



## Datenschutzrechtliche Empfehlungen zur Erstellung einer Einwilligungserklärung im Rahmen von Forschungsvorhaben

Teilnehmende an Forschungsvorhaben (Versuchspersonen) haben ein Recht auf den Schutz ihrer personenbezogenen Daten. Teilnehmende müssen in die Nutzung der personenbezogenen Daten einwilligen. In aller Regel erfolgt diese Einwilligung mit Hilfe einer Einwilligungserklärung von Seiten der Versuchsperson. Im Folgenden werden Ihnen Hinweise zur Erstellung einer Einwilligungserklärung gegeben, die sich aus der Datenschutz-Grundverordnung ([DSGVO](#)) ergeben. Details zu Ihren Informationspflichten gegenüber Teilnehmern und Teilnehmerinnen an Studien finden Sie in [Artikel 13 ff.](#) der DSGVO.

Darüber hinaus muss die Einwilligungserklärung in Einklang mit den forschungsethischen Richtlinien der DGPs stehen, die in den [berufsethischen Richtlinien](#) formuliert sind. Die Ethikkommissionen prüfen Ihre Angaben zu den mit dem Datenschutz beauftragten Personen und Aufsichtsbehörden nicht auf Richtigkeit. Datenschutzrechtliche Aspekte von Forschungsvorhaben werden durch die Ethikkommission grundsätzlich nur cursorisch geprüft. Das Votum der Ethikkommission ersetzt nicht die Konsultation von zuständigen Datenschutzbeauftragten. Ziehen Sie Datenschutzbeauftragte insbesondere hinzu, wenn Sie planen, sensible personenbezogene Daten zu verarbeiten.

Zu Beginn finden Sie allgemeine Informationen zu datenschutzrechtlichen Einwilligungen und deren gesetzlichen Grundlagen. Ein Muster mit Ausfüllhilfen finden Sie im zweiten Teil des Textes. Am Ende finden Sie noch eine Liste der Landesdatenschutzbehörden.

### Teil 1: Grundsätzliches zu Einwilligungen und Informationspflicht

Bei Forschungsvorhaben kann man in den meisten Fällen davon ausgehen, dass es keine gesetzliche Grundlage für die Erhebung der Daten gibt. Eine Einwilligung in die Erhebung personenbezogener Daten durch die Teilnehmenden ist daher erforderlich.

Nach Art. 4 Ziffer 11 DSGVO ist „eine ‚Einwilligung‘ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung [...] mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.“ Personenbezogene Daten sind (Art. 4, Ziffer 1 DSGVO) „[...] 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“

Wenn Forschende eine datenschutzrechtliche Einwilligung einholen, um personenbezogene Daten zu erheben, muss gleichzeitig der gesetzlichen Informationspflicht nachgekommen werden. Beispiele dafür finden Sie im zweiten Teil.

Folgende Anforderungen an Einwilligungen müssen grundsätzlich erfüllt sein:

#### a. Nachweis,

dass eine Einwilligung abgegeben wurde. Der/Die Verantwortliche muss eine Einwilligung für die Erhebung der personenbezogenen Daten vorweisen können. Eine schriftliche Form ist nicht zwingend notwendig, erleichtert aber den späteren Nachweis. Die Einwilligung kann

per Unterschrift in Papierform oder elektronisch erfolgen. Bei letzterem muss [§ 126a BGB](#) beachtet werden (Namen, qualifizierte elektronische Signatur<sup>1</sup>).

**b. Nennung des/der Verantwortlichen**

Am besten mit Briefkopf, Nennung des/der Verantwortlichen inkl. kompletter Anschrift.

**c. Informiertheit**

Die Versuchsperson ist über Art, Umfang und Zweck der Erhebung und Speicherung der personenbezogenen Daten ausführlich schriftlich und für sie verständlich zu unterrichten. Wenn die Verarbeitung mehreren Zwecken dient, sollten für alle Verarbeitungszwecke Einwilligungen abgegeben werden. Den Teilnehmenden muss die Möglichkeit gegeben werden, Fragen zu stellen. Die Einwilligung muss in einer klaren und einfachen Sprache erfolgen. Die Einwilligung muss von anderen Sachverhalten klar zu unterscheiden sein. Die Einwilligung muss aktiv erfolgen, z. B. durch Ankreuzen von Optionen (opt-in Verfahren).

**d. Der/Die Einwilligende muss mindestens 16 Jahre alt sein**

Für die Verarbeitung von personenbezogenen Daten von Kindern/Jugendlichen müssen die Eltern/Sorgeberechtigten bis zum vollendeten 16. Lebensjahr einwilligen (Art. 8 DSGVO).

**e. Rechte des/der Einwilligenden**

Die Teilnehmer/-innen einer Studie haben das Recht auf Widerspruch, Auskunft, Datenübertragbarkeit, Löschung, Einschränkung der Verarbeitung und Berichtigung. Auf diese Rechte und die Möglichkeit zur Wahrnehmung derselben muss hingewiesen werden (Ansprechpartner/-innen mit Kontaktdaten nennen).

**f. Freiwilligkeit**

Die Teilnahme an der Untersuchung muss freiwillig sein. Eine Kopplung an andere Dienste oder einen Vertrag ist unzulässig. Eine allgemeingültige, uneingeschränkte Einwilligung ist ebenso nicht möglich. Es muss eine konkrete Zweckbindung der Datenverarbeitung gegeben sein. Der/Die Einwilligende muss eine „echte“ Wahl haben, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

## **Was ist zu beachten, wenn eine Studie geplant wird?**

Ein Merkblatt zum Datenschutz bei Studien mit Patienten und Patientinnen hat z. B. der Bayerische Landesbeauftragte für den Datenschutz herausgegeben ([https://www.datenschutz-bayern.de/technik/orient/merkblatt\\_med\\_studien.html](https://www.datenschutz-bayern.de/technik/orient/merkblatt_med_studien.html), Abfrage 01.09.2018).

### **Beschreibung des Arbeitsablaufs**

Eine Beschreibung der Erhebung und Verarbeitung der personenbezogenen Daten ist zur Beurteilung der Datenschutzkonformität essentiell. Typische anzusprechende Punkte (keine erschöpfende Liste) sind

- Aufnahme der Versuchsperson in eine Studie
- Erhebung der Daten
- Evtl. Entnahme von Proben/Erstellung von Aufnahmen
- Beschriftung der Proben/Aufnahmen
- Übermittlung von Daten und/oder Proben/Aufnahmen
- Wissenschaftliche Auswertung, Veröffentlichung von Ergebnissen

---

<sup>1</sup> Eine qualifizierte elektronische Signatur ist eine Signatur, die zum Zeitpunkt der Unterschrift auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wurde.

- Widerruf der Teilnahme durch die Versuchsperson, inkl. Datenlöschung, Vernichtung von Proben, Auskunft über gespeicherte personenbezogene Daten an Teilnehmende
- Art und Dauer der Datenspeicherung.

### Qualitätssicherung, Monitoring

Es muss festgelegt sein, wer zum Zugriff auf die Daten berechtigt ist, wie dieser Zugriff erfolgt und auf welche Daten zugegriffen werden darf. Der Zugriff kann entsprechend den Empfehlungen der DGPs zum Management und der Bereitstellung von Forschungsdaten<sup>2</sup> grundsätzlich in vier Zugriffsklassen unterteilt werden. Die offenste Form des Datenzugriffs ist die Zugriffsklasse 0 („open data“), da sie weder eine Restriktion des Zugriffs noch der Nutzung vorsieht. Die Zugriffsklassen 1 („open data/conditional access“) und 2 („restricted access“) beinhalten hingegen vertraglich definierte Einschränkungen bezüglich Zugriff und Nutzung. So kann die Nutzung bei Zugriffsklasse 1 beispielsweise auf ausschließlich wissenschaftliche Zwecke beschränkt werden (der sog. „Scientific Use Case“); in Zugriffsklasse 2 können individuelle Nutzungsregelungen zur Abdeckung spezieller Konstellationen formuliert werden. Die konservativste Zugriffsregelung ist diejenige, welche der sogenannten Zugriffsklasse 3 („secure use“) entspricht und einen Datenzugriff nur unter streng kontrollierten Bedingungen (z.B. durch ein Forschungsdatenzentrum) vorsieht. Hierzu zählt beispielsweise die kontrollierte Datenfernverarbeitung. Dabei wird eine von Forschenden auf Basis von Testdatensätzen erstellte Syntax an das Forschungsdatenzentrum übermittelt und ausschließlich durch das Personal vor Ort auf Grundlage der Originaldaten verarbeitet.

Sind Daten anonymisiert, kommt die Datenschutz-Grundverordnung (DSGVO) nicht zur Anwendung (s. DSGVO, Erwägungsgrund 26, Satz 6). Anonymisierung bedeutet, dass die Identifizierung einer konkreten Person aufgrund der Informationen, die von ihr bzw. über sie erhoben werden, gar nicht oder nur theoretisch (also mit einem unverhältnismäßig hohen Aufwand) möglich ist<sup>3</sup>. Die DSGVO kommt auch dann nicht zur Anwendung, wenn individuelle Einstellungen, Meinungen, Selbstauskünfte zu Persönlichkeitseigenschaften etc. erhoben werden, jedenfalls dann, wenn sie nach allgemeinem Ermessen<sup>4</sup> keinen Rückschluss auf die Identität der jeweiligen Person zulassen. Die Unterscheidung in faktische und absolute Anonymisierung wurde in der DSGVO aufgegeben.

Im Unterschied zur Anonymisierung bezeichnet Pseudonymisierung die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können. Das ist bspw. dann der Fall, wenn jeder Person ein individueller Code zugeordnet wird, der an sich keinen Rückschluss auf die Identität der jeweiligen Person zulässt. Die zusätzlichen Informationen (also bspw. die Zuordnung von Codes zu Personen) müssen getrennt von den pseudonymisierten Daten aufbewahrt werden. Es müssen technische und organisatorische Maßnahmen ergriffen werden, um sicherzustellen, dass die personenbezogenen Daten nicht einer Person zugeordnet werden können.

Die Bereitstellung von Forschungsdaten im Sinne der DGPs-Empfehlungen sollte auf vertrauenswürdigen Repositorien (und nicht auf privaten Webseiten oder Journal-Webseiten) oder in einem zertifizierten Forschungsdatenzentrum erfolgen. Was als „vertrauenswürdig“ zu bezeichnen ist, wird in den DGPs-Empfehlungen ausführlich erörtert.

---

<sup>2</sup> Gollwitzer, M., Abele-Brehm, A., Fiebach, C. J., Ramthun, R., Scheel, A., Schönbrodt, F. & Steinberg, U. (2021). Management und Bereitstellung von Forschungsdaten in der Psychologie: Überarbeitung der DGPs-Empfehlungen. *Psychologische Rundschau*, 72, 132-146. <https://doi.org/10.1026/0033-3042/a000514>

<sup>3</sup> Laut DSGVO (ErwG 26, Satz 5) sind anonyme Informationen solche, „... die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann.“

<sup>4</sup> Die Formulierung „nach allgemeinem Ermessen“ ist naturgemäß schwammig. Die DSGVO schreibt hierzu: „Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind“ (ErwG 26, Satz 4).

## **Technische Ausgestaltung**

Welche technischen Mittel werden zur Datenerhebung und -verarbeitung herangezogen?  
Wie läuft die elektronische Datenerfassung ab?

(siehe auch Arbeitsablauf)

- Beschreibung der verwendeten Datenbanken und zugehörigen Server (bei wem liegen die Server? Wer betreibt die Software und hat Zugriff auf personenbezogene Daten?)
- Beschreibung der Komponenten bei Datenlieferanten und Datenabrufen (Clients)
- Vernetzungsstruktur zwischen den beteiligten Komponenten
- Verantwortlichkeiten für die Komponenten
- Anwendungen, eingesetzte Software.

## **Technisch-organisatorische Sicherheitsmaßnahmen (TOMS)**

Die Sicherheit der Datenverarbeitung muss gewährleistet sein und die dazu getroffenen Maßnahmen müssen beschrieben werden (§ 32 DSGVO). Dies betrifft unter anderem:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten
- Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- Verfügbarkeit und Zugang zu personenbezogenen Daten bei einem physischen/technischen Zwischenfall rasch wiederherzustellen
- Regelmäßige Überprüfung der TOMS auf Wirksamkeit.

## **Verfahrensverzeichnis**

Eventuell müssen Sie, falls noch nicht in Ihrer Organisation erfolgt, ein Verfahrensverzeichnis erstellen. Ein Verfahrensverzeichnis ist eine Aufstellung aller Verarbeitungstätigkeiten personenbezogener Daten (siehe Arbeitshilfe Verfahrensverzeichnis).

## **Teil 2: Muster mit Ausfüllhilfen**

Der „kursiv“ dargestellte Text dient der Information und sollte gelöscht werden.

Musterformulierungen sind in schwarz formatiert. Verwenden Sie also das Muster, um ein eigenes Dokument für Ihre Einwilligung bspw. auf Ihrem jeweiligen Briefbogen zu erstellen.

Bitte fügen Sie Ihre eigenen Kopf- und Fußzeilen ein und verwenden Sie Ihren Briefkopf. Lassen Sie die Seitenzahlen stehen.

# Datenschutzrechtliche Aufklärung und Einwilligung inkl. Information gem. Art. 13 EU-DSGVO

.....  
Name des Einwilligenden in Druckbuchstaben

geb. am .....

## 1. Ausführliche Beschreibung des Forschungsvorhabens

*Bitte beschreiben Sie Ihr Forschungsvorhaben ausführlich in leicht verständlicher Form. Die teilnehmende Person soll eine Vorstellung dafür bekommen, was in dem Vorhaben untersucht wird. Ethisch problematisches Verhalten (Täuschung usw.) spielt für die datenschutzrechtliche Betrachtung keine Rolle, sehr wohl aber für die forschungsethische Beurteilung. Die teilnehmende Person muss in die Lage versetzt werden, eine Abwägung der Schwere des Eingriffs in die Privatsphäre vorzunehmen.*

## 2. Inhalt und Zweck der Studie

*Der Zweck ist so anzugeben, dass ein Überblick über den Umfang der erhobenen Daten möglich ist. Die Daten können nur für den Zweck des Forschungsvorhabens verwendet werden. Eine spätere „Umwidmung“ ist nicht möglich.*

*Hinweis: Wenn die genaue Verwendung von Daten noch nicht bekannt ist, sollten Forschungsbereiche oder Forschungsprojekte genannt werden. Grundsätzlich sollte der Zweck möglichst weit gefasst werden, um eine nachträgliche erneute Einwilligung in die Datenerhebung zu vermeiden. Eine pauschale Einwilligung ist jedoch nicht möglich.*

*Liegen mehrere Forschungsbereiche vor, müssen alle aufgeführt werden und eine aktive Möglichkeit zur Auswahl (Zustimmung, Ablehnung, opt-in, Art.4 Nr. 11 DSGVO) muss gegeben sein.*

① Zustimmung Fragestellung 1

② Zustimmung Fragestellung 2 usw.

*Möchte der/die Verantwortliche die Daten für einen weiteren/ anderen Zweck weiterverarbeiten als für jenen, für den sie ursprünglich erhoben wurden und für welchen die Einwilligung vorliegt, so muss er/sie die betroffenen Personen vor der Weiterverarbeitung über diesen weiteren Zweck informieren und deren Einwilligung für die Weiterverarbeitung einholen.*

## 3. Betroffener Personenkreis

*Gruppe der anvisierten Teilnehmenden. Gibt es nicht einwilligungsfähige Personen? Werden auch Informationen zu weiteren Personenkreisen (z. B. Partner/innen, Verwandte, Freunde oder Freundinnen ) erhoben?*

## 4. Zu erhebende Daten

*Welche personenbezogenen Daten werden erhoben?*

## 5. Analyseergebnisse der Daten

*Welche Analysen werden aus den Daten gewonnen oder können potentiell gewonnen werden? Ergeben sich durch die Analysen eventuell schützenswerte Daten?*

## 6. Lagerung und Weitergabe von Daten

Wie werden die Daten aufbewahrt bzw. weitergegeben?<sup>5</sup>

## 7. Beteiligte, Datenflüsse und speichernde Stellen

Wer ist an der Studie beteiligt und wie sind die Aufgaben verteilt? Welche Stellen erheben Daten und welche Stellen bewahren sie auf? Was wird an wen weitergegeben und wer hat im Rahmen der Forschungsaufgaben Zugriff auf die Daten (evtl. mit Bezug zu Patienten / Patientinnen oder auf die i.d.R. pseudonymisierten/anonymisierten Forschungsdaten)? Wer übernimmt die Verantwortung für die Einhaltung des Datenschutzes?

Achtung: bei internationalen Studien muss geschaut werden, ob ggf. von Personen, die einen Unterauftrag haben, oder von Kooperationspartnern bzw. -partnerinnen Daten gespeichert werden, wie diese die Daten speichern bzw. ob nur ein zentraler Zugriff auf datenschutzsicheren Servern möglich ist. Werden Daten in Drittländern gespeichert? Bitte beachten Sie, dass Datenflüsse an Einrichtungen Ihrer Universität auch externe Stellen im Sinne des Datenschutzes sein können (z. B.: An-Institute, Institutsambulanzen, Kliniken, Rechenzentrum usw.).

Empfänger/-in 1 (Name, Adresse): \_\_\_\_\_

Daten: \_\_\_\_\_

Empfänger/-in 2 (Name, Adresse): \_\_\_\_\_

Daten: \_\_\_\_\_

## 8. Konkrete Dauer der Speicherung

Geben Sie die Dauer der Datenspeicherung an. Werden sie anschließend gelöscht/gesperrt/anonymisiert (Löschung Zuordnungsschlüssel)? Was passiert mit den Daten bei Dritten? Gibt es rechtliche Grundlagen für die Dauer der Speicherung?

## 9. Pseudonymisierungsverfahren

Ort der Pseudonymisierung; Beschreibung des Gesamtablaufs; Verwaltung der Zuordnung Pseudonym - Probandendaten

## 10. Rechtsgrundlagen

Welche rechtliche Basis erlaubt die Datenerhebung? Meist ist dies die informierte Einwilligung der Teilnehmenden (Aufklärung der Teilnehmer/-innen und Einwilligungserklärung). Die Einwilligung in die Verarbeitung personenbezogener Daten sollte aus Gründen der Nachweisbarkeit schriftlich erfolgen.

Mustertext:

Die Rechtsgrundlage zur Verarbeitung der genannten personenbezogenen Daten bildet die Einwilligung gemäß Art. 6 (1) Buchstabe a EU-DSGVO im zweiten Teil dieses Dokumentes.

---

<sup>5</sup> Planen Sie die Daten auf open-data Servern zu speichern, verwenden Sie für pseudonymisierte Daten nur open-data Server (Forschungsdatenzentren), die die Nutzung auf wissenschaftliche Zwecke begrenzen (scientific use). Alternativ zur Speicherung auf einem open-data Server können Sie auch eine kontrollierte Datenfernverarbeitung anbieten. Dabei wird eine von Forschenden auf der Basis von Testdatensätzen erstellte Syntax an das Forschungsdatenzentrum übermittelt und ausschließlich durch das Personal vor Ort auf Grundlage der Originaldaten verarbeitet.

### **11. Widerruf seitens des/der Betroffenen**

Weisen Sie auf das jederzeitige Widerrufsrecht hin (Art. 21 DSGVO). Führen Sie aus, dass durch den Widerruf die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung nicht berührt wird (Widerruf mit Wirkung für die Zukunft, Art. 7, Abs 3 DSGVO). Was passiert mit übermittelten Daten an Dritte bei Widerruf? (Hinweis: Daten, die im Rahmen von Forschung bereits in Statistiken etc. eingeflossen sind, können i.d.R. nicht rückwirkend herausgenommen werden). Der Widerruf muss so einfach sein wie die Einwilligung.

Was passiert ansonsten bei Widerruf? Z. B. im Forschungskontext: ist die Teilnahme an der Studie damit beendet?

*Mustertext:* Sie haben das Recht, jederzeit die datenschutzrechtliche Einwilligung zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt (Widerruf mit Wirkung für die Zukunft). Richten Sie den Widerruf an die Verantwortlichen.

Ihnen entstehen durch den Widerruf keine Nachteile (*ggf. erwähnen, welche Folgen der Widerruf hat*).

*Sofern möglich:* Nach Eingang des Widerrufs werden die personenbezogenen Daten gelöscht/gesperrt/anonymisiert. (*Nichtzutreffendes bitte streichen*)

### **12. Namen, Kontaktdaten des/der Verantwortlichen**

*Dies ist im Sinne der DSGVO in aller Regel die/der Präsident/-in, Rektor/-in der Universität bzw. die/der Leiter/-in der Forschungseinrichtung. Informieren Sie sich bei Ihrer/Ihrem Datenschutzbeauftragten, wer an Ihrer Einrichtung die Verantwortung übernimmt.*

*Verantwortlich im Sinne der DSGVO ist eine natürliche oder juristische Person, Behörde oder Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4, Ziffer 8, DSGVO-, Begriffsbestimmungen). Davon zu unterscheiden ist die/der fachliche Verantwortliche. Das ist eine Person, die die Datenverarbeitung veranlasst hat bzw. sie leitet. Die Verantwortung für die Verarbeitung der personenbezogenen Daten hat: Hier bitte die Kontaktdaten eintragen.*

### **13. Kontaktdaten des/der Datenschutzbeauftragten**

#### **14. Hinweis auf Rechte der Betroffenen**

Gemäß Art. 13 Abs.2 lit. b der Datenschutzgrundverordnung haben Sie das Recht auf

Auskunft (Art. 15 DSGVO und §34 BDSG)

Widerspruch (Art. 21 DSGVO und §36 BDSG)

Datenübertragbarkeit (Art. 20 DSGVO)

Löschung (Art. 17 DSGVO und §35 BDSG)

Einschränkung der Verarbeitung (Art. 18 DSGVO)

Berichtigung (Art. 16 DSGVO).

Möchten Sie eines dieser Rechte in Anspruch nehmen, wenden Sie sich bitte an die Verantwortlichen.

*Forschungseinrichtung inkl. Anschrift, Telefon, E-Mail eintragen.*

Weiterhin haben Sie das Recht, Beschwerde bei der Aufsichtsbehörde einzulegen:

*Jeweilige Landesbehörde für Datenschutz mit Kontaktdetails eintragen*

### **15. Einwilligung in die Erhebung und Verarbeitung personenbezogener Daten**

Hiermit willige ich freiwillig in die Erhebung und Verarbeitung meiner personenbezogenen Daten ein. Ich bin ausreichend informiert worden und hatte die Möglichkeit, Fragen zu stellen. Über die Folgen eines jederzeit möglichen Widerrufs der datenschutzrechtlichen Einwilligung bin ich aufgeklärt worden. Ich bin darüber informiert worden, dass durch meinen Widerruf der Einwilligung die

Rechtmäßigkeit der aufgrund der Einwilligung erfolgten Verarbeitung bis zum Widerruf nicht berührt wird.

Die schriftliche Aufklärung und Einwilligung habe ich erhalten.

---

Ort, Datum

---

Unterschrift Betroffene/-r

---

Unterschrift Sorgeberechtigte/-r

## Adressliste der Datenschutzbeauftragten des Bundes und der Länder (Stand 06.09.2018)

Die folgenden Adressen stammen von den Webseiten der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

([https://www.bfdi.bund.de/DE/Infothek/Anschriften\\_Links/anschriften\\_links-node.html](https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html)) abgerufen am 01.07.2018. Dort finden sich auch Adressen der internationalen Datenschutzbeauftragten.

### Bund

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Husarenstr. 30

53117 Bonn

Telefon: +49 (0)228-997799-0

E-Mail: [poststelle@bfdi.bund.de](mailto:poststelle@bfdi.bund.de)

Homepage: [https://www.bfdi.bund.de/DE/Home/home\\_node.html](https://www.bfdi.bund.de/DE/Home/home_node.html)

### Baden-Württemberg

Dr. Stefan Brink

Postfach 10 92 32

70025 Stuttgart

Telefon: 0711 615541-0

E-Mail: [poststelle@lfdi.bwl.de](mailto:poststelle@lfdi.bwl.de)

Homepage: <http://www.baden-wuerttemberg.datenschutz.de>

### Bayern

Dr. Thomas Petri

Postfach 22 12 19

80502 München

Telefon: 089/21 26 72-0

E-Mail: [poststelle@datenschutz-bayern.de](mailto:poststelle@datenschutz-bayern.de)

Homepage: <http://www.datenschutz-bayern.de>

### Berlin

Maja Smoltczyk

Friedrichstraße 219

10969 Berlin

Telefon: 030/138 89-0

E-Mail: [mailbox@datenschutz-berlin.de](mailto:mailbox@datenschutz-berlin.de)

Homepage: <http://www.datenschutz-berlin.de>

### Brandenburg

Dagmar Hartge

Stahnsdorfer Damm 77

14532 Kleinmachnow

Telefon: 03 32 03/356-0

E-Mail: [poststelle@lda.brandenburg.de](mailto:poststelle@lda.brandenburg.de)

Homepage: <http://www.lda.brandenburg.de>

## Bremen

Dr. Imke Sommer  
Arndtstraße 1  
27570 Bremerhaven  
Telefon: 04 21/361-2010  
E-Mail: [office@datenschutz.bremen.de](mailto:office@datenschutz.bremen.de)  
Homepage: <http://www.datenschutz.bremen.de/>

## Hamburg

Prof. Dr. Johannes Caspar  
Klosterwall 6(Block C)  
20095 Hamburg  
Telefon: 040/428 54-40 40  
E-Mail: [mailbox@datenschutz.hamburg.de](mailto:mailbox@datenschutz.hamburg.de)  
Homepage: <http://www.datenschutz-hamburg.de>

## Hessen

Prof. Dr. Michael Ronellenfitsch  
Gustav-Stresemann-Ring 1  
65189 Wiesbaden  
Telefon: 06 11/140 80  
E-Mail: [poststelle@datenschutz.hessen.de](mailto:poststelle@datenschutz.hessen.de)  
Homepage: <http://www.datenschutz.hessen.de>

## Mecklenburg-Vorpommern

Heinz Müller  
Lennéstraße 1, Schloss Schwerin  
19053 Schwerin  
Telefon: 0385/59494-0  
E-Mail: [info@datenschutz-mv.de](mailto:info@datenschutz-mv.de)  
Homepage: <http://www.lfd.m-v.de>

## Niedersachsen

Barbara Thiel  
Prinzenstraße 5  
30159 Hannover  
Telefon: 05 11/120-45 00  
E-Mail: [poststelle@lfd.niedersachsen.de](mailto:poststelle@lfd.niedersachsen.de)  
Homepage: <http://www.lfd.niedersachsen.de>

## Nordrhein-Westfalen

Helga Block  
Kavalleriestraße 2-4  
40213 Düsseldorf  
Telefon: 02 11/384 24-0  
E-Mail: [poststelle@ldi.nrw.de](mailto:poststelle@ldi.nrw.de)  
Homepage: <http://www.ldi.nrw.de>

## Rheinland-Pfalz

Prof. Dr. Dieter Kugelmann  
Postfach 30 40  
55020 Mainz  
Telefon: 061 31/208-24 49  
E-Mail: [poststelle@datenschutz.rlp.de](mailto:poststelle@datenschutz.rlp.de)  
Homepage: <http://www.datenschutz.rlp.de>

## Saarland

Monika Grethel  
Fritz-Dobisch-Straße 12  
66111 Saarbrücken  
Telefon: 06 81/947 81-0  
E-Mail: [poststelle@datenschutz.saarland.de](mailto:poststelle@datenschutz.saarland.de)  
Homepage: <http://www.datenschutz.saarland.de>

## Sachsen

Andreas Schurig  
Bernhard-von-Lindenau-Platz 1  
01067 Dresden  
Telefon: 03 51/49 3-5401  
E-Mail: [saechsdsb@slt.sachsen.de](mailto:saechsdsb@slt.sachsen.de)  
Homepage: <http://www.datenschutz.sachsen.de>

## Sachsen-Anhalt

Dr. Harald von Bose  
Postfach 19 47  
39009 Magdeburg  
Telefon: 03 91/818 03-0  
E-Mail: [poststelle@lfd.sachsen-anhalt.de](mailto:poststelle@lfd.sachsen-anhalt.de)  
Homepage: <http://www.datenschutz.sachsen-anhalt.de>

## Schleswig-Holstein

Marit Hansen  
Postfach 71 16  
24171 Kiel  
Telefon: 04 31/988-12 00  
E-Mail: [mail@datenschutzzentrum.de](mailto:mail@datenschutzzentrum.de)  
Homepage: <http://www.datenschutzzentrum.de>

## Thüringen

Dr. Lutz Hasse  
Postfach 90 04 55  
99107 Erfurt  
Telefon: 03 61/57 311 29 00  
E-Mail: [poststelle@datenschutz.thueringen.de](mailto:poststelle@datenschutz.thueringen.de)  
Homepage: <http://www.tlfdi.de>

## ULR-Verzeichnis

DSGVO 2018: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L:2016:119:FULL&from=DE>

Berufsethische Richtlinien:

[https://www.dgps.de/fileadmin/documents/Empfehlungen/berufsethische\\_richtlinien\\_dgps.pdf](https://www.dgps.de/fileadmin/documents/Empfehlungen/berufsethische_richtlinien_dgps.pdf)

Elektronische Signatur: [https://www.gesetze-im-internet.de/bgb/\\_126a.html](https://www.gesetze-im-internet.de/bgb/_126a.html)