Merkblatt Datenschutz

für Antragstellerinnen und Antragsteller bei der Ethik-Kommission der Medizinischen Fakultät der Martin-Luther-Universität Halle-Wittenberg (Stand 6/2018)

HINWEIS
Dieses Merkblatt dient dazu, grundlegend über die datenschutzrechtliche Gestaltung von Forschungsvorhaben zu informieren und Fehler im Rahmen der Antragstellung zu vermeiden. Es kann allerdings eine eingehende Beschäftigung mit dem Datenschutz **nicht ersetzen**. Jede Antragstellerin und jeder Antragsteller bleibt selbst dafür verantwortlich, die datenschutzrechtlichen Bestimmungen einzuhalten. Jegliche Haftung für die Folgen der Verwendung dieses Merkblattes ist ausgeschlossen.

1. Allgemeines

Durch die Datenschutz-Grundverordnung der EU (DS-GVO) wird das Datenschutzrecht ab dem 25. Mai 2018 grundlegend geändert. Die DS-GVO ist unmittelbar verbindliches Recht und Bedarf keiner Umsetzung in deutsches Recht. Die in der Verordnung gegebenen Spielräume und Öffnungsklauseln werden durch ein neues BDSG konkretisiert, das alte BDSG wird ersetzt.

Da bislang nur das BDSG neu gefasst wurde, das DSG LSA aber nicht, **steht diese Handreichung unter dem Vorbehalt einer entsprechenden Regelung für Sachverhalte, die dem DSG LSA unterfallen**. Das neue BDSG gilt für die öffentlichen Stellen der Länder – und damit auch für das Universitätsklinikum – nur dann, wenn kein Landesgesetz zum Datenschutz vorhanden ist und nur soweit Bundesrecht ausgeführt wird (z.B. AMG, MPG etc.).

2. Begriffsbestimmungen

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen.

Identifizierbar ist eine natürliche Person, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Verarbeitung ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte 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.

Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Verantwortlicher ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Genetische Daten sind personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

Biometrische Daten sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten.

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

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

3. Anwendungsbereich der DS-GVO

a) Grundsatz

Die DSG-GVO gilt für

- die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für
- die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder werden sollen.

b) Ausnahmen

- **Anonyme Daten**

  Die DS-GVO ist jedoch nicht anwendbar, wenn kein Personenbezug vorliegt, also dann, wenn die Daten **anonymisiert** sind. **Anonymisieren** meint das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

  CAVE

  Werden Daten, die für den Verantwortlichen anonym sind, an eine Stelle übermittelt, die eine Zuordnung herstellen kann, ist der Übermittlungstatbestand der Verordnung gegeben und diese deshalb anwendbar!

- **Pseudonyme Daten?**

  Bei **pseudonymisierten Daten** ist zu unterscheiden:

  → Hat nur der Betroffene selbst die Möglichkeit der Reidentifizierung, weil er den Schlüssel selbst bestimmt und kein anderer diesen kennt, sind sie wie anonymisierte Daten zu behandeln.

  → Hat allerdings die datenverarbeitende Stelle (z.B. Studienleitung) den Zuordnungsschlüssel generiert und kennt die Zuordnung, so besteht für diese die Möglichkeit der Identifizierung, sodass diese Daten dann wie personenbezogene Daten zu handhaben sind.

4. Grundsätze der DS-GVO

Die DS-GVO stellt detaillierte Grundsätze für die Verarbeitung personenbezogener Daten auf:

- **Rechtmäßigkeit und Transparenz** der Verarbeitung
- Verarbeitung nach **Treu und Glauben**
- **Zweckbindung** der erhobenen Daten

  = Erhebung für festgelegte, eindeutige und legitime Zwecke und Verarbeitung nur in einer Weise, die mit diesen Zwecken vereinbar ist
- **Datenminimierung**

  = Beschränkung der Verarbeitung auf das notwendige Maß
- **Richtigkeit**

  = Daten müssen richtig und auf dem neusten Stand sein
  = Notwendigkeit zur Löschung oder Berichtigung von unrichtigen Daten
- **Speicherbegrenzung**

  = Speicherung nur so lange, wie dem Zweck nach erforderlich
- **Integrität und Vertraulichkeit**

  = Schutz vor unbefugtem oder unrechtmäßigen Verarbeiten, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung

Der Verantwortliche ist für die Einhaltung dieser Grundsätze verantwortlich und muss **deren Einhaltung nachweisen** können (**Rechenschaftspflicht**).

5. Rechtmäßige Datenverarbeitung – Einwilligung

a) Grundsätzliches

Die Voraussetzungen für eine rechtmäßige Datenverarbeitung sind in Art. 6 DS-GVO niedergelegt. Für den Bereich der Forschung dürfte nur der Fall der Einwilligung und der Fall der rechtlichen Verpflichtung zur Verarbeitung relevant sein. Hier soll der häufigste Fall – die Verarbeitung aufgrund Einwilligung – erörtert werden.

Einwilligung der betroffenen Person meint jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

b) Voraussetzungen einer wirksamen Einwilligung

- **Freiwilligkeit und Koppelungsverbot**

  Die Einwilligung muss freiwillig sein. Das heißt es darf kein Druck oder Zwang auf die betroffene Person ausgeübt werden. Der Einwilligende muss eine echte Entscheidungsfreiheit haben. Die Erfüllung von Verträgen, Dienstleistungen oder anderer Gegenleistungen dürfen nicht von der Einwilligung in die Verarbeitung von personenbezogen Daten abhängig gemacht werden, die dafür nicht erforderlich sind.

- **Information (Aufklärung) bei der direkten Erhebung der Daten beim Betroffenen**

  Der Betroffene ist **zum Zeitpunkt der Erhebung** zu informieren über:

  - Name und Kontaktdaten des Verantwortlichen (und ggf. eines Vertreters)
  - Kontaktdaten des Datenschutzbeauftragten
  - Zwecke, zu denen die Daten verarbeitet werden
  - Rechtsgrundlage der Verarbeitung
  - ggf. Empfänger oder Kategorien von Empfängern der personenbezogenen Daten
  - ggf. Absicht der Übermittlung der Daten in ein Drittland oder an eine internationale Organisation und:
    - → Vorhandensein oder Fehlen eines Angemessenheitsbeschlusses der Europäischen Kommission oder
    - → Hinweis auf geeignete oder angemessene Garantien (im Falle von Art. 46, 47 oder 49 DS-GVO)
  - Dauer der Speicherung oder, wenn nicht möglich, Kriterien zur Festlegung der Dauer
  - Rechte der Betroffenen auf Auskunft, Löschung, Einschränkung der Verarbeitung oder Widerspruch sowie auf Datenübertragbarkeit
  - Widerrufsrecht des Betroffenen
  - Beschwerderecht des Betroffenen bei Aufsichtsbehörden

- **Information, wenn die Daten nicht bei der betroffenen Person erhoben werden**

  Der Verantwortliche hat der betroffenen Person, wenn Daten ohne ihr Wissen erhoben werden, **zusätzlich** zu den gerade erörterten Informationen folgende Informationen mitzuteilen:

  - Kategorien personenbezogener Daten, die verarbeitet werden
  - Quelle, aus der die Daten stammen

  Die Mitteilung muss innerhalb einer angemessenen Zeit nach der Erlangung der Daten, **spätestens jedoch innerhalb eines Monats**, erfolgen. Werden Daten zur Kommunikation mit der Person verwendet, so ist diese spätestens beim ersten Kontakt zu informieren. Werden Daten an andere Empfänger offengelegt, muss die Information spätestens zum Zeitpunkt der ersten Offenlegung erfolgen.

  Die Information muss nur dann nicht erfolgen, wenn sie unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert. Das gilt insbesondere im Rahmen der wissenschaftlichen Forschung, wenn diese sonst unmöglich oder erheblich beeinträchtigt wäre. Hier muss der Verantwortliche aber geeignete Maßnahmen zum Schutz des Betroffenen sicherstellen.

- **Gestaltung**

  Bei der Gestaltung der Einwilligungserklärung und des „Ersuchens“ um die Einwilligung gilt:

  - **Verständlichkeit (hier sind ggf. die standardisierten Bildsymbole, die die EU-Kommission erlässt, zu verwenden)**
  - **Zugänglichkeit**
  - **Klare und einfache Sprache**
  - **Hervorhebung gegenüber anderen Erklärungen (Fettdruck, Rahmen, Farbe etc.)**

- **Besondere Daten**

  Die Verarbeitung besonderer personenbezogener Daten, also solcher über die rassische und **ethnische Herkunft**, politische Meinung, religiöse oder weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit sowie **genetische Daten**, **biometrische Daten**, **Gesundheitsdaten**, Daten zum **Sexualleben** oder der **sexuellen Orientierung**, ist grundsätzlich **verboten**.

  Die Verarbeitung ist dann ausnahmsweise erlaubt, wenn die betroffene Person ausdrücklich in die Verarbeitung der Daten für einen festgelegten Zweck einwilligt. **Dazu muss sie auf die Verarbeitung der besonderen Daten explizit hingewiesen werden.**

CAVE
Eine nachfolgende Anonymisierung hebt die Pflicht zur expliziten Einwilligung nicht auf!

- **Einwilligungsfähigkeit**

  Wie auch bei der Einwilligung in die medizinische Behandlung ist die Fähigkeit, seine Einwilligung in datenschutzrechtlichen Belangen abzugeben, nicht an ein fixes Alter geknüpft, sondern von den individuellen Fähigkeiten abhängig. Die DS-GVO geht aber davon aus, dass „Kinder“ eines besonderen Schutzes bedürfen und legt deshalb ein „Mindesteinwilligungsalter“ fest. Es gilt:

  - Die Mitgliedstaaten können eine Altersgrenze festlegen, die nicht unter dem vollendeten 13. Lebensjahr liegen darf.
  - Legen die Mitgliedstaaten das – wie in Deutschland bislang – nicht selbst fest, so ist die Einwilligung eines Minderjährigen nach der DS-GVO nur wirksam, wenn dieser das 16. Lebensjahr vollendet hat.
  - Ist die Altersgrenze nicht erreicht, ist die Datenverarbeitung nur dann rechtmäßig, wenn die gesetzlichen Vertreter die Einwilligung erteilen oder das Kind mit ihrer Zustimmung einwilligt.
  - Der Verantwortliche hat alle angemessenen Anstrengungen zu unternehmen, um zu verifizieren, dass die Einwilligung durch den gesetzlichen Vertreter oder mit dessen Zustimmung erteilt wurde.

6. Zweckänderung

Sind Daten zu einem bestimmten Zweck erhoben worden – beispielsweise für die Krankenversorgung – können und dürfen sie nicht ohne Weiteres im Rahmen der Forschung verwendet werden. Hierfür ist eine Zweckänderung bzw. Umwidmung nötig. Diese ist in folgenden Fällen möglich:

- Die betroffene Person hat in die Zweckänderung eingewilligt (die entsprechenden Vorschriften zu Information etc. gelten auch hier).
- Die Zweckänderung ist durch eine Rechtsvorschrift gestattet.
- Der neue Zweck ist mit dem Zweck, zu dem die Daten erhoben worden sind, vereinbar. Das setzt eine Prüfung der Vereinbarkeit und der Interessen der betroffenen Person voraus. Dabei muss der Verantwortliche mindestens die folgenden Punkte berücksichtigen:
  - → Verbindung zwischen den ursprünglichen und den geänderten Zwecken
  - → Zusammenhang in dem die Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen betroffener Person und Verantwortlichem
  - → Art der personenbezogenen Daten, insbesondere bei besonderen Kategorien von Daten (s.o.)
  - → Mögliche Folgen der Weiterverarbeitung für die betroffene Person
  - → Vorhandensein geeigneter Garantien wie Verschlüsselung oder Pseudonymisierung

  Im Bereich der **wissenschaftlichen Forschung** wird die Vereinbarkeit der Zwecke gesetzlich vermutet, sodass hier kein Kompatibilitätstest oder eine andere Rechtsgrundlage erforderlich ist. Trotzdem sollte insbesondere bei Daten, die im Rahmen der Krankenversorgung in einer Druck- bzw. Zwangssituation abgegeben werden (ohne Daten keine Behandlung?), eine angemessen begründete **Interessenabwägung** im Studienprotokoll erfolgen. Dies dient nicht nur Dokumentationszwecken, sondern auch der Erfüllung der Deklaration von Helsiniki.

Erfolgt eine Weiterverarbeitung der Daten zu einem anderen Zweck muss die betroffene Person **vor der Weiterverarbeitung** über den geänderten Zweck und alle anderen maßgeblichen Informationen (s.o.) informiert werden.

7. Rechte der betroffenen Person

- **Recht auf Information** (Faire und transparente Datenverarbeitung) → s.o. Informationspflichten
- **Recht auf Auskunft**

  Die betroffene Person kann eine Bestätigung vom Verantwortlichen verlangen, ob bei ihm personenbezogene Daten dieser Person verarbeitet werden und zugleich Auskunft über die entsprechenden Daten verlangen. Ebenso steht ihr das Recht auf Erhalt einer kostenlosen Kopie der gespeicherten Daten zu.
- **Recht auf Berichtigung**

  Der Verantwortliche hat unrichtige oder unvollständige Daten auf Verlangen unverzüglich zu korrigieren oder zu ergänzen.
- **Recht auf Löschung (Recht auf Vergessenwerden)**

  Die betroffene Person hat das Recht vom Verantwortlichen die unverzügliche Löschung der sie betreffenden personenbezogen Daten zu verlangen. Diesem Verlangen muss der Verantwortliche nachkommen, wenn einer der folgende Fälle vorliegt:
  - Die Daten sind für den Zweck, zu dem sie erhoben wurden, nicht mehr notwendig.
  - Die betroffene Person hat die Einwilligung widerrufen.
  - Die betroffene Person hat der Verarbeitung widersprochen.
  - Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.

Der Verantwortliche hat bei Daten, die er öffentlich gemacht hat, auch die Pflicht, andere Verantwortliche über die Löschungsverpflichtung zu informieren.

Das Recht auf Löschung besteht in bestimmten Fällen nicht. Hier ist insbesondere die Forschung zu nennen. Das gilt aber nur, wenn durch die Löschung die Verwirklichung der Ziele der Forschung unmöglich gemacht oder ernsthaft beeinträchtigt werden.

- **Recht auf Einschränkung der Verarbeitung (früher „Sperrung“)**

  Unter bestimmten Voraussetzungen – insbesondere in der Schwebezeit, bis geklärt ist, ob Daten unrichtig sind oder ein Widerspruch berechtigt ist – hat die betroffene Person das Recht auf Einschränkung der Datenverarbeitung. In diesem Fall dürfen die Daten, abgesehen von der Speicherung, nur mit Einwilligung der Person oder zur Rechtsdurchsetzung verwendet werden.

- **Recht auf Datenübertragbarkeit**

  Der betroffenen Person steht – und das ist ein Novum – ein Recht auf Datenübertragbarkeit zu. Das bedeutet, dass die Person das Recht hat, eine maschienenlesbare Kopie der Daten zu erhalten und diese an einen anderen Verantwortlichen weiterzugeben, wenn die Daten aufgrund einer Einwilligung oder eines Vertrages erhoben worden sind und die Datenverarbeitung automatisiert erfolgt. Soweit dies technisch machbar ist, darf die Person auch die direkte Übermittlung verlangen.

- **Widerspruchsrecht**

  Unter bestimmten Voraussetzungen kann die betroffene Person einen Widerspruch gegen die Verarbeitung von Daten erheben, die aufgrund gesetzlicher Grundlage verarbeitet werden.

  CAVE Der Widerspruch ist streng vom Widerruf der Einwilligung zu trennen!

Durch das **neue BDSG** werden bestimmte Betroffenenrechte im Bereich der Forschung eingeschränkt, wenn die Forschung unmöglich würde oder ernsthaft gefährdet wäre. Die Daten sind aber zu anonymisieren, sobald es der Forschungszweck erlaubt. Diese Einschränkug der Rechte wird aktuell als teilweise europarechtswidrig bewertet – eine abschließende Klärung liegt noch nicht vor.

8. Pflichten des Verantwortlichen

- **Pflicht zur Sicherstellung der Vereinbarkeit mit der DS-GVO**

  Der Verantwortliche hat die geeigneten technischen und organisatorischen Maßnahmen zu treffen, um die Datenverarbeitung im Einklang mit der DS-GVO vorzunehmen und diese regelmäßig zu überprüfen und zu aktualisieren.

- **Privacy by design**

  Der Verantwortliche muss zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung und zum Zeitpunkt der eigentlichen Verarbeitung durch eine datenschutzfreundliche Technikgestaltung dafür sorgen, dass die Grundsätze der DS-GVO wirksam umgesetzt werden. Dazu zählt z.B. eine Pseudonymisierung.

- **Privacy by default**

  Überdies muss der Verantwortliche Voreinstellungen (z.B. bei Computerprogrammen) so treffen, dass sie möglichst datenschutzfreundlich sind.

- **Nachweispflicht**

  Jeder Verantwortliche muss ein **Verzeichnis aller Verarbeitungstätigkeiten** führen, das folgende Angaben enthalten muss:

  - Name und Kontaktdaten des Verantwortlichen
  - Zwecke der Verarbeitung
  - Beschreibung der Kategorien betroffener Personen
  - Beschreibung der Kategorien der personenbezogen Daten
  - Kategorien der Empfänger
  - ggf. Übermittlung in ein Drittland oder an eine internationale Organisation (inkl. der Dokumentation der geeigneten Garantien)
  - Fristen für die Löschung der verschiedenen Datenkategorien
  - Beschreibung der technischen und organisatorischen Maßnahmen zur Datensicherheit

  Ein Verzeichnis muss nicht geführt werden, wenn ein Unternehmen weniger als 250 Mitarbeiter hat. Es muss **in jedem Fall** geführt werden, wenn ein Risiko für die Rechte und Freiheiten der betroffenen Person besteht, die Verarbeitung nicht nur gelegentlich erfolgt oder besondere personenbezogene Daten (z.B. Gesundheitsdaten) verarbeitet werden.

  Zudem muss der Verantwortliche **nachweisen können**, dass die betroffene Person in die Verarbeitung der Daten eingewilligt hat.

- **Datensicherheit**

  Die Verantwortlichen müssen, nach einer Einschätzung des mit der Datenverarbeitung verbundenen Risikos, geeignete technische und organisatorische Maßnahmen zur Realisierung eines dem Risiko angemessen Schutzniveaus implementieren. Die DS-GVO nennt hier insbesondere folgende Maßnahmen:

  - Pseudonymisierung und Verschlüsselung
  - Sicherstellung der Integrität, Vertraulichkeit, Verfügbarkeit und Belastbarkeit der datenverarbeitenden Systeme
  - Sicherstellung der raschen Wiederherstellung der Daten nach einem Zwischenfall
  - Verfahren zu regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Sicherungsmaßnahmen

- **Personelle Sicherung**

  Die Verantwortlichen stellen sicher, dass ihnen untergebene Personen nur auf Anweisung Daten verarbeiten und implementieren die dafür erforderlichen Schritte.

- **Meldepflicht**

  Wird der Schutz der personenbezogen Daten verletzt (egal ob unbeabsichtigt oder beabsichtigt), besteht eine Meldepflicht an die zuständige Aufsichtsbehörde. Der Vorfall muss innerhalb von 72 Stunden gemeldet werden. Die Pflicht entfällt, wenn die Verletzung zu keinem Risiko für die Rechte der betroffenen Person führt.

- **Benachrichtigungspflicht**

  Über eine Verletzung des Schutzes personenbezogener Daten ist die betroffene Person ebenfalls zu benachrichtigen, wenn das Risiko für die Rechte der Person durch nachträglich getroffene Maßnahmen nicht ausgeschlossen werden kann.

- **Datenschutz-Folgenabschätzung (DSFA)**

  Sind besonders hohe Risiken für die Rechte der betroffenen Personen vorhanden oder werden besondere Arten von personenbezogenen Daten (z.B. Gesundheitsdaten) in besonderem Umfang verarbeitet, muss der Verantwotliche selbst – und nicht der Datenschutzbeauftragte – eine Datenschutz-Folgeabschätzung durchführen. Ungeklärt ist bislang, wann von einem „besonderen Umfang" zu sprechen ist. Es wird daher von verschiedenen Seiten darauf hingewiesen, dass es im Zweifel sicherer ist, die DSFA durchzuführen. Diese muss zumindest Folgendes umfassen:

  - Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem für die Verarbeitung Verantwortlichen verfolgten berechtigten Interessen.
  - Eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck.
  - Eine Bewertung der Risiken der Rechte und Freiheiten der betroffenen Personen.
  - Die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen der DS-GVO eingehalten werden, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen werden soll.

- **Konsultationspflicht**

  Der Verantwortliche hat vor der Verarbeitung die zuständige Aufsichtsbehörde zu kontaktieren, wenn eine DSFA ein Risiko ergibt, dass er nicht durch geeignete Maßnahmen eindämmen kann.

CAVE

Die Verletzung der Pflichten bzw. des Schutzes personenbezogener Daten löst eine Reihe von Ansprüchen und Sanktionen aus. Die betroffene Person kann Schadensersatz verlangen, die Aufsichtsbehörde muss ein Bußgeld festsetzen und hat hierbei kein Ermessen. Das Bußgeld kann bis zu 4 % des Unternehmensgewinns bzw. bis zu 20 Millionen Euro betragen. Bestimmte Verstöße sind sogar mit Strafe bewehrt!

Der Verantwortliche kann sich den Pflichten auch nicht durch Auslagerung der Datenverarbeitung entziehen; denn die DS-GVO regelt auch die Pflichten bei Auftragsdatenverarbeitung neu und umfassend.

9. Datentransfer ins Ausland

Grundsatz bei einer Datenübermittlung an Empfänger, Verantwortliche, Auftragsverarbeiter in Drittländern – also solche, die nicht zur EU gehören – oder an internationale Organisationen soll der Schutzstandard der DS-GVO gewahrt bleiben.

Eine Übermittlung in Drittländer oder an internationale Organisationen ist nur in folgenden Fällen zulässig:

- Es liegt ein **Angemessenheitsbeschluss** der Europäischen Kommission vor, aus dem hervorgeht, dass das Zielland (zumindest für den Sektor, in den übermittelt werden soll) ein angemessenes Schutzniveau bietet.
- Sofern kein Angemessenheitsbeschluss vorliegt muss der Verantwortliche **geeignete Garantien** vorsehen und der betroffenen Person müssen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Diese Garantien können beispielsweise Standarddatenschutzklauseln, die von der EU-Kommission gebilligt wurden, eine Zertifizierung des Empfängers oder eine Unterwerfung des Empfängers unter das europäische Recht, sein.

10. Übergangsregelung?

Die DS-GVO ist ab dem 25. Mai 2018 in Geltung und anzuwenden. Ab diesem Zeitpunkt muss die Datenverarbeitung der DS-GVO genügen. Eine Übergangsregelung oder Altfallregelung ist in der DS-GVO nicht vorgesehen. Erwägungsgrund 171 der Verordnung sieht aber vor, dass Einwilligungen, die vor der Geltung der Verordnung erteilt worden sind, wirksam bleiben, wenn die Art der bereits erteilten Einwilligung den Bedingungen der DS-GVO entspricht. Gemeint ist damit, dass die wesentlichen Kernbestandteile der Einwilligung nach der DS-GVO vorhanden sein müssen. Das dürfte für die Einwilligungen nach bisherigem Recht gelten (Beschluss des Düsseldorfer Kreises v. 13./14.9.2016). **Ab dem 25. Mai 2018 sind aber Einwilligungen nach dem neuen Recht einzuholen. Bereits laufende Datenverarbeitungen sind spätestens innerhalb von zwei Jahren anzupassen.**