben zum Familienstand und Verwandtschaft (insb. Kinder) sowie Staatsangehörigkeit
- Sprachkenntnisse in Wort und/oder Schrift
- personenbezogenen Angaben in Ausweisdokumenten (z.B. Reisepass) und Korrespondenz mit Dritten (etwa Behörden, Rechtsanwält*innen, gemeinnützigen Einrichtungen)
- [andere ggf. unter Ziffer 2 der Hinweise zur Datenverarbeitung im Einzelfall eingefügte Kategorien von personenbezogenen Daten, die Rückschlüsse auf das Sexualleben, die rassische und ethnische Herkunft, die religiöse Überzeugung oder die Gesundheit zulassen können]

in dem für die Rechtsberatung notwendigen Umfang verarbeitet werden, auch wenn man daraus im Einzelfall auf mein Sexualleben, meine rassische und ethnische Herkunft, meine religiösen Überzeugungen oder meine Gesundheit schließen kann.

Ich bin außerdem einverstanden, dass die obigen, von mir freiwillig mitgeteilten oder bei Dritten mit meiner Einwilligung erhobenen oder an die XY-LC übermittelten personenbezogenen Daten an folgende Empfänger*innen übermittelt und von diesen verarbeitet werden:

!!Bitte Zutreffendes ankreuzen!!!:

☐ an alle öffentlichen Stellen, gegen deren Vorgehen sich d. Klient*in– vertreten durch eine*n XY-LC-Angehörige*n – wendet bzw. von denen d. Klient*in Leistungen beansprucht oder beanspruchen möchte,

☐ an die Beratungsstelle, die den Fall d. Klient*in an die XY-LC weiterverwiesen hat, zur Information über das Ergebnis und zur weiteren Beratung und Bearbeitung des Anliegens,

☐ an die Supervisor*innen in pseudonymisierter Form, sofern das im Einzelfall erforderlich ist oder wird.

Diese Einwilligung erteile ich freiwillig.

Ich kann meine Einwilligung ohne Angabe von Gründen jederzeit bei der XY-LC

→ schriftlich: XY-Law Clinic, Postanschrift

→ per E-Mail an: mail@XY-LC.de

mit Wirkung für die Zukunft ganz oder zum Teil **widerrufen**.

Ich habe verstanden, dass meine Daten nur insoweit erhoben werden, als die XY-LC sie braucht, um den Beratungsvertrag mit d. Klient*in zu erfüllen und eine sachgerechte und erfolgreiche Rechtsberatung zu ermöglichen.

_____

Ort, Datum

Unterschrift/en der betroffenen Person; bei Kindern, die noch nicht die erforderliche Einsichtsfähigkeit erlangt haben: Unterschrift/en beider Elternteile oder sonstiger gesetzlicher Vertreter

2. Hinweise zur Datenverabreitung für Drittbetroffene

Hinweise zur Datenverarbeitung von Daten Dritter zur Erfüllung der Informationspflicht nach Art. 13,14 DS-GVO

1. Wer verarbeitet Ihre Daten?

Im Folgenden möchten wir, die

XY-Universität / XY-Uni Law Clinic („**XY-LC**“)

Postanschrift

Mail@XY-LC.de

Webseite

(die aktuelle Telefonnummer sowie weitere Kontaktdaten können Sie der Homepage entnehmen)

Sie über die Verarbeitung Ihrer personenbezogenen Daten im Rahmen unserer studentischen Rechtsberatung und die Ihnen nach dem Datenschutzrecht zustehenden Rechte informieren. Wir sind der für die Verarbeitung Ihrer personenbezogenen Daten **Verantwortliche** gemäß Art. 4 Nr. 7 DS-GVO[27].

Wenn Sie Fragen über die Verarbeitung Ihrer Daten oder Sorgen wegen des vertraulichen Umgangs mit Ihren Daten haben, sprechen Sie uns gerne an!

Sie können sich auch an unseren [**behördlichen] Datenschutzbeauftragten** [der XY-Universität] wenden:

Name, Postanschrift, Telefon, Fax, E-Mail

2. Welche Daten erheben wir, von wem, für welchen Zweck?

Wir erheben im Zuge der rechtlichen Beratung von [Name d. Klient*in] („**Klient*in**“) folgende (Kategorien von) **personenbezogenen Daten** über Ihre Person, **jedoch nur falls und soweit dies tatsächlich für die Rechtsberatung unseres/r Klient*in notwendig ist:**

- Ihr Name, Vorname, Geschlecht, Geburtsdatum/-ort und Staatsangehörigkeit
- Angaben zum Familienstand nebst Verwandtschaft (insb. Kinder)
- Wohn-/Meldeanschrift, Telefonnummer, E-Mail-Adresse
- Ihr ausländerrechtlicher bzw. aufenthaltsrechtlicher Status, Ordnungsmerkmale (Aktenzeichen etc.)
- Ihre Sprachkenntnisse in Wort und/oder Schrift
- [Angabe weiterer Datenkategorien, die möglicherweise im Einzelfall erhoben werden müssen]

Die Erhebung dieser Daten erfolgt grundsätzlich **bei Ihnen**. Die Daten können auch Ihren Angaben entnommen werden, die Sie bei Immatrikulation an oder bei Unterschrift eines Arbeitsvertrages mit der XY-Universität gemacht haben.

Wir erheben, speichern und verarbeiten diese Daten, um d. **Klient*in sachgerecht beraten und vertreten zu können**. Diese Datenverarbeitung stützen wir, sofern Sie Ihre Einwilligung erklären, ausschließlich auf Art. 6 I S.1 lit. a DS-GVO, anderenfalls auf berechtigtes Interesse (Art. 6 I S. 1 lit. f DS-GVO). Das berechtigte Interesse besteht an einer sachgerechten Beratung unserer/s Klient*in durch uns. Eine Verarbeitung sensibler Daten iSd. Art. 9 I DS-GVO, wie z.B. Ihre ethnische Herkunft oder religiöse Überzeugung, erfolgt nur insoweit diese notwendig ist und wird, sofern Sie Ihre Einwilligung erklären, ausschließlich auf Art. 6 I S. 1 lit. a, Art. 7, Art. 9 II lit. a DS-GVO gestützt. Anderenfalls stützen wir die Verarbeitung sensibler Daten auf Art. 9 II lit. c, f DS-GVO. Zur Abgabe einer Einwilligung können Sie sich des beiliegenden Musters bedienen.

Die Datenverarbeitung dient ggf. auch der **Abwicklung von Haftungsansprüchen**, die Sie gegen uns erheben, auf Basis von Art. 6 I S. 1 lit. f DS-GVO.

3. Wie lange speichern wir Ihre Daten?

Ihre von uns erhobenen personenbezogenen Daten werden grundsätzlich nach **Wegfall des Beratungszwecks** bzw. des **Widerrufs Ihrer Einwilligung** gelöscht. Falls gesetzliche **Aufbewahrungsfristen** bestehen, werden die Daten nach deren Ablauf gelöscht. Diese Erforderlichkeit der weiteren Speicherung Ihrer Daten wird in diesem Sinne regelmäßig zum kalendarischen Jahresende geprüft.

Im begründeten **Einzelfall** können sämtliche zur Beweisführung erforderlichen Daten bis zu 10 Jahre aufbewahrt werden, wenn Tatsachen die Annahme rechtfertigen, dass Sie die Geltendmachung von Haftungsansprüchen gegen uns beabsichtigen.

4. An wen übermitteln wir Ihre Daten?

Eine Übermittlung erfolgt grundsätzlich nur an die Beratungsstelle, die d. Klient*in an die XY-LC weiterverwiesen hat, sowie an alle öffentlichen Stellen, gegen deren Vorgehen sich d. Klient*in – vertreten durch die XY-LC wenden bzw. von denen er/sie Leistungen beansprucht oder beanspruchen möchte.

Innerhalb der XY-LC erhalten nur die Mitarbeiter Zugriff, die mit der Bearbeitung Ihrer Rechtsangelegenheit betraut sind.

[27] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („**DS-GVO**“).

An die zur Supervision eingesetzten Volljurist*innen werden Ihre Daten grds. nur in anonymisierter Form[28] übermittelt.

Im Einzelfall und soweit für die Rechtsberatung erforderlich übermitteln wir Ihre Daten ggf. in pseudonymisierter Form[29].

5. Welche Rechte haben Sie?

Sie können

- falls Sie eine **Einwilligung** erteilt haben, diese jederzeit gegenüber uns **widerrufen** (Art. 7 III DS-GVO). Wir werden dann die Datenverarbeitung, die auf dieser Einwilligung beruhte, in der Zukunft nicht mehr vornehmen,
- **Auskunft** über Ihre von uns verarbeiteten personenbezogenen Daten erhalten (Art. 15 DS-GVO),
- die **Berichtigung** unrichtiger oder **Vervollständigung** Ihrer von uns verarbeiteten personenbezogenen Daten verlangen (Art. 16 DS-GVO),
- die **Löschung** Ihrer bei uns verarbeiteten personenbezogenen Daten verlangen, wenn
  - Ihre personenbezogenen Daten für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind,
  - Sie Ihre Einwilligung widerrufen (falls erteilt)
  - Sie gemäß Art. 21 DS-GVO erfolgreich Widerspruch gegen die Verarbeitung eingelegt haben,
  - Ihre personenbezogenen Daten unrechtmäßig verarbeitet wurden, oder
  - die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

  Dies gilt jedoch nicht, falls die Verarbeitung erforderlich ist (Art. 17 III DS-GVO)

  - zur Ausübung des Rechts auf freie Meinungsäußerung und Information
  - zur Erfüllung einer rechtlichen Verpflichtung,
  - aus Gründen des öffentlichen Interesses,
  - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

  oder die Verarbeitung im Einzelfall nach anderen gesetzlichen Vorschriften weiterhin zulässig ist.
- die **Einschränkung der Verarbeitung** Ihrer bei uns verarbeiteten personenbezogenen Daten verlangen (Art. 18 DS-GVO), soweit
  - die Richtigkeit der Daten von Ihnen bestritten wird,
  - die Verarbeitung unrechtmäßig ist, Sie aber deren Löschung ablehnen,
  - wir diese Daten nicht länger benötigen, Sie jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen, oder
  - gemäß Art. 21 DS-GVO Widerspruch gegen die Verarbeitung eingelegt haben,
- Ihre uns bereitgestellten personenbezogenen Daten in einem **strukturierten, gängigen und maschinenlesbaren Format erhalten**, und diese Daten **einem anderen Verantwortlichen** durch uns **übermitteln** lassen (Art. 20 DS-GVO).

Sie können **Widerspruch** gegen die Verarbeitung Ihrer personenbezogenen Daten einlegen (Art. 21 DS-GVO), wenn Sie aufgrund Ihrer besonderen Situation dafür Gründe haben und soweit wir die Verarbeitung auf berechtigtes Interesse stützen (Art. 6 I S. 1 **lit. f** DS-GVO).

Wir dürfen Ihre personenbezogenen Daten dann nur noch verarbeiten, wenn wir zwingende schutzwürdige Gründe dafür nachweisen, die schwerer wiegen, als Ihre Interessen, Rechte und Freiheiten oder die weitere Verarbeitung ausschließlich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erfolgt.

Es genügt jeweils eine formlose Mitteilung an:

Mail@XY-LC.de

Sie können sich außerdem gemäß Art. 77 DS-GVO sich bei einer Aufsichtsbehörde **beschweren**, wenn Sie der Ansicht sind, dass unsere Verarbeitung Ihrer personenbezogenen Daten gegen diese Verordnung verstößt.

Ihre Beschwerde nimmt etwa der

Landesbeauftragte für Datenschutz und Informationsfreiheit
Postanschrift

Telefon
Webseite

entgegen.

6. Schlussbemerkungen

Wir beabsichtigen keine Übermittlung Ihrer Daten in Drittländer außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums.

Eine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Art. 22 DS-GVO findet nicht statt

[28] Die Informationen werden derart verändert, dass nicht mehr auf Sie geschlossen werden kann.
[29] Ihr Name oder andere Identifikationsmerkmale werden durch ein Pseudonym ersetzt, um die Rückschlüsse auf Ihre Person wesentlich zu erschweren.

IV. *Anhang 4: Einwilligung Supervisor*innen/Beirät*innen (inkl. Hinweisen zur Datenverarbeitung)*

1. Einwilligung für Supervisor*innen/Beirät*innen

Datenschutzrechtliche Einwilligung (für Supervisor*innen/Beirät*innen)

Vor-, Nachname d. betroffenen Person

Ich, _____,

willige hiermit ein,

dass die XY-LC und Ihre XY-LC-Angehörigen für die Kontaktaufnahme, Dokumentation, administrative Durchführbarkeit der Beratungspraxis und Förderung der Zusammenarbeit meine personenbezogenen Daten, die in Ziffer 2 der

Hinweise zur Datenverarbeitung

aufgelisteten personenbezogenen Daten, die ich freiwillig zur Verfügung stelle, für die in Ziffer 3 der *Hinweise zur Datenverarbeitung* angegebene Dauer verarbeitet (Art. 4 Nr. 2 DS-GVO).

Ich kann meine Einwilligung ohne Angabe von Gründen jederzeit bei der XY-LC

→ schriftlich: XY-Law Clinic,Postanschrift

→ per E-Mail an: mail@XY-LC.de

mit Wirkung für die Zukunft ganz oder zum Teil **widerrufen**.

Ich habe verstanden, dass meine Daten nur insoweit erhoben werden, als die XY-LC sie für die genannten Zwecke braucht.

_____

Ort, Datum

Unterschrift/en der betroffenen Person

2. Hinweise zur Datenverabeitung für Supervisor*innen/Beirät*innen

Hinweise zur Datenverarbeitung von Supervisor*innen nach Art. 13 DS-GVO

1. Wer verarbeitet Ihre Daten?

Im Folgenden möchten wir, die

XY-Universität / XY-Law Clinic („**XY-LC**“)

Postanschrift

Mail@XY-LC.de

Webseite

(die aktuelle Telefonnummer sowie weitere Kontaktdaten können Sie der Homepage entnehmen)

Sie über die Verarbeitung Ihrer personenbezogenen Daten im Rahmen unserer studentischen Rechtsberatung und die Ihnen nach dem Datenschutzrecht zustehenden Rechte informieren. Wir sind der für die Verarbeitung Ihrer personenbezogenen Daten **Verantwortliche** gemäß Art. 4 Nr. 7 DS-GVO[30].

Wenn Sie Fragen über die Verarbeitung Ihrer Daten haben, sprechen Sie uns gerne an!

Sie können sich auch an unseren [**behördlichen] Datenschutzbeauftragten** [der XY-Universität] wenden:

Name, Postanschrift, Telefon, Fax, E-Mail

2. Welche Daten erheben wir, von wem, für welchen Zweck?

Wir erheben folgende (Kategorien von) **personenbezogenen Daten**, jedoch nur in dem tatsächlich notwendigen Umfang:

- Ihre Kontaktdaten (Name, Vorname, berufliche E-Mail-Adresse, Telefonnummer, Kanzleianschrift)
- Ihre Fachrichtung
- Die von Ihnen supervidierten Fälle
- Falls zutreffend, bei Ihnen absolvierte Praktika durch stud. Hilfskräfte/Berater*innen der XY-LC

Die Erhebung dieser Daten erfolgt grundsätzlich **bei Ihnen**.

Wir erheben, speichern und verarbeiten diese Daten, um Sie **kontaktieren zu können, Ihre Beteiligung an der XY-LC zu dokumentieren, unsere Beratungspraxis administrativ durchführen zu können und zur Förderung der Zusammenarbeit.**

Diese Datenverarbeitung stützen wir grds. auf Art. 6 I S. 1 lit. b DS-GVO.

Die Datenverarbeitung dient ggf. in Einzelfällen auch der **Abwicklung von Haftungsansprüchen**, die Sie gegen uns erheben, auf Basis von berechtigtem Interesse (Art. 6 I S. 1 lit. f DS-GVO).

3. Wie lange speichern wir Ihre Daten?

Ihre von uns erhobenen personenbezogenen Daten werden grundsätzlich nach **Wegfall des Zwecks** bzw. Ablauf der gesetzlichen **Aufbewahrungsfristen** gelöscht. Diese Erforderlichkeit der weiteren Speicherung Ihrer Daten wird in diesem Sinne regelmäßig zum kalendarischen Jahresende geprüft.

Im begründeten **Einzelfall** können sämtliche zur Beweisführung erforderlichen Daten bis zu 10 Jahre aufbewahrt werden, wenn Tatsachen die Annahme rechtfertigen, dass Sie die Geltendmachung von Haftungsansprüchen gegen uns beabsichtigen.

4. An wen übermitteln wir Ihre Daten?

Innerhalb der XY-LC erhalten nur die XY-LC-Angehörigen Zugriff. Eine weitere Übermittlung findet nicht statt.

5. Welche Rechte haben Sie?

Sie können

- **Auskunft** über Ihre von uns verarbeiteten personenbezogenen Daten erhalten (Art. 15 DS-GVO),
- die **Berichtigung** unrichtiger oder **Vervollständigung** Ihrer von uns verarbeiteten personenbezogenen Daten verlangen (Art. 16 DS-GVO),
- die **Löschung** Ihrer bei uns verarbeiteten personenbezogenen Daten verlangen, wenn
  - Ihre personenbezogenen Daten für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind,
  - Sie gemäß Art. 21 DS-GVO erfolgreich Widerspruch gegen die Verarbeitung eingelegt haben,
  - Ihre personenbezogenen Daten unrechtmäßig verarbeitet wurden, oder
  - die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

  Dies gilt jedoch nicht, falls die Verarbeitung erforderlich ist (Art. 17 III DS-GVO)

  - zur Ausübung des Rechts auf freie Meinungsäußerung und Information
  - zur Erfüllung einer rechtlichen Verpflichtung,
  - aus Gründen des öffentlichen Interesses,
  - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

  oder die Verarbeitung im Einzelfall nach anderen gesetzlichen Vorschriften weiterhin zulässig ist.

[30] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („**DS-GVO**“).

– die **Einschränkung der Verarbeitung** Ihrer bei uns verarbeiteten personenbezogenen Daten verlangen (Art. 18 DS-GVO), soweit
  - die Richtigkeit der Daten von Ihnen bestritten wird,
  - die Verarbeitung unrechtmäßig ist, Sie aber deren Löschung ablehnen,
  - wir diese Daten nicht länger benötigen, Sie jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen, oder
  - gemäß Art. 21 DS-GVO Widerspruch gegen die Verarbeitung eingelegt haben,

Ihre uns bereitgestellten personenbezogenen Daten in einem **strukturierten, gängigen und maschinenlesbaren Format erhalten**, und diese Daten **einem anderen Verantwortlichen** durch uns **übermitteln** lassen (Art. 20 DS-GVO).

Nach Art. 21 DS-GVO haben Sie grds. ein **Widerspruchsrecht** gegen die Verarbeitung Ihrer personenbezogenen Daten einlegen, wenn Sie aufgrund Ihrer besonderen Situation dafür Gründe haben und soweit wir die Verarbeitung lediglich auf berechtigtes Interesse stützen (Art. 6 S. 1 **lit. f** DS-GVO).

Wir weisen aber darauf hin, dass wir Ihre personenbezogenen Daten trotzdem weiterverarbeiten dürfen, soweit die Verarbeitung Ihrer Daten lediglich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erfolgt.

Es genügt jeweils eine formlose Mitteilung an:

Mail@XY-LC.de

Sie können sich außerdem gemäß Art. 77 DS-GVO bei einer Aufsichtsbehörde **beschweren**, wenn Sie der Ansicht sind, dass unsere Verarbeitung Ihrer personenbezogenen Daten gegen diese Verordnung verstößt.

Ihre Beschwerde nimmt etwa der

Landesbeauftragte für Datenschutz und Informationsfreiheit
Postanschrift

Telefon

Webseite

entgegen.

6. Schlussbemerkungen

Wir beabsichtigen keine Übermittlung Ihrer Daten in Drittländer außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums.

Eine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Art. 22 DS-GVO findet nicht statt.

Wir weisen abschließend darauf hin, dass die internetbasierte, unverschlüsselte Datenübertragung von Anfragen oder Dokumenten (etwa per E-Mail) keinen Schutz vor dem Zugriff durch Dritte bietet.

V. *Anhang 5: Einwilligung Dolmetscher*innen (inkl. Hinweise zur Datenverarbeitung)*

1. Einwilligung für Dolmetscher*innen

Datenschutzrechtliche Einwilligung (für Dolmetscher*innen)

Vor-, Nachname d. betroffenen Person

Ich, _____,

willige hiermit ein,

dass die XY-LC und Ihre XY-LC-Angehörigen für die Kontaktaufnahme und administrative Durchführbarkeit der Beratungspraxis meine personenbezogenen Daten, die in Ziffer 2 der

Hinweise zur Datenverarbeitung

aufgelisteten personenbezogenen Daten, die ich freiwillig zur Verfügung stelle, für die in Ziffer 3 der *Hinweise zur Datenverarbeitung* angegebene Dauer verarbeitet (Art. 4 Nr. 2 DS-GVO).

Ich kann meine Einwilligung ohne Angabe von Gründen jederzeit bei der XY-LC

→ schriftlich: XY-Law Clinic,Postanschrift

→ per E-Mail an: mail@XY-LC.de

mit Wirkung für die Zukunft ganz oder zum Teil **widerrufen**.

Ich habe verstanden, dass meine Daten nur insoweit erhoben werden, als die XY-LC sie für die genannten Zwecke braucht.

_____
Ort, Datum

Unterschrift/en der betroffenen Person

2. Hinweise zur Datenverarbeitung für Dolmetscher*innen

Hinweise zur Datenverarbeitung von Dolmetscher*innen nach Art. 13 DS-GVO

1. Wer verarbeitet Ihre Daten?

Im Folgenden möchten wir, die

XY-Universität / XY-Uni Law Clinic („**XY-LC**“)

Postanschrift

Mail@XY-LC.de

Webseite

(die aktuelle Telefonnummer sowie weitere Kontaktdaten können Sie der Homepage entnehmen)

Sie über die Verarbeitung Ihrer personenbezogenen Daten im Rahmen unserer studentischen Rechtsberatung und die Ihnen nach dem Datenschutzrecht zustehenden Rechte informieren. Wir sind der für die Verarbeitung Ihrer personenbezogenen Daten **Verantwortliche** gemäß Art. 4 Nr. 7 DS-GVO[31].

Wenn Sie Fragen über die Verarbeitung Ihrer Daten haben, sprechen Sie uns gerne an!

Sie können sich auch an unseren [**behördlichen] Datenschutzbeauftragten** [der XY-Universität] wenden:

Name, Postanschrift, Telefon, Fax, E-Mail

2. Welche Daten erheben wir, von wem, für welchen Zweck?

Wir erheben folgende (Kategorien von) **personenbezogenen Daten von Ihnen**, jedoch nur in dem tatsächlich notwendigen Umfang:

– Ihre Kontaktdaten (Name, Vorname, E-Mail-Adresse, Telefonnummer, Wohnanschrift)

Die Erhebung dieser Daten erfolgt grundsätzlich **bei Ihnen**. Wir erheben, speichern und verarbeiten diese Daten, um sie **kontaktieren zu können und um unsere Beratungspraxis administrativ durchführen zu können.** Diese Datenverarbeitung stützen wir grds. auf Ihre Einwilligung (Art. 6 I S. 1 lit. a DS-GVO).

Die Datenverarbeitung dient ggf. auch der **Abwicklung von Haftungsansprüchen**, die Sie gegen uns erheben, auf Basis von berechtigtem Interesse (Art. 6 I S. 1 lit. f DS-GVO).

3. Wie lange speichern wir Ihre Daten?

Ihre von uns erhobenen personenbezogenen Daten werden grundsätzlich nach **Wegfall des Zwecks** bzw. Ablauf der gesetzlichen Aufbewahrungsfristen gelöscht. Diese Erforderlichkeit der weiteren Speicherung Ihrer Daten wird in diesem Sinne regelmäßig zum kalendarischen Jahresende geprüft.

Im begründeten **Einzelfall** können sämtliche zur Beweisführung erforderlichen Daten bis zu 10 Jahre aufbewahrt werden, wenn Tatsachen die Annahme rechtfertigen, dass Sie die Geltendmachung von Haftungsansprüchen gegen uns beabsichtigen.

4. An wen übermitteln wir Ihre Daten?

Innerhalb der XY-LC erhalten nur die XY-LC-Angehörigen Zugriff. Eine Übermittlung der Daten findet nicht statt.

5. Welche Rechte haben Sie?

Sie können

– Ihre Einwilligung jederzeit uns gegenüber **widerrufen** (Art. 7 III DS-GVO),
– **Auskunft** über Ihre von uns verarbeiteten personenbezogenen Daten erhalten (Art. 15 DS-GVO),
– die **Berichtigung** unrichtiger oder **Vervollständigung** Ihrer von uns verarbeiteten personenbezogenen Daten verlangen (Art. 16 DS-GVO),
– die **Löschung** Ihrer bei uns verarbeiteten personenbezogenen Daten verlangen, wenn
  - Ihre personenbezogenen Daten für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind,
  - Sie Ihre Einwilligung widerrufen
  - Sie gemäß Art. 21 DS-GVO erfolgreich Widerspruch gegen die Verarbeitung eingelegt haben,
  - Ihre personenbezogenen Daten unrechtmäßig verarbeitet wurden, oder
  - die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

  Dies gilt jedoch nicht, falls die Verarbeitung erforderlich ist (Art. 17 III DS-GVO)

  - zur Ausübung des Rechts auf freie Meinungsäußerung und Information
  - zur Erfüllung einer rechtlichen Verpflichtung,
  - aus Gründen des öffentlichen Interesses,
  - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

  oder die Verarbeitung im Einzelfall nach anderen gesetzlichen Vorschriften weiterhin zulässig ist.
– die **Einschränkung der Verarbeitung** Ihrer bei uns verarbeiteten personenbezogenen Daten verlangen (Art. 18 DS-GVO), soweit
  - die Richtigkeit der Daten von Ihnen bestritten wird,
  - die Verarbeitung unrechtmäßig ist, Sie aber deren Löschung ablehnen,

[31] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („**DS-GVO**“).

- wir diese Daten nicht länger benötigen, Sie jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen, oder
- gemäß Art. 21 DS-GVO Widerspruch gegen die Verarbeitung eingelegt haben,

– Ihre uns bereitgestellten personenbezogenen Daten in einem **strukturierten, gängigen und maschinenlesbaren Format erhalten**, und diese Daten **einem anderen Verantwortlichen** durch uns **übermitteln** lassen (Art. 20 DS-GVO).

Nach Art. 21 DS-GVO haben Sie grds. ein **Widerspruchsrecht** gegen die Verarbeitung Ihrer personenbezogenen Daten einlegen, wenn Sie aufgrund Ihrer besonderen Situation dafür Gründe haben und soweit wir die Verarbeitung für einen Verarbeitungszweck lediglich auf berechtigtes Interesse stützen (Art. 6 I S. 1 **lit. f** DS-GVO).

Wir weisen aber darauf hin, dass wir Ihre personenbezogenen Daten trotzdem weiterverarbeiten dürfen, soweit die Verarbeitung Ihrer Daten lediglich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erfolgt.

Es genügt jeweils eine formlose Mitteilung an:

Mail@XY-LC.de

Sie können sich außerdem gemäß Art. 77 DS-GVO bei einer Aufsichtsbehörde **beschweren**, wenn Sie der Ansicht sind, dass unsere Verarbeitung Ihrer personenbezogenen Daten gegen diese Verordnung verstößt.

Ihre Beschwerde nimmt etwa der

Landesbeauftragte für Datenschutz und Informationsfreiheit
Postanschrift

Telefon
Webseite

entgegen.

6. Schlussbemerkungen

Wir beabsichtigen keine Übermittlung Ihrer Daten in Drittländer außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums.

Eine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Art. 22 DS-GVO findet nicht statt.

Wir weisen abschließend darauf hin, dass die internetbasierte, unverschlüsselte Datenübertragung von Anfragen oder Dokumenten (etwa per E-Mail) keinen Schutz vor dem Zugriff durch Dritte bietet.

VI. *Anhang 6: Einwilligung Sozialarbeiter*innen (inkl. Hinweise zur Datenverarbeitung)*

1. Einwilligung für Sozialarbeiter*innen

Datenschutzrechtliche Einwilligung (für Sozialarbeiter*innen)

Vor-, Nachname d. betroffenen Person

Ich, _____,

willige hiermit ein, dass die XY-LC und Ihre XY-LC-Angehörigen für die Kontaktaufnahme und administrative Durchführbarkeit der Beratungspraxis meine personenbezogenen Daten, die in Ziffer 2 der *Hinweise zur Datenverarbeitung* aufgelisteten personenbezogenen Daten und die ich freiwillig zur Verfügung stelle, für die in Ziffer 3 der *Hinweise zur Datenverarbeitung* angegebene Dauer verarbeitet (Art. 4 Nr. 2 DS-GVO).

Ich kann meine Einwilligung ohne Angabe von Gründen jederzeit bei der XY-LC

→ schriftlich: XY-Law Clinic, Postanschrift

→ per E-Mail an: mail @XY-LC.de

mit Wirkung für die Zukunft ganz oder zum Teil **widerrufen**.

Ich habe verstanden, dass meine Daten nur insoweit erhoben werden, als die XY-LC sie für die genannten Zwecke braucht.

_____

Ort, Datum

Unterschrift/en der betroffenen Person; bei Kindern, die noch nicht die erforderliche Einsichtsfähigkeit erlangt haben: Unterschrift/en beider Elternteile oder sonstiger gesetzlicher Vertreter

2. Hinweise zur Datenverarbeitung für Sozialarbeiter*innen

Hinweise zur Datenverarbeitung von Sozialarbeiter*innen nach Art. 13 DS-GVO

1. Wer verarbeitet Ihre Daten?

Im Folgenden möchten wir, die

XY-Universität XY-Law Clinic („**XY-LC**“) Postanschrift

Mailadresse

Webseite

(die aktuelle Telefonnummer sowie weitere Kontaktdaten können Sie der Homepage entnehmen)

Sie über die Verarbeitung Ihrer personenbezogenen Daten im Rahmen unserer studentischen Rechtsberatung und die Ihnen nach dem Datenschutzrecht zustehenden Rechte informieren. Wir sind der für die Verarbeitung Ihrer personenbezogenen Daten **Verantwortliche** gemäß Art. 4 Nr. 7 DS-GVO[32].

Wenn Sie Fragen über die Verarbeitung Ihrer Daten haben, sprechen Sie uns gerne an!

Sie können sich auch an unseren [**behördlichen**] **Datenschutzbeauftragten** [der XY-Universität] wenden:

Name, Postanschrift, Telefon, Fax, E-Mail

2. Welche Daten erheben wir, von wem, für welchen Zweck?

Wir erheben folgende (Kategorien von) **personenbezogenen Daten von Ihnen**, jedoch nur in dem tatsächlich notwendigen Umfang:

– Ihre Kontaktdaten (Name, Vorname, E-Mail-Adresse, Telefonnummer, Wohnanschrift)

Die Erhebung dieser Daten erfolgt grundsätzlich **bei Ihnen oder bei d. Klient*in**. Wir erheben, speichern und verarbeiten diese Daten, um Sie und ggf. über Sie d. Klient*in **kontaktieren zu können und um unsere Beratungspraxis administrativ durchführen zu können.** Diese Datenverarbeitung stützen wir grds. auf Ihre Einwilligung (Art.6 I S. 1 lit. a DS-GVO).

Die Datenverarbeitung dient ggf. auch der **Abwicklung von Haftungsansprüchen**, die Sie gegen uns erheben, auf Basis von berechtigtem Interesse (Art. 6 I S. 1 lit. f DS-GVO).

3. Wie lange speichern wir Ihre Daten?

Ihre von uns erhobenen personenbezogenen Daten werden grundsätzlich nach **Wegfall des Zwecks** bzw. Ablauf der gesetzlichen **Aufbewahrungsfristen** gelöscht. Diese Erforderlichkeit der weiteren Speicherung Ihrer Daten wird in diesem Sinne regelmäßig zum kalendarischen Jahresende geprüft.

Im begründeten **Einzelfall** können sämtliche zur Beweisführung erforderlichen Daten bis zu 10 Jahre aufbewahrt werden, wenn Tatsachen die Annahme rechtfertigen, dass Sie die Geltendmachung von Haftungsansprüchen gegen uns beabsichtigen.

4. An wen übermitteln wir Ihre Daten?

Innerhalb der XY-LC erhalten nur die XY-LC-Angehörigen Zugriff. Eine Übermittlung der Daten findet nicht statt.

5. Welche Rechte haben Sie?

Sie können

– Ihre Einwilligung jederzeit uns gegenüber **widerrufen** (Art. 7 III DS-GVO),
– **Auskunft** über Ihre von uns verarbeiteten personenbezogenen Daten erhalten (Art. 15 DS-GVO),
– die **Berichtigung** unrichtiger oder **Vervollständigung** Ihrer von uns verarbeiteten personenbezogenen Daten verlangen (Art. 16 DS-GVO),
– die **Löschung** Ihrer bei uns verarbeiteten personenbezogenen Daten verlangen, wenn
  - Ihre personenbezogenen Daten für die Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind,
  - Sie Ihre Einwilligung widerrufen
  - Sie gemäß Art. 21 DS-GVO erfolgreich Widerspruch gegen die Verarbeitung eingelegt haben,
  - Ihre personenbezogenen Daten unrechtmäßig verarbeitet wurden, oder
  - die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.

  Dies gilt jedoch nicht, falls die Verarbeitung erforderlich ist (Art. 17 III DS-GVO)

  - zur Ausübung des Rechts auf freie Meinungsäußerung und Information
  - zur Erfüllung einer rechtlichen Verpflichtung,
  - aus Gründen des öffentlichen Interesses,
  - zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen

  oder die Verarbeitung im Einzelfall nach anderen gesetzlichen Vorschriften weiterhin zulässig ist.
– die **Einschränkung der Verarbeitung** Ihrer bei uns verarbeiteten personenbezogenen Daten verlangen (Art. 18 DS-GVO), soweit
  - die Richtigkeit der Daten von Ihnen bestritten wird,
  - die Verarbeitung unrechtmäßig ist, Sie aber deren Löschung ablehnen,

[32] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG („**DS-GVO**“).

- wir diese Daten nicht länger benötigen, Sie jedoch diese zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigen, oder
- gemäß Art. 21 DS-GVO Widerspruch gegen die Verarbeitung eingelegt haben,

– Ihre uns bereitgestellten personenbezogenen Daten in einem **strukturierten, gängigen und maschinenlesbaren Format erhalten**, und diese Daten **einem anderen Verantwortlichen** durch uns **übermitteln** lassen (Art. 20 DS-GVO).

Nach Art. 21 DS-GVO haben Sie grds. ein **Widerspruchsrecht** gegen die Verarbeitung Ihrer personenbezogenen Daten einlegen, wenn Sie aufgrund Ihrer besonderen Situation dafür Gründe haben und soweit wir die Verarbeitung für einen Verarbeitungszweck lediglich auf berechtigtes Interesse stützen (Art. 6 I S. 1 lit. f DS-GVO).

Wir weisen aber darauf hin, dass wir Ihre personenbezogenen Daten trotzdem weiterverarbeiten dürfen, soweit die Verarbeitung Ihrer Daten lediglich zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erfolgt.

Es genügt jeweils eine formlose Mitteilung an:

mail@XY-LC.de

Sie können sich außerdem gemäß Art. 77 DS-GVO bei einer Aufsichtsbehörde **beschweren**, wenn Sie der Ansicht sind, dass unsere Verarbeitung Ihrer personenbezogenen Daten gegen diese Verordnung verstößt.

Ihre Beschwerde nimmt etwa der

Landesbeauftragte für Datenschutz und Informationsfreiheit
Postanschrift

Telefon
Mail/Webseite

entgegen.

6. Schlussbemerkungen

Wir beabsichtigen keine Übermittlung Ihrer Daten in Drittländer außerhalb der Europäischen Union und des Europäischen Wirtschaftsraums.

Eine automatisierte Entscheidungsfindung einschließlich Profiling gemäß Art. 22 DS-GVO findet nicht statt.

Wir weisen abschließend darauf hin, dass die internetbasierte, unverschlüsselte Datenübertragung von Anfragen oder Dokumenten (etwa per E-Mail) keinen Schutz vor dem Zugriff durch Dritte bietet.

VII. *Anhang 7: Verarbeitungsverzeichnis (inkl. TOM)*

Hinweis zum Verarbeitungsverzeichnis (inkl. TOM)

Das nachfolgend aufgeführte Verarbeitungsverzeichnis soll gleichzeitig als Vorlage zum Entwurf eines eigenen Verzeichnisses und als Orientierung für die korrekte Eintragung dienen. Daher sollte hier ganz besonders darauf geachtet werden, dass die nachfolgende Vorlage eine beispielhafte Verarbeitung der Goethe-Uni LC darstellt. Diese kann sich stark von Ort zu Ort unterscheiden.

Dieses Verzeichnis kann aber sehr gut als Ausganspunkt eines eigenen Verzeichnisses dienen. Da sich eine generelle Kopie dieses Dokuments grundsätzlich nicht empfiehlt, wurde auf die gelbe Markierung der zu bearbeitenden Bereiche hier ausnahmsweise verzichtet.

Das Verarbeitungsverzeichnis enthält in Nr. 7 auch einen Bereich, in dem die technischen und organisatorischen Maßnahmen (kurz: TOM) eingefügt werden können. **Unterhalb dieser Vorlage (siehe *E.VII.2*)** befindet sich eine **Anleitung zur Erarbeitung dieser TOM**.

1. Verzeichnis von Verarbeitungstätigkeiten (Art. 30 Abs. 1 DS-GVO

Verzeichnis von Verarbeitungstätigkeiten (Art. 30 Abs. 1 DS-GVO)

1.0 lfd. Nr. ☒ neues Verfahren ☐ Änderung

1. Angaben zum Verantwortlichen

1.1	Name und Anschrift, Kontaktdaten Johann Wolfgang Goethe-Universität Frankfurt SdöR Goethe-Uni Law Clinic (Im Folgenden: „**GLC**“) Theodor W. Adorno-Platz 4 60323 Frankfurt a.M. GLC@uni-frankfurt.de http://www.glc.uni-frankfurt.de
	Interne Datenschutzkoordinatorin (nicht zugleich behördlicher Datenschutzbeauftragter der Universität Frankfurt, vgl. www.uni-frankfurt.de/47859992/datenschutzbeauftragte): Frau Maximiliane Musterfrau, XY-Straße, 6000 Frankfurt (Anschrift s.o.)
	Behördlicher Datenschutzbeauftragter der Universität Frankfurt: Maximilian Mustermann Fachbereich Informatik und Mathematik Institut für Informatik, Rechnerbetriebsgruppe Informatik (RBI)

	XY-Straße 6000 Frankfurt am Main
1.2	Organisationskennziffer, Amt, Abteilung, ggf. Sachgebiet Lehrstuhl für Öffentliches Recht mit Schwerpunkt Sozialrecht, Institut für Öffentliches Recht, Fachbereich 01 Rechtswissenschaft, RuW Gebäude,
1.3	Name u. Anschrift von Auftragnehmern gemäß Art. 28 DS-GVO Es findet keine Auftragsverarbeitung statt.

2. Zweckbestimmung und Rechtsgrundlagen der Datenverarbeitung

2.1	Zweckbestimmung Die GLC am Lehrstuhl für Öffentliches Recht mit Schwerpunkt Sozialrecht, zugehörig dem Institut für Öffentliches Recht der Johann Wolfgang Goethe-Universität Frankfurt, betreibt kostenlose, studentische Rechtsberatung Dritter (sog. Klient*innen) insb. auf dem Gebiet des Aufenthalts, Asyl- und Sozialrechts unter Supervision gemäß § 6 II 2 RDG zu Forschungs- und Ausbildungszwecken (sog. „*Clinical Legal Education*“). Dazu werden von den Klient*innen sowie von den diese beratenden Studierenden sowie supervidierenden Personen mit Befähigung zum Richteramt (i.d.R. Rechtsanwält*innen), Sozialarbeiter*innen bzw. anderen Kontaktpersonen d. Klient*in im Inland, behördlichen Ansprechpartner*innen, fallrelevanten Dritten und Dolmetscher*innen personenbezogene Daten im nachfolgend beschriebenen Umfang erhoben, verarbeitet und genutzt.
2.2	ggf. Bezeichnung des Verfahrens Erhebung, Verarbeitung (inkl. Übermittlung) und Nutzung personenbezogener Daten von Klient*innen, sowie, falls erforderlich, Dritter (z.B. Familienangehörige, Bezugspersonen, etc.) zum Zwecke der Rechtsberatung und ggf. zur Verteidigung gegen Haftungsansprüche im Einzelfall; Erhebung, Verarbeitung und Nutzung personenbezogener Daten von GLC-Angehörigen (wissenschaftliche Mitarbeiter*innen, Studentische Hilfskräfte und Studentische Berater*innen), in Einzelfällen Dolmetscher*innen sowie Sozialarbeiter*innen bzw. anderen Kontaktpersonen d. Klient*in im Inland, behördlichen Ansprechpartner*innen und Supervisor*innen für das geschützte, interne Zugriffsportal zum Zweck der Dokumentation der Beteiligung der betroffenen Personen an der GLC und der administrativen Durchführbarkeit der Beratungspraxis (z.B. Verteilung von Aufgaben und Zuständigkeiten, Koordinierung, Erreichbarkeit d. Klient*in, etc.) sowie der Förderung der Zusammenarbeit zwischen den bei der GLC Engagierten und ggf. zur Verteidigung gegen Haftungsansprüche im Einzelfall;
2.3	Rechtsgrundlage Erhebung, Verarbeitung (inkl. Übermittlung) und Nutzung personenbezogener Daten zum Zwecke der ***Rechtsberatung d. Klient*in***: – Klient*innen: Art. 6 I S. 1 lit. a DS-GVO ; sofern sensible Daten betroffen sind Art. 6 I S. 1 lit. a, 7, 9 II lit. a DS-GVO. – fallrelevante Dritte: Falls eine Einwilligung erteilt wurde: Art. 6 I S. 1 lit. a DS-GVO bzw. bei sensiblen Daten Art. 6 I S. 1 lit. a, 7,Art. 9 II lit. a DS-GVO. Im Falle des Widerrufs der Einwilligung erfolgt keine weitere Verarbeitung. Falls keine Einwilligung erteilt wurde: Art. 6 I S. 1 lit. f DS-GVO bzw. Art. 9 II lit. c, f DS-GVO, sollte eine Erhebung sensibler Daten im Einzelfall erforderlich sein. Erhebung, Verarbeitung (inkl. Übermittlung) und Nutzung personenbezogener Daten für Zwecke der ***Administration und Förderung*** *(s. genauer ausgeführt in 2.2.)*: – Supervisor*innen: Art. 6 I S. 1 lit. b DS-GVO – GLC-Angehörige: Art. 6 I S. 1 lit. b DS-GVO – Dolmetscher*innen: Art. 6 I S. 1 lit. a DS-GVO – Sozialarbeiter*innen bzw. andere Kontaktpersonen d. Klient*in im Inland: Art. 6 I S. 1 lit. a DS-GVO – Behördliche Ansprechpartner*innen: Art. 6 I S. 1 lit. f DS-GVO

Zum Zwecke der ***Verteidigung gegen Haftungsansprüche im Einzelfall*** wird die Verarbeitung der personenbezogenen Daten aller hier aufgezählten betroffenen Personen auf Art. 6 I S. 1 lit. f DS-GVO gestützt. Dies gilt auch, wenn eine Einwilligung vorliegt.
Im Übrigen wird auf folgende datenschutzrechtliche Grundlagen der Johann Wolfgang Goethe-Universität verwiesen: - Hessisches Hochschulgesetz iVm. der Hessischen Immatrikulationsverordnung vom 24.02.2010 GVBl. II 70-261 - Satzung zum Schutz personenbezogener Daten in E-Learning-Verfahren an der Johann Wolfgang Goethe-Universität Frankfurt am Main (genehmigt durch Beschluss des Präsidiums am 6. Dezember 2016) - Satzung der Johann Wolfgang Goethe-Universität zum Studienausweis als Chipkarte vom 6. September 2006 (Chipkartensatzung) in der Fassung vom 11. September 2008 - Dienstvereinbarung über die Einrichtung und Anwendung elektronischer Schließsysteme an der Johann Wolfgang Goethe-Universität (DV Schließsysteme) - Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikations-Infrastruktur der Johann Wolfgang Goethe-Universität (Allgemeine IuK-Nutzungsordnung) vom 5. Juni 2001 in der Fassung vom 11. September 2008 - Dienstvereinbarung zu DV-Systemen für Sprachkommunikation vom 28. Oktober 2016 - IT-Sicherheitsordnung der Goethe-Universität Frankfurt am Main, Beschluss des Präsidiums vom 7. Mai 2013 gemäß § 37 XIII Hessisches Hochschulgesetz vom 14. September 2009 in der geltenden Fassung (HHG, GVBl I S. 666ff.)

3. Kategorien personenbezogener Daten

lfd. Nr.		Datum nach Art. 9 I DS-GVO	
		Ja	Nein
1	Ausgewählte Angaben zum Personenstand der Klient*innen: Name, Vorname, Geschlecht, Geburtsdatum und –ort und Staatsangehörigkeit von Klient*innen	☐	☒
2	**Ggf. personenbez. Datum besonderer Kategorie:** Angaben zum Familienstand der Klient*innen nebst Verwandtschaft (insb. Kinder)	☒	☐
3	Kontaktdaten der Klient*innen: Wohn-/Melde-/Postanschrift, Telefonnummer, E-Mailadresse	☐	☒
4	Name, Vorname und Kontaktdaten (Wohn-/Melde-/Postanschrift, Telefonnummer, E-Mailadresse) von Sozialarbeiter*innen bzw. Kontaktpersonen d. Klient*in im Inland	☐	☒
5	Ausländerrechtlicher bzw. Aufenthaltsstatus, Ordnungsmerkmale (Aktenzeichen)	☐	☒
6	Wirtschaftliche Verhältnisse (Vermögen, Einkommen, Verbindlichkeiten) d. Klient*innen und der Angehörigen derselben Bedarfsgemeinschaft	☐	☒
7	**Ggf. personenbez. Datum besonderer Kategorie:** Sprachkenntnisse in Wort und/oder Schrift d. Klient*innen	☒	☐
8	**Ggf. personenbez. Datum besonderer Kategorie:** Zur Prüfung und Beratung überlassene, kopierte bzw. eingescannte Unterlagen (z.B. Reisepass, Behördenbescheide etc.) d. Klient*innen	☒	☐
9	**Ggf. personenbez. Datum besonderer Kategorie:** Korrespondenz mit Klient*innen und Dritten (Behörden, Rechtsanwält*innen, gemeinnützigen Einrichtungen)	☒	☐

10	**Ggf. personenbez. Daten höheren Schutzbedarfs:** Auszüge aus dem Ausländerzentralregister	☒	☐
11	Kontaktdaten der GLC-Angehörigen (Name, Vorname, Matrikelnummer, Uni- und private E-Mail-Adresse/n, Telefonnummer, Wohn-/Postanschrift) sowie deren jeweilige zeitliche Verfügbarkeit	☐	☒
12	Kontaktdaten der Supervisor*innen (Name, Vorname, berufliche E-Mail-Adresse, Telefonnummer, Kanzleianschrift), Fachrichtung/Expertise, supervidierte Fälle, durch studentische Berater*innen bei Supervisor*innen absolvierte Praktika	☐	☒
13	Kontaktdaten der behördlichen Ansprechpartner*innen (Name, Vorname, E-Mail-Adresse, Telefonnummer, Anschrift, ggf. Abteilung bzw. Dezernat)	☐	☒
14	Kontaktdaten der Dolmetscher*innen (Name, Vorname, berufliche E-Mail-Adresse, Telefonnummer, Postanschrift), angebotene Sprache/n	☐	☒
15	IT-Protokolldaten der GLC-Angehörigen (Bearbeitungsprotokoll, Zugriffslogs)	☐	☒

4. Kategorien betroffener Personen

lfd. Nr.	
1	Klient*innen der Goethe-Uni Law Clinic Migration und Teilhabe
2	Angehörige und Mitglieder der Bedarfsgemeinschaft (Personen mit persönlicher oder verwandtschaftlicher Beziehung, auch Lebenspartnerschaften und eheähnliche Verhältnisse, vgl. § 7 III, IIIa SGB II) der unter Ziffer 4 Nr. 1 genannten Klient*innen, soweit deren Daten zur Wahrnehmung der Interessen d. Klient*innen erforderlich sind und ggf. andere fallrelevante Dritte
3	GLC-Angehörige (wiss. Mitarbeiter*innen, stud. Hilfsräfte, stud. Berater*innen)
4	Supervisor*innen (Personen mit Befähigung zum Richteramt; i.d.R. Rechtsanwält*innen)
5	Dolmetscher*innen
6	Sozialarbeiter*innen bzw. andere Kontaktpersonen d. Klient*in im Inland, behördliche Ansprechpartner

5. Kategorien von Empfängern, inkl. Übermittlungen an Empfänger in Drittländern oder internationalen Organisationen

5.1	
lfd. Nr. aus Ziffer 3	Empfänger der Daten
1-11	Supervisor*in: Eine Person mit Befähigung zum Richteramt (i.d.R. Rechtsanwalt/anwältin), die zuvor von der GLC im Einzelfall zur Supervision der stud. Berater*innen zugeordnet wurde. An diese findet grundsätzlich eine Übermittlung zuvor anonymisierter Daten statt, deren Personenbezug unwiderruflich nicht herstellbar ist. Im Einzelfall erfolgt eine Übermittlung (i) pseudonymisierter Sachverhalte, soweit dies zur Rechtsberatung erforderlich ist, (ii) nach vorheriger Einwilligung durch d. Klient*in eine Übermittlung offener personenbezogener Daten d. Klient*in, wenn dies notwendig ist, um insbesondere eine mögliche Übernahme des Mandats durch d. Supervisor*in zu prüfen. Den Supervisor*innen werden im Einzelfall Kontaktdaten der GLC-Angehörigen übermittelt. Eine Auflistung der fallbezogen zugeordneten Supervisor*innen liegt in den Akten im Büro der GLC vor, auf den wiederum nur die wiss. Mitarbeiter*innen und stud. Hilfskräfte Zugriff haben.
1-11	Öffentliche Stellen, insb. Sozial-/Ausländer-/Arbeitsämter bei Einwilligung durch und zur Interessens-wahrnehmung der Klient*innen oder bei Vorliegen vorrangiger Rechtsvorschriften.
1-11	Eine d. Klient*in überweisende Einrichtung (Beratungsstelle), die den Beratungsfall an die GLC weiterverwiesen hat, bei Einwilligung durch und zur Interessenswahrnehmung der Klient*innen oder bei Vorliegen vorrangiger Rechtsvorschriften.

1-11	Dolmetscher*innen, die als Verständigungshilfe durch die GLC zur Beratung hinzugezogen werden.

5.2	
lfd. Nr. aus Ziffer 3	Herkunft der Daten
1-10	Freiwillige Angaben d. Klient*innen bzw. von Klient*innen überlassene Unterlagen
1-10	Angaben von einer d. Klient*in überweisenden Einrichtung oder zuvor mandatierten Anwält*innen, sofern d. Klient*in dort in die Datenweitergabe an die Goethe-Uni Law Clinic eingewilligt hat
1-10	Angaben von öffentlichen Stellen, denen gegenüber die Goethe-Uni Law Clinic die Interessen d. Klient*in wahrnimmt
11	Angaben von GLC-Angehörigen bei Immatrikulation und Beginn der Berater-Ausbildung bzw. bei Unterzeichnung des Arbeitsvertrags
12	Angaben d. Supervisor*innen bei Abschluss der Supervisionsvereinbarung
13	Angaben d. Behörde
14	Angaben d. Dolmetscher*innen bei Aufnahme in die Dolmetscher-Kartei der GLC
15	Erhebung durch HRZ-IT

5.3	Beabsichtigte Datenübermittlung nach Art. 30 I lit. e DS-GVO an Empfänger in Drittländern oder internationalen Organisationen
	Eine Übermittlung an Empfänger in Drittländern oder an internationale Organisationen findet derzeit nicht statt und ist nicht beabsichtigt.

6. Zugriffsberechtigte Personen oder Personengruppen

lfd. Nr. aus Ziffer 3	Personengruppe	Einsichtnahme Personallisten für die entsprechende Personengruppe	Entscheidungsbefugnis über Rechtevergabe
1-14	Wissenschaftliche Mitarbeiter*innen (unbeschränkter Zugriff auf sämtliche von der GLC verarbeiteten personenbezogenen Daten) am Lehrstuhl für Öffentliches Recht mit Schwerpunkt Sozialrecht am Institut für öffentliches Recht der Johann Wolfgang Goethe-Universität Frankfurt	In der Personalabteilung der Universität bzw. beim DV-Referat des Fachbereichs 01.	Projektleitung (Inhaber*in des Lehrstuhls für Öffentliches Recht mit Schwerpunkt Sozialrecht am Institut für Öffentliches Recht der Johann Wolfgang Goethe-Universität Frankfurt) mit Beginn und für die Dauer des Arbeitsvertrages
1-14	stud. Hilfskräfte (unbeschränkter Zugriff) der Goethe-Uni Law Clinic		wiss. Mitarbeiter*innen der Goethe-Uni Law Clinic mit Beginn und für die Dauer des Arbeitsvertrages
1-10	Das Team aus (zwei) stud. Berater*innen der GLC, das die Beratung im Einzelfall übernommen bzw. zugewiesen bekommen hat (lediglich Zugriff auf Einzelfall-bezogenen PowerFolder nach vorheriger Freigabe)	Elektronisch auf dem Server bzw. in den Akten im Büro der Goethe-Uni Law Clinic.	wiss. Mitarbeiter*innen der GLC im Verlaufe des 2. Ausbildungssemesters, wenn die erforderliche Ausbildungsreife erreicht und die Verpflichtungserklärung unterzeichnet ist, bis zum Ausscheiden aus der GLC

11-14	Alle stud. Berater*innen der Goethe-Uni Law Clinic	Elektronisch auf dem Server bzw. in den Akten im Büro der Goethe-Uni Law Clinic.	wiss. Mitarbeiter*innen der GLC mit Beginn der GLC-Ausbildung und Unterzeichnung der daten-schutzrechtlichen Vereinbarungen bis zum Ausscheiden aus der GLC
15	Mitarbeiter*innen des HRZ der GU und im Einzelfall (zur Überprüfung eventueller Verstöße) wiss. Mitarbeiter*innen der GLC	In der Personalabteilung der Universität bzw. beim DV-Referat des FB 01.	HRZ der GU bzw. Projektleitung (s.o.) mit Beginn und für die Dauer des Arbeitsvertrages

7. Technische und organisatorische Maßnahmen (Art. 32 DS-GVO)

[Unter *E.VII.2* findet sich eine umfangreiche Anleitung zur Erstellung der technischen und organisatorischen Maßnahmen (TOM)]

Folgende aufeinander aufbauende Maßnahmen wurden getroffen:

☒ Hinsichtlich der allgemeinen Sicherheitsmaßnahmen wird auf das vorhandene Sicherheitskonzept der Uni Frankfurt, insb. auf Ziffer 3 der am 25.02.2017 in Kraft getretenen „IT-Sicherheitsrichtlinie für die Goethe-Universität Frankfurt“, Version 1.0.12, verwiesen.

☒ Erläuterungen zu den einzelnen Maßnahmen, insbesondere soweit diese das vorliegende Verfahren betreffen:

1. Schutzziel „Vertraulichkeit“

Zutrittskontrolle

- Gesicherter Eingang. Pfortendienst des RuW-Gebäudes, außerhalb der Arbeitszeiten Objektschutz.
- Besucher- und Schlüsselregelung: kein eigenständiger Zutritt zu GLC-Räumen und –Technik durch stud. Berater*innen oder Dritte (jeweils Zutrittsgewährung durch wissenschaftliche Mitarbeiter*innen).
- Abschließen der Räume mit Sicherheitsschlössern bzw. Codekarten inkl. Gastkarte.

Zugangs- und Zugriffskontrolle

- Virenschutz, Firewall und weitere IT-Sicherheitsmaßnahmen wie in der o.g. IT-Sicherheitsrichtlini beschrieben.
- Postfächer und Powerfolder des Hochschulrechenzentrums (im Folgenden „HRZ“) per HRZ-Kennung gesichert.
- Passwortrichtlinie: Passworte mit min. 8 Zeichen (A-Z; a-z; 0-9 + Sonderzeichen), kein Teil aus dem Login oder Namen.
- GLC-Mitarbeiter*innen sind angewiesen, das jeweils verwendete IT-System beim Verlassen zu sperren.
- Stud. Berater*innen wird nur Zugriff zu Dateien eingeräumt, die ihre Beratungsfälle betreffen. Verantwortliche/r Besitzer*in/Administrator*in von Webmail und Powerfolder ist eine*r der beiden wiss. Mitarbeiter*innen gem. Ziff. 6.1. Wiss. Mitarbeiter*innen gem. Ziff. 6.1 können jeweils stud. Hilfskräften gem. Ziff. 6.2 Zugriff einräumen, diesen beschränken und löschen. Mitarbeiter*innen gem. Ziff. 6.1 und Hilfskräfte gem. Ziff. 6.2 können jeweils einzeln stud. Berater*innen gem. Ziff. 6.3 Zugriff einräumen, diesen beschränken und löschen.
  - Enge (fallbezogene) Begrenzung und Protokollierung der befugten Benutzer sowie etwaiger Missbrauchsversuche, Zugrifflogdateien. Die Aufbewahrung und Löschung der Protokolldaten erfolgt nach den allgemeinen datenschutzrechtlichen Löschregeln des DV-Referats im FB 01 und des Hochschulrechenzentrums der Goethe-Universität.
  - Zugriff auf Protokolle nur für wissenschaftliche Mitarbeiter*innen und HRZ-IT-Administratoren.
  - Aufbewahrung des GLC-Notebooks in abgeschlossenem Schrank.
  - Über den Zugriff auf den USB-Stick, der den jeweiligen stud. Hilfskräften/Berater*innen nur für die Dauer der Sprechstunde bzw. Fallbearbeitung gewährt wird und nach Arbeitsende stets zurückzugeben ist, entscheidet im Einzelfall ein*e wissenschaftliche*r Mitarbeiter*in, die den Stick an seinem*ihrem Schlüsselbund bzw. im verschlossenen Schreibtisch im verschlossenen Büro verwahrt.
  - Kein Zugriff der GLC-Mitarbeiter*innen auf Betriebssystemebene.

Trennungskontrolle

- Personenbezogene Daten von Mitarbeiter*innen werden von personenbezogenen Daten der Klient*innen getrennt (in separatem Ordner unter Verschluss im GLC-Büro bzw. elektronisch auf den Uni-Servern mit Zugriff nur für die wiss. Mitarbeiter*innen) verarbeitet.
- Es existieren separate Ordnerstrukturen pro Beratungsfall. Stud. Berater*innen wird nur Zugriff zu Dateien eingeräumt, die ihre Beratungsfälle betreffen.
- Auf dem GLC-Notebook, der reinen Recherchezwecken während der Beratungen dient, werden keine personenbezogenen Daten der Klient*innen gespeichert.

Pseudonymisierung und Verschlüsselung

- Softwareseitige Verschlüsselung des USB-Sticks (Dateien oder Dateisystem).
- Übermittlung lediglich anonymisierter „Case Studies“ an Supervisor*innen. Sämtliche Mitarbeiter der GLC werden vor Tätigkeitsbeginn hinsichtlich entsprechender Methoden (etwa Löschung direkter Merkmale, Datenaggregation, Gruppenbildung) gesondert geschult. Im Einzelfall und nach vorheriger Einwillligung durch Klient*in Übermittlung pseudonymisierter Sachverhalte, soweit zur Rechtsberatung erforderlich.

2. Schutzziel „Integrität“

Eingabe- und Weitergabekontrolle

- Protokollierung der eingebenden Person und des wesentlichen Inhalts durch Bearbeitungsprotokolle und interne Falllisten (Zugriff nur für Wiss. Mitarbeiter*innen).
- Löschkonzept und Sicherstellung der Rückgabe aller im Besitz der stud. Hilfskräften/Berater*innen befindlichen Dokumente.
- Zur Weitergabe s. zunächst unter 1. Schutzziel „Vertraulichkeit“. Beschränkung der Weitergabe nach dem Erforderlichkeitsgrundsatz. Kein Versand personenbezogener Klardaten via E-Mail; Einsatz von Verschlüsselungsmechanismen (z.B. verschlüsselte und passwortgeschützte PDF-Dokumente und Mitteilung des Passworts möglichst auf einem zweiten Kommunikationskanal).

3. Schutzziel „Verfügbarkeit und Belastbarkeit“

- Vgl. Maßnahmenkatalog der o.g. IT-Sicherheitsrichtlinie. Feuer- und Rauchmeldeanlagen.
- Regelmäßige Datensicherungen des USB-Sticks.

4. Schutzziel „Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung“

Behördlicher Datenschutzbeauftragter ist bestellt. Die GLC benennt eine*n ständige*n interne*n Datenschutzkoordinator*in (s. Angaben unter Ziffer 1.1).

- Sämtliche GLC-Angehörige nehmen an Schulungsmaßnahmen vor Tätigkeitsbeginn via eLearning teil (inkl. Online-Kurs des HRZ zu „Grundlagen der IT-Sicherheit“). Leitlinien und Prozessbeschreibungen bei Tätigkeitsbeginn/-ende (*On-/Offboarding Procedures*) werden entworfen.
- Sämtliche GLC-Angehörige werden vor Tätigkeitsbeginn über datenschutzrechtliche Grundsätze (Art. 5 DS-GVO) und entsprechende Sanktionen in dokumentierter Weise belehrt (Verpflichtung auf Vertraulichkeit). Weitere Rechte und Pflichten der Nutzer in § 6 Allgemeiner IuK-Nutzungsordnung.
- Betroffenenanfragen werden in Zusammenarbeit mit dem behördlichen Datenschutzbeauftragten beantwortet.
- Eine Datenschutz-Folgenabschätzung wird nach derzeitiger Einschätzung für nicht erforderlich gehalten; das Ergebnis der Risikoevaluierung ist in Ziffer 10 enthalten.
- Datenschutzvorfälle werden von GLC-Angehörigen unverzüglich an die interne Datenschutzkoordinatorin gemeldet, die das weitere Vorgehen mit dem behördlichen Datenschutzbeauftragten abstimmt.

8. Technik der Verarbeitung

8.1

☐ **Einzelplatzrechner / Arbeitsplatzrechner / stand alone PC**

Betriebssystem:

☐ Unix ☐ Windows NT ☐ Windows ☐ anderes

weiter mit Ziff. 8.3

8.2

☒ **Vernetzte Rechner**

vgl. dazu insb. die Angaben des Hochschulrechenzentrums sowie das am 25.02.2017 in Kraft getretene Sicherheitskonzept der Uni Frankfurt.

8.2.1 **Hardware**

☐ Großrechner

Betriebssystem: (z. B. UNIX / OS)

Datenendgerät: ☐ Terminal / Netz-PC (ohne Laufwerk/Festplatte)

☐ PC (Arbeitsplatzrechner / Workstation)

☐ Server

Betriebssystem: (z. B. Windows NT)

Datenendgerät: ☐ Terminal / Netz-PC (ohne Laufwerk/Festplatte)

☐ PC (Arbeitsplatzrechner / Workstation)

☐ Sonstige eingesetzte Hardware (z. B. Chipkarte, Kartenlesegeräte, Videogeräte)

8.2.2 **Netzstruktur**

☒ Netz innerhalb der Behörde (Intranet)

☒ Lan ☒ Intranet ☐ sonstiges

☐ Netz über externe Leitungen innerhalb eines geschlossenen Benutzerkreises

(z. B. KIV, KGRZ, Hessische Landesverwaltung)

☐ KIV/KGRZ ☐ Netz der Landesverwaltung (HCN 2000) ☐ sonstiges

☒ Offene Netze (z. B. Internet)

8.2.3	**Datenspeicherung auf:**	**Art der Daten (lfd. Nr. aus Ziffer 3):**
☐	Großrechner	
☒	Server innerhalb der Behörde	Sämtliche vorgenannte Kategorien.
☐	Server bei anderen Institutionen	
☒	PC / Arbeitsplatzrechner	Universitärer Arbeitsplatzrechner (Windows 7) der wiss. Mitarbeiter*innen gem. Ziff. 6.1; vom DV-Referat des Fachbereichs zur Verfügung gestelltes Notebook der Goethe-Uni Law Clinic; ein GLC-interner USB-Stick

8.3 **Eingesetzte Software** (einschl. Standardverfahren)

Webmail/Horde (HRZ)

DLIST-Server/Mailman (HRZ)

PowerFolder (HRZ)

9. Löschung personenbezogener Daten

Sämtliche Daten (lfd. Nr. 1-15 aus Ziffer 3) werden grundsätzlich nach Durchführung des Vertrages, Wegfall des Zweckes bzw. Ablauf der gesetzlichen Aufbewahrungsfristen gelöscht. Erfolgt die Verarbeitung auf Grundlage einer Einwilligung werden die personenbezogenen Daten nach Widerruf der Einwilligung gelöscht. Zur sachgemäßen Verteidigung etwaiger Haftungsansprüche aus den geschlossenen Vereinbarungen mit den Klient*innen, den GLC-Angehörigen, Supervisor*innen, Dolmetscher*innen, behördlichen Ansprechpartnern und den Sozialarbeiter*innen/anderen Kontaktpersonen d. Klient*in im Inland werden – im begründeten Einzelfall – aber sämtliche zur Beweisführung erforderlichen Daten bis zu 10 Jahre aufbewahrt. In Anlehnung an die kenntnisunabhängige Verjährungshöchstfrist (§§ 195, 199 III S. 1 Nr. 1 BGB) beginnt die Frist in S. 2 ohne Rücksicht auf die Kenntnis oder grob fahrlässige Unkenntnis d. betroffenen Person in dem Zeitpunkt, zu dem der Beratungsfall zum Abschluss gebracht bzw. das Engagement bei der GLC beendet wurde oder sonst der letzte Kontakt der betroffenen Person mit der GLC bestand.

Für Daten, die indirekt (insb. über fallrelevante Dritte) erhoben wurden, gelten Satz 2 und 3 mit der Maßgabe, dass die Frist des Satz 2 im Zeitpunkt der Erhebung der Daten beginnt.

Ausnahme: Zu Forschungs- und Lehrzwecken (sog. *„case studies“*) dürfen die Daten gem. § 24 I S. 1, III HDSIG in anonymisierter Form (ohne dass auf d. betreffende*n Klient*in geschlossen werden kann) auch über die Löschungsfrist hinaus gespeichert oder übermittelt werden.

Die Erforderlichkeit der Datenbestände wird jeweils am kalendarischen Jahresende überprüft.

10. Begründetes Ergebnis der Risikoevaluierung und Eintrittswahrscheinlichkeit i.S.v. Art. 35 I DS-GVO

Aus Sicht der maßgeblichen Vorschriften der DS-GVO und des HDSIG (vgl. § 1 I, V, IX HDSIG) wird die Durchführung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO für die vorbeschriebenen Verarbeitungstätigkeiten derzeit als nicht zwingend erachtet.

Die Notwendigkeit einer Datenschutz-Folgenabschätzung für die personenbezogenen Daten d. Klient*in folgt nicht bereits aus Art. 35 III lit. b SGVO, da die Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 DS-GVO unter Berücksichtigung von Erwägungsgrund 91 der DS-GVO nicht als „umfangreich“ anzusehen ist. Die Erhebung der von den Art. 9 DS-GVO erfassten Daten wird zunächst in Umfang und Detailgrad auf das zur Rechtsberatung notwendige Mindestmaß begrenzt; es werden insbesondere keine ganzheitlichen Profile der Person erstellt. Zudem wird der Kreis der zugriffsberechtigten Personen möglichst klein gehalten, sodass die vorliegende Verarbeitungssituation der GLC unter Supervision d. Datenschutzkoordinator*in gemäß § 6 II 2 RDG einer Verarbeitung durch eine/n Einzelanwalt/anwältin nebst einzelner zuarbeitender Praktikant*innen und Sekretär*innen nahekommt. Externe Supervisor*innen erhalten grundsätzlich lediglich anonymisierte Daten, von denen *per se* kein Risiko für die Rechte und Freiheiten der Klient*innen ausgeht. Für die Annahme einer nicht „umfangreichen“ Verarbeitung streitet Nr. 1 der Liste von Verarbeitungsvorgängen nach Art. 35 IV DS-GVO (Stand Juni 2018) des Hessischen Beauftragten für Datenschutz und Informationsfreiheit, der eine „umfangreiche“ Verarbeitung von Daten typischerweise erst bei „[g]*roße*[n] *Anwaltssozietät*[en]“ gegeben sieht und als konkretes Beispiel anführt: *„Ein Unternehmen bietet ein umfassendes Verzeichnis über Privatinsolvenzen an.*“ Ein solcher Umfang ist mit der vorbeschriebenen Verarbeitungstätigkeit nicht gegeben.

Die Notwendigkeit einer Datenschutz-Folgenabschätzung resultiert auch nicht aus dem (allgemeineren) Art. 35 I DS-GVO, da aus der vorliegenden Verarbeitungsaktivität kein „hohes“ Risiko für die Rechte und Freiheiten der betroffenen Personen erwächst. Hinsichtlich personenbezogener Daten d. Klient*in oder betroffener Dritter ist zwar die z.B. nach dem Modell des BayLDA bestimmte Schadensschwere, die durch eine Verletzung des Schutzes der vorliegend verarbeiteten Daten potentiell entstehen kann, als ‚wesentlich‘ einzuordnen. Dies folgt insb. aus dem höheren Schutzbedarf der verarbeiteten personenbezogenen Daten besonderer Kategorien (Art. 9 DS-GVO, etwa Gesundheitsdaten oder Daten zur rassischen und ethnischen Herkunft).

Ausschlaggebend ist jedoch, dass die jedenfalls nach dem Modell des BayLDA bestimmte Eintrittswahrscheinlichkeit des mit dieser Verarbeitung verbundenen Risikos als ‚begrenzt‘ einzustufen ist. Dies folgt aus der vorstehenden Begründungen zum begrenzten Umfang der Verarbeitung von Daten i.S.d. Art. 9 DS-GVO sowie daraus, dass:

- ausschließlich bereits als datenschutzrechtlich zulässig befundene und kontinuierlich gewartete IT-Infrastruktur der Goethe-Universität Frankfurt unter Aufsicht durch den behördlichen Datenschutzbeauftragten benutzt wird und insbesondere keine Auftragsdatenverarbeitung oder ein Drittstaatentransfer stattfindet oder beabsichtigt ist,

- einbezogene Supervisor*innen i.d.R. gegenwärtig zugelassene Rechtsanwält*innen sind, die straf- und standesrechtlichen Verschwiegenheitspflichten unterliegen und grundsätzlich lediglich anonymisierte Daten erhalten,
- zuarbeitende studentische Hilfskräfte und Berater*innen zur Verschwiegenheit (auch nach-)vertraglich verpflichtet und über datenschutzrechtliche Grundsätze belehrt wurden (sog. Verpflichtung zur Vertraulichkeit zur Erfüllung von Art. 5 I lit. f DS-GVO) und – zur Einschränkung des potenziell auf die Daten zugreifenden Personenkreises – jeweils einzeln für einen entsprechenden Fall per Benutzerzugriffskontrolle freigeschaltet werden,
- auch Dolmetscher*innen nach datenschutzrechtlichen Grundsätzen belehrt werden (sog. Verpflichtung zur Vertraulichkeit zur Erfüllung von Art. 5 lit. f DS-GVO) und sich zur Verschwiegenheit verpflichten,
- datenschutzrelevante Fragen oder Unklarheiten bei gemeinsamen Treffen angesprochen und geklärt werden, wodurch gleichzeitig das Bewusstsein der GLC-Angehörigen für den Datenschutz geschärft wird,
- zuarbeitende studentische Hilfskräfte und Berater*innen im Hinblick auf die diese treffenden Datenschutzpflichten stichprobenartig überwacht und auf etwaige Verstöße hingewiesen sowie bei wiederholten Verstößen sanktioniert werden,
- die Daten physisch und technisch nicht außerhalb des Uni-Rechenzentrums verarbeitet werden, da auf dem vom DV-Referat des Fachbereichs zur Verfügung gestellten und regelmäßig gewarteten Notebook der GLC keine personenbezogenen Daten der Klient*innen verarbeitet werden,
- sich bei der Datenerhebung, -verarbeitung und -nutzung strikt an die Grundsätze der Erforderlichkeit und Datenminimierung gehalten wird, worauf die zuarbeitenden studentischen Hilfskräfte und Berater*innen belehrt und verpflichtet werden,
- die verarbeiteten personenbezogenen Daten besonderer Kategorien (u.a. Sprachkenntnisse, Daten aus Ausweisdokumenten oder behördlicher Korrespondenz) im Regelfall bloße Indizien für die Annahme solcher Daten bilden und nur im Einzelfall sicheren Aufschluss etwa über die tatsächliche rassische und ethnische Herkunft oder religiöse Überzeugungen zulassen,
- die vorliegenden Verarbeitungsaktivitäten neben den beschriebenen Ausbildungszwecken für den konkreten Verarbeitungsvorgang im vordergründigen Interesse d. Klient*innen liegen, deren konkrete, erforderliche, schriftliche, informierte und freiwillige Einwilligungserklärung vorab eingeholt wird, der Katalog der technisch-organisatorischen Maßnahmen gemäß Art. 32 DS-GVO stets überwacht und dem Stand der Technik entsprechend angepasst wird,

sodass schließlich das Produkt aus Schadensschwere und Eintrittswahrscheinlichkeit zu einem Risiko für die Rechte und Freiheiten der Klient*innen führt, das jedoch kein „hohes" Risiko gemäß Art. 35 I DS-GVO darstellt und eine Datenschutz-Folgenabschätzung daher jedenfalls nicht zwingend durchzuführen ist.

Ggf. Rat des behördlichen Datenschutzbeauftragten gemäß Art. 35 II DS-GVO:

11. Ergänzungen

Für die Richtigkeit:

Ort, Datum	Ort, Datum
- Maximiliane Musterfrau –	- Maximilian Mustermann –
Wiss. Mitarbeiterin & Supervisorin	Wiss. Mitarbeiter

2. Anleitung zur Erarbeitung technischer und organisatorischer Maßnahmen (TOM, Art. 32 DS-GVO)

Hinweis zu dieser Anleitung

Die folgende Anleitung orientiert sich an der Anlage zu § 9 BDSG a.F. Diese Anlage findet sich mittlerweile sogar teilweise im Normtext des Art. 32-DS-GVO. Die nachfolgenden Erläuterungen passen daher auch auf Art. 32-DS-GVO.

Zunächst werden zur Systematisierung abstrakt mögliche Maßnahmen beschrieben und im Anschluss die konkreten Beispiele aufgezählt. Die konkreten Beispiele im hinteren Teil sind aufgegliedert nach den verschiedenen Schutzzielen, die die IT-Sicherheit kennt.

Es empfiehlt sich, die TOM in das Verarbeitungsverzeichnis aufzunehmen (siehe Nr. 7 der Vorlage zum Verarbeitungsverzeichnis), um unnötige Doppelungen zu vermeiden und die TOM gleich den verschiedenen Verarbeitungsprozessen zuzuordnen. So wird auch nichts übersehen.

1. Zutrittskontrolle

Es ist hierbei der physische Zutritt von Personen zu beachten. Es sollen nur Befugte Zutritt zu den Räumen haben, in denen die Datenverarbeitung stattfindet. Dieser Punkt hat beim Einsatz von IT-Dienstleistern für die RLC keinen großen Anwendungsbereich, da der Dienstleister im Wesentlichen für diese Maßnahmen verantwortlich ist. Entsprechende Pflichten ergeben sich aus der Vereinbarung einer Auftragsverarbeitung (Art. 28 Abs. 3 S. 2 lit. c DS-GVO). Im Rahmen der Auftragsverarbeitung muss auch der Auftragsverarbeiter kontrolliert werden! Dieser stellt jedoch regelmäßig entsprechende Audits und Übersichten zu diesem Thema bereit, die dokumentiert werden sollten.

2. Zugangskontrolle

Die Zugangskontrolle betrifft nicht den räumlichen Zugang (s.o.), sondern die Benutzung der Datenverarbeitungssysteme.

Mögliche Maßnahmen:

- Regelmäßige Überprüfung der Zugangsberechtigung, unbedingt sinnvoll nach dem Austritt von Mitgliedern
- Technische Maßnahmen zur Kontrolle des Zugangs können etwa Passwörter oder - bei analogen Daten - Schlüssel sein
- Verschlüsselung der Kommunikation (Verschlüsselung der Webseite (SSL/TLS) oder der Mails (PGP)) nach dem Stand der Technik

3. Zugriffskontrolle

Die Zugriffskontrolle befasst sich mit der Frage, wer auf welche personenbezogenen Daten Zugriff haben darf. Unberechtigte Mitglieder oder Dritte dürfen keinen Zugriff erlagen.

Mögliche Maßnahmen:

- Erstellung eines Rollen- und Maßnahmekonzepts für die Mitglieder des Vereins und sonstigen möglichen Zugriffsberechtigten. Zum Beispiel dürfen die Fallakten – neben den Administratoren – nur den jeweiligen Beratern und deren Supervisoren zugänglich sein. Anderes Beispiel: Verschiedene Mitglieder des Organisationsteams haben jeweils nur Zugriff auf die personenbezogenen Daten in ihrem Bereich. Sind personenbezogene Daten z.B. wegen Aufbewahrungsfristen gesperrt, ist sicherzustellen, dass grundsätzlich niemand mehr Zugriff auf die Daten aus Gründen bekommt, die nicht zum Zweck der Sperrung passen.

Denkbar sind hier verschiedene Benutzerkonten mit begrenzten Berechtigungen oder Zugriffsprotokollierung. Die Maßnahmen sollten regelmäßig überprüft werden.

Wie genau die Zugriffskontrolle ermöglicht werden kann, richtet sich nach der technischen Infrastruktur der jeweiligen RLC.

4. Weitergabekontrolle

Die Weitergabekontrolle soll sicherstellen, dass personenbezogene Daten nicht bei der Übermittlung oder beim Transport abhandenkommen.

Mögliche Maßnahmen:

- Verschlüsselung der Daten und der digitalen Daten bei der Übermittlung oder dem Transport
- Erforderlichenfalls eine Überprüfung einer Person im Einzelfall daraufhin, dass sie tatsächlich die Daten erhalten darf (Identität/Berechtigung)

5. Eingabekontrolle

Die Eingabekontrolle soll eine Überprüfbarkeit herstellen, von wem und wieso welche Daten eingegeben wurden.

Mögliche Maßnahmen:

- Protokollierung der Zugriffe
- Auch die oben angeführte Beschränkung des Zugriffs lässt Rückschlüsse zu, wer welche Daten eingegeben hat.

6. Auftragskontrolle

Sie soll sicherstellen, dass personenbezogene Daten nur nach Weisung des Verantwortlichen erfolgen.

Mögliche Maßnahmen:

- Verbindliche Festlegung von Arbeitsabläufen und - soweit möglich - Kontrollen.
- Auch hier kann eine sinnvolle Zugriffsberechtigung viel bewirken. So können Vorgaben der Verarbeitung technisch festgelegt werden.
- Große IT-Dienstleister, die regelmäßig Auftragnehmer im Rahmen einer Auftragsverarbeitung sind, stellen hierzu vielfach Prüfergebnisse von Audits bereit, die die Einhaltung der Vorgaben bestätigen. Diese sollten sicherheitshalber dokumentiert werden!

7. Verfügbarkeitskontrolle

Hierdurch soll die Verfügbarkeit der Daten sichergestellt werden. Daten soll nicht durch Zufall oder Absicht gelöscht werden bzw. müssen wiederhergestellt werden können. Die genaue Realisierung hängt von den technischen Gegebenheiten bei der jeweiligen RLC ab. Auch hier kann es sein, dass ein

technischer Dienstleister die wesentlichen Aufgaben bereits im Rahmen einer Auftragsverarbeitung übernimmt.

Mögliche Maßnahmen:

- Sicherheitsvorkehrungen am PC: Malwareschutz, Verschlüsselung etc.
- Datensicherungsmaßnahmen (z.B. Versionierung, gespiegelte Datenträger, regelmäßige und sinnvollerweise auch automatische Backups)
- Festlegung von Aufbewahrungsfristen

8. Trennung der Verarbeitung bei verschiedenen Zwecken

Punkt 8 betrifft eine Selbstverständlichkeit. So soll durch eine logisch getrennte Speicherung der jeweiligen Daten der Zweck der verarbeiteten Daten ersichtlich bleiben, weil hiervon einiges abhängt. Ein großer Anwendungsbereich ergibt sich bei einer RLC dennoch wohl nicht.

Mögliche Maßnahmen:

- Getrennte Speicherung (natürlich nicht zwingend technisch auf verschiedenen Datenträgern) von Daten mit verschiedenen Zweckrichtungen
- Hierzu zwingt aber bereits ein sinnvolles Berechtigungskonzept

VIII. *Anhang 8: Vertraulichkeitsverpflichtung RLC-Angehörige & Supervisor*innen/Beirät*innen*

1. Vertraulichkeitsverpflichtung

Vertraulichkeitsverpflichtung für RLC-Angehörige & Supervisor*innen/Beirät*innen

zur Erfüllung von Art. 5 Abs. 1 lit. f der Datenschutz-Grundverordnung[33] („**DS-GVO**“) und zur Einhaltung weiterer Vorschriften zur Wahrung des Sozialgeheimnisses[34]

Für die Verarbeitung Verantwortliche*r:

XY-Universität, XY Law Clinic (im Folgenden „**Verantwortlicher**“)
Postanschrift

XY-LC-Angehörige*r bzw. Supervisor*in (im Folgenden „**Verpflichtete*r**“):

_____

Name der/s Verpflichteten

Position: ☐ wiss. Mitarbeiter*in ☐ stud. Hilfskraft ☐ studentische*r Berater*in ☐ Supervisor*in/Beirät*in

1. Verpflichtung

a) … auf die Vertraulichkeit

Die einschlägigen gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Daher ist es Ihnen als Verpflichteter*m nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der Ihnen übertragenen Aufgaben erforderlich ist. Dabei ist es grundsätzlich unerheblich, ob diese Daten „digital“ (in IT-Systemen) oder „analog“ (Akten der Ratsuchenden des Verantwortlichen, behördliche Korrespondenz, Ausweisdokumente, Mitschriften, Kopien etc.) verarbeitet werden.

Ihre Verpflichtung besteht umfassend. Nach den einschlägigen gesetzlichen Vorschriften ist es untersagt, personenbezogene Daten unbefugt oder unrechtmäßig zu verarbeiten oder absichtlich oder unabsichtlich die Sicherheit der Verarbeitung in einer Weise zu verletzen, die zur Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung oder zu unbefugtem Zugang führt. Dies gilt für Ihre Tätigkeit innerhalb und außerhalb des Verantwortlichen, z.B. gegenüber Ratsuchenden und Interessierten. Die Pflicht zur Wahrung der Vertraulichkeit bleibt auch im Falle einer Änderung oder Beendigung des Beschäftigungsverhältnisses (wiss. Mitarbeiter*innen und stud. Hilfskräfte) oder des Engagements für den Verantwortlichen (stud. Berater*innen und Supervisor*innen) ohne zeitliche Begrenzung bestehen.

b) … zur Wahrung des Sozialgeheimnisses

Ihre Tätigkeit bei dem Verantwortlichen berührt das Sozialgeheimnis (§§ 35 SGB I, 67, 78 SGB X). Sofern Daten verarbeitet werden, die dem Sozialgeheimnis unterliegen, haben Sie diese im gleichen Umfang geheim zu halten, wie die ursprünglich übermittelnde Stelle. Insbesondere dürfen Sie Sozialdaten Dritter nicht an Unbefugte preisgeben.

2. Rechtsfolgen bei Verstößen

Verstöße gegen die Datenschutzvorschriften bzw. die Vorschriften zum Sozialgeheimnis können nach den gesetzlichen Vorschriften ggf. mit Geldbuße, Geld- oder Freiheitsstrafe geahndet werden (§§ 41 BDSG iVm. 14 OWiG, 85 SGB X iVm. 42 BDSG). Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt zudem einen Verstoß gegen die Pflichten aus Ihrem Beschäftigungsverhältnis bzw. aus Ihrer Verpflichtungs- oder Supervisionsvereinbarung dar, der entsprechend geahndet werden kann. Entsteht der von der Datenverarbeitung betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden, kann ein Schadenersatzanspruch entstehen. Datenschutzverstöße Ihrerseits sind außerdem mit möglicherweise sehr hohen Bußgeldern für den Verantwortlichen bedroht (Art. 83 DS-GVO), die gegebenenfalls zu Ersatzansprüchen Ihnen gegenüber führen können.

3. Unterrichtung über die vorgenannten Verpflichtungen

Über diese Verpflichtungen und die zu ihrer Erfüllung erforderlichen Verhaltensweisen wurde ich als Verpflichtete*r unterrichtet Ich bin mir über die bei einem Verstoß drohenden Sanktionen bewusst.

_____
Ort, Datum

_____ _____
Unterschrift der/s Verpflichteten Unterschrift der/s Verantwortlichen

[33] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.
[34] Ein Abdruck relevanter Vorschriften ist als *„Anlage zur Verpflichtung auf die Vertraulichkeit“* beigefügt.

2. Anlage zur Verpflichtung auf die Vertraulichkeit

Anlage zur Vertraulichkeitsverpflichtung (für RLC-Angehörige & Supervisor*innen/Beirät*innen)

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim **behördlichen/Vereins-Datenschutzbeauftragten**:

N.N.
Postanschrift

Vorschriften zur Vertraulichkeitsverpflichtung

Art. 4 DS-GVO – Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck:

3. „**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;
4. „**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;[…]

Art. 5 DS-GVO - Grundsätze für die Verarbeitung personenbezogener Daten
(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden ("**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**");
b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken ("**Zweckbindung**");
c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein ("**Datenminimierung**");
d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden ("**Richtigkeit**");
e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden ("**Speicherbegrenzung**");
f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen ("**Integrität und Vertraulichkeit**").

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

Art. 29 DS-GVO – Verarbeitung unter der Aufsicht des Verantwortlichen […]
Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Vorschriften zur Wahrung des Sozialgeheimnisses

§ 67 SGB X – Begriffsbestimmungen
(1) […]
(2) **Sozialdaten** sind personenbezogene Daten (Artikel 4 Nummer 1 der Verordnung (EU) 2016/679), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden. Betriebs- und Geschäftsgeheimnisse sind alle betriebs- oder geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben.

(3)-(5) […]

§ 35 SGB I – Sozialgeheimnis

(1) Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Absatz 2 Zehntes Buch) von den Leistungsträgern nicht unbefugt verarbeitet werden (**Sozialgeheimnis**). Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. […]

(2) […]

(2a) Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(3) […]

(4) Betriebs- und Geschäftsgeheimnisse stehen Sozialdaten gleich.

(5)-(7)[…]

§ 78 SGB X – Zweckbindung und Geheimhaltungspflicht eines Dritten, an den Daten übermittelt werden

(1) Personen oder Stellen, die nicht in § 35 des Ersten Buches genannt und denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, zu dem sie ihnen befugt übermittelt worden sind. Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. Die **Dritten** haben die Daten in demselben Umfang geheim zu halten wie die in § 35 des Ersten Buches genannten Stellen. […]

(2) Werden Daten an eine nicht-öffentliche Stelle übermittelt, so sind die dort beschäftigten Personen, welche diese Daten speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, von dieser Stelle vor, spätestens bei der Übermittlung auf die Einhaltung der Pflichten nach Absatz 1 hinzuweisen.

(3)-(4) […]

<u>Vorschriften zu Sanktionen bei Verstößen</u>

Art. 83 DS-GVO – Allgemeine Bedingungen für die Verhängung von Geldbußen

(1) Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung gemäß den Absätzen 4, 5 und 6 in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

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

a) Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Zahl der von der Verarbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;

b) Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;

c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;

d) Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

e) etwaige einschlägige frühere Verstöße des Verantwortlichen oder des Auftragsverarbeiters;

f) Umfang der Zusammenarbeit mit der Aufsichtsbehörde, um dem Verstoß abzuhelfen und seine möglichen nachteiligen Auswirkungen zu mindern;

g) Kategorien personenbezogener Daten, die von dem Verstoß betroffen sind;

h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;

i) Einhaltung der nach Artikel 58 Absatz 2 früher gegen den für den betreffenden Verantwortlichen oder Auftragsverarbeiter in Bezug auf denselben Gegenstand angeordneten Maßnahmen, wenn solche Maßnahmen angeordnet wurden;

j) Einhaltung von genehmigten Verhaltensregeln nach Artikel 40 oder genehmigten Zertifizierungsverfahren nach Artikel 42 und

k) jegliche anderen erschwerenden oder mildernden Umstände im jeweiligen Fall, wie unmittelbar oder mittelbar durch den Verstoß erlangte finanzielle Vorteile oder vermiedene Verluste.

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

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

a) die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

b) die Pflichten der Zertifizierungsstelle gemäß den Artikeln 42 und 43;

c) die Pflichten der Überwachungsstelle gemäß Artikel 41 Absatz 4.

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

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

(6) – (9) […]

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

(1) Für Verstöße nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 679/2016 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten sinngemäß. Die §§ 17, 35 und 36 des Gesetzes über Ordnungswidrigkeiten finden keine Anwendung.

(2) Für Verfahren wegen eines Verstoßes nach Artikel 83 Absatz 4 bis 6 der Verordnung (EU) 679/2016 gelten, soweit dieses Gesetz nichts anderes bestimmt, die Vorschriften des Gesetzes über Ordnungswidrigkeiten und der allgemeinen Gesetze über das Strafverfahren, namentlich der Strafprozessordnung und des Gerichtsverfassungsgesetzes, entsprechend. […]

§ 14 OWiG – Beteiligung

(1) Beteiligen sich mehrere an einer Ordnungswidrigkeit, so handelt jeder von ihnen ordnungswidrig. Dies gilt auch dann, wenn besondere persönliche Merkmale (§ 9 Abs. 1), welche die Möglichkeit der Ahndung begründen, nur bei einem Beteiligten vorliegen.

(2) […]

(3) Handelt einer der Beteiligten nicht vorwerfbar, so wird dadurch die Möglichkeit der Ahndung bei den anderen nicht ausgeschlossen. Bestimmt das Gesetz, daß besondere persönliche Merkmale die Möglichkeit der Ahndung ausschließen, so gilt dies nur für den Beteiligten, bei dem sie vorliegen.

(4) […]

Art. 82 DS-GVO – Haftung und Recht auf Schadenersatz

(1) Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

(2)-(6) […]

§ 85 SGB X – Strafvorschriften

(1) Für Sozialdaten gelten die Strafvorschriften des § 42 Absatz 1 und 2 des Bundesdatenschutzgesetzes entsprechend.

(2)-(3) […]

§ 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)-(4) […]

IX. *Anhang 9: Vertraulichkeitsverpflichtung Dolmetscher*innen*

1. Vertraulichkeitsverpflichtung

Vertraulichkeitsverpflichtung für Dolmetscher*innen

*zur Erfüllung von Art. 5 Abs. 1 lit. f der Datenschutz-Grundverordnung[35] (im Folgenden „**DS-GVO**“) und zur Einhaltung weiterer Vorschriften zur Wahrung des Sozialgeheimnisses*

Für die Verarbeitung Verantwortliche*r:

XY-Universität / XY-Law Clinic (im Folgenden „**Verantwortlicher**“)
Postanschrift

Dolmetscher*in für die XY-LC (im Folgenden „**Verpflichtete*r**“)**:**

_____
(Name der/s Verpflichteten)

1. Tätigkeitsumfang d. Verpflichteten

Sie werden für den Verantwortlichen bei Beratungsgesprächen als Sprachmittler zwischen den Angehörigen des Verantwortlichen und d. Klient*in tätig, um zwischen den Gesprächsteilnehmer*innen eine Verständigungsmöglichkeit zu schaffen und so die Beratungspraxis zu ermöglichen. Sie übersetzen die Aussagen d. Gesprächsteilnehmer*innen mündlich in die jeweils andere Sprache oder geben schriftliche Dokumente mündlich in der jeweils anderen Sprache wieder. Ihnen wird dabei nur insofern Zugriff zu personenbezogenen Daten gegeben, als das zur Erfüllung Ihrer Aufgabe notwendig ist, und nur für die Zeit des Beratungsgespräches.

2. Verpflichtung auf die Vertraulichkeit

Im Rahmen dieser Tätigkeit erlangen Sie Kenntnis von vertraulichen Informationen, insb. personenbezogenen Daten. Sie sind verpflichtet, die Vertraulichkeit dieser Informationen zu wahren. Soweit Sie mit Sozialdaten in Berührung kommen, unterliegen Sie auch der gesetzlichen Pflicht zur Wahrung des Sozialgeheimnisses. Insbesondere dürfen Sie die erlangten Informationen nicht nach außen tragen. Nach Beendigung des jeweiligen Beratungsgespräches müssen Sie Dokumente, die Ihnen während des Beratungsgespräches zur Übersetzung ausgehändigt wurden, zurückgeben und von Ihnen eventuell angefertigte Notizen vernichten. Die Pflicht zur Wahrung der Vertraulichkeit und des Sozialgeheimnisses bleibt auch nach Beendigung Ihres Engagements als Dolmetscher für den Verantwortlichen ohne zeitliche Begrenzung bestehen. Verstöße gegen Vertraulichkeitspflichten können nach den gesetzlichen Vorschriften ggf. mit einer Geldbuße, Geld- oder Freiheitsstrafe geahndet werden (- siehe Anhang).

3. Unterrichtung über die vorgenannten Verpflichtungen

Über diese Verpflichtungen und die zu ihrer Erfüllung erforderlichen Verhaltensweisen wurde ich als Verpflichtete*r unterrichtet. Ich bin mir über die bei einem Verstoß drohenden Sanktionen bewusst.

Ein Abdruck der wichtigsten Vorschriften ist in der beigefügten „*Anlage zur Verpflichtung auf die Vertraulichkeit*“ enthalten.

_____	_____
Ort, Datum	Unterschrift XY-LC-Angehörige*r
_____	_____
Ort, Datum	Unterschrift Dolmetscher*in

[35] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG.

2. Anlage zur Vertraulichkeitsverpflichtung

Anlage zur Vertraulichkeitsverpflichtung (für Dolmetscher*innen)

Die vorliegende Auswahl gesetzlicher Vorschriften soll Ihnen einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Weitere Informationen zu datenschutzrechtlichen Fragestellungen erhalten Sie beim **behördlichen Datenschutzbeauftragten**:

N.N.
Postanschrift

Vorschriften zur Vertraulichkeitsverpflichtung

Art. 4 DS-GVO – Begriffsbestimmungen
Im Sinne dieser Verordnung bezeichnet der Ausdruck:

5. „**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;
[…]

Vorschriften zur Wahrung des Sozialgeheimnisses

§ 67 SGB X – Begriffsbestimmungen
(1) […]
(2) **Sozialdaten** sind personenbezogene Daten (Artikel 4 Nummer 1 der Verordnung (EU) 2016/679), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden. Betriebs- und Geschäftsgeheimnisse sind alle betriebs- oder geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben.
(3)-(5) […]

§ 35 SGB I – Sozialgeheimnis
(1) Jeder hat Anspruch darauf, dass die ihn betreffenden Sozialdaten (§ 67 Absatz 2 Zehntes Buch) von den Leistungsträgern nicht unbefugt verarbeitet werden (**Sozialgeheimnis**). Die Wahrung des Sozialgeheimnisses umfasst die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. […]
(2) […]
(2a) Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.
(3) […]
(4) Betriebs- und Geschäftsgeheimnisse stehen Sozialdaten gleich.
(5)-(7)[…]

§ 78 SGB X – Zweckbindung und Geheimhaltungspflicht eines Dritten, an den Daten übermittelt werden
(1) Personen oder Stellen, die nicht in § 35 des Ersten Buches genannt und denen Sozialdaten übermittelt worden sind, dürfen diese nur zu dem Zweck speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, zu dem sie ihnen befugt übermittelt worden sind. Eine Übermittlung von Sozialdaten an eine nicht-öffentliche Stelle ist nur zulässig, wenn diese sich gegenüber der übermittelnden Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dem sie ihr übermittelt werden. Die **Dritten** haben die Daten in demselben Umfang geheim zu halten wie die in § 35 des Ersten Buches genannten Stellen. […]
(2) Werden Daten an eine nicht-öffentliche Stelle übermittelt, so sind die dort beschäftigten Personen, welche diese Daten speichern, verändern, nutzen, übermitteln, in der Verarbeitung einschränken oder löschen, von dieser Stelle vor, spätestens bei der Übermittlung auf die Einhaltung der Pflichten nach Absatz 1 hinzuweisen. (3)-(4) […]

Strafvorschriften

§ 85 SGB X – Strafvorschriften
(1) Für Sozialdaten gelten die **Strafvorschriften** des § 42 Absatz 1 und 2 des Bundesdatenschutzgesetzes entsprechend.
(2)-(3) […]

§ 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)-(4) […]

X. *Anhang 10: Bestellung eines/einer Datenschutzbeauftragten*

Bestellung eines/einer Datenschutzbeauftragten

Die

Refugee Law Clinic-XY

- Auftraggeber -

bestellt hiermit Herrn/Frau _____

Fax:

E-Mail:

- Datenschutzbeauftragte*r -

mit Wirkung zum 01.08.2018 zur/zum Datenschutzbeauftragten des Auftraggebers.

Der Auftraggeber stellt sicher, dass der/die Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der/die Datenschutzbeauftragte darf vom Auftraggeber wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Eine Abberufung darf nur dann erfolgen, wenn eine gesetzliche Grundlage für eine Abberufung vorliegt.

Der/die Datenschutzbeauftragte berichtet unmittelbar dem Vorstand des Auftraggebers.

Der Auftraggeber wird den/die Datenschutzbeauftragte*n ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einbinden.
Der Auftraggeber unterstützt den/die Datenschutzbeauftragte*n bei der Erfüllung seiner Aufgaben gemäß Art. 39 der Datenschutz-Grundverordnung (DS-GVO), indem er die für die Erfüllung der Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

Betroffene Personen können den/die Datenschutzbeauftragte*n zu allen Fragen im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte nach der DS-GVO zu Rate ziehen.

Der/die Datenschutzbeauftragte ist bei der Erfüllung ihrer/seiner Aufgaben an die Wahrung der Geheimhaltung gebunden. Weiter ist der Datenschutzbeauftragte zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie/er nicht davon durch die betroffene Person befreit wird.

Die Aufgaben des/der Datenschutzbeauftragten ergeben sich aus der DS-GVO. Dazu gehören insbesondere:

- Unterrichtung und Beratung des Auftraggebers und der Mitarbeiter*innen/Mitglieder, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DS-GVO oder anderen jeweils geltenden datenschutzrechtlichen Vorschriften;
- Überwachung der Einhaltung der Vorgaben der DS-GVO und anderer Datenschutzvorschriften sowie der Strategien des Auftraggebers für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter/Mitglieder und der diesbezüglichen Überprüfungen;
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35 DS-GVO;
- Zusammenarbeit mit der Aufsichtsbehörde;
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36 DS-GVO, und gegebenenfalls Beratung zu allen sonstigen Fragen.

Der/die Datenschutzbeauftragte erklärt mit der Unterschrift auf diesem Dokument ihr/sein Einverständnis mit der Benennung ihrer/seiner Person zur/zum Datenschutzbeauftragten.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
- Auftraggeber -	- Datenschutzbeauftragte*r -

XI. *Anhang 11: Vorschlag für einen Satzungspassus für Vereins-(R)LCs*

§ X Datenschutzbestimmungen

1. *Der Verein gibt sich eine Datenschutzordnung.*
2. *Der Verein erhebt, speichert und nutzt ausschließlich Daten, wenn und soweit dies zur Erreichung des Vereinszweckes und zur Ausübung der auf Erfüllung des Vereinszweckes gerichteten Tätigkeiten erforderlich ist.*
3. *Der Verein ernennt eine*n Datenschutzbeauftragte*n.*

XII. *Anhang 12: Vorschlag für eine Datenschutzordnung für Vereins-(R)LCs*

Datenschutzordnung der RLC-XY

§ 1 Allgemeines

(1) Diese Datenschutzordnung regelt die Grundzüge der Datenerhebung, der Datenverarbeitung und der Datennutzung personenbezogener Daten, die im Rahmen der Verwaltung der Refugee Law Clinic XY e.V. (Im Folgenden: RLC-XY) anfallen.

(2) Personenbezogene Daten im Sinne des Abs. 1 sind Daten der eigentlichen Mitgliederverwaltung sowie Daten zur Durchführung der Lehrveranstaltungen zum Zwecke der Ausbildung der Mitglieder und der Betreuung der der RLX-XY erteilten Mandate im Rahmen der Beratung gemäß Vereinszweck.

(3) Die grundlegenden rechtlichen Regelungen finden sich im Bundesdatenschutzgesetz (BDSG) sowie in der DS-GVO, die in ihrer jeweils geltenden Fassung Anwendung finden.

§ 2 Datenerhebung

(1) Mit der Antragstellung auf Aufnahme in die RLX-XY werden durch den zuständigen Verantwortlichen für die Datenverarbeitung in der Geschäftsstelle die nachfolgend genannten Daten erfasst:
- Vor- und Nachname
- Geburtsdatum
- Vollständige Postanschrift
- Telefonnummer, ggf. Fax
- Email-Adresse
- Tätigkeitsbeschreibung bzw. Berufsangabe/ Studienfach
- Zahlungsart sowie die zur Durchführung der Zahlung erforderlichen Bankdaten
- Sonstige Informationen, wenn und soweit sie zur Erfüllung des Vereinszweckes erforderlich sind oder im Zusammenhang mit der Tätigkeit des Mitgliedes im Verein stehen (etwa Vorstandsmitgliedschaft, Beratungstätigkeit).

(2) Die Mitgliedschaft kann nur erworben werden, wenn in die Erfassung der für die Mitgliedschaft erforderlichen persönlichen Daten eingewilligt wird. Es müssen mindestens die Grunddaten (Vollständiger Vor- und Zunahme, Geburtsdatum, Anschrift, Zahlungsart) erfasst werden. Die vorgenannten Daten werden für die Mitgliedschaft in der RLC-XY erhoben und gespeichert. Das Mitglied kann die Einwilligung jederzeit schriftlich widerrufen. Dies hat aber zur Folge, dass die Mitgliedschaft in der RLC-XY gestrichen werden muss, da die Datenspeicherung hierfür erforderlich ist.

(3) Ist die Bezahlung von Rechnungen mittels des SEPA-Lastschriftverfahrens gewünscht, so werden hierfür auf einem separaten Formular die Konto- und Bankdaten erfasst und gespeichert.

(4) Die RLC-XY erhebt außerdem im Rahmen der Beratung gem. Vereinszweck auch die zur Beratung erforderlichen Daten ihrer Klienten. Dies sind:
- Vor- und Zuname
- Geburtsdatum
- Meldeadresse
- Emailadresse
- Telefonnummer
- ggf. Aktenzeichen von für die Mandatsbearbeitung relevanten Behördenvorgängen der beratenen Klienten.
- ggf. Herkunftsland des Ratsuchenden/ Erteilers des Mandates
- ggf. ethnische Herkunft, Religion, Krankheiten oder politische Anschauungen, wenn dies für die Beratung und Bearbeitung des konkreten Falles relevant und damit erforderlich ist
- ggf. Daten über Dritte, die der Klient für die Bearbeitung seines Anliegens erforderlich oder relevant hält

Die Mandatsdaten werden nach Beendigung des Mandates ordnungsgemäß vernichtet und gelöscht.

(5) Außerdem werde Daten von Bewerbern auf Stellen als studentische Hilfskräfte in der Geschäftsstelle der RLX-XY erhoben. Dies sind
- Vollständiger Name des Bewerbers
- Postanschrift
- Emailadresse.

Soweit mit dem Bewerber ein Vertragsverhältnis angestrebt wird, werden diese Daten [an die Personalabteilung der Universität] weitergegeben, sowie darüber hinaus
- Geburtsdatum
- Matrikelnummer
- Krankenkasse
- Steueridentifikationsnummer
- Staatsangehörigkeit
- ggf. bereits vorhandene Personalnummer der Universität

(6) Des Weiteren erhebt die RLC-XY personenbezogene Daten der Referenten der Lehrveranstaltungen, die zur Veranstaltung und der Durchführung der Lehrveranstaltungen erforderlich sind.
Dies sind:
- Vollständiger Name
- Anschrift und Kontaktdaten (Telefonnummer, Emailadresse)

(7) Die RLC-XY erhebt außerdem die Daten der Teilnehmer ihrer Vorlesungsveranstaltungen, um die Teilnahme an den Veranstaltungen zu ermöglichen und durchzuführen, und zwar
- Vollständiger Name
- Emailadresse
- Postanschrift des Teilnehmers
- Ggf. Matrikelnummer des jeweiligen Teilnehmers, soweit dieser an der Universität immatrikuliert ist

§ 3 Datenspeicherung und Verwendung von Daten durch die einzelnen Referate

(1) Die unter § 1 erhobenen Daten werden in EDV-Systemen der Geschäftsstelle der RLC-XY gespeichert. Jedem Mitglied des Vereins wird dabei eine Mitgliedsnummer zugeordnet. Die personenbezogenen Daten werden hierbei durch geeignete technische und organisatorische Maßnahmen vor der Kenntnisnahme Dritter geschützt. Sonstige Informationen zu den Mitgliedern und Informationen über Nichtmitglieder werden vom Verein grundsätzlich nur verarbeitet oder genutzt, wenn sie der Förderung des Vereinszwecks nützlich sind und keine Anhaltspunkte bestehen, dass die betroffene Person ein schutzwürdiges Interesse hat, das der Verarbeitung oder Nutzung entgegenstehen würde. Nur Mitglieder, die eine besondere Funktion ausüben, für welche die Kenntnis bestimmter Mitgliedsdaten erforderlich ist, wie etwa zur Mitgliederverwaltung, haben Zugriff auf die genannten Daten.

(2) Zusätzlich zur Datenspeicherung wird das Beitrittsformular aus Gründen der Nachweispflicht in einem EDV-System oder papiergebunden archiviert, solange und soweit dies zur Bearbeitung des Anliegens erforderlich ist. Auch diese personenbezogenen Daten werden durch geeignete technische und organisatorische Maßnahmen vor der Kenntnisnahme Dritter geschützt.

(3) Schriftliche Kontaktaufnahmen (z.B. Briefe) der Mitglieder mit der Geschäftsstelle werden ebenso papiergebunden archiviert. Bei einigen Dokumenten (z.B. SEPA-Lastschriftmandat) erfolgt eine Digitalisierung und Speicherung in der elektronischen Mitgliederdatei. Dies dient ausschließlich der prozessoptimierten Arbeit der Geschäftsstelle und des Vorstandes.

(4) Die Mitglieder des Vorstandes verfügen über diejenigen personenbezogenen Daten sich aus ihrer konkreten Tätigkeit für die RLC-XY ergeben, insbesondere verfügt (also erhebt, speichert und verwendet)

a. Das Referat Mitgliederverwaltung über die Daten der Mitglieder zum Zwecke der Verwaltung,
b. Das Referat Ausbildung über die erforderlichen Kontaktdaten der Dozenten (Postanschrift, Email-adresse, ggf. Telefonnummer) sowie über die erforderlichen Daten der Mitglieder und der übrigen Teilnehmer der Vorlesungen, die den Ausbildungszyklus durchlaufen, um erstens die Durchführung der Ausbildung sicherzustellen und zweitens den Ausbildungsteilnehmern nach Abschluss der Ausbildung die beendete Ausbildung auf Wunsch bestätigen zu können.
c. Das Referat Presse und Öffentlichkeitsarbeit über die zur Bewerbung von Veranstaltungen erforderlichen Daten der Dozenten, die Namen der Vorstandsmitglieder und die bei Veranstaltungen von den Teilnehmern nach Einwilligung angefertigten Bilder, die Facebook-Aliase von Personen, die Anfragen an die Facebook-Seite schicken
d. Das Referat Beratung über die Kontaktdaten der als Berater tätigen Absolventen des Ausbildungszyklus der RLC-XY sowie die Kontaktdaten der Organisationen, mit denen die Beratungstätigkeit kooperativ durchgeführt wird.
e. die Kassenverwaltung über die zur Einziehung der Mitgliedsbeiträge erforderlichen Kontaktdaten der Mitglieder, die zur Abrechnung mit den Dozenten im Rahmen deren Tätigkeit im Ausbildungszyklus erforderlichen Daten zur Vergütung der Dozenten
f. das Referat Fundraising über die zur Spendenakquise erforderlichen Daten sowie über die Daten der bisherigen Spender, soweit diese in die Speicherung und Verarbeitung ihrer Kontaktdaten zu diesem Zweck eingewilligt haben
g. das Referat Öffentlichkeitsarbeit über die Daten, die im Rahmen der Nutzung der Facebook-Seite von Facebook geriert werden und zur Betreuung der Facebookseite erforderlich sind
h. die einzelnen Berater über Vor- und Zunamen, Geburtsdatum, Staatsangehörigkeit. Meldeadresse, Emailadresse Telefonnummer und ggf. Aktenzeichen von für die Mandatsbearbeitung relevanten Behördenvorgängen der beratenen Klienten, sowie im Einzelfall für die konkrete Beratung relevante personenbezogene Daten wie etwa die sexuelle Orientierung. Soweit Mitschriften zur Gedächtnisstütze angefertigt werden, werden diese sicher gelagert und vernichtet, sobald sie nicht mehr benötigt werden. Die Beratungsprotokolle sind passwortgeschützt gespeichert.
i. Die RLC-XY stellt dabei sicher, dass die einzelnen Referate nur über die zur Ausübung des konkreten Aufgabenbereiches erforderlichen Daten verfügen.

(5) Sollten im Rahmen der Tätigkeit der Vorstandsmitglieder weitere personenbezogene Unterlagen anfallen, so sind diese entsprechend der datenschutzrechtlichen Bestimmungen aufzubewahren. Nach dem Ausscheiden aus dem Vorstand werde eventuell gesammelte Daten an den unmittelbaren Amtsnachfolger oder die Geschäftsstelle der RLC-XY übergeben.

§ 4 Datennutzung und Verwendung

(1) Die erhobenen und erfassten Daten werden ausschließlich zum Zwecke der Vereinsverwaltung sowie zum Zwecke der Tätigkeiten nach dem Vereinszweck erhoben, gespeichert und verwendet.

(2) Die Daten dürfen im Rahmen ihrer Zweckbestimmung in einer automatisierten Datei (Verwaltungssoftware) gespeichert werden.

(3) Die Weitergabe von persönlichen Daten erfolgt nur nach vorheriger Einwilligung. Eine Veröffentlichung von Mitgliederdaten (zB Mitgliederverzeichnis) im Internet oder in anderen Publikationswegen erfolgt nicht.

(4) Sofern von Teilnehmern der von der RLC-XY angebotenen Lehrveranstaltungen nach deren Abschluss eine Bestätigung der Teilnahme gewünscht wird, insbesondere zwecks Anerkennung der Teilnahme als Studienleistung, erfolgt auf Wunsch des jeweiligen Teilnehmers die Weitergabe der zur Ausstellung dieser Bestätigungen erforderlichen Daten wie Name, Anschrift und Matrikelnummer an das [Dekanat der rechtswissenschaftlichen Fakultät der Universität].

(5) Die gespeicherten Daten werden ohne Zustimmung des Betroffenen nicht an Personen oder Institutionen außerhalb des Vereins (insbesondere für Werbezwecke) weitergegeben oder in sonstiger Weise zugänglich gemacht. Auch bei einer erwünschten Weitergabe von Daten, etwa nach Abs. 3 Unterabsatz 2 an [das Dekanat der rechtswissenschaftlichen Fakultät der Universität], erfolgt diese nur mit vorheriger Zustimmung des Vorlesungsteilnehmers. Innerhalb des Vereins darf die Weitergabe der Daten nur nach Maßgabe dieser Datenschutzordnung erfolgen.

(6) Bestimmte Mitarbeiter der Geschäftsstelle, die mit der Mitgliederverwaltung beauftragt sind bzw. die für die Betriebsbereitschaft des Mitgliederverwaltungssystems verantwortlich sind, haben vollen Zugriff auf die Mitgliederdaten. Die Mitglieder des Vorstandes, abgesehen vom zuständigen Referat Mitgliederverwaltung, können nur auf Teile der Mitgliederdaten zugreifen.

(7) Daten, die für andere Zwecke der Verwaltung des Vereins anfallen, dürfen nur noch von den für diesen Zweck bestimmten Personen genutzt werden.

(8) Den unter Abs. 5 und 6 genannten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Vor der Aufnahme ihrer Tätigkeit sind diese Personen auf das Datengeheimnis gem. § 5 BDSG zu verpflichten.

(9) Die zur Betreuung der der RLC-XY erteilten Beratungsmandate erforderlichen Daten wie Name des Klienten werden in der Geschäftsstelle papiergebunden archiviert und ausschließlich zur Erfüllung und Bearbeitung der Mandate verwendet. Die das Mandat erteilenden Personen werden darüber informiert und willigen in die zum Mandat erforderliche Nutzung im Rahmen der Beratungsvereinbarung ein.

§ 5 Beendigung der Mitgliedschaft, Sperrung und Löschung von Mitgliederdaten und anderer Daten

(1) Wird die Mitgliedschaft gekündigt oder Ende aus einem sonstigen Grund, so werden die erhobenen persönlichen Daten mit dem rechtlichen Austritt ([Datum je nach Maßgabe der jeweiligen Refugee Law Clinic]) gesperrt und nicht mehr weiter verwendet.

(2) Wünscht ein Mitglied die komplette Löschung der erhobenen Daten, so kann dies formlos bei der Geschäftsstelle beantragt werden. Die Geschäftsstelle wird diese Datenlöschung vorbehaltlich der Pflichten aus Abs. 3 umgehend veranlassen.

(3) Eine etwaige Verpflichtung zur Aufbewahrung von Unterlagen oder Speicherung von Daten, die sich aus Bestimmungen des Handels-, Steuerrechtes oder nach anderen Vorschriften ergibt, bleibt von den Regelungen in Abs. 1 und 2 unberührt.

(4) Die zur Durchführung der Lehrveranstaltungen erforderlichen Daten, die gemäß dieser Datenschutzordnung erhoben wurden, werden nur aufbewahrt, solange und soweit dies für die Durchführung laufender und künftiger Lehrveranstaltungen erforderlich ist.

(5) Wünscht ein Vorlesungsteilnehmer oder –dozent die Löschung der ihn betreffenden Daten, so kann dies formlos bei der Geschäftsstelle beantragt werden. Die Geschäftsstelle wird diese Datenlöschung umgehend veranlassen.

(6) Die für die Mandatsbearbeitung erforderlichen Daten werden bis zum Abschluss des Mandates in der Geschäftsstelle [auf die von der jeweiligen Refugee Law Clinic verwendeten Weise, etwa in einem verschlossenen Aktenschrank o.ä.] aufbewahrt. Die RLC-XY stellt sicher, dass nur die beratenden Mitglieder Zugriff auf die von ihnen betreuten Mandatsdaten haben, soweit sie diese zur Betreuung des Mandates benötigen. Wünscht ein Klient die Löschung und/ oder Vernichtung der ihn betreffenden Daten, so kann dies formlos bei der Geschäftsstelle beantragt werden. Die Geschäftsstelle wird diese Datenlöschung sowie die ordnungsgemäße Vernichtung der papiergebundenen Daten umgehend veranlassen. Abgesehen davon werden die Handakten für die Dauer der gesetzlichen Fristen gem. § 50 BRAO aufbewahrt.

§ 6 Löschung der Daten

(1) Beim Vereinsaustritt bzw. mit Beendigung der Mitgliedschaft werden Name, Adressdaten, Geburtsdatum und weitere persönliche Daten des Mitglieds aus der Mitgliedsverwaltung gelöscht. Hiervon ausgenommen sind personenbezogene Daten des austretenden Mitglieds, die die Kassenverwaltung betreffen. Entsprechende Daten werden gemäß den steuerrechtlichen Bestimmungen bis zu zehn Jahre ab der schriftlichen Bestätigung des Austritts durch den Vorstand aufbewahrt. Alle Mitglieder sind ihrerseits verpflichtet, ihre Daten gemäß BDSG-neu und DS-GVO zu verwalten.

(2) Die Daten aus den Mandaten werden nach Beendigung des Mandates gelöscht, soweit keine Aufbewahrungspflichten bestehen.

(3) Alle übrigen erhobenen und gespeicherten Daten werden gelöscht, sobald der Verarbeitungszweck weggefallen ist.

(4) Die Datenlöschung der ihn betreffenden Daten auf Wunsch des Betroffenen nach Art. 17 DS-GVO und § 7 dieser Datenschutzordnung bleibt von diesen Regeln unberührt.

§ 7 Rechte der betroffenen Personen

(1) Werden erstmals personenbezogene Daten für eine Mitgliedschaft, ein Mandat, die Teilnahme an einer

Lehrveranstaltung, die Durchführung einer Lehrveranstaltung oder zur Erfüllung sonstiger Zwecke des Vereins gespeichert, so wird der Betroffene hierüber informiert und um seine Zustimmung gebeten. Dies erfolgt bei Mitgliedern über den Antrag auf Mitgliedschaft auf einem Formblatt.

(2) Mitglieder können jederzeit Auskunft zu den über sie gespeicherten Daten verlangen. Sollten die Daten fehlerhaft sein, so besteht der Anspruch auf Berichtigung nach Art. 16 DS-GVO. Gespeicherte Daten, die zur Verwaltung und Arbeit des Vereins nicht erforderlich sind, werden auf Antrag durch das betroffene Mitglied ebenfalls gelöscht.

(3) Auskunftsersuchen nach §§ 19, 34 BDSG sind schriftlich in formloser Art an die Geschäftsstelle der [Refugee Law Clinic] zu richten.

§ 8 Datenschutzbeauftragter

(1) Die RLC-XY ernennt eine*n Datenschutzbeauftragte*n. Diese/r überwacht die Einhaltung der Datenschutzordnung (insbesondere die praktische Umsetzung der technischen Datenschutzmaßnahmen und die Dokumentation der Verarbeitungsverzeichnisse), ist Ansprechpartner für alle Fragen des Datenschutzes und führt halbjährlich Schulungen für alle Mitglieder der RLC-XY durch.

(2) Der Datenschutzbeauftragte kann intern (Vereinsmitglied) oder extern ernannt werden, darf aber kein Vorstandsmitglied sein und nicht über Datenerhebung und -verwendung entscheiden (Verbot der Selbstkontrolle).

(3) Über die Ernennung des/ der Datenschutzbeauftragten entscheidet der Vorstand gemäß Vereinssatzung.

§ 9 Verzeichnis der Verarbeitungstätigkeiten

Der Verein führt ein schriftliches Verzeichnis der Verarbeitungstätigkeiten. Das Formular für die Dokumentation der Verarbeitungstätigkeiten wird von allen Vereinsmitgliedern und –mitarbeitern ausgefüllt, die für die Refugee Law Clinic Saarbrücken Daten erheben, verarbeiten, nutzen oder weitergeben. Das Verzeichnis wird papiergebunden in der Geschäftsstelle aufbewahrt.

§ 10 Beschluss und Änderung der Datenschutzordnung

(1) Diese Datenschutzordnung wird durch den Vorstand der RLC-XY beschlossen und den Mitgliedern durch Veröffentlichung auf der Internetseite der RLC-XY bekannt gegeben.

(2) Änderungen können nur durch schriftlichen Antrag von mindestens einem Mitglied gegenüber dem Vorstand beantragt werden. Der Vorstand beträgt über den Änderungsantrag und verfügt ggf. die Änderung der Datenschutzordnung.

§ 11 Schlussbestimmungen

Sofern Teile oder einzelne Formulierungen dieser Datenschutzordnung der geltenden Rechtslage nicht, nicht mehr oder nicht vollständig entsprechen sollten, bleiben die übrigen Teil der Ordnung in ihrem Inhalt und ihrer Gültigkeit davon unberührt.

Diese Datenschutzordnung wurde auf der Vorstandssitzung am XX.XX.XXXX in XY vom Vorstand beschlossen und tritt zum XX.XX.XXXX in Kraft.

_____	_____	_____
Ort, Datum	Ort, Datum	Ort, Datum
_____	_____	_____
- 1. Vorstand -	- 2. Vorstand -	- 3. Vorstand -

XIII. *Anhang 13: Datenschutzerklärung für die Website*

Datenschutzerklärung der RLC XY

1. Information über die Erhebung personenbezogener Daten

1.1. Im Folgenden informieren wir über die Erhebung personenbezogener Daten bei Nutzung unserer Website. Bitte nehmen Sie sich einen Augenblick Zeit, um sich mit den Informationen vertraut zu machen.

1.2. Diese Website enthält Links zu anderen Websites. Diese Datenschutzerklärung gilt nur für diese Website. Wir sind nicht verantwortlich für die Datenschutzpraktiken oder den Inhalt der verlinkten Websites. Für weitere Informationen lesen Sie bitte deren eigene Datenschutzerklärungen.

1.3. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder eine identifizierbare natürliche Person beziehen.

1.4. Verantwortlicher für die Datenverarbeitung gem. Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) ist der Refugee Law Clinic XXX e.V., ladungsfähige Anschrift (nachfolgend „RLC XX", „wir" oder „uns"). Sie können uns unter der vorstehenden Postanschrift oder unter der Telefonnummer +49 XXX XXXXX oder unter der E-Mailadresse rlcXX@XX.de erreichen.

1.5. Bei Ihrer Kontaktaufnahme mit uns per E-Mail oder über ein Kontaktformular werden die von Ihnen mitgeteilten Daten (Ihre E-Mail-Adresse, ggf. Ihr Name und Ihre Telefonnummer) von uns gespeichert, um Ihre Fragen zu beantworten. Die in diesem Zusammenhang anfallenden Daten löschen wir, nachdem die Speicherung nicht mehr erforderlich ist, oder schränken die Verarbeitung ein, falls gesetzliche Aufbewahrungspflichten bestehen.

1.6. Falls wir für einzelne Funktionen unseres Angebots auf beauftragte Dienstleister zurückgreifen oder Ihre Daten für werbliche Zwecke nutzen möchten, werden wir Sie untenstehend im Detail über die jeweiligen Vorgänge informieren. Dabei nennen wir auch die festgelegten Kriterien der Speicherdauer.

2. Erhebung personenbezogener Daten bei Besuch unserer Website

2.1. Bei der bloß informatorischen Nutzung der Website, also wenn Sie uns nicht anderweitig Informationen übermitteln, erheben wir nur die personenbezogenen Daten, die Ihr Browser an unseren Server übermittelt. Wenn Sie unsere Website betrachten möchten, erheben wir die folgenden Daten, die für uns technisch erforderlich sind, um Ihnen unsere Website anzuzeigen und die Stabilität und Sicherheit zu gewährleisten (Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO):

- IP-Adresse
- Datum und Uhrzeit der Anfrage
- Zeitzonendifferenz zur Greenwich Mean Time (GMT)
- Inhalt der Anforderung (konkrete Seite)
- Zugriffsstatus/HTTP-Statuscode
- jeweils übertragene Datenmenge
- Website, von der die Anforderung kommt
- Browser
- Betriebssystem und dessen Oberfläche
- Sprache und Version der Browsersoftware.

2.2. Zusätzlich zu den zuvor genannten Daten werden bei Ihrer Nutzung unserer Website Cookies auf Ihrem Rechner gespeichert. Bei Cookies handelt es sich um kleine Textdateien, die auf Ihrer Festplatte dem von Ihnen verwendeten Browser zugeordnet gespeichert werden und durch welche der Stelle, die den Cookie setzt (hier durch uns), bestimmte Informationen zufließen. Cookies können keine Programme ausführen oder Viren auf Ihren Computer übertragen. Sie dienen dazu, das Internetangebot insgesamt nutzerfreundlicher und effektiver zu machen.

2.3. Einsatz von Cookies:

Diese Website nutzt folgende Arten von Cookies, deren Umfang und Funktionsweise im Folgenden erläutert werden:

2.3.1. Transiente Cookies werden automatisiert gelöscht, wenn Sie den Browser schließen. Dazu zählen insbesondere die Session-Cookies. Diese speichern eine sogenannte Session-ID, mit welcher sich verschiedene Anfragen Ihres Browsers der gemeinsamen Sitzung zuordnen lassen. Dadurch kann Ihr Rechner wiedererkannt werden, wenn Sie auf unsere Website zurückkehren. Die Session-Cookies werden gelöscht, wenn Sie sich ausloggen oder den Browser schließen.

2.3.2. Persistente Cookies werden automatisiert nach einer vorgegebenen Dauer gelöscht, die sich je nach Cookie unterscheiden kann. Sie können die Cookies in den Sicherheitseinstellungen Ihres Browsers jederzeit löschen.

2.3.3. Sie können Ihre Browser-Einstellung entsprechend Ihren Wünschen konfigurieren und z. B. die Annahme von Third-Party-Cookies oder allen Cookies ablehnen. Wir weisen Sie darauf hin, dass Sie eventuell nicht alle Funktionen dieser Website nutzen können.

3. Weitere Funktionen und Angebote unserer Website

3.1. Neben der rein informatorischen Nutzung unserer Website bieten wir verschiedene Leistungen an, die Sie bei Interesse nutzen können. Dazu müssen Sie in der Regel weitere personenbezogene Daten angeben, die wir zur Erbringung der jeweiligen Leistung nutzen und für die die zuvor genannten Grundsätze zur Datenverarbeitung gelten.

3.2. Teilweise bedienen wir uns zur Verarbeitung Ihrer Daten externer Dienstleister. Diese wurden von uns sorgfältig ausgewählt und beauftragt, sind an unsere Weisungen gebunden und werden regelmäßig kontrolliert.

3.3. Soweit unsere Dienstleister oder Partner ihren Sitz in einem Staat außerhalb des Europäischen Wirtschaftsraumen (EWR) haben, informieren wir Sie über die Folgen dieses Umstands in der Beschreibung des Angebotes.

4. Datenverarbeitung bei Beratungsanfragen

4.1. Personenbezogene Daten und Zweck Ihrer Erhebung

4.1.1. Wenn Sie ohne Beratungsvereinbarung mit der XY-LC Kontakt aufnehmen, bitten wir Sie um ihren *Namen* (damit wir wissen, wer unser*e Klient*in sein wird), ihre *Kontaktdaten* (damit wir mit Ihnen in Kontakt treten können), ihre *Nationalität* (wenn Sie eine Frage zum Aufenthalts- oder Asylrecht haben), ihr *Geburtsdatum* (um zu wissen, ob Sie volljährig sind) und *Auskunft darüber, ob Sie einen Dolmetscher benötigen* (zur Einschätzung der Verständigungsmöglichkeiten); wir kommunizieren mit Ihnen in Deutsch oder Englisch.

4.1.2. Wenn Sie uns vorab solche personenbezogenen Daten nicht mitteilen wollen, kommen Sie stattdessen einfach in unsere offene Sprechstunde. Dort erklären wir Ihnen, welche Beratung wir anbieten, was im Falle einer Beratung mit Ihren Daten geschieht und wie wir diese schützen. In diesem ersten Gespräch können Sie anonym bleiben.

4.1.3. Bitte teilen Sie uns bei der Kontaktaufnahme auf keinen Fall personenbezogene Daten mit, die sich auf Dritte beziehen (z.B. von Geflüchteten, die Sie zur Beratung an uns verweisen wollen); das ist datenschutzrechtlich nicht ohne Weiteres zulässig. Ob entsprechende Daten für die Beratung nötig sind und wie wir diese Daten erheben dürfen, können wir bei Abschluss des Beratungsvertrages klären.

4.2. Weiterer Umgang mit Ihren Daten

4.2.1. Wir machen die Daten, die Sie uns zukommen lassen, den Berater*innen zugänglich, die Ihnen ein Erstgespräch oder die nächste/n Sprechstunde/n anbieten. Wenn wir bereits zu diesem Zeitpunkt eine*n Supervisor*in für Ihren Fall einschalten, geben wir die Daten zudem anonymisiert (d.h. ohne dass auf die betreffende Person geschlossen werden kann) an d. Supervisor*in weiter. Außerdem nutzen wir die Daten für die Kommunikation mit Ihnen und zur Dokumentation in unserer Fallakte. Wir geben vor Abschluss eines Beratungsvertrages keine Daten an andere Stellen oder Personen oder gar an Drittstaaten weiter. Die gespeicherten Daten sind allerdings im Falle eines strafrechtlichen Ermittlungsverfahrens nicht vor Beschlagnahme geschützt.

4.3. Rechtsgrundlage der Datenverarbeitung

4.3.1. Die Erhebung und Speicherung der Daten von Ratsuchenden, sowie deren Weitergabe (s.o. unter II Nr. 2), erfolgt auf Grundlage von Art. 6 Abs. 1 S. 1 lit. b Alt. 2 DS-GVO. Die Daten sind erforderlich um feststellen zu können, ob der Abschluss eines Beratungsvertrages mit Ihnen möglich und sinnvoll ist.

4.4. Besondere Kategorien personenbezogener Daten (Sensible Daten)

4.4.1. Bitte übermitteln Sie uns bei der ersten Kontaktaufnahme per E-Mail nur die unter Nr. 1 genannten Daten zu Ihnen und den Umständen Ihres Falls und insbesondere keine sensiblen Daten, wie z.B. Ihre ethnische Herkunft oder religiöse Weltanschauung (Art. 9 DS-GVO). Uns reichen die unter Nr. 4.1.1 genannten Daten für eine vorläufige Einschätzung. Wenn wir mit Ihnen einen Beratungsvertrag schließen, nehmen wir uns dann gern Zeit für eine genaue Auseinandersetzung mit Ihrem Anliegen. Es ist nicht auszuschließen, dass der Inhalt unverschlüsselter E-Mails von Dritten eingesehen werden kann, sodass eine hinreichende Vertraulichkeit der Daten nicht besteht. Sofern wir weitere, sensible Daten zur Bearbeitung Ihres Falles benötigen, werden wir Sie bei Abschluss eines Beratungsvertrages um Ihre ausdrückliche Einwilligung bitten.

5. Datenverarbeitung bei Spendenangeboten

5.1. Für Ihre freiwillige Spende sind wir dankbar! Die Bearbeitung Ihrer Spende wird uns erleichtert, wenn Sie uns schon bei Kontaktaufnahme ihren *Namen*, ihre *Anschrift*, die *Höhe des Spendenbetrages* und den *gewünschten Verwendungszweck* mitteilen. Diese Angaben benötigen wir, damit wir Ihre Spende zuordnen und Ihnen eine Spendenbescheinigung ausstellen können.

5.2. Wir übermitteln Ihre Daten (in Papierform) an die Finanzabteilung der Universität, die für die Verbuchung des Geldes auf das Spendenkonto der XY-LC und die Ausstellung der Spendenquittung verantwortlich ist.

5.3. Die Verarbeitung der Daten von Spender*innen erfolgt auf Grundlage von Art. 6 Abs. 1 S. 1 lit. b Alt. 2, c DS-GVO.

6. Newsletter

6.1. Mit Ihrer Einwilligung können Sie unseren Newsletter abonnieren, mit dem wir Sie über die neusten Ereignisse in unserer Organisation informieren.

6.2. Für die Anmeldung zu unserem Newsletter verwenden wir das sog. Double-opt-in-Verfahren. Das heißt, dass wir Ihnen nach Ihrer Anmeldung eine E-Mail an die angegebene E-Mail-Adresse senden, in welcher wir Sie um Bestätigung bitten, dass Sie den Versand des Newsletters wünschen. Wenn Sie Ihre Anmeldung nicht innerhalb von [24 Stunden] bestätigen, werden Ihre Informationen gesperrt und nach einem Monat automatisch gelöscht. Darüber hinaus speichern wir jeweils Ihre eingesetzten IP-Adressen und Zeitpunkte der Anmeldung und Bestätigung. Zweck des Verfahrens ist, Ihre Anmeldung nachweisen und ggf. einen möglichen Missbrauch Ihrer persönlichen Daten aufklären zu können.

6.3. Pflichtangabe für die Übersendung des Newsletters ist allein Ihre E-Mail-Adresse. Nach Ihrer Bestätigung speichern wir Ihre E-Mail-Adresse zum Zweck der Zusendung des Newsletters. Rechtsgrundlage ist Art. 6 Abs. 1 S. 1 lit. a DS-GVO.

6.4. Ihre Einwilligung in die Übersendung des Newsletters können Sie jederzeit widerrufen und den Newsletter abbestellen. Den Widerruf können Sie durch Klick auf den in jeder Newsletter-E-Mail bereitgestellten Link, über dieses Formular der Website (Link einfügen), per E-Mail an [Newsletter@example.com] oder durch eine Nachricht an die im Impressum angegebenen Kontaktdaten erklären.

7. Einsatz von Google Analytics

7.1. Diese Website benutzt Google Analytics, einen Webanalysedienst der Google Inc. („Google"). Google Analytics verwendet sog. „Cookies", Textdateien, die auf Ihrem Computer gespeichert werden und die eine Analyse der Benutzung der Website durch Sie ermöglichen. Die durch den Cookie erzeugten Informationen über Ihre Benutzung dieser Website werden in der Regel an einen Server von Google in den USA übertragen und dort gespeichert. Im Falle der Aktivierung der IP-Anonymisierung auf dieser Website, wird Ihre IP-Adresse von Google jedoch innerhalb von Mitgliedstaaten der Europäischen Union oder in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zuvor gekürzt. Nur in Ausnahmefällen wird die volle IP-Adresse an einen Server von Google in den USA übertragen und dort gekürzt. Im Auftrag des Betreibers dieser Website wird Google diese Informationen benutzen, um Ihre Nutzung der Website auszuwerten, um Reports über die Website-Aktivitäten zusammenzustellen und um weitere mit der Website-Nutzung und der Internetnutzung verbundene Dienstleistungen gegenüber dem Website-Betreiber zu erbringen.

7.2. Die im Rahmen von Google Analytics von Ihrem Browser übermittelte IP-Adresse wird nicht mit anderen Daten von Google zusammengeführt.

7.3. Sie können die Speicherung der Cookies durch eine entsprechende Einstellung Ihrer Browser-Software verhindern; wir weisen Sie jedoch darauf hin, dass Sie in diesem Fall gegebenenfalls nicht sämtliche Funktionen dieser Website vollumfänglich werden nutzen können. Sie können darüber hinaus die Erfassung der durch das Cookie erzeugten und auf Ihre Nutzung der Website bezogenen Daten (inkl. Ihrer IP-Adresse) an Google sowie die Verarbeitung dieser Daten durch Google verhindern, indem sie das unter dem folgenden Link verfügbare Browser-Plug-in herunterladen und installieren: http://tools.google.com/dlpage/gaoptout?hl=de.

7.4. Diese Website verwendet Google Analytics mit der Erweiterung „_anonymizeIp()". Dadurch werden IP-Adressen gekürzt weiterverarbeitet, eine Personenbeziehbarkeit kann damit ausgeschlossen werden. Soweit den über Sie erhobenen Daten ein Personenbezug zukommt, wird dieser also sofort ausgeschlossen und die personenbezogenen Daten damit umgehend gelöscht.

7.5. Wir nutzen Google Analytics, um die Nutzung unserer Website analysieren und regelmäßig verbessern zu können. Über die gewonnenen Statistiken können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Für die Ausnahmefälle, in denen personenbezogene Daten in die USA übertragen werden, hat sich Google dem EU-US Privacy Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework. Rechtsgrundlage für die Nutzung von Google Analytics ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

7.6. Informationen des Drittanbieters: Google Dublin, Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland, Fax: +353 (1) 4361001. Nutzerbedingungen: http://www.google.com/analytics/terms/de.html, Übersicht zum Datenschutz: http://www.google.com/intl/de/analytics/learn/privacy.html, sowie die Datenschutzerklärung: http://www.google.de/intl/de/policies/privacy.

8. Einsatz von Matomo (ehemals Piwik)

8.1. Diese Website nutzt den Webanalysedienst Matomo (ehemals Piwik), um die Nutzung unserer Website analysieren und regelmäßig verbessern zu können. Über die gewonnenen Statistiken können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Rechtsgrundlage für die Nutzung von Matomo ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

8.2. Für diese Auswertung werden Cookies (näheres dazu in Ziffer 2) auf Ihrem Computer gespeichert. Die so erhobenen Informationen speichert der Verantwortliche ausschließlich auf seinem Server in [Deutschland]. Die Auswertung können Sie einstellen durch Löschung vorhandener Cookies und die Verhinderung der Speicherung von Cookies. Wenn Sie die Speicherung der Cookies verhindern, weisen wir darauf hin, dass Sie gegebenenfalls diese Website nicht vollumfänglich nutzen können. Die Verhinderung der Speicherung von Cookies ist durch die Einstellung in

ihrem Browser möglich. Die Verhinderung des Einsatzes von Matomo ist möglich, indem Sie den folgenden Haken entfernen und so das Opt-out-Plug-in aktivieren: [Matomo iFrame].

8.3. Diese Website verwendet Matomo mit der Erweiterung „AnonymizeIP". Dadurch werden IP-Adressen gekürzt weiterverarbeitet, eine direkte Personenbeziehbarkeit kann damit ausgeschlossen werden. Die mittels Matomo von Ihrem Browser übermittelte IP-Adresse wird nicht mit anderen von uns erhobenen Daten zusammengeführt.

8.4. Das Programm Matomo ist ein Open-Source-Projekt. Informationen des Drittanbieters zum Datenschutz erhalten Sie unter https://matomo.org/privacy-policy/

9. Einsatz von eTracker

9.1. Auf dieser Website werden mit Technologien der etracker GmbH (http://www.etracker.com) Daten zu Marketing- und Optimierungszwecken gesammelt und gespeichert. Aus diesen Daten können unter einem Pseudonym Nutzungsprofile erstellt werden. Hierzu können Cookies eingesetzt werden. Bei Cookies handelt es sich um kleine Textdateien, die lokal im Zwischenspeicher des Internet-Browsers des Seitenbesuchers gespeichert werden. Die Cookies ermöglichen die Wiedererkennung des Internet-Browsers. Die mit den eTracker-Technologien erhobenen Daten werden ohne die gesondert erteilte Zustimmung des Betroffenen nicht dazu benutzt, den Besucher dieser Website persönlich zu identifizieren und nicht mit personenbezogenen Daten über den Träger des Pseudonyms zusammengeführt. Der Datenerhebung und -speicherung kann jederzeit mit Wirkung für die Zukunft widersprochen werden.
Bitte schließen Sie mich von der eTracker-Zählung aus. [Link]

9.2. Wir nutzen eTracker, um die Nutzung unserer Website analysieren und regelmäßig verbessern zu können. Über die gewonnenen Statistiken können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Die erhobenen Daten werden dauerhaft gespeichert und pseudonym analysiert. Rechtsgrundlage für die Nutzung von eTracker ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

9.3. Informationen des Drittanbieters: etracker GmbH, Erste Brunnenstraße 1, 20459 Hamburg; https://www.etracker.com/de/datenschutz.html. Rechtsgrundlage für die Nutzung von eTracker ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

10. Einsatz von Jetpack/ehem. Wordpress.com-Stats

10.1. Diese Website nutzt den Webanalysedienst Jetpack (früher: WordPress.com-Stats), um die Nutzung unserer Website analysieren und regelmäßig verbessern zu können. Über die gewonnenen Statistiken können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Weiterhin nutzen wir das System für Maßnahmen zum Schutz der Sicherheit der Website, z.B. dem Erkennen von Angriffen oder Viren. Für die Ausnahmefälle, in denen personenbezogene Daten in die USA übertragen werden, hat sich Automattic Inc. dem EU-US Privacy Shield unterworfen, https://www.privacyshield.gov. Rechtsgrundlage für die Nutzung von Jetpack ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

10.2. Für diese Auswertung werden Cookies (näheres dazu in Ziffer 2) auf Ihrem Computer gespeichert. Die so erhobenen Informationen werden auf einem Server in den USA gespeichert. Wenn Sie die Speicherung der Cookies verhindern, weisen wir darauf hin, dass Sie gegebenenfalls diese Website nicht vollumfänglich nutzen können. Die Verhinderung der Speicherung von Cookies ist möglich durch die Einstellung in ihrem Browser oder indem Sie den Button „Click here to Opt-out" unter http://www.quantcast.com/opt-out betätigen.

10.3. Diese Website verwendet Jetpack mit einer Erweiterung, durch die IP-Adressen direkt nach ihrer Erhebung gekürzt weiterverarbeitet werden, um so eine Personenbeziehbarkeit auszuschließen.

10.4. Informationen des Drittanbieters: Automattic Inc., 6029th Street #343, San Francisco, CA 94110–4929, USA, https://automattic.com/privacy, sowie des Drittanbieters der Trackingtechnologie: Quantcast Inc., 2013rd St, Floor 2, San Francisco, CA 94103–3153, USA, https://www.quantcast.com/privacy.

11. Einsatz von Adobe Analytics (Omniture)

11.1. Diese Website nutzt den Webanalysedienst Adobe Analytics (Omniture), um die Nutzung unserer Website analysieren und regelmäßig verbessern zu können. Über die gewonnenen Statistiken können wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten. Für die Ausnahmefälle, in denen personenbezogene Daten in die USA übertragen werden, hat sich Adobe dem EU-US Privacy Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework. Rechtsgrundlage für die Nutzung von Adobe Analytics ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

11.2. Für diese Auswertung werden Cookies (näheres dazu in Ziffer 2) auf Ihrem Computer gespeichert. Die so erhobenen Informationen werden auf Servern, auch in den USA, gespeichert. Wenn Sie die Speicherung der Cookies verhindern, weisen wir darauf hin, dass Sie dann gegebenenfalls diese Website nicht vollumfänglich nutzen können. Die Verhinderung der Speicherung von Cookies ist möglich durch die Einstellung in ihrem Browser oder indem Sie die Buttons „Abmelden" unter http://www.adobe.com/de/privacy/opt-out.html betätigen.

11.3. Diese Website verwendet Adobe Analytics (Omniture) mit den Einstellungen „Before Geo-Lookup: Replace visitor's last IP octet with 0" und „Obfuscate IP-Removed", durch die Ihre IP-Adresse um das letzte Oktett gekürzt und durch eine generische IP-Adresse, also eine nicht mehr zuordenbare, ersetzt wird. Eine Personenbeziehbarkeit ist damit auszuschließen.

11.4. Informationen des Drittanbieters: Adobe Systems Software Ireland Limited, Ireland, 4–6 Riverwalk, Citywest Business Campus, Dublin 24, Republic of Ireland; privacy@adobe.com; Datenschutzhinweise:http://www.adobe.com/de/privacy/policy.html.

12. Einsatz von Social-Media-Plug-ins

12.1. Wir setzen derzeit folgende Social-Media-Plug-ins ein: Facebook, Google+, Twitter, Xing, T3N, LinkedIn, Flattr. Wir nutzen dabei die sog. Zwei-Klick-Lösung. Das heißt, wenn Sie unsere Seite besuchen, werden zunächst grundsätzlich keine personenbezogenen Daten an die Anbieter der Plug-ins weitergegeben. Den Anbieter des Plug-ins erkennen Sie über die Markierung auf dem Kasten über seinen Anfangsbuchstaben oder das Logo. Wir eröffnen Ihnen die Möglichkeit, über den Button direkt mit dem Anbieter des Plug-ins zu kommunizieren. Nur wenn Sie auf das markierte Feld klicken und es dadurch aktivieren, erhält der Plug-in-Anbieter die Information, dass Sie die entsprechende Website unseres Online-Angebots aufgerufen haben. Zudem werden die unter Ziffer 2 dieser Erklärung genannten Daten übermittelt. Im Fall von Facebook wird nach Angaben der jeweiligen Anbieter in Deutschland die IP-Adresse sofort nach Erhebung anonymisiert. Durch die Aktivierung des Plug-ins werden also personenbezogene Daten von Ihnen an den jeweiligen Plug-in-Anbieter übermittelt und dort (bei US-amerikanischen Anbietern in den USA) gespeichert. Da der Plug-in-Anbieter die Datenerhebung insbesondere über Cookies vornimmt, empfehlen wir Ihnen, vor dem Klick auf den ausgegrauten Kasten über die Sicherheitseinstellungen Ihres Browsers alle Cookies zu löschen.

12.2. Wir haben weder Einfluss auf die erhobenen Daten und Datenverarbeitungsvorgänge, noch sind uns der volle Umfang der Datenerhebung, die Zwecke der Verarbeitung, die Speicherfristen bekannt. Auch zur Löschung der erhobenen Daten durch den Plug-in-Anbieter liegen uns keine Informationen vor.

12.3. Der Plug-in-Anbieter speichert die über Sie erhobenen Daten als Nutzungsprofile und nutzt diese für Zwecke der Werbung, Marktforschung und/oder bedarfsgerechten Gestaltung seiner Website. Eine solche Auswertung erfolgt insbesondere (auch für nicht eingeloggte Nutzer) zur Darstellung von bedarfsgerechter Werbung und um andere Nutzer des sozialen Netzwerks über Ihre Aktivitäten auf unserer Website zu informieren. Ihnen steht ein Widerspruchsrecht gegen die Bildung dieser Nutzerprofile zu, wobei Sie sich zur Ausübung dessen an den jeweiligen Plug-in-Anbieter wenden müssen. Über die Plug-ins bieten wir Ihnen die Möglichkeit, mit den sozialen Netzwerken und anderen Nutzern zu interagieren, so dass wir unser Angebot verbessern und für Sie als Nutzer interessanter ausgestalten können. Rechtsgrundlage für die Nutzung der Plug-ins ist Art. 6 Abs. 1 S. 1 lit. f DS-GVO.

12.4. Die Datenweitergabe erfolgt unabhängig davon, ob Sie ein Konto bei dem Plug-in-Anbieter besitzen und dort eingeloggt sind. Wenn Sie bei dem Plug-in-Anbieter eingeloggt sind, werden Ihre bei uns erhobenen Daten direkt Ihrem beim Plug-in-Anbieter bestehenden Konto zugeordnet. Wenn Sie den aktivierten Button betätigen und z. B. die Seite verlinken, speichert der Plug-in-Anbieter auch diese Information in Ihrem Nutzerkonto und teilt sie Ihren Kontakten öffentlich mit. Wir empfehlen Ihnen, sich nach Nutzung eines sozialen Netzwerks regelmäßig auszuloggen, insbesondere jedoch vor Aktivierung des Buttons, da Sie so eine Zuordnung zu Ihrem Profil bei dem Plug-in-Anbieter vermeiden können.

12.5. Weitere Informationen zu Zweck und Umfang der Datenerhebung und ihrer Verarbeitung durch den Plug-in-Anbieter erhalten Sie in den im Folgenden mitgeteilten Datenschutzerklärungen dieser Anbieter. Dort erhalten Sie auch weitere Informationen zu Ihren diesbezüglichen Rechten und Einstellungsmöglichkeiten zum Schutze Ihrer Privatsphäre.

12.6. Adressen der jeweiligen Plug-in-Anbieter und URL mit deren Datenschutzhinweisen:

12.6.1. Facebook Inc., 1601 S California Ave, Palo Alto, California 94304, USA; http://www.facebook.com/policy.php; weitere Informationen zur Datenerhebung: http://www.facebook.com/help/186325668085084, http://www.facebook.com/about/privacy/your-info-on-other#applications sowie http://www.facebook.com/about/privacy/your-info#everyoneinfo. Facebook hat sich dem EU-US-Privacy-Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.

12.6.2. Google Inc., 1600 Amphitheater Parkway, Mountainview, California 94043, USA; https://www.google.com/policies/privacy/partners/?hl=de. Google hat sich dem EU-US-Privacy-Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.

12.6.3. Twitter, Inc., 1355 Market St, Suite 900, San Francisco, California 94103, USA; https://twitter.com/privacy. Twitter hat sich dem EU-US-Privacy-Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.

13. Einbindung von YouTube-Videos

13.1. Wir haben YouTube-Videos in unser Online-Angebot eingebunden, die auf http://www.YouTube.com gespeichert sind und von unserer Website aus direkt abspielbar sind. Diese sind alle im „erweiterten Datenschutz-Modus" eingebunden, d. h., dass keine Daten über Sie als Nutzer an YouTube übertragen werden, wenn Sie die Videos nicht

abspielen. Erst wenn Sie die Videos abspielen, werden die in Absatz 2 genannten Daten übertragen. Auf diese Datenübertragung haben wir keinen Einfluss.

13.2. Durch den Besuch auf der Website erhält YouTube die Information, dass Sie die entsprechende Unterseite unserer Website aufgerufen haben. Zudem werden die unter Ziffer 2 dieser Erklärung genannten Daten übermittelt. Dies erfolgt unabhängig davon, ob YouTube ein Nutzerkonto bereitstellt, über das Sie eingeloggt sind, oder ob kein Nutzerkonto besteht. Wenn Sie bei Google eingeloggt sind, werden Ihre Daten direkt Ihrem Konto zugeordnet. Wenn Sie die Zuordnung mit Ihrem Profil bei YouTube nicht wünschen, müssen Sie sich vor Aktivierung des Buttons ausloggen. YouTube speichert Ihre Daten als Nutzungsprofile und nutzt sie für Zwecke der Werbung, Marktforschung und/oder bedarfsgerechten Gestaltung seiner Website. Eine solche Auswertung erfolgt insbesondere (selbst für nicht eingeloggte Nutzer) zur Erbringung von bedarfsgerechter Werbung und um andere Nutzer des sozialen Netzwerks über Ihre Aktivitäten auf unserer Website zu informieren. Ihnen steht ein Widerspruchsrecht zu gegen die Bildung dieser Nutzerprofile, wobei Sie sich zur Ausübung dessen an YouTube richten müssen.

13.3. Weitere Informationen zu Zweck und Umfang der Datenerhebung und ihrer Verarbeitung durch YouTube erhalten Sie in der Datenschutzerklärung. Dort erhalten Sie auch weitere Informationen zu Ihren Rechten und Einstellungsmöglichkeiten zum Schutze Ihrer Privatsphäre: https://www.google.de/intl/de/policies/privacy. Google verarbeitet Ihre personenbezogenen Daten auch in den USA und hat sich dem EU-US-Privacy-Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.

13.4. Informationen des Drittanbieters: Google Dublin, Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland, Fax: +353 (1) 4361001. Nutzerbedingungen: http://www.google.com/analytics/terms/de.html, Übersicht zum Datenschutz: http://www.google.com/intl/de/analytics/learn/privacy.html, sowie die Datenschutzerklärung: http://www.google.de/intl/de/policies/privacy.

14. Einbindung von Google Maps

14.1. Auf dieser Webseite nutzen wir das Angebot von Google Maps. Dadurch können wir Ihnen interaktive Karten direkt in der Website anzeigen und ermöglichen Ihnen die komfortable Nutzung der Karten-Funktion.

14.2. Durch den Besuch auf der Website erhält Google die Information, dass Sie die entsprechende Unterseite unserer Website aufgerufen haben. Zudem werden die unter Ziffer 2 dieser Erklärung genannten Daten übermittelt. Dies erfolgt unabhängig davon, ob Google ein Nutzerkonto bereitstellt, über das Sie eingeloggt sind, oder ob kein Nutzerkonto besteht. Wenn Sie bei Google eingeloggt sind, werden Ihre Daten direkt Ihrem Konto zugeordnet. Wenn Sie die Zuordnung mit Ihrem Profil bei Google nicht wünschen, müssen Sie sich vor Aktivierung des Buttons ausloggen. Google speichert Ihre Daten als Nutzungsprofile und nutzt sie für Zwecke der Werbung, Marktforschung und/oder bedarfsgerechten Gestaltung seiner Website. Eine solche Auswertung erfolgt insbesondere (selbst für nicht eingeloggte Nutzer) zur Erbringung von bedarfsgerechter Werbung und um andere Nutzer des sozialen Netzwerks über Ihre Aktivitäten auf unserer Website zu informieren. Ihnen steht ein Widerspruchsrecht zu gegen die Bildung dieser Nutzerprofile, wobei Sie sich zur Ausübung dessen an Google richten müssen.

14.3. Weitere Informationen zu Zweck und Umfang der Datenerhebung und ihrer Verarbeitung durch den Plug-in-Anbieter erhalten Sie in den Datenschutzerklärungen des Anbieters. Dort erhalten Sie auch weitere Informationen zu Ihren diesbezüglichen Rechten und Einstellungsmöglichkeiten zum Schutze Ihrer Privatsphäre: http://www.google.de/intl/de/policies/privacy. Google verarbeitet Ihre personenbezogenen Daten auch in den USA und hat sich dem EU-US Privacy Shield unterworfen, https://www.privacyshield.gov/EU-US-Framework.

14.4. Informationen des Drittanbieters: Google Dublin, Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland, Fax: +353 (1) 4361001. Nutzerbedingungen: http://www.google.com/analytics/terms/de.html, Übersicht zum Datenschutz: http://www.google.com/intl/de/analytics/learn/privacy.html, sowie die Datenschutzerklärung: http://www.google.de/intl/de/policies/privacy.

15. Datensicherheit

Wir haben geeignete technische und organisatorische Maßnahme ergriffen, die eine angemessene Sicherheit Ihrer personenbezogenen Daten gewährleisten. Das gilt insbesondere für den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

16. Betroffenenrechte

16.1. Unter der Datenschutz-Grundverordnung stehen Ihnen die unten genannten Rechte zu. Bitte haben Sie dafür Verständnis, dass einzelne Rechte in bestimmten Fällen eingeschränkt sein können. Sollte dies der Fall sein, werden wir Ihnen den Grund hierfür mitteilen.

16.1.1. Recht auf Widerruf (Art. 7 Abs. 3 DS-GVO)

Sie haben nach Art. 7 Abs. 3 DS-GVO das Recht, Ihre Einwilligung jederzeit zu widerrufen.

16.1.2. Recht auf Auskunft (Art. 15 DS-GVO)

Sie können Auskunft gemäß Art. 15 DS-GVO über Ihre von uns verarbeiteten personenbezogenen Daten verlangen. In Ihrem Auskunftsantrag sollten Sie Ihr Anliegen präzisieren, um uns das Zusammenstellen der erforderlichen Daten zu erleichtern. Bitte beachten Sie, dass Ihr Auskunftsrecht unter bestimmten Umständen gemäß den gesetzlichen Vorschriften eingeschränkt sein kann.

16.1.3. Recht auf Berichtigung (Art. 16 DS-GVO)
Sollten die Sie betreffenden Angaben nicht (mehr) zutreffend sein, können Sie nach Art. 16 DS-GVO eine Berichtigung verlangen. Sollten Ihre Daten unvollständig sein, können Sie eine Vervollständigung verlangen.

16.1.4. Recht auf Löschung (Art. 17 DS-GVO)
Sie können unter den Bedingungen des Art. 17 DS-GVO die Löschung Ihrer personenbezogenen Daten verlangen. Ihr Anspruch auf Löschung hängt u. a. davon ab, ob die Sie betreffenden Daten von uns zur Erfüllung einer rechtlichen Verpflichtung noch benötigt werden.

16.1.5. Recht auf Einschränkung der Datenverarbeitung (Art. 18 DS-GVO)
Sie haben im Rahmen der Vorgaben des Art. 18 DS-GVO das Recht, eine Einschränkung der Verarbeitung der Sie betreffenden Daten zu verlangen.

16.1.6. Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)
Sie haben nach Art. 20 DS-GVO das Recht, Ihre Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

16.1.7. Recht auf Widerspruch (Art. 21 DS-GVO)
Sie haben nach Art. 21 DS-GVO das Recht, jederzeit der Verarbeitung der Sie betreffenden Daten zu widersprechen, sofern wir Ihre Daten aufgrund von Art. 6 Abs. 1 lit. e oder f DS-GVO verarbeiten oder sofern wir Ihre Daten verarbeiten, um Direktwerbung zu betreiben.

16.1.8. Für die Ausübung Ihrer in Ziffer 2.1.1 bis 2.1.7 bezeichneten Rechte wenden Sie sich bitte an die unter Ziffer 1 genannten Kontaktadressen.

16.2. Wenn Sie der Auffassung sind, dass wir bei der Verarbeitung Ihrer Daten datenschutzrechtliche Vorschriften nicht beachtet haben, können Sie sich nach Art. 77 DS-GVO mit einer Beschwerde an die zuständige Aufsichtsbehörde wenden. Die für unsere RLC zuständige Aufsichtsbehörde ist das Bayrische Landesamt für Datenschutzaufsicht (BayLDA), Postfach 606, 91511 Ansbach, poststelle@lda.bayern.de.

17. Ansprechpartner

17.1. Für die Geltendmachung Ihrer Rechte oder für Anregungen und Verbesserungsvorschläge können Sie sich gerne an unseren Datenschutzbeauftragten wenden.

17.2. Unser Datenschutzbeauftragter ist XXX. Sie können unseren Datenschutzbeauftragten unter der E-Mailadresse XXX@XXX.de erreichen.

18. Änderungen

18.1. Diese Datenschutzerklärung kann von Zeit zu Zeit geändert werden, z.B. um sie rechtlichen Rahmenbedingungen oder tatsächlichen Gegebenheiten anzupassen. Alle Änderungen der Datenschutzerklärung werden von uns auf dieser Seite veröffentlicht.

18.2. Diese Datenschutzerklärung ist auf dem Stand vom XX.XX.XXXX.

XIV. *Anhang 14: Datenschutzerklärung für Facebook*

Datenschutzerklärung für Facebook (RLC XY)

1. Information über die Erhebung personenbezogener Daten

1.1. Im Folgenden informieren wir über die Erhebung personenbezogener Daten bei Nutzung dieser Facebook-Fanpage. Bitte nehmen Sie sich einen Augenblick Zeit, um sich mit den Informationen vertraut zu machen.

1.2. Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder eine identifizierbare natürliche Person beziehen.

1.3. Verantwortliche für die Datenverarbeitung gem. Art. 4 Nr. 7 Datenschutz-Grundverordnung (DS-GVO) sind im Wege der gemeinsamen Verantwortlichkeit (gem. Art. 26 Abs. 1 S.1 DS-GVO):

1.3.1. *der Refugee Law Clinic XY* nachfolgend „RLCXY", „wir" oder „uns"). Sie können uns unter der E-Mailadresseinfo@rlcbeispieladresse.de erreichen;

1.3.2. die *Facebook Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland* (nachfolgend „Facebook"). Sie können Facebook über ihr Kontaktformular oder per Post bei der soeben angegebenen Adresse erreichen.

2. Erhebung personenbezogener Daten beim Aufruf dieser Facebook-Fanpage

2.1. Bei dem Aufruf dieser Facebook-Fanpage können von Facebook Daten über Sie durch Cookies erhoben werden, unabhängig davon, ob Sie ein Facebook-Konto besitzen oder nicht. Über den Einsatz dieser Cookies entscheidet alleine Facebook. Wir haben hierauf keinen Einfluss. Rechtsgrundlage für das Setzen von Cookies ist Ihre Einwilligung (gem. Art. 6 Abs. 1 lit. a., Art. 7 DS-GVO), die Sie durch die Nutzung der Facebook-Webseiten erteilen.

2.2. Als Betreiber dieser Fanpage sind aber auch wir Verantwortlicher im Sinne des Datenschutzrechts. Dies bedeutet, dass auch wir dafür einstehen muss, dass Ihre Daten über diese Fanpage rechtmäßig verarbeitet werden und dass Sie Ihre Rechte bezüglich Ihrer Daten auch gegenüber uns ausüben können.

2.3. Bei den von Facebook verwendeten Cookies handelt es sich um Datenpakete, die die Computer, Smartphones und sonstigen Endgeräte des Nutzers mit einer bestimmten Kennung markieren. Sie werden regelmäßig beim Besuch einer Facebook-Seite, darunter auch dieser Fanpage, auf dem Endgerät des Nutzers gespeichert. Cookies werden vor allem gesetzt, um den Besuchern der Facebook-Webseiten, darunter auch einer Fanpage, personalisierte Werbung anzeigen zu können. Dies geschieht dadurch, dass dem Nutzer auf Facebook (d.h. auch auf der Fanpage) Anzeigen von Werbepartnern von Facebook angezeigt werden, deren Webseiten der Nutzer zuvor besucht hat. Daneben ermöglichen es Cookies, Statistiken über die Nutzung einer Fanpage zu erstellen, sodass Facebook und wir die Nutzung einer Fanpage nachvollziehen können.

2.4. Die Erfassung Ihrer Daten durch Cookies im Rahmen der Nutzung der Fanpage ist weder gesetzlich noch vertraglich vorgeschrieben. Auch ist dies nicht für einen Vertragsschluss erforderlich. Eine Verpflichtung zur Übermittlung Ihrer Daten an Facebook besteht daher nicht. Die Nichtübermittlung Ihrer Daten (z.B. durch Blockieren von Cookies) hat jedoch zur Folge, dass wir Ihnen die Fanpage nicht oder nur eingeschränkt anbieten können.

2.5. Ihre Daten können durch die Cookies von Facebook an Facebook Inc. in den USA weitergegeben werden. Facebook ist für den EU-US-Privacy-Shield zertifiziert, d.h. Facebook muss Nutzern in Europa gegenüber einen Datenschutzstandard einhalten, der von der Europäischen Kommission für mit dem europäischen Standard vergleichbar befunden wurde.

2.6. Zweck und Umfang der Datenerhebung und die weitere Verarbeitung und Nutzung der Daten durch Facebook sowie die diesbezüglichen Rechte und Einstellungsmöglichkeiten zum Schutz der Privatsphäre der Nutzer, können Sie den Datenschutzhinweisen von Facebook und der Cookie-Richtlinie von Facebook entnehmen. Sie können ferner Ihre eigenen Facebook – Daten direkt bei Facebook herunterladen (Herunterladen des sog. „erweiterten Archivs" in Ihren Account – Einstellungen).

2.7. Für die Betroffenen besteht die Möglich die Verknüpfung der erhobenen Daten mit einschlägigen Werbeinhalten durch Facebook einzuschränken. Dazu bietet Facebook eine sog. Opt-Out-Möglichkeit auf ihrer eigenen Website. Zudem kann dafür der Service Your Online Choices herangezogen werden.

3. Vereinbarung zwischen den Verantwortlichen und Datensicherheit

3.1. Wir haben mit Facebook die gem. Art. 26 Abs. 1 S. 2 DS-GVO zwischen gemeinsamen Verantwortlichen verpflichtende Vereinbarung (sog. „Controller Addendum") getroffen, in der insbesondere die datenschutzrechtlichen Verpflichtungen und die Umsetzung von Betroffenenrechten vereinbart sind. Diese Vereinbarung kann hier abgerufen werden.

3.2. Wir haben geeignete technische und organisatorische Maßnahme ergriffen, die eine angemessene Sicherheit Ihrer personenbezogenen Daten gewährleisten. Das gilt insbesondere für den Schutz vor unbefugter oder

unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

4. Betroffenenrechte

4.1. Unter der Datenschutz-Grundverordnung stehen Ihnen die unten genannten Rechte zu. Bitte haben Sie dafür Verständnis, dass einzelne Rechte in bestimmten Fällen eingeschränkt sein können. Sollte dies der Fall sein, werden wir Ihnen den Grund hierfür mitteilen.

4.1.1. Recht auf Widerruf (Art. 7 Abs. 3 DS-GVO)
Sie haben nach Art. 7 Abs. 3 DS-GVO das Recht, Ihre Einwilligung jederzeit zu widerrufen.

4.1.2. Recht auf Auskunft (Art. 15 DS-GVO)
Sie können Auskunft gemäß Art. 15 DS-GVO über Ihre von uns verarbeiteten personenbezogenen Daten verlangen. In Ihrem Auskunftsantrag sollten Sie Ihr Anliegen präzisieren, um uns das Zusammenstellen der erforderlichen Daten zu erleichtern. Bitte beachten Sie, dass Ihr Auskunftsrecht unter bestimmten Umständen gemäß den gesetzlichen Vorschriften eingeschränkt sein kann.

4.1.3. Recht auf Berichtigung (Art. 16 DS-GVO)
Sollten die Sie betreffenden Angaben nicht (mehr) zutreffend sein, können Sie nach Art. 16 DS-GVO eine Berichtigung verlangen. Sollten Ihre Daten unvollständig sein, können Sie eine Vervollständigung verlangen.

4.1.4. Recht auf Löschung (Art. 17 DS-GVO)
Sie können unter den Bedingungen des Art. 17 DS-GVO die Löschung Ihrer personenbezogenen Daten verlangen. Ihr Anspruch auf Löschung hängt u. a. davon ab, ob die Sie betreffenden Daten von uns zur Erfüllung einer rechtlichen Verpflichtung noch benötigt werden.

4.1.5. Recht auf Einschränkung der Datenverarbeitung (Art. 18 DS-GVO)
Sie haben im Rahmen der Vorgaben des Art. 18 DS-GVO das Recht, eine Einschränkung der Verarbeitung der Sie betreffenden Daten zu verlangen.

4.1.6. Recht auf Datenübertragbarkeit (Art. 20 DS-GVO)
Sie haben nach Art. 20 DS-GVO das Recht, Ihre Daten, die Sie uns bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.

4.1.7. Recht auf Widerspruch (Art. 21 DS-GVO)
Sie haben nach Art. 21 DS-GVO das Recht, jederzeit der Verarbeitung der Sie betreffenden Daten zu widersprechen, sofern wir Ihre Daten aufgrund von Art. 6 Abs. 1 lit. e oder f DS-GVO verarbeiten oder sofern wir Ihre Daten verarbeiten, um Direktwerbung zu betreiben.

4.1.8. Für die Ausübung Ihrer in Ziffer 4.1.1 bis 4.1.7 bezeichneten Rechte wenden Sie sich bitte an die unter Ziffer 1.3 genannten Kontaktadressen der Verantwortlichen.

4.2. Wenn Sie der Auffassung sind, dass wir bei der Verarbeitung Ihrer Daten datenschutzrechtliche Vorschriften nicht beachtet haben, können Sie sich nach Art. 77 DS-GVO mit einer Beschwerde an die zuständige Aufsichtsbehörde wenden.

5. Ansprechpartner

5.1. Ihre Betroffenenrechte (gem. Ziff. 4 dieser DS-Erklärung) können Sie sowohl gegenüber Facebook, als auch gegenüber uns geltend machen. Wir sind durch das Controller Addendum (Ziff. 3.1) verpflichtet diese Anfragen unverzüglich, spätestens jedoch innerhalb von 7 Kalendertagen, an Facebook weiterzuleiten.

5.2. Deshalb möchten wir Sie darauf hinweisen, dass im Fall von Auskunftsanfragen und der Geltendmachung von Betroffenenrechten, diese am effektivsten **direkt bei Facebook** geltend gemacht werden können. Nur Facebook hat jeweils Zugriff auf die Daten der Nutzer und kann direkt entsprechende Maßnahmen ergreifen und Auskünfte geben. Für eine Kontaktaufnahme zu Facebook nutzen Sie am besten das in Ziff. 1.3.2. dieser DS-Erklärung genannte Kontaktformular.

6. Änderungen

6.1. Diese Datenschutzerklärung kann von Zeit zu Zeit geändert werden, z.B. um sie rechtlichen Rahmenbedingungen oder tatsächlichen Gegebenheiten anzupassen. Alle Änderungen der Datenschutzerklärung werden von uns auf dieser Seite veröffentlicht.

6.2. Diese Datenschutzerklärung ist auf dem Stand vom XX.XX.XXXX.

XV. *Anhang 15: Abwägungshilfe für berechtigte Interessen (3x5 Matrix)*

Die nachfolgende Matrix stammt von Herfurth, ZD 2018, 514 und soll als Anhaltspunkt für die Abwägung der Interessen der*des Betroffenen mit den Interessen des Verantwortlichen dienen.

Eine genaue Erläuterung zu den einzelnen Kriterien und zur Verwendung dieser Matrix findet sich bei der angegeben Fundstelle.

	Gering	Mittel	Schwer
Daten			
Personenbezug der Daten			
Art der Daten			
Menge der Daten			
Quelle der Daten			
Qualität der Daten			
Akteure			
Menge der datenverarbeitenden Akteure			
Menge der betroffenen Personen			
Machtverhältnis zwischen Verantwortlichem und betroffener Person			
Vernünftige Erwartungen der betroffenen Person			
Drittstaatbezug eines			

datenverarbeitenden Akteurs			
Verarbeitung			
Art der Datenerhebung			
Art der Datenverarbeitung			
Dauer der Datenspeicherung			
Häufigkeit der Datenverarbeitung			
Zwecke der Datenverarbeitung			

F. Urheberrechtliche Hinweise

- Das verwendete Symbol “Lightbulb idea free icon” wurde erstellt von [Freepik] und stammt von www.flaticon.com.

- Das verwendete Symbol “Attachment free icon” wurde erstellt von [Chanut] und stammt von www.flaticon.com.

- Das verwendete Symbol “Rubbish bin free icon” wurde erstellt von [Icon Works] und stammt von www.flaticon.com.

- Die verwendeten Screenshots unter *C.II.1* stammen in Teilen von 9dreamstudio – www.Fotolia.com.