



# **Datenschutz und Offenlegungspolitik**

Gültig ab dem: 11. Juli 2023.

# **Buch I - Datenschutzrichtlinie**

## Inhaltsübersicht

<b>Präambel</b> .....	5
1. ALLGEMEINE BESTIMMUNGEN .....	5
1.1. Zweck der Richtlinie .....	5
1.2. Geltungsbereich der Richtlinie .....	5
1.3. Geltende Rechtsvorschriften, Definitionen, Formulare .....	6
1.4. Grundsätze, Rechtsgrundlage und Zwecke der Datenverarbeitung .....	6
1.5. Datenschutz durch Technik, Datenschutz-Folgenabschätzung .....	9
1.6. Durchsetzung der Datenschutzgrundsätze und Gewährleistung der Rechenschaftspflicht 10	
1.7. Datenmanagement und Sicherheitsstandards im Rahmen der Verwaltung .....	12
1.8. Allgemeine Zwecke der Verarbeitung, Verarbeitung von Dokumenten und Unterlagen .....	14
1.9. Aufzeichnungen über Verarbeitungstätigkeiten .....	15
1.10. Übermittlung von Daten und Aufzeichnung der übermittelten Daten .....	15
1.11. Aufzeichnungen über Verarbeitungstätigkeiten .....	16
1.12. Dispositionsregister .....	18
1.13. Register der Auftragsverarbeiter, gemeinsam für die Verarbeitung Verantwortlichen, Datenverarbeitung .....	19
1.14. Datenschutzvorfälle und deren Aufzeichnung .....	20
1.15. Lokale Datenschutzbeauftragte und ihre Aufzeichnungen .....	21
2. DIE RECHTE DER BETROFFENEN PERSONEN IN BEZUG AUF DIE DATENVERARBEITUNG ZU GEWÄHRLEISTEN .....	21
2.1. Sicherstellung der Rechte der betroffenen Person .....	21
2.2. Information der betroffenen Personen .....	22
2.3. Gewährleistung des Rechts auf Änderung und Berichtigung von Daten .....	23
2.4. Sicherstellung des Rechts auf Löschung .....	24
2.5. Gewährleistung des Rechts auf Einschränkung der Verarbeitung .....	24
2.6. Gewährleistung des Rechts auf Datenübertragbarkeit .....	25
2.7. Gewährleistung des Rechts auf Widerspruch gegen die Verarbeitung .....	25
2.8. Sicherstellung des Rechts auf Zugang zu Daten .....	26
2.9. Prüfung der Rechtsgrundlage für die Verarbeitung .....	26
2.10. Besondere Datenverwaltung .....	28
2.11. Verhinderung von Datenverlusten .....	29
3. DAS DATENSCHUTZSYSTEM DER UNIVERSITÄT .....	29
3.1. Die/der Datenschutzbeauftragte .....	29
3.2. Das Zentrum für Datenschutz und Patientenrechte (ABK) .....	30
3.3. Benennung und Aufgaben des örtlichen Datenschutzbeauftragten .....	32

3.4. Das System zur Überwachung des Datenschutzes .....	32
4. UNTERSTÜTZUNG DER DATENVERARBEITUNGSABTEILUNGEN DER UNIVERSITÄT BEI DER EINHALTUNG DER VORSCHRIFTEN .....	33
5. Anhänge .....	34

## **Präambel**

der Semmelweis-Universität, (im Folgenden: Universität) gemäß dem Gesetz CCIV von 2011 über die nationale Hochschulbildung (im Folgenden: Nftv.), Gesetz CXII von 2011 über das Recht auf informationelle Selbstbestimmung und Informationsfreiheit (im Folgenden: Infotv.), Gesetz CLIV von 1997 über die Gesundheitsversorgung (im Folgenden: Eütv.), Gesetz XLVII von 1997 über die Verarbeitung und den Schutz personenbezogener Gesundheitsdaten und verwandter personenbezogener Daten (im Folgenden: Eüak.) und der Verordnung (EU) Nr. 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 95/46/EG (im Folgenden: Verordnung) legt sie die folgenden Regeln für die Datenverwaltung an der Universität fest.

Die Datenschutzrichtlinie (im Folgenden: Richtlinie) werden im Einklang mit den Bestimmungen der Satzung ausgelegt und angewendet. Zur Förderung einer einheitlichen Auslegung und Anwendung hat das Zentrum für Datenschutz und Patientenrechte (im Folgenden: ABK) bietet Unterstützung.

### **1. ALLGEMEINE BESTIMMUNGEN**

#### **1.1. Zweck der Richtlinie**

Festlegung der Regeln für die von der Universität als für die Datenverarbeitung Verantwortlicher durchgeführten Tätigkeiten.

#### **1.2. Geltungsbereich der Richtlinie**

- (1) Der Geltungsbereich der Richtlinie erstreckt sich auf Folgendes:
  - a) alle Daten, die nach den geltenden Rechtsvorschriften als personenbezogene Daten gelten;
  - b) die Universität und alle ihre Dienststellen, in denen personenbezogene Daten verarbeitet werden;
  - c) für jeden, der personenbezogene Daten verarbeitet oder im Rahmen seiner Tätigkeit an der Universität Kenntnis von personenbezogenen Daten erhält.
- (2) Der Geltungsbereich dieser Richtlinie erstreckt sich nicht auf Einrichtungen, die von der Universität unterhalten werden, auf Geschäftseinheiten, die sich im Besitz der Universität befinden, und auf jede Einheit mit Rechtspersönlichkeit, die am Betrieb der Universität beteiligt ist oder damit in Verbindung steht (im Folgenden als "Einheiten" bezeichnet), aber die Universität als Trägerin, Eigentümerin oder teilnehmendes Mitglied solcher Einheiten ermutigt und erwartet von diesen Einheiten, dass sie ihre eigenen Datenschutzsysteme im Einklang mit dieser Richtlinie entwickeln.

### 1.3. Geltende Rechtsvorschriften, Definitionen, Formulare

- (1) Die in dieser Regelung verwendeten Begriffe entsprechen den in den geltenden Rechtsvorschriften definierten Begriffen.
- (2) Für die Zwecke der Richtlinie:
  - a) Organisationseinheit, die verpflichtet ist, einen lokalen Datenschutzbeauftragten zu ernennen: die Organisationseinheit, die im Register der Organisationseinheiten der Organisations- und Betriebsordnung der Universität als Stufe I eingestuft ist, die Organisationseinheit für die Patientenversorgung (Kliniken und die Abteilung für Rehabilitation und Gesundheitspflege von Pető András), die studentische Selbstverwaltung der Universität und die Selbstverwaltung der Doktoranden unter den anderen Organisationen, die als Stufe I eingestuft sind.
- (3) Die Verwendung der in der Formularbibliothek veröffentlichten Formulare - mit dem angegebenen Dateninhalt - ist obligatorisch.

### 1.4. Grundsätze, Rechtsgrundlage und Zwecke der Datenverarbeitung

- (1) Die Universität führt ihre Datenverwaltungstätigkeiten im Einklang mit den Grundsätzen der Rechtmäßigkeit, Fairness und Transparenz, der Zweckbindung, der Datenminimierung und der begrenzten Aufbewahrung, der Genauigkeit und den Grundsätzen der Integrität und Vertraulichkeit durch, wie in Artikel 5 Absatz 1 der Verordnung dargelegt.
- (2) Die Universität ergreift geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die Verarbeitung von Daten durch die Universität im Einklang mit dem Grundsatz des Datenschutzes durch Technik und durch datenschutzfreundliche Voreinstellungen gemäß Artikel 25 der Verordnung erfolgt.
- (3) Alle Abteilungen der Universität stellen sicher, dass die Universität in der Lage ist, die Einhaltung der Grundsätze und Regeln der Datenverwaltung nachzuweisen (Grundsatz der Rechenschaftspflicht).
- (4) Im Falle einer Tätigkeit, die die Verarbeitung personenbezogener Daten umfasst, nimmt die betreffende Dienststelle die dem für die Verarbeitung Verantwortlichen obliegenden Aufgaben gemäß den vom DSB festgelegten Leitlinien wahr.
- (5) Die Universität wird personenbezogene Daten nur verarbeiten, wenn
  - a) die betroffene Person hat ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten für einen bestimmten Zweck gegeben;
  - b) <sup>1</sup>die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung von Maßnahmen erforderlich, die auf Antrag der betroffenen Person vor Abschluss des Vertrags erfolgen;
  - c) <sup>2</sup>die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der für die Verarbeitung Verantwortliche unterliegt;
  - d) <sup>3</sup>die Verarbeitung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich;

---

<sup>1</sup> VERORDNUNG Artikel 6 Absatz 1 lit. b)

<sup>2</sup> VERORDNUNG Artikel 6 Absatz 1 lit. c)

<sup>3</sup> VERORDNUNG Artikel 6 Absatz 1 lit. d)

- e) <sup>4</sup>die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde;
  - f) <sup>5</sup>zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere wenn es sich bei der betroffenen Person um ein Kind handelt.
- (6) Besondere Daten können verarbeitet werden, wenn
- a) <sup>6</sup>die betroffene Person hat ausdrücklich in die Verarbeitung der besonderen Kategorien personenbezogener Daten für einen oder mehrere festgelegte Zwecke eingewilligt, es sei denn, das Unionsrecht oder das Recht der Mitgliedstaaten sieht vor, dass das allgemeine Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten durch die Einwilligung der betroffenen Person nicht aufgehoben werden kann;
  - b) <sup>7</sup>die Verarbeitung ist zur Erfüllung der Verpflichtungen des für die Verarbeitung Verantwortlichen oder der betroffenen Person aus Rechtsvorschriften über Beschäftigung, soziale Sicherheit und sozialen Schutz sowie zur Ausübung ihrer spezifischen Rechte erforderlich, sofern die Verarbeitung durch Rechtsvorschriften der Union oder der Mitgliedstaaten, einschließlich Rechtsvorschriften der Union oder der Mitgliedstaaten, die angemessene Garantien zum Schutz der Grundrechte und Interessen der betroffenen Person vorsehen, oder durch Tarifverträge nach nationalem Recht zulässig ist;
  - c) <sup>8</sup>die Verarbeitung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich;
  - d) <sup>9</sup>die Verarbeitung erfolgt im Rahmen der rechtmäßigen Tätigkeiten einer politischen, weltanschaulichen, religiösen, gewerkschaftlichen oder sonstigen nicht auf Gewinn ausgerichteten Stiftung, Vereinigung oder sonstigen Organisation ohne Erwerbsscharakter mit angemessenen Garantien unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf derzeitige oder ehemalige Mitglieder einer solchen Organisation oder auf Personen bezieht, die im Zusammenhang mit den Zwecken der Organisation regelmäßig mit ihr in Kontakt stehen, und dass die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen an Personen außerhalb der Organisation weitergegeben werden;
  - e) <sup>10</sup>die Verarbeitung zu Zwecken der Gesundheitsvorsorge oder der Gesundheit am Arbeitsplatz, zur Beurteilung der Arbeitsfähigkeit eines Mitarbeiters, zur Erstellung einer medizinischen Diagnose, zur Bereitstellung von Gesundheits- oder Sozialfürsorge oder Behandlung oder zur Verwaltung von Gesundheits- oder Sozialfürsorgesystemen und -diensten, wie dies nach dem Recht der EU oder eines

---

<sup>4</sup>VERORDNUNG Artikel 6 Absatz 1 lit. e)

<sup>5</sup>VERORDNUNG Artikel 6 Absatz 1 lit. f)

<sup>6</sup>VERORDNUNG Artikel 9 Absatz 2 lit. a)

<sup>7</sup>VERORDNUNG Artikel 9 Absatz 2 lit. b)

<sup>8</sup>VERORDNUNG Artikel 9 Absatz 2 lit. c)

<sup>9</sup>VERORDNUNG Artikel 9 Absatz 2 lit. d)

<sup>10</sup>VERORDNUNG Artikel 9 Absatz 2 lit. h)

- Mitgliedstaats oder im Rahmen eines Vertrags mit einem Angehörigen der Gesundheitsberufe erforderlich ist;
- f) <sup>11</sup>die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich, etwa zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsbedrohungen oder zur Gewährleistung eines hohen Qualitäts- und Sicherheitsniveaus der Gesundheitsversorgung, von Arzneimitteln und Medizinprodukten, und beruht auf dem Unionsrecht oder dem Recht der Mitgliedstaaten, das angemessene und spezifische Maßnahmen zum Schutz der Rechte und Freiheiten der betroffenen Person vorsieht, insbesondere das Berufsgeheimnis;
  - g) <sup>12</sup>die Verarbeitung ist für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke auf der Grundlage von Rechtsvorschriften der Union oder der Mitgliedstaaten erforderlich, die in einem angemessenen Verhältnis zu dem verfolgten Zweck stehen, den wesentlichen Inhalt des Rechts auf Schutz der personenbezogenen Daten wahren und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen.
- (7) <sup>13</sup>Die betroffene Person ist vor der Erhebung der Daten über die Informationen zu unterrichten, auf deren Grundlage die Verarbeitung gemäß den Artikeln 13 und 14 der Verordnung durchgeführt wird. Dies geschieht in Form der Veröffentlichung eines Datenschutzhinweises.
- (8) <sup>14</sup>Auf der Grundlage der Einwilligung, wenn die betroffene Person freiwillig, ausdrücklich, in Kenntnis der Sachlage und unmissverständlich in die Verarbeitung der sie betreffenden personenbezogenen Daten einwilligt.
- a) Die Einwilligung gilt für alle Verarbeitungen, die zu demselben Zweck oder denselben Zwecken durchgeführt werden.
  - b) Im Falle einer Verarbeitung zu mehreren Zwecken muss die Einwilligung für jeden einzelnen Zweck, für den die Daten verarbeitet werden, erteilt werden.
  - c) Bei Einwilligung darf die Verarbeitung nur in Übereinstimmung mit den Anforderungen der Vorabinformation und auf freiwilliger Basis erfolgen. Die Freiwilligkeit kann nicht gerechtfertigt werden, wenn die betroffenen Personen ihre Einwilligung zur Verarbeitung von Daten ausschließlich im Interesse der Universität in einem untergeordneten Verhältnis, massenhaft, in einer bestimmten Personengruppe und ohne Ausnahme gegeben haben.
  - d) Die Einwilligung kann in jeder Form gegeben werden, in der die betroffene Person identifiziert werden kann und die Tatsache der Einwilligung festgehalten wird,
  - e) die Zustimmung kann nicht mündlich oder telefonisch erteilt werden
  - f) die Zustimmung kann insbesondere zu folgenden Punkten erteilt werden:
    - fa) schriftlich (mit Unterschrift der betreffenden Person);

---

<sup>11</sup>VERORDNUNG Artikel 9 Absatz 2 lit. i)

<sup>12</sup>VERORDNUNG Artikel 9 Absatz 2 lit. j)

<sup>13</sup>VERORDNUNG Artikel 12 Absatz 1

<sup>14</sup>VERORDNUNG Artikel 7

- fb) elektronisch, nach der individuellen Identifizierung der betroffenen Person (z. B. Identifizierung mit dem Studiensystem), wenn die Tatsache der Einwilligung aufgezeichnet (protokolliert) wird;
  - fc) auf elektronischem Wege von einer bei der betreffenden Universität registrierten E-Mail-Adresse, sofern die Nachricht aufgezeichnet und unverändert aufbewahrt wird.
- (9) Der örtliche Datenschutzbeauftragte führt ein Protokoll über die von den betroffenen Personen erteilten Einwilligungen mit folgendem Inhalt:
- a) den Namen und das Aktenzeichen des Verarbeitungsregisters,
  - b) die Registrierungsnummer der Zustimmung zur Verarbeitung,
  - c) die Daten zur Identifizierung der natürlichen Person,
  - d) das Datum, an dem die Zustimmung erteilt wurde,
  - e) die Registrierungsnummer der Datenschutzrichtlinie,
  - f) das Datum des Widerrufs der Zustimmung.
- (10)<sup>15</sup> Beschäftigte, die in den Dienststellen der Universität mit Daten umgehen, sind gemäß Artikel 8 Abs. 4 des Gesetzes I aus dem Jahr 2012 über das Arbeitsgesetzbuch, das Eütv und das Eüak sowie anderen Vorschriften, die eine Geheimhaltung vorschreiben, zur zeitlich unbegrenzten Geheimhaltung der im Rahmen ihrer Tätigkeit gewonnenen personenbezogenen Daten verpflichtet. Die Vertraulichkeit erstreckt sich nicht auf die gesetzlichen Verpflichtungen zur Erteilung von Auskünften, Beschwerden und Mitteilungen von öffentlichem Interesse sowie auf die Offenlegung von Daten von öffentlichem Interesse und auf die Verpflichtung zur Erteilung von Auskünften und Mitteilungen von öffentlichem Interesse.
- <sup>16</sup>Eine neue Mitarbeiterin/ein neuer Mitarbeiter der Universität erhält bei ihrem/seinem Arbeitsantritt grundlegende Datenschutzinformationen als Teil ihres/seines Einführungspakets. Fort- und Weiterbildungsmaßnahmen werden von der ABK organisiert. Der örtliche Datenschutzbeauftragte führt Aufzeichnungen über die Schulung der Mitarbeiter, einschließlich der folgenden Punkte:
- a) den Namen des Teilnehmers an der Schulung,
  - b) das Datum der Grundausbildung,
  - c) datum der Fortbildung.

### 1.5. Datenschutz durch Technik, Datenschutz-Folgenabschätzung

- (1)<sup>17</sup>Auf Ersuchen des örtlichen Datenschutzbeauftragten führt die ABK vor der Aufnahme neuer Verarbeitungsvorgänge (insbesondere beim Einsatz neuer Verarbeitungstechnologien) eine Folgenabschätzung der Auswirkungen der geplanten Verarbeitung auf den Schutz personenbezogener Daten durch, wenn diese wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen.

---

<sup>15</sup>2012 Gesetz Nr.: I Artikel 8 Absatz (4), Artikel 25 des Gesetzes CLIV von 1997 über die Gesundheitsversorgung und Artikel 219 des Gesetzes C von 2012 über das Strafgesetzbuch

<sup>16</sup>VERORDNUNG Artikel 39 Absatz 1 lit. b)

<sup>17</sup>VERORDNUNG Artikel 25 und 35

- (2) Bei der Durchführung einer Datenschutz-Folgenabschätzung muss der behördliche Datenschutzbeauftragte fachlichen Rat einholen.
- (3) In den folgenden Fällen sollte eine Folgenabschätzung durchgeführt werden:
  - a) bei der Durchführung einer systematischen und umfassenden Bewertung bestimmter persönlicher Aspekte natürlicher Personen auf der Grundlage einer automatisierten Verarbeitung, einschließlich Profiling, auf die sich Entscheidungen stützen, die rechtliche Folgen für eine natürliche Person haben oder eine natürliche Person in ähnlicher Weise erheblich beeinträchtigen,
  - b) groß angelegte systematische Überwachung öffentlicher Plätze, z. B. durch den Einsatz eines elektronischen Überwachungssystems (Kamera), das diese Bedingungen erfüllt;
  - c) für die Verarbeitung einer großen Anzahl von Gesundheitsdaten und anderen sensiblen Daten; für die Verarbeitung, die auf der Liste der Aufsichtsbehörde für obligatorische Datenschutz-Folgenabschätzungen steht.
  - d) Kommt die Datenschutz-Folgenabschätzung zu dem Schluss, dass die geplante Verarbeitung tatsächlich ein hohes Risiko darstellt, wenn keine Maßnahmen zur Risikominderung ergriffen werden, konsultiert die/der DSB vor der Verarbeitung personenbezogener Daten die Aufsichtsbehörde.
- (4) Die Universität stellt sicher, dass ihre internen Richtlinien, Arbeitsanweisungen und Verträge den Datenschutzerfordernungen entsprechen. Vor dem Erlass von Verordnungen, Anweisungen, (internen Regelungsdokumenten), Arbeitsanweisungen und Musterverträgen wird die Stellungnahme der ABK zu Fragen der Verarbeitung personenbezogener Daten eingeholt. Bei der Genehmigung von Verordnungen und Anweisungen ist gegebenenfalls die Genehmigung der Verordnung anzugeben.

#### 1.6. Durchsetzung der Datenschutzgrundsätze und Gewährleistung der Rechenschaftspflicht

- (1) <sup>18</sup>Die Universität kann personenbezogene Daten verarbeiten, wenn:
  - a) Die Verarbeitung ist gesetzlich vorgeschrieben (Pflichtverarbeitung). Diese Verarbeitung umfasst insbesondere die Verarbeitung im Zusammenhang mit Tätigkeiten im Bereich der Hochschulbildung, der Beschäftigung, des öffentlichen Bildungswesens oder der Erbringung von Gesundheitsdienstleistungen.
  - b) Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich. Dabei handelt es sich insbesondere um Verarbeitungen, die für die Erfüllung einer rechtlichen Verpflichtung unbedingt erforderlich sind (z. B. die Bereitstellung von Daten).
  - c) Die betroffene Person muss der Verarbeitung gemäß Punkt 1.4. (8) lit. a) bis c) zustimmen. Zu diesen Verarbeitungen gehören insbesondere Verarbeitungen im Zusammenhang mit dem Versand von Newslettern auf der Grundlage freiwilliger

---

<sup>18</sup> VERORDNUNG Artikel 5 Absatz 2, Artikel 5 Absatz 1 und Artikel 6

- Abonnements, der Teilnahme an Veranstaltungen, Gewinnspielen, dem Ausfüllen von Fragebögen oder der Teilnahme an wissenschaftlichen Untersuchungen.
- d) Die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung von Maßnahmen erforderlich, die auf Antrag der betroffenen Person vor Abschluss des Vertrags erfolgen; die Verarbeitung kann insbesondere im Rahmen einer freiwilligen Leistung der Universität erfolgen.
  - e) Die Verarbeitung ist für die Wahrung lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich;
  - f) Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere wenn es sich bei der betroffenen Person um ein Kind handelt.
- (2) <sup>19</sup>Die Universität ergreift die folgenden Maßnahmen, um sicherzustellen, dass die Grundsätze des Datenmanagements bei der Verarbeitung personenbezogener Daten eingehalten werden:
- a) <sup>20</sup>Für Rechtmäßigkeit, Fairness und Transparenz: Die Verarbeitung personenbezogener Daten muss rechtmäßig, fair und für die betroffene Person transparent sein. Bei der Verarbeitung personenbezogener Daten sollten natürliche Personen transparent über die Rechtsgrundlage, die Art und Weise der Erhebung und Verwendung ihrer personenbezogenen Daten, den Umfang der verarbeiteten Daten sowie die Möglichkeit und die Mittel des Zugangs zu diesen Daten informiert werden. Um sicherzustellen, dass die Verarbeitung personenbezogener Daten für die betroffene Person transparent ist, führt der örtliche Datenschutzbeauftragte ein Verzeichnis aller Verarbeitungen für jeden Verarbeitungszweck und erstellt für jede darin aufgezeichnete Verarbeitung einen Verarbeitungshinweis, der registriert und auf der Website seiner Dienststelle öffentlich und uneingeschränkt zugänglich gemacht wird.
  - b) <sup>21</sup>Zielorientierung: Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Personenbezogene Daten dürfen nicht in einer Weise verarbeitet werden, die mit diesen Zwecken unvereinbar ist.
  - c) <sup>22</sup>Datensparsamkeit: Personenbezogene Daten müssen dem Zweck entsprechen, für den sie verarbeitet werden, dafür erheblich sein und sich auf das beschränken, was für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
  - d) <sup>23</sup>Genauigkeit: Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein, d. h. es sind alle angemessenen Maßnahmen zu treffen, um sicherzustellen, dass personenbezogene Daten, die für die Zwecke, für die sie verarbeitet werden, unrichtig sind, unverzüglich gelöscht oder berichtigt werden.
  - e) <sup>24</sup>Eingeschränkte Speicherbarkeit: Personenbezogene Daten dürfen nur so lange, wie

---

<sup>19</sup> VERORDNUNG Artikel 5 Absatz 2, Artikel 5 Absatz 1 und Artikel 6

<sup>20</sup>VERORDNUNG Artikel 5 Absatz 1 lit. a)

<sup>21</sup>VERORDNUNG Artikel 5 Absatz 1 lit. b)

<sup>22</sup>VERORDNUNG Artikel 5 Absatz 1 lit. c)

<sup>23</sup>VERORDNUNG Artikel 5 Absatz 1 lit. d)

<sup>24</sup>VERORDNUNG Artikel 5 Absatz 1 lit. e)

es für die Erreichung der Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht; personenbezogene Daten dürfen nur dann länger aufbewahrt werden, wenn ein berechtigtes Interesse an der weiteren Verarbeitung besteht. Um sicherzustellen, dass die Speicherung personenbezogener Daten auf den erforderlichen Zeitraum begrenzt ist, legt die Universität in ihrer Datenverwaltungspolitik eine Frist für die Löschung personenbezogener Daten für alle ihre Verarbeitungen fest und vermerkt diese Frist in ihren Datenverwaltungsunterlagen.

- f) Integrität und Vertraulichkeit: Personenbezogene Daten müssen so verarbeitet werden, dass eine angemessene Sicherheit der personenbezogenen Daten gewährleistet ist, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Beschädigung, indem geeignete technische und organisatorische Maßnahmen getroffen werden.
- g) <sup>25</sup>Rechenschaftspflicht: Die ABK leistet praktische Hilfe, um die Einhaltung der Anforderungen dieser Politik bei der Gestaltung der mit der Datenverwaltung verbundenen Prozesse zu gewährleisten. Die/der Datenschutzbeauftragte prüft jährlich die Einhaltung der Datenschutzrichtlinie, und der Datenschutzbeauftragte prüft die Einhaltung im Laufe des Jahres von Fall zu Fall. Die ABK überprüft regelmäßig den aktuellen Stand der Einhaltung der Vorschriften durch jährliche Selbstprüfungsberichte, die von den örtlichen Datenschutzbeauftragten erstellt werden.

### 1.7. Datenmanagement und Sicherheitsstandards im Rahmen der Verwaltung

- (1) <sup>26</sup>Die/der Angestellte der Universität bewahrt Unterlagen, die Daten enthalten, die nach den Bestimmungen des Infotv., der Verordnung und dieser Ordnung als personenbezogene Daten gelten, außerhalb der Arbeitszeit und nach Möglichkeit auch während der Arbeitszeit in einem verschlossenen Schrank auf. Offizielle Dokumente dürfen nur für den Zweck und die Dauer der Arbeit auf dem Schreibtisch und an anderen Orten im Büro aufbewahrt werden.
- (2) <sup>27</sup>Ein Dokument mit personenbezogenen Daten, das sich im Besitz des Verwalters oder in den Archiven befindet, kann von einer anderen Person als dem Verwalter und dem Leiter des Verwalters nur dann eingesehen werden, wenn das Gesetz dies zulässt oder wenn der Verwalter in einem Antrag bescheinigt, dass die Erfüllung ihrer Aufgaben dies erfordert.
- (3) <sup>28</sup>In Ermangelung einer gesetzlichen Ermächtigung dürfen Daten nur mit Zustimmung der betroffenen Person an einen Dritten übermittelt werden. Stimmt die betroffene Person der Übermittlung ihrer Daten an eine andere Stelle nicht zu, muss ihr mitgeteilt werden, dass ihrem Wunsch nicht oder nicht vollständig entsprochen werden kann.

---

<sup>25</sup>VERORDNUNG Artikel 5 Absatz 2

<sup>26</sup>VERORDNUNG Artikel 5 Absatz 1 lit. f)

<sup>27</sup>VERORDNUNG Artikel 5 Absatz 1 lit. f)

<sup>28</sup>VERORDNUNG Artikel 6 Absatz 1

- (4) Bei der Übermittlung von Daten innerhalb der Universität muss der Anfragende stets den Zweck und die Rechtsgrundlage der Datenanforderung begründen. Die Übermittlung von Daten kann erst erfolgen, wenn dies überprüft wurde.
- (5) <sup>29</sup>Bei der Ausübung des Auskunftsrechts muss die betroffene Person oder ihr Vertreter so handeln, dass die Rechte anderer nicht verletzt werden (personenbezogene oder geschützte Daten einer anderen Person müssen verborgen oder auf andere Weise unkenntlich gemacht werden). Bei der Anfertigung einer Kopie oder eines Auszugs ist das gleiche Verfahren anzuwenden.
- (6) <sup>30</sup>Für die sichere Verwahrung der in Absatz 1 genannten Dokumente ist die Verwalterin/der Verwalter verantwortlich, die/der sie bei Arbeitsschluss in ihrem/seinem Besitz hat. Neben anderen Erwägungen sollten Räumlichkeiten, in denen gemeinsam genutzte Drucker oder Kopierer betrieben werden, aus Gründen des Datenschutzes in Übereinstimmung mit den Anforderungen an die Datensicherheit genutzt werden.
- (7) <sup>31</sup>Neben anderen Erwägungen sollten Räumlichkeiten, in denen gemeinsam genutzte Drucker oder Kopierer betrieben werden, aus Gründen des Datenschutzes in Übereinstimmung mit den Anforderungen an die Datensicherheit genutzt werden. Der Administrator verwaltet und speichert den Computer und die damit verbundenen Datenträger so, dass die zu schützenden Daten für Unbefugte unzugänglich sind. Sie sind außerdem verpflichtet, den Arbeitsplatz bei Arbeitsende auszuschalten - außer bei Arbeitsplätzen, die ständig eingeschaltet und online sind - und die Tür abzuschließen.
- (8) <sup>32</sup>Dokumente, die personenbezogene Daten enthalten, dürfen nur mit Genehmigung des unmittelbaren Vorgesetzten aus den Räumlichkeiten der Universität entfernt werden, es sei denn, sie dienen der Erfüllung dienstlicher Aufgaben. Der Verwalter muss dafür sorgen, dass sie nicht verloren geht, beschädigt oder zerstört wird und dass ihr Inhalt nicht an Unbefugte weitergegeben wird.
- (9) <sup>33</sup>Die Daten sind für die Zwecke, für die sie verarbeitet wurden, nicht mehr erforderlich, und Daten, für die die Zwecke, für die sie verarbeitet wurden, weggefallen sind oder geändert wurden, werden unverzüglich oder nach Ablauf der in der Datenverwaltungspolitik vorgesehenen Aufbewahrungsfrist vernichtet. Andere Dokumente, die personenbezogene Daten enthalten, müssen ebenfalls mit den erforderlichen Sicherheitsmaßnahmen vernichtet werden.
- (10) <sup>34</sup>Der Leiter der Dienststelle legt die Zugriffsrechte auf einzelne Datensätze und die Datenverwaltung nach Personen und Funktionen gemäß den Bestimmungen der Informationssicherheitspolitik fest.
- (11) <sup>35</sup>In Verfahren, die auf Antrag oder Initiative der betroffenen Person eingeleitet werden, gilt die Einwilligung in Bezug auf die für die Durchführung des Verfahrens erforderlichen personenbezogenen Daten als erteilt, wenn die Verarbeitung auf der Einwilligung der betroffenen Person beruht.

---

<sup>29</sup>VERORDNUNG Artikel 5 Absatz 1 lit. f)

<sup>30</sup>VERORDNUNG Artikel 32

<sup>31</sup>VERORDNUNG Artikel 5 Absatz 1 lit. f)

<sup>32</sup>VERORDNUNG Artikel 5 Absatz 1 lit. f)

<sup>33</sup>VERORDNUNG Artikel 32

<sup>34</sup>VERORDNUNG Artikel 32

<sup>35</sup>VERORDNUNG Artikel 6 Absatz 1

- (12) <sup>36</sup>Die Verarbeitung auf der Grundlage einer Einwilligung erfordert die schriftliche Einwilligung der betroffenen Person (die ihre personenbezogenen Daten und ihre Erklärung enthält, dass sie auf der Grundlage des von dem für die Verarbeitung Verantwortlichen veröffentlichten Hinweises auf die Verarbeitung, von dem sie Kenntnis erlangt hat (Name und Ort des Hinweises), aus freien Stücken in die Verarbeitung ihrer personenbezogenen Daten durch den für die Verarbeitung Verantwortlichen zu den dort genannten Zwecken und auf der dort genannten Rechtsgrundlage einwilligt.
- (13) <sup>37</sup>Es dürfen nur personenbezogene oder spezifische Daten verarbeitet werden, die für den Zweck des Falles unbedingt erforderlich sind und deren Zweck gerechtfertigt werden kann. Die Daten dürfen nur für den Zweck des betreffenden Falles verwendet und nicht mit anderen Verfahren und Daten verknüpft werden, es sei denn, das Gesetz sieht etwas anderes vor.
- (14) <sup>38</sup>Um die Qualität der Daten zu gewährleisten, dürfen personenbezogene Daten nur anhand eines gültigen amtlichen Ausweises, der die betroffene Person identifiziert, und bestimmte Daten nur mit schriftlicher Zustimmung der betroffenen Person erfasst werden.
- (15) <sup>39</sup>Bei der Erhebung und Weiterverarbeitung von Daten muss auf die Richtigkeit, Vollständigkeit und Aktualität der personenbezogenen Daten geachtet werden, damit die Rechte der Betroffenen nicht beeinträchtigt werden.
- (16) <sup>40</sup>Nicht in der Akte enthaltene personenbezogene und spezifische Daten, die in einer Papierakte erfasst sind, müssen unkenntlich gemacht werden, um ihre weitere Verwendung zu verhindern. Arbeitskopien, die während des computergestützten Verfahrens erstellt wurden, oder Kopien, die beschädigt oder aus anderen Gründen überflüssig geworden sind, müssen vernichtet werden.

#### 1.8. Allgemeine Zwecke der Verarbeitung, Verarbeitung von Dokumenten und Unterlagen

- (1) <sup>41</sup>Die Universität verarbeitet Daten zu Verwaltungs- und Archivierungszwecken auf der Grundlage eines anderen Zwecks.
- (2) Die in dieser Richtlinie geforderten Aufzeichnungen und Dokumente werden vom örtlichen Datenschutzbeauftragten geführt und erstellt. Die Leiterin/der Leiter der Dienststelle, die den örtlichen Datenschutzbeauftragten bestellt, ist für die Vollständigkeit der Aufzeichnungen sowie für die Richtigkeit und Aktualität der darin enthaltenen Daten verantwortlich.

---

<sup>36</sup>VERORDNUNG Artikel 7

<sup>37</sup>VERORDNUNG Artikel 5 Absatz 1 lit. b)

<sup>38</sup>VERORDNUNG Artikel 5 Absatz 1 lit. d)

<sup>39</sup>VERORDNUNG Artikel 5 Absatz 1 lit. d)

<sup>40</sup>VERORDNUNG Artikel 5 Absatz 1 lit. f)

<sup>41</sup>VERORDNUNG Artikel 6

### 1.9. Aufzeichnungen über Verarbeitungstätigkeiten

- (1) <sup>42</sup> Die Verarbeitung personenbezogener Daten an der Universität erfolgt nach der Registrierung der Datenverarbeitung gemäß Artikel 30 der Verordnung.
- (2) Die Universität als für die Datenverarbeitung Verantwortliche führt und pflegt das Datenverwaltungsregister dezentral über die lokalen Datenschutzbeauftragten.
- (3) Die Leiterin/der Leiter der Dienststelle, die/der die Datei zu Aufzeichnungszwecken führt, meldet der EAV die Anlage einer neuen Datei vor Beginn der Tätigkeit. Stellt die ABK oder die/der Datenschutzbeauftragte bei der Wahrnehmung ihrer Aufgaben fest, dass die Verarbeitung personenbezogener Daten die Führung eines Registers erfordert, unterrichtet sie/er den Leiter der Dienststelle und leistet methodische Unterstützung bei der Durchführung der Aufgaben im Zusammenhang mit dem Register.
- (4) Das Register der Datenverwaltung enthält eine Aufzeichnung der Datenverwaltung aller Teile der Dienststelle entsprechend ihrer internen Organisation. Die Abteilung führt eine in den Prozess integrierte Selbstkontrolle durch, und die ABK prüft jährlich die Angemessenheit und Aktualität des Inhalts der veröffentlichten Unterlagen. Die Abteilung vervollständigt und ändert das Datenverwaltungsregister nach Bedarf. Im Falle einer eingestellten Verarbeitung archiviert das Departement die Verarbeitungsunterlagen, und im Falle einer neuen Verarbeitung erstellt es eine neue Verarbeitungsakte.
- (5) Das Register wird auf den Websites der Dienststellen, die verpflichtet sind, einen lokalen DSB zu benennen, im xls-Format veröffentlicht.
- (6) Ein Muster des Datenverwaltungsregisters finden Sie in der Formularbibliothek.

### 1.10. Übermittlung von Daten und Aufzeichnung der übermittelten Daten

- (1) <sup>43</sup> Personenbezogene Daten werden an andere Personen als die betroffene Person weitergegeben, die ausdrücklich auf die Zwecke und die Rechtsgrundlage der Verarbeitung hingewiesen haben und die aufgrund gesetzlicher Bestimmungen ein Recht auf Zugang zu den Daten haben.
- (2) Die Übermittlung von Daten muss protokolliert werden, damit festgestellt werden kann, welche Daten von dem für die Verarbeitung Verantwortlichen an wen, mit welcher Befugnis und zu welchem Zeitpunkt (z. B. im Rahmen der Rechtshilfe im Inland usw.) übermittelt oder bereitgestellt wurden. Ist die Eintragung eines neuen Eintrags in das Register gerechtfertigt, wenn die Bestimmung des Rechtstitels nicht eindeutig ist, prüft die ABK die Rechtsgrundlage und die Rechtmäßigkeit der Übertragung auf der Grundlage eines individuellen Antrags des örtlichen Datenschutzbeauftragten und nimmt zur Durchführbarkeit der Übertragung Stellung.
- (3) Das Register wird von dem örtlichen Datenschutzbeauftragten jeder Dienststelle geführt.
- (4) Die Leiterin/der Leiter der Dienststelle ist gegenüber der betroffenen Person für die Rechtmäßigkeit der Übermittlung der von ihm verarbeiteten Daten verantwortlich.

---

<sup>42</sup>VERORDNUNG Artikel 30

<sup>43</sup> VERORDNUNG Artikel 5 Absatz 2

- (5) Kann die Übermittlung nicht rechtmäßig durchgeführt werden oder werden die für die Beurteilung des Ersuchens erforderlichen Informationen von der betroffenen Person nach dem Ersuchen nicht vorgelegt, wird die Übermittlung abgelehnt.
- (6) Jede Verweigerung der Datenübermittlung wird dem Antragsteller unter Angabe der Gründe schriftlich mitgeteilt.
- (7) In Ermangelung einer gesetzlichen Ermächtigung zur Datenübermittlung wird die betroffene Person in dem auf ihren Antrag hin eingeleiteten Verfahren schriftlich um ihre Zustimmung zur Übermittlung ihrer personenbezogenen Daten gebeten, sofern die Bearbeitung ihres Falles die Einschaltung einer anderen Stelle erfordert.
- (8) Die betroffene Person hat das Recht, Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu erhalten und die Berichtigung, Löschung oder Sperrung ihrer personenbezogenen Daten zu verlangen, sofern es sich nicht um eine obligatorische Verarbeitung handelt. Ersuchen um Auskunft über die Datenverarbeitung müssen vorbehaltlich der rechtlichen Bedingungen innerhalb von höchstens 30 Tagen, vorzugsweise jedoch unverzüglich, beantwortet werden.
- (9) Personenbezogene Daten dürfen nur dann übermittelt oder bereitgestellt werden, und verschiedene Verarbeitungsvorgänge dürfen nur dann miteinander kombiniert werden, wenn die betroffene Person eingewilligt hat oder wenn dies gesetzlich vorgeschrieben oder zulässig ist und die Voraussetzungen für die Verarbeitung der einzelnen personenbezogenen Daten erfüllt sind.
- (10) Der örtliche Datenschutzbeauftragte überprüft das Übermittlungsregister bis zum 31. Dezember eines jeden Jahres, ändert es erforderlichenfalls und erstellt einen Bericht über die Überprüfung. Das Protokoll ist der ABK bis zum 10. Januar des auf das betreffende Jahr folgenden Jahres elektronisch zu übermitteln.
- (11) Die ABK veröffentlicht ein Muster des gemäß Artikel 30 der Verordnung erstellten Übermittlungsregisters und ein Muster des für die Überprüfung des Registers erforderlichen Protokolls in der Formularbibliothek.

#### 1.11. Aufzeichnungen über Verarbeitungstätigkeiten

- (1) <sup>44</sup>Werden personenbezogene Daten über die betroffene Person bei der betroffenen Person erhoben, so unterrichtet der für die Verarbeitung Verantwortliche die betroffene Person mittels eines Datenschutzhinweises zum Zeitpunkt der Erhebung der personenbezogenen Daten oder, falls diese nicht bei der betroffenen Person erhoben werden, innerhalb einer angemessenen Frist nach Erhebung der Daten, spätestens jedoch innerhalb eines Monats.
- (2) Die Universität verwendet zwei Arten von Datenschutzhinweisen:
  - a) ein allgemeiner Informationsvermerk zum Datenmanagement als Zusammenfassung der Datenmanagementaktivitäten der Universität (vorbereitend: ABK, Veröffentlichung durch den Rektor, den Kanzler und den Präsidenten des Klinikums),
  - b) individuelle Hinweise zur Datenverarbeitung, in denen die einzelnen Verarbeitungstätigkeiten für jeden Zweck beschrieben werden (vom örtlichen

---

<sup>44</sup> VERORDNUNG Artikel 13 und 14

Datenschutzbeauftragten erstellt und vom Leiter der für den örtlichen Datenschutzbeauftragten zuständigen Abteilung veröffentlicht).

- (3) <sup>45</sup>Der allgemeine Datenschutzhinweis enthält:
- a) den Namen und die Anschrift der Universität,
  - b) den Namen und die Kontaktdaten des Vertreters der Universität,
  - c) den Namen und die Kontaktdaten des Vertreters der Universität,
  - d) die Zwecke, für die die personenbezogenen Daten von der Universität verarbeitet werden,
  - e) die Rechtsgrundlage für die Verarbeitung von Daten durch die Universität,
  - f) die wichtigsten Kategorien der von der Universität verarbeiteten personenbezogenen Daten,
  - g) die wichtigsten Kategorien von Personen, die von der Verarbeitung betroffen sind,
  - h) die allgemeine Aufbewahrungs- und Speicherdauer der von der Universität verarbeiteten Daten,
  - i) die allgemeinen organisatorischen und technischen Maßnahmen, die die Universität zur Gewährleistung der Datensicherheit getroffen hat,
  - j) die Datenschutzvorfälle und -risiken, die im Rahmen der Datenverarbeitung der Universität auftreten können, sowie die Maßnahmen, die zur Bewältigung dieser Risiken ergriffen wurden,
  - k) die Empfänger der von der Universität regelmäßig erbrachten personenbezogenen Datendienste,
  - l) die Kategorien der gemeinsam für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter, die bei der Datenverarbeitung der Universität eingesetzt werden, und die Art ihrer Tätigkeiten.
- (4) <sup>46</sup>Allgemeine Informationen zur Datenverwaltung nach Kategorien von betroffenen Personen
- a) die Verarbeitung der Daten der Beschäftigten,
  - b) die Verarbeitung der Daten der Studierenden,
  - c) über die Verarbeitung von Gesundheitsdaten,
  - d) datenverarbeitung zu Forschungszwecken,
  - e) die Verarbeitung personenbezogener Daten, die durch besondere Rechtsvorschriften geschützte Persönlichkeitsrechte enthalten
- die Informationsbroschüren.
- (5) <sup>47</sup>Zusätzlich zu Absatz 3 enthält der besondere Datenschutzhinweis die folgenden Informationen über die Universität
- a) die Zwecke, für die die personenbezogenen Daten verarbeitet werden, für die Zwecke, für die sie verarbeitet werden,
  - b) die Rechtsgrundlage für die Verarbeitung der Daten für die Zwecke, für die sie verarbeitet werden,

---

<sup>45</sup> VERORDNUNG Artikel 13

<sup>46</sup> VERORDNUNG Artikel 13

<sup>47</sup> VERORDNUNG Artikel 13

- c) die Kategorien personenbezogener Daten, die für die Zwecke, für die sie erhoben werden, verarbeitet werden,
  - d) die Kategorien von Personen, die von der Verarbeitung für die vorgesehenen Zwecke betroffen sind,
  - e) die allgemeine Verarbeitung und die Aufbewahrungsfrist der verarbeiteten Daten,
  - f) die allgemeinen organisatorischen und technischen Maßnahmen, die zur Gewährleistung der Datensicherheit getroffen werden,
  - g) die Datenschutzvorfälle und -risiken, die bei der Verarbeitung für die Zwecke, für die die Daten verarbeitet werden, auftreten können, und die Maßnahmen, die zur Behebung dieser Risiken getroffen wurden,
  - h) die Empfänger der Datenübermittlung für die Zwecke, für die sie verarbeitet werden,
  - i) die Namen und Tätigkeiten der gemeinsam für die Verarbeitung Verantwortlichen und der Auftragsverarbeiter, die für die Zwecke der Verarbeitung eingesetzt werden.
- (6) <sup>48</sup>Die Universität informiert die betroffenen Personen durch die auf ihrer Website veröffentlichten Hinweise zur Datenverwaltung über ihre Aktivitäten.
- a) Die allgemeinen Datenschutzhinweise werden von der ABK auf der Hauptseite der Website der Universität veröffentlicht.
  - b) Die spezifischen Datenschutzhinweise sind auf der Hauptseite der Website der für die Benennung des örtlichen DSB zuständigen Dienststelle, auf der Website der Generaldirektion Recht und Verwaltung (im Folgenden: JIF)-Website, und es muss ein Link zu diesen Websites angegeben werden.
- (7) <sup>49</sup>Über die Veröffentlichung spezieller Datenschutzhinweise ist ein Protokoll mit folgendem Inhalt zu führen
- a) das Aktenzeichen des Datenschutzhinweises,
  - b) den Titel des Datenschutzhinweises,
  - c) das Datum der Veröffentlichung des Datenschutzhinweises,
  - d) den Titel des Datenschutzhinweises,
- (8) <sup>50</sup>Der örtliche Datenschutzbeauftragte überprüft das Register der individuellen Datenschutzhinweise bis zum 31. Dezember eines jeden Jahres, ändert es erforderlichenfalls und erstellt einen Bericht über die Ergebnisse der Überprüfung. Das Protokoll ist der ABK bis zum 10. Januar des auf das betreffende Jahr folgenden Jahres elektronisch zu übermitteln.
- (9) Das Muster des ABK-Registers und das Muster des für die Überprüfung des Registers erforderlichen Protokolls sind in der Formularbibliothek veröffentlicht.

## 1.12. Dispositionsregister

- (1) <sup>51</sup>Der örtliche Datenschutzbeauftragte übt die in den Artikeln 15 bis 22 der Verordnung vorgesehenen Rechte der betroffenen Person aus
- a) Informationen,

---

<sup>48</sup> VERORDNUNG Artikel 5 Absatz 2

<sup>49</sup> VERORDNUNG Artikel 5 Absatz 2

<sup>50</sup> VERORDNUNG Artikel 5 Absatz 1 lit. d)

<sup>51</sup> VERORDNUNG Artikel 5 Absatz 2

- b) Zugang,
  - c) Korrektur/en,
  - d) Einschränkungen,
  - e) löschen/vergessen,
  - f) Datenübertragbarkeit,
  - g) Protest/e,
  - h) Beitrag/Beiträge
- ein Verzeichnis der Mittelzuweisungen nach Abteilungen führen.
- (2) Der örtliche Datenschutzbeauftragte überprüft das Register der Verwaltungen bis zum 31. Dezember jeden Jahres, ändert es erforderlichenfalls und erstellt einen Bericht über die Ergebnisse der Überprüfung. Das Protokoll und seine Anhänge werden der ABK bis zum 10. Januar des auf das betreffende Jahr folgenden Jahres elektronisch übermittelt.
  - (3) Das Muster des ABK-Registers und das Muster des für die Überprüfung des Registers erforderlichen Protokolls sind in der Formularbibliothek veröffentlicht.

### 1.13. Register der Auftragsverarbeiter, gemeinsam für die Verarbeitung Verantwortlichen, Datenverarbeitung

- (1) Verarbeitungs-, Gemeinschaftsverarbeitungs- und Drittverarbeitungsverträge, die von der Universität für einen dritten Verantwortlichen abgeschlossen werden, unterliegen ebenfalls der Stellungnahme der ABK im Rahmen des Rechtsgutachtens.
- (2) Die ABK führt ein Register der Verträge im Sinne von Absatz 1, das Folgendes enthält:
  - a) Name, Anschrift und Vertreter des Datenverarbeiters, des gemeinsam für die Verarbeitung Verantwortlichen, des für die Verarbeitung Verantwortlichen, des Datenverarbeiters oder des für die Verarbeitung Verantwortlichen;
  - b) den Namen und die Kontaktdaten des Datenschutzbeauftragten des Datenverarbeiters, des gemeinsam für die Verarbeitung Verantwortlichen oder des für die Verarbeitung Verantwortlichen oder der für die Verarbeitung Verantwortlichen Organisation;
  - c) den Zweck der Verarbeitung;
  - d) die Rechtsgrundlage für die Verarbeitung von Daten zum Zweck der Datenverwaltung und -verarbeitung;
  - e) die Kategorien personenbezogener Daten, die für die Zwecke der Verarbeitung verarbeitet werden;
  - f) die Kategorien von Personen, die von der Verarbeitung betroffen sind, für die Zwecke der Verarbeitung;
  - g) den Geltungsbereich des Abkommens über die Datenverarbeitung;
  - h) die betreffende Abteilung der Universität.
- (3) Die Verarbeitung unterliegt einer Vereinbarung gemäß Artikel 28 der Verordnung und die gemeinsam für die Verarbeitung Verantwortlichen einer Vereinbarung gemäß Artikel 30 der Verordnung als Untervertrag zum Grundvertrag. Ein Muster davon wird von der ABK in der Formularbibliothek veröffentlicht.

#### 1.14. Datenschutzvorfälle und deren Aufzeichnung

- (1) <sup>52</sup>Die Mitarbeiter sind verpflichtet, mutmaßliche Datenschutzverletzungen (nachstehend "Vorfälle" genannt) innerhalb von 24 Stunden, nachdem sie davon Kenntnis erlangt haben, dem örtlichen Datenschutzbeauftragten (oder, falls es keinen Datenschutzbeauftragten gibt, dem Abteilungsleiter) zu melden.
- (2) Der örtliche Datenschutzbeauftragte meldet den Vorfall spätestens 36 Stunden, nachdem er davon Kenntnis erlangt hat, schriftlich an den DSB und den Beauftragten für Informationssicherheit.
- (3) Wird die Frist nicht eingehalten, erstellt der Leiter der betreffenden Abteilung einen Bericht an den Rektor und den Kanzler, die nach Rücksprache mit dem DSB über das weitere Vorgehen entscheiden.
- (4) <sup>53</sup>Die Universität führt über den Datenschutzbeauftragten ein Verzeichnis der betroffenen personenbezogenen Daten, der Anzahl und der Art der von dem Vorfall betroffenen Personen, des Datums des Vorfalls, der Umstände, der Auswirkungen und der zur Behebung des Vorfalls ergriffenen Maßnahmen sowie sonstiger Daten, die in den Rechtsvorschriften, die die Verarbeitung vorschreiben, festgelegt sind, um die im Zusammenhang mit dem Vorfall ergriffenen Maßnahmen zu überwachen und die betroffenen Personen zu informieren.
- (5) <sup>54</sup>Innerhalb von 48 Stunden nach der Meldung entscheidet der DSB, ob die Universität im Zusammenhang mit dem Vorfall eine Meldepflicht hat. Wenn die Universität verpflichtet ist, der Datenschutzbehörde Bericht zu erstatten, wird der Bericht zur Entscheidung durch den Rektor und den Kanzler vorbereitet, so dass der Bericht innerhalb von 72 Stunden erfolgen kann.
- (6) <sup>55</sup>Der behördliche Datenschutzbeauftragte wird den Vorfall bei der Bewertung des Risikos untersuchen:
  - a) die Art der Datenschutzverletzung,
  - b) den Umfang und die ungefähre Anzahl der betroffenen Personen,
  - c) die Kategorien und die ungefähre Anzahl der von dem Vorfall betroffenen Daten,
  - d) den Namen und die Kontaktdaten des örtlichen Datenschutzbeauftragten oder einer anderen Kontaktperson, die weitere Auskünfte erteilen kann,
  - e) die wahrscheinlichen Folgen des Vorfalls,
  - f) die ergriffenen oder geplanten Maßnahmen zur Behebung des Vorfalls, gegebenenfalls einschließlich Maßnahmen zur Abmilderung etwaiger negativer Folgen des Vorfalls.
- (7) Die Formulare, die für die Meldung eines Vorfalls an den Datenschutzbeauftragten, für die Bewertung des Vorfalls, für die Entscheidung über die Behandlung des Vorfalls, für die Meldung des Vorfalls an die Aufsichtsbehörde und für die Unterrichtung der betroffenen Personen über den Vorfall erforderlich sind, werden von der ABK im Formularspeicher veröffentlicht.

---

<sup>52</sup> VERORDNUNG Artikel 33

<sup>53</sup> VERORDNUNG Artikel 5 Absatz 2

<sup>54</sup> VERORDNUNG Artikel 33 Absatz 1

<sup>55</sup> VERORDNUNG Artikel 33 Absatz 3 Artikel 39 Absatz 19 lit. d)

- (8) <sup>56</sup>Der Datenschutzbeauftragte meldet der Aufsichtsbehörde nach Ermessen des Rektors und des Kanzlers einen Vorfall innerhalb von 72 Stunden, nachdem er davon Kenntnis erlangt hat, wenn der Vorfall ein Risiko für die Rechte der betroffenen Person darstellen könnte.
- (9) <sup>57</sup>Wenn die Verletzung des Schutzes personenbezogener Daten wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person zur Folge hat, informiert die Universität die betroffene Person im Einklang mit der Entscheidung des Rektors unverzüglich und innerhalb von höchstens 30 Tagen.
- (10) Der örtliche Datenschutzbeauftragte überprüft die von ihm geführten Aufzeichnungen über Vorfälle bis zum 31. Dezember eines jeden Jahres, ändert sie erforderlichenfalls und erstellt einen Bericht über die Ergebnisse der Überprüfung, die der ABK bis zum 10. Januar des folgenden Jahres auf elektronischem Wege übermittelt wird.
- (11) Die ABK veröffentlicht ein Muster des Ereignismanagementregisters und das für die Überprüfung des Registers erforderliche Protokoll im Formularspeicher.

#### 1.15. Lokale Datenschutzbeauftragte und ihre Aufzeichnungen

- (1) Zu 1.3. Der Leiter der nach Absatz 2 zu benennenden Dienststelle unterrichtet die ABK innerhalb von 8 Tagen über die Benennung des örtlichen Datenschutzbeauftragten und über den Widerruf der Benennung.
- (2) Die ABK führt ein Verzeichnis der örtlichen Datenschutzbeauftragten.
- (3) Das Register enthält die folgenden Angaben:
  - a) Name der Organisationseinheit
  - b) den Namen, die Position und die Kontaktdaten des örtlichen Datenschutzbeauftragten,
  - c) das Datum der Benennung/des Widerrufs der Benennung des örtlichen Datenschutzbeauftragten.

## 2. DIE RECHTE DER BETROFFENEN PERSONEN IN BEZUG AUF DIE DATENVERARBEITUNG ZU GEWÄHRLEISTEN

### 2.1. Sicherstellung der Rechte der betroffenen Person

- (1) Die Universität wird die Ausübung der Rechte der betroffenen Person erleichtern. Um ihre Rechte wahrnehmen zu können, muss die betroffene Person ihre Identität und ihre Berechtigung zum Zeitpunkt der Anfrage nachweisen. Wird der Antrag nicht von der antragsberechtigten Person gestellt oder kann der Antragsteller nicht ermittelt werden, so wird der Antrag abgelehnt. Der Antrag ist unter Verwendung des Formulars im Anhang der Geschäftsordnung einzureichen, das auf der JIF-Website für jedermann frei zugänglich ist.
- (2) Die Bewerbung ist elektronisch zu übermitteln an [adatvedelem@semmelweis.hu](mailto:adatvedelem@semmelweis.hu) oder auf dem Postweg an die folgende Adresse: Semmelweis Universität, Zentrum für Datenschutz und Patientenrechte, 1428 Budapest, Pf. 2.

---

<sup>56</sup> VERORDNUNG Artikel 33 Absatz 1

<sup>57</sup> VERORDNUNG Artikel 34

- (3) Wird der Antrag bei einer anderen Stelle der Universität eingereicht, muss er innerhalb von drei Arbeitstagen an die ABK weitergeleitet werden.
- (4) Wenn der Antrag unvollständig ist, fordert die ABK den Antragsteller auf, innerhalb von 8 Tagen einen Antrag zu stellen. Die Frist für das Ausfüllen des Antrags wird nicht auf die 8-tägige Übermittlungsfrist oder die 30-tägige Frist für das Ausfüllen des Antrags angerechnet.
- (5) Innerhalb von acht Arbeitstagen übermittelt die ABK das Ersuchen zusammen mit ihrer Stellungnahme zur Förderungswürdigkeit des Antragstellers und zur Durchführbarkeit des Ersuchens an die an der Erledigung beteiligte Dienststelle.
- (6) Die Leiterin/der Leiter der Dienststelle unterrichtet den Betroffenen unverzüglich, spätestens jedoch innerhalb von 30 Tagen nach Eingang des Antrags, über die aufgrund des Antrags getroffenen Maßnahmen.
- (7) Unter Berücksichtigung der Komplexität des Antrags und der Anzahl der Anträge kann die Frist erforderlichenfalls um weitere zwei Monate verlängert werden. Die ABK und die mit der Durchführung des Antrags befasste Stelle sind ebenfalls berechtigt, die Frist zu verlängern.
- (8) Die Leiterin/der Leiter der Dienststelle teilt dem Betroffenen die Fristverlängerung unter Angabe der Gründe innerhalb eines Monats nach Eingang des Antrags mit und unterrichtet gleichzeitig die ABK. Hat die betroffene Person den Antrag auf elektronischem Wege gestellt, so werden die Informationen nach Möglichkeit auf elektronischem Wege erteilt, sofern die betroffene Person nichts anderes verlangt.
- (9) Die Leiterin/der Leiter der den Antrag prüfenden Dienststelle unterrichtet den Antragsteller und die ABK innerhalb eines Monats nach Eingang des Antrags schriftlich über die Ablehnung des Antrags und gibt die Gründe für die Ablehnung an.
- (10) Der örtliche Datenschutzbeauftragte führt ein Verzeichnis der eingegangenen Ersuchen und ihrer Erledigung oder Ablehnung. Das Register enthält die folgenden Angaben:
  - a) das Aktenzeichen,
  - b) die Identifizierungsdaten des Antragstellers,
  - c) den Gegenstand des Antrags und die Art des betreffenden Rechts,
  - d) das Datum des Eingangs des Antrags,
  - e) das Datum und die Uhrzeit der Antragserfüllung,
  - f) den Grund und das Datum der Ablehnung,
  - g) die für die Bearbeitung des Antrags benötigte Zeitspanne.

## 2.2. Information der betroffenen Personen

- (1) <sup>58</sup>Um sicherzustellen, dass die betroffenen Personen ordnungsgemäß über die gesamte Datenverarbeitung informiert werden, wird die Universität einen Datenschutzhinweis herausgeben.
- (2) Zusätzlich zu den Informationen, die im Register über die Verarbeitung personenbezogener Daten enthalten sind, enthält die Mitteilung Informationen über die Tatsache, dass die betroffene Person

---

<sup>58</sup> VERORDNUNG Artikel 15

- a) haben das Recht, eine Bestätigung und Informationen über die über sie verarbeiteten Daten zu erhalten,
  - b) wie sie ihre Rechte in Bezug auf die Verarbeitung ausüben können,
  - c) kann von dem für die Verarbeitung Verantwortlichen Zugang zu den ihn betreffenden personenbezogenen Daten sowie deren Änderung, Berichtigung, Löschung oder Einschränkung der Verarbeitung verlangen und gegen die Verarbeitung dieser personenbezogenen Daten Widerspruch einlegen,
  - d) die Übertragbarkeit ihrer Daten bei dem für die Verarbeitung Verantwortlichen beantragen,
  - e) kann seine Einwilligung in die Verarbeitung jederzeit widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zu ihrem Widerruf erfolgten Verarbeitung berührt wird,
  - f) können zum Schutz ihrer Rechte eine Beschwerde bei der Aufsichtsbehörde einreichen,
  - g) ob die Bereitstellung personenbezogener Daten auf einer gesetzlichen oder vertraglichen Verpflichtung beruht oder eine Voraussetzung für den Abschluss eines Vertrags ist,
  - h) zur Bereitstellung der personenbezogenen Daten verpflichtet ist und welche Folgen die Nichtbereitstellung der Daten haben kann.
- (3) Im Falle einer Datenverarbeitung aufgrund einer Rechtsvorschrift, der Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Autorität erfolgt, der Erfüllung einer rechtlichen Verpflichtung der Universität, einer vertraglichen Verpflichtung, eigener berechtigter Interessen oder berechtigter Interessen Dritter oder der Interessen der betroffenen Person stellt die Universität die Informationen elektronisch zur Verfügung; die Universität stellt die Informationen auf ihrer zentralen Website zur Verfügung. Die Universität informiert die betroffenen Personen über den Ort, an dem der Hinweis auf die Zugänglichkeit der Informationen bei jeder Verarbeitung zu finden ist.
- (4) Im Falle einer Verarbeitung, die auf der Zustimmung der betroffenen Person beruht, muss die Mitteilung an die betroffene Person erfolgen - durch Empfangsbestätigung, Postzustellung oder elektronische Post - und das Dokument, das den Empfang bestätigt, muss bei der Verarbeitung aufbewahrt werden. Die Unterrichtung der betroffenen Person erfolgt, bevor die Daten bei ihr erhoben werden, um eine transparente Information, Kommunikation und geeignete Maßnahmen zur Ausübung der Rechte der betroffenen Person zu gewährleisten. Stammen die Daten nicht von der betroffenen Person, muss diese innerhalb von 30 Tagen informiert werden.
- (5) Die Leiterin/Leiter der für die Benennung des örtlichen Datenschutzbeauftragten zuständigen Dienststelle ist für die Bereitstellung der Informationen verantwortlich.

### 2.3. Gewährleistung des Rechts auf Änderung und Berichtigung von Daten

- (1) Bei der Gewährung des Rechts auf Berichtigung hat die betroffene Person das Recht, auf ihren Antrag hin von der Universität ohne unangemessene Verzögerung die Berichtigung oder Korrektur der sie betreffenden personenbezogenen Daten zu verlangen. Unter Berücksichtigung des Zwecks der Verarbeitung hat die betroffene Person das Recht, die

Vervollständigung unvollständiger personenbezogener Daten - auch mittels einer ergänzenden Erklärung - zu verlangen.

- (2) Die Änderung oder Löschung von Gesundheitsdaten sollte nur in der Weise erfolgen, dass die ursprünglich erfassten Daten lesbar bleiben.
- (3) Die Leiterin/der Leiter der Abteilung, die die Daten verarbeitet, ist für die Berichtigung der Daten verantwortlich.

#### 2.4. Sicherstellung des Rechts auf Löschung

- (1) Bei der Gewährung des Rechts auf Berichtigung hat die betroffene Person das Recht, auf ihren Antrag hin von der Universität ohne unangemessene Verzögerung die Berichtigung oder Korrektur der sie betreffenden personenbezogenen Daten zu verlangen.
  - a) ob die Verarbeitung personenbezogener Daten für die Zwecke, für die sie erhoben oder anderweitig verarbeitet wurden, noch erforderlich ist,
  - b) ob die betroffene Person die Einwilligung, auf die sich die Verarbeitung stützt, widerrufen hat und ob es eine andere Rechtsgrundlage für die Verarbeitung gibt,
  - c) ob die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und kein vorrangiger Rechtsgrund für die Verarbeitung vorliegt,
  - d) die Verarbeitung zu Zwecken der Direktwerbung erfolgt und ob die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat,
  - e) ob die personenbezogenen Daten unrechtmäßig verarbeitet wurden,
  - f) ob die personenbezogenen Daten gelöscht werden müssen, um einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten nachzukommen, dem der für die Verarbeitung Verantwortliche unterliegt,
  - g) ob die personenbezogenen Daten im Zusammenhang mit der Bereitstellung von Diensten der Informationsgesellschaft erhoben wurden.
- (2) Sind die Voraussetzungen für die Löschung der Daten erfüllt, wird die Universität die Löschung entsprechend dem Antrag der betroffenen Person unverzüglich vornehmen.
- (3) Ist die Verarbeitung der Daten gesetzlich vorgeschrieben und zulässig, so teilt der für die Verarbeitung Verantwortliche dies der betroffenen Person gleichzeitig mit der Ablehnung des Antrags mit.
- (4) Die Leiterin/der Leiter der Abteilung, die die Daten verarbeitet hat, ist für die Löschung der Daten verantwortlich.

#### 2.5. Gewährleistung des Rechts auf Einschränkung der Verarbeitung

- (1) Bei der Ausübung des Rechts auf Einschränkung der Verarbeitung hat die betroffene Person das Recht, von der Universität auf Antrag und ohne unnötige Verzögerung die Einschränkung der Verarbeitung in den folgenden Fällen zu verlangen:
  - a) wenn die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet, gilt die Einschränkung für den Zeitraum, der erforderlich ist, damit der für die Verarbeitung Verantwortliche die Richtigkeit der personenbezogenen Daten überprüfen kann,

- b) wenn die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der Daten ablehnt und stattdessen die Einschränkung ihrer Verwendung beantragt hat,
  - c) der für die Verarbeitung Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht mehr benötigt, die betroffene Person sie jedoch zur Begründung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt,
  - d) die betroffene Person hat gegen die Verarbeitung Widerspruch eingelegt; in diesem Fall gilt die Einschränkung für den Zeitraum, bis festgestellt ist, ob die berechtigten Gründe des für die Verarbeitung Verantwortlichen gegenüber denen der betroffenen Person überwiegen.
- (2) Sind die Voraussetzungen für die Einschränkung der Verarbeitung erfüllt, so kommt die Universität dem Antrag der betroffenen Person unverzüglich nach.
- (3) Die Leiterin/der Leiter der Abteilung, die die Daten verarbeitet, ist für die Einschränkung der Verarbeitung verantwortlich.

#### 2.6. Gewährleistung des Rechts auf Datenübertragbarkeit

- (1) Bei der Ausübung des Rechts auf Einschränkung der Verarbeitung hat die betroffene Person das Recht, von der Universität auf Antrag und ohne unnötige Verzögerung die Einschränkung der Verarbeitung in den folgenden Fällen zu verlangen:
- a) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder für die Durchführung von Maßnahmen erforderlich, die auf Antrag der betroffenen Person vor Abschluss des Vertrags erfolgen; oder
  - b) auf der Einwilligung der betroffenen Person beruht.
- (2) Sind die Voraussetzungen für die Datenübertragbarkeit erfüllt, so wird die Universität unverzüglich und entsprechend dem Antrag der betroffenen Person tätig,
- a) die Daten in einem strukturierten, allgemein gebräuchlichen, maschinenlesbaren Format bereitstellen,
  - b) die Daten direkt an den von der betroffenen Person benannten für die Verarbeitung Verantwortlichen zu übermitteln.
- (3) Die Leiterin/der Leiter der Abteilung, die die Daten verarbeitet, ist für die Übermittlung der Daten verantwortlich.

#### 2.7. Gewährleistung des Rechts auf Widerspruch gegen die Verarbeitung

- (1) Um das Recht auf Widerspruch gegen die Verarbeitung zu gewährleisten, hat die betroffene Person das Recht, auf ihren Antrag hin unverzüglich von der Universität prüfen zu lassen, ob das Recht auf Widerspruch gegen die Verarbeitung durchsetzbar ist, d.h.
- a) ob die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich war, die im öffentlichen Interesse wahrgenommen wurde,
  - b) ob die Verarbeitung zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich war.
- (2) Sind die Voraussetzungen für die Ausübung des Widerspruchsrechts erfüllt und gibt es keine andere Rechtsgrundlage für die Verarbeitung der Daten, so stellt die Universität die Verarbeitung der Daten gemäß den Anweisungen der betroffenen Person unverzüglich ein.

- (3) Die Leiterin/der Leiter der Abteilung, die die Daten verarbeitet, ist für die Beendigung der Datenverarbeitung verantwortlich.

## 2.8. Sicherstellung des Rechts auf Zugang zu Daten

- (1) Im Rahmen des Auskunftsrechts hat die betroffene Person das Recht, von dem für die Verarbeitung Verantwortlichen Auskunft darüber zu erhalten, ob ihre personenbezogenen Daten verarbeitet werden oder nicht, und, falls eine solche Verarbeitung stattfindet, das Recht auf Zugang zu den personenbezogenen Daten und auf die folgenden Informationen:
- a) die Kategorien der betroffenen personenbezogenen Daten;
  - b) die Zwecke der Verarbeitung;
  - c) die Empfänger oder Kategorien von Empfängern, an die die personenbezogenen Daten weitergegeben wurden oder werden, insbesondere auch an Empfänger in Drittländern und internationale Organisationen;
  - d) die vorgesehene Dauer der Speicherung der personenbezogenen Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
  - e) können von dem für die Verarbeitung Verantwortlichen die Berichtigung, Löschung oder Einschränkung der Verarbeitung sie betreffender personenbezogener Daten verlangen und gegen die Verarbeitung dieser personenbezogenen Daten Widerspruch einlegen;
  - f) das Recht haben, eine Beschwerde bei einer Aufsichtsbehörde einzureichen;
  - g) falls die Daten nicht bei der betroffenen Person erhoben wurden, alle verfügbaren Informationen über ihre Herkunft;
  - h) die Tatsache einer automatisierten Entscheidungsfindung, einschließlich Profiling, gemäß Artikel 22 Absätze 1 und 4 der Verordnung und zumindest in diesen Fällen die angewandte Logik sowie klare Informationen über die Bedeutung einer solchen Verarbeitung und ihre voraussichtlichen Folgen für die betroffene Person.
- (2) Werden personenbezogene Daten in ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien für die Übermittlung gemäß Artikel 46 der Verordnung informiert zu werden.
- (3) Die Leiterin/der Leiter der Abteilung, die die Daten verarbeitet, ist für die Übermittlung der Daten verantwortlich.

## 2.9. Prüfung der Rechtsgrundlage für die Verarbeitung

- (1) <sup>59</sup>Die Universität prüft jedes Jahr die Dokumentation aller im Datenverwaltungsregister erfassten Verarbeitungen personenbezogener Daten, um sicherzustellen, dass die darin enthaltenen Daten in Übereinstimmung mit dem Gesetz und den Richtlinien der Universität verarbeitet wurden, dass die entsprechende Rechtsgrundlage für die Verarbeitung weiterhin besteht und dass die Daten auf der Grundlage der entsprechenden Rechtsgrundlage verarbeitet werden. Die Leiterin/der Leiter der Abteilung handelt auf der

---

<sup>59</sup> VERORDNUNG Artikel 5 Absatz 1 lit. a) und Artikel 6

Grundlage der methodischen Leitlinien der ABK in Bezug auf die Rechtsgrundlage für die Datenverarbeitung.

- (2) Bei der Prüfung der Verarbeitung von Daten muss die Rechtsgrundlage für die Verarbeitung und das Vorhandensein von Unterlagen, die die Rechtsgrundlage für die Verarbeitung belegen, festgestellt werden. Die ABK wird Sie gegebenenfalls bei der Ermittlung der Rechtsgrundlage unterstützen.
- (3) <sup>60</sup>Die Rechtsgrundlage für die Verarbeitung durch die Universität und die erforderlichen Unterlagen:
  - a) Datenverarbeitung auf der Grundlage der Einwilligung der betroffenen Person: eine Verarbeitung, die auf der freien und ausdrücklichen Willensbekundung der betroffenen Person oder ihres gesetzlichen Vertreters beruht, die sich auf angemessene Informationen stützt (Zweck, Rechtsgrundlage, Dauer, Name des für die Verarbeitung Verantwortlichen, Anschrift des Auftragsverarbeiters und die Tätigkeit, für die die Daten verarbeitet werden) und mit der die betroffene Person ihre eindeutige Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten, ganz oder teilweise, erteilt;
  - b) die Verarbeitung, die für die Erfüllung eines mit der betroffenen Person geschlossenen oder zu schließenden Vertrags erforderlich ist: der mit der betroffenen Person geschlossene Vertrag - eine Erklärung über den Vertragsabschluss (mit Angabe der erforderlichen Verarbeitung im Vertrag oder mittels eines gesonderten Blatts, welche Verarbeitung für die Erfüllung welcher Vertragsbestimmung erforderlich ist);
  - c) die Verarbeitung, die zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der für die Verarbeitung Verantwortliche unterliegt: die genaue Rechtsvorschrift, die die Verarbeitung vorschreibt oder verlangt;
  - d) die Verarbeitung, die zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist: ob eine Interessenabwägung stattgefunden hat
    - da) den Zweck der Verarbeitung,
    - db) ob die Verarbeitung personenbezogener Daten für die Zwecke der betroffenen Person oder einer anderen natürlichen Person unbedingt erforderlich ist,
    - dc) ob alternative Mittel zur Verfügung stehen, um den beabsichtigten Zweck ohne Verarbeitung personenbezogener Daten zu erreichen,
    - dd) die möglichst genaue Definition des Begriffs "berechtigtes Interesse",
    - de) welche personenbezogenen Daten und wie lange das berechtigte Interesse die Verarbeitung erfordert,
    - df) welches die Interessen der anderen Partei sind, die rechtmäßig sicherstellen können, dass die Verarbeitung auf den Interessen der anderen Partei beruht;
  - e) die Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde: genaue Bezeichnung und Wortlaut der Rechtsvorschrift, in der das öffentliche Interesse des für die Verarbeitung Verantwortlichen oder der dem für die Verarbeitung Verantwortlichen übertragenen

---

<sup>60</sup>VERORDNUNG Artikel 6

- öffentlichen Gewalt definiert ist, sowie die von dieser Behörde festgelegte Notwendigkeit der Verarbeitung;
- f) <sup>61</sup>die Verarbeitung, die zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist: ob eine Interessenabwägung stattgefunden hat,
- fa) für den, für die Verarbeitung Verantwortlichen oder einen Dritten zur Erfüllung seiner Zwecke erforderlich ist ob die Verarbeitung der personenbezogenen Daten notwendig ist,
- fb) ob alternative Mittel zur Verfügung stehen, um den beabsichtigten Zweck ohne Verarbeitung personenbezogener Daten zu erreichen,
- fc) die möglichst genaue Definition des Begriffs "berechtigtes Interesse",
- fd) den Zweck der Verarbeitung,
- fe) wie lange das berechtigte Interesse die Verarbeitung der personenbezogenen Daten erfordert,
- ff) welches die Interessen der anderen Partei sind, die rechtmäßig sicherstellen können, dass die Verarbeitung auf den Interessen der anderen Partei beruht;
- (4) <sup>62</sup>Bei der Dokumentation der Verarbeitung auf der Grundlage einer Einwilligung sollte überprüft werden, dass
- a) die Unterlagen, die die Rechtsgrundlage belegen, sind verfügbar und wurden rechtmäßig erlangt,
- b) ob die Einwilligung die geeignete Rechtsgrundlage für die Verarbeitung der Daten war,
- c) die Zustimmung in der richtigen Form erteilt wurde,
- d) ob die betroffene Person vor der Erteilung der Einwilligung angemessene Informationen erhalten hat.
- (5) Die Universität bietet der betroffenen Person das Recht, ihre frühere Erklärung zurückzuziehen, zu ändern oder einzuschränken, indem sie auf ihrer Website das Formular "ANTRAG AUF ANWENDUNG DER KONTROLLRECHTE" zur Verfügung stellt, das ohne Einschränkung heruntergeladen werden kann.
- (6) Der örtliche Datenschutzbeauftragte ist für die Prüfung der Rechtsgrundlage für die Verarbeitung zuständig.

## 2.10. Besondere Datenverwaltung

- (1) Die Universität verarbeitet sensible Daten nur, wenn eine der in Artikel 9 Absatz 2 der Verordnung genannten Bedingungen erfüllt ist.
- (2) <sup>63</sup>Bei der Verarbeitung besonderer Kategorien personenbezogener Daten prüft der örtliche Datenschutzbeauftragte bei jedem Verarbeitungsvorgang, ob die Verarbeitung auf der Grundlage einer Einwilligung im Einklang mit den Vorschriften für die Datenverarbeitung erfolgt ist. Der Standpunkt der ABK zur Vereinbarkeit der Datenverarbeitung mit dem Gesetz ist maßgebend.

---

<sup>61</sup> VERORDNUNG Artikel 6 Absatz 1 lit. f), Präambel Absatz 69.

<sup>62</sup> VERORDNUNG Artikel 7

<sup>63</sup> VERORDNUNG Artikel 9

## 2.11. Verhinderung von Datenverlusten

- (1) <sup>64</sup> Die Universität verfügt über geeignete Verfahren zur Verhinderung, Aufdeckung, Meldung und Untersuchung von Datenlecks.
- (2) Die Universität ergreift die folgenden Maßnahmen, um die Weitergabe personenbezogener Daten im Einklang mit der Informationssicherheitspolitik zu verhindern:
  - a) die kontinuierliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste zu bewerten, die zur Verarbeitung personenbezogener Daten genutzt werden,
  - b) die Fähigkeit zu untersuchen, den Zugang zu personenbezogenen Daten und deren Verfügbarkeit im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen,
  - c) ein Verfahren für die regelmäßige Prüfung, Bewertung und Beurteilung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung im Rahmen der Informationssicherheit einzuführen,
  - d) eine Risikoanalyse durchzuführen, um das angemessene Sicherheitsniveau zu bestimmen, damit die Risiken der versehentlichen oder unrechtmäßigen Zerstörung, des Verlusts, der Veränderung, der unbefugten Weitergabe oder des Zugriffs auf übermittelte, gespeicherte oder anderweitig verarbeitete personenbezogene Daten und die damit verbundenen Schäden ermittelt werden können.

## 3. DAS DATENSCHUTZSYSTEM DER UNIVERSITÄT

### 3.1. Die/der Datenschutzbeauftragte

- (1) <sup>65</sup>Die Kanzlerin/der Kanzler ernennt im Einvernehmen mit dem Rektor einen unabhängigen Datenschutzbeauftragten aus dem JIF, der über einen Abschluss in Rechtswissenschaften und mindestens drei Jahre Erfahrung im Datenschutz verfügt, um die Aufgaben der Universität als Datenverantwortlicher und Datenverarbeiter wahrzunehmen, entweder im Wege einer Ausschreibung oder durch Zuweisung, bis die Bewerbung bewertet wurde.
- (2) <sup>66</sup> Die Universität stellt sicher, dass die/der Datenschutzbeauftragte angemessenen und rechtzeitigen Zugang zu allen Angelegenheiten hat, die die Verarbeitung und den Umgang mit personenbezogenen Daten betreffen. Um ihre/seine Aufgaben zu erfüllen, hat sie/er das Recht, auf die von den Dienststellen verwalteten Daten zuzugreifen und von den Dienststellen Daten anzufordern.
- (3) Die Universität stellt der/dem Datenschutzbeauftragten die zur Erfüllung dieser Aufgaben erforderlichen Mittel zur Verfügung, damit sie/er Zugang zu personenbezogenen Daten und Datenverarbeitungsvorgängen hat und ihr/sein Fachwissen aufrechterhalten kann.

---

<sup>64</sup> VERORDNUNG Artikel 32

<sup>65</sup> VERORDNUNG Artikel 37 Absatz 5 und 6

<sup>66</sup> VERORDNUNG Artikel 39

- (4) <sup>67</sup>Die/der DSB darf im Zusammenhang mit der Wahrnehmung ihrer/seiner Aufgaben von niemandem Weisungen entgegennehmen. Die/der DSB ist direkt der obersten Leitung der Universität unterstellt.
- (5) <sup>68,69</sup>
- (6) <sup>70</sup>Der DSB ist im Rahmen seiner Tätigkeit unabhängig von der Dauer des Rechtsverhältnisses und ohne zeitliche Begrenzung zur Vertraulichkeit verpflichtet.
- (7) Zu den Aufgaben des Datenschutzbeauftragten gehören insbesondere:
- a) um dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter Informationen und technische Beratung zukommen zu lassen,
  - b) die Umsetzung der datenschutzrechtlichen Steuerungsinstrumente und die Einhaltung der Vorschriften auf der Grundlage eines jährlichen Arbeitsplans zu überwachen und dem Rektor und dem Kanzler jährlich Bericht zu erstatten,
  - c) die Schulung des Personals zum Thema Datenschutz professionell zu überwachen,
  - d) auf Anfrage technische Beratung zur Datenschutz-Folgenabschätzung und Überwachung der Durchführung der Folgenabschätzung,
  - e) mit der Aufsichtsbehörde zusammenarbeiten,
  - f) als Kontaktstelle für die Aufsichtsbehörde in Fragen der Datenverarbeitung, einschließlich der vorherigen Konsultation, zu fungieren und sie gegebenenfalls in allen anderen Fragen zu konsultieren,
  - g) zur integrierten Risikobewertung der Universität beizutragen, um Datenschutzrisiken zu ermitteln,
  - h) im Rahmen ihrer beratenden Funktion schlagen sie die Themen für Datenschutzs Schulungen vor.
  - i) <sup>71</sup>unterstützt die betroffene Person bei der Wahrnehmung ihrer Rechte und leitet die erforderlichen Maßnahmen ein, damit der für die Verarbeitung Verantwortliche die Beschwerde prüfen und ihr abhelfen kann.
- (8) Die/der Datenschutzbeauftragte ist zu den Folgenden berechtigt:
- a) alle unter diese Richtlinie fallenden Verarbeitungen zu kontrollieren und alle Räumlichkeiten zu betreten, in denen eine Verarbeitung stattfindet,
  - b) Informationen und Klarstellungen zu allen unter diese Richtlinie fallenden Verarbeitungen anfordern,
  - c) mit Beratungs- und Zustimmungsrecht an allen Gremien der Universität und ihrer Dienststellen teilzunehmen, wenn Angelegenheiten aus seinem Zuständigkeitsbereich auf der Tagesordnung stehen.

### 3.2. Das Zentrum für Datenschutz und Patientenrechte (ABK).

- (1) Die ABK arbeitet als eine Abteilung des JIF unter der Leitung des Generaldirektors des JIF und unter der fachlichen Aufsicht des Datenschutzbeauftragten.

---

<sup>67</sup> VERORDNUNG Artikel 38 Absatz 3

<sup>68</sup> VERORDNUNG Artikel 38 Absatz 6

<sup>69</sup> Geändert durch Senatsbeschluss 54/2023 (29. Juni) Anhang 2, Artikel 1 Gültig ab dem: 11. Juli 2023.

<sup>70</sup> VERORDNUNG Artikel 38 Absatz 5

<sup>71</sup> VERORDNUNG Artikel 38 Absatz 4, Infotv. Artikel 25/M

- (2) Die ABK wird vom Direktor für Datenschutz und Patientenrechte geleitet.
- (3) Die Rolle der ABK im Prozess der Regulierung:
  - a) regelmäßige Überprüfung der Maßnahmen zur Datenverwaltung und Datensicherheit und Sicherstellung, dass sie auf dem neuesten Stand sind,
  - b) die Erstellung und Veröffentlichung der in dieser Verfahrensordnung vorgesehenen Formulare in der Formularbibliothek,
  - c) Mitwirkung und fachliche Beratung der Dienststellen bei der Ausarbeitung und Aktualisierung der Teile des Regelwerks, die die Datenverwaltung betreffen, einschließlich der Regeln für die Datenverwaltung.
- (4) Die Rolle der ABK bei der Beratung:
  - a) Anleitung und individuelle Beratung der lokalen Datenschutzbeauftragten und der Abteilungsleiter zu den Verfahren des Datenschutzes und der Patientenrechte innerhalb der Universität (Bearbeitung von Beschwerden, Offenlegung von Daten, Aufbewahrung von Unterlagen),
  - b) Ausarbeitung methodischer Leitfäden,
  - c) Unterstützung des Beauftragten für Informationssicherheit der Universität durch Beratung zu Datenschutzaspekten bei den Genehmigungs- und Zulassungsverfahren im Rahmen ihrer Tätigkeit.
- (5) Die Zuständigkeiten der ABK in Bezug auf Beschwerden und Meldungen von betroffenen Personen sind in den einschlägigen internen Vorschriften festgelegt.
- (6) Die ABK hat die Aufgabe, Folgendes zu überwachen:
  - a) bei Meldung oder Aufdeckung einer unrechtmäßigen Datenverarbeitung an deren Untersuchung mitzuwirken und bei deren Beseitigung mitzuwirken,
  - b) die Tätigkeiten der Dienststellen und der örtlichen Datenschutzbeauftragten im Zusammenhang mit den Datenschutzaufgaben zu überwachen.
- (7) Die ABK hat die Aufgabe, die Ausbildung zu organisieren:
  - a) Ausarbeitung eines Schulungsprogramms auf der Grundlage eines Vorschlags des DSB,
  - b) Erstellung von Schulungsmaterial zum Datenschutz für neue Mitarbeiter auf der Grundlage des Themas Datenschutzeschulung,
  - c) Organisation von Schulungen für lokale Datenschutzbeauftragte,
  - d) im Falle von Gesetzesänderungen die Informationen je nach Art und Umfang der Änderung zu organisieren.
- (8) Die ABK wirkt bei der Überprüfung von Verträgen über den Datenschutz und die Verarbeitung personenbezogener Daten im Rahmen der Vertragsordnung der Universität mit.
- (9) Um ihre Aufgaben zu erfüllen, sind die Mitarbeiter/innen von der ABK berechtigt, auf die von den Dienststellen verwalteten Daten zuzugreifen und Daten von den Dienststellen anzufordern. Die Mitarbeiter/innen der ABK sind im Zusammenhang mit diesen Tätigkeiten zur Verschwiegenheit verpflichtet, unabhängig von der Dauer ihres Arbeitsverhältnisses.

### 3.3. Benennung und Aufgaben des örtlichen Datenschutzbeauftragten

- (1) Die Leiterin/der Leiter der Abteilung, die verpflichtet ist, einen lokalen Datenschutzbeauftragten zu benennen, ist für die Datenverwaltung der ihr/ihm unterstellten Abteilung(en) verantwortlich.
- (2) Die Leiterin/Leiter der Abteilung, die für die Benennung des örtlichen Datenschutzbeauftragten zuständig ist
  - a) benennt einen örtlichen Datenschutzbeauftragten,
  - b) überwacht ihre/seine Aktivitäten in regelmäßigen Abständen durch Berichterstattung,
  - c) entscheidet über die weitere Speicherung oder Vernichtung der aufgezeichneten Daten nach Ablauf der vorgeschriebenen Aufbewahrungsfrist.
- (3) Der örtliche Datenschutzbeauftragte muss eine fachlich kompetente Person sein, die insbesondere über Fachkenntnisse im Datenschutzrecht und in der Datenschutzpraxis verfügt und in der Lage ist, die gesetzlich vorgeschriebenen Aufgaben zu erfüllen.
- (4) Der örtliche Datenschutzbeauftragte
  - a) sorgt für die Erstellung, Pflege, Veröffentlichung und Überprüfung der Aufzeichnungen und Informationen des Ressorts zum Datenmanagement und informiert die ABK über die Ergebnisse der Überprüfung gemäß den Bestimmungen dieser Richtlinie,
  - b) organisiert Datenschutzbildungen für Personen, die in der Dienststelle mit der Datenverwaltung und -verarbeitung befasst sind,
  - c) hilft auf Ersuchen der ABK bei der Beantwortung von Beschwerden über die Verarbeitung personenbezogener Daten durch die Dienststelle,
  - d) gibt auf Anfrage der ABK Auskunft über Beschwerden, Datenanfragen und ergriffene Maßnahmen,
  - e) den behördlichen Datenschutzbeauftragten über die mutmaßliche Datenschutzverletzung zu informieren,
  - f) stellt dem JIF Daten zur Verfügung, wenn das Ministerium Daten von öffentlichem Interesse anfordert oder wenn das Ministerium sie findet.
- (5) Wird kein örtlicher Datenschutzbeauftragter benannt, nimmt der Leiter der Dienststelle, die zur Benennung eines örtlichen Datenschutzbeauftragten befugt ist, die Aufgaben des örtlichen Datenschutzbeauftragten gemäß dieser Regelung wahr.

### 3.4. Das System zur Überwachung des Datenschutzes

- (1) <sup>72</sup>Die Rektorin/der Rektor, die Kanzlerin/der Kanzler und die Präsidentin/der Präsident des Klinikums überprüfen über den Datenschutzbeauftragten und der örtlichen Datenschutzbeauftragten die Umsetzung der Rechtsvorschriften zur Datenverwaltung und zum Datenschutz. Der Datenschutzbeauftragte erstellt jährlich bis zum 1. Februar einen Informationsbericht über den aktuellen Stand des Datenschutzes für den Rektor, den Kanzler und den Präsidenten des Klinikums.
- (2) Die Abteilungen überprüfen ihre eigenen Datenverwaltungsprozesse und deren Einhaltung durch prozessbegleitende Selbstprüfungen.

---

<sup>72</sup> VERORDNUNG Artikel 39; Artikel 5 Absatz 2

- (3) Die örtlichen Datenschutzbeauftragten überprüfen die von ihnen geführten Aufzeichnungen und die veröffentlichten Datenschutzhinweise bis zum 31. Dezember eines jeden Jahres und unterrichten die ABK bis zum 10. Januar des Jahres, das auf das betreffende Jahr folgt, über die Ergebnisse der Überprüfung, wie in dieser Regelung vorgesehen.
- (4) Die örtlichen Datenschutzbeauftragten prüfen auf der Grundlage eines jährlichen Prüfungsplans, ob die Dienststellen der Universität
  - a) ihren Verpflichtungen zum Schutz personenbezogener Daten nachkommen, und zwar insbesondere
    - aa) die Verpflichtung zur Information der betroffenen Personen,
    - ab) ihre Verpflichtung, das Auskunftsrecht der betroffenen Personen zu gewährleisten,
    - ac) ihre Verpflichtungen zur Wahrung der Rechte der betroffenen Personen.
  - b) ihren Verpflichtungen im Zusammenhang mit Datenschutzverletzungen nachzukommen,
- (5) Der Datenschutzbeauftragte führt ein Protokoll über die Kontrolle und ergreift die folgenden Maßnahmen:
  - a) im Falle der Feststellung eines Mangels den Leiter der betreffenden Dienststelle auffordern, innerhalb von 15 Tagen Maßnahmen zu ergreifen, wobei eine Frist von 15 Tagen gilt,
  - b) wird innerhalb von 30 Tagen nach Ablauf der Frist für die Durchführung der Maßnahme eine Nachkontrolle durchführen, um die Einhaltung der Maßnahme zu überprüfen.
  - c) Innerhalb von 15 Tagen nach der Nachkontrolle überprüft sie die Umsetzung der Maßnahme und informiert den Bundeskanzler mit der Aufforderung, tätig zu werden, falls die Maßnahme nicht oder nicht ordnungsgemäß umgesetzt wird.
- (6) Die ABK prüft die von den örtlichen Datenschutzbeauftragten erstellten jährlichen Überprüfungsberichte und leistet im Falle von Mängeln über die vom Generaldirektor für Rechts- und Verwaltungsangelegenheiten benannte Person Unterstützung, um die Einhaltung der Vorschriften sicherzustellen.
- (7) Die Revisionsdirektion handelt bei der Durchführung von Untersuchungen zum Datenschutz nach den für sie geltenden Vorschriften.

#### 4. UNTERSTÜTZUNG DER DATENVERARBEITUNGSABTEILUNGEN DER UNIVERSITÄT BEI DER EINHALTUNG DER VORSCHRIFTEN

- (1) Der Generaldirektor der JIF hat einen speziellen Mitarbeiter zur Förderung der Einhaltung des Datenschutzes ernannt, der in Zusammenarbeit mit dem örtlichen Datenschutzbeauftragten der Abteilung den Abteilungen nach einem vom Generaldirektor der JIF in vorheriger Absprache mit dem Direktor der ABK festgelegten Zeitplan methodische Unterstützung bietet
  - a) die Erstellung und Pflege der Datenschutzdokumentation (Prüfung der Angemessenheit des Datenschutzes),

- b) die Bewertung der operationellen Angemessenheit der Abteilungen (operationelles Datenschutzaudit) gemäß den von der Datenschutzbehörde festgelegten professionellen methodischen Standards,
  - c) zur Sicherstellung des in dieser Strategie geforderten Datenschutzbewusstseins die vom Abteilungsleiter auf Vorschlag des DSB benannten Bediensteten gemäß dem vom DSB aufgestellten Schulungsprogramm in Sachen Datenschutz schulen und bewerten,
  - d) regelmäßige Berichterstattung an den Generaldirektor des JIF über den aktuellen Stand der Maßnahmen zur Unterstützung der Einhaltung der Vorschriften.
  - e) Die/der benannte Mitarbeiterin/Mitarbeiter informiert den betreffenden örtlichen Datenschutzbeauftragten über ihre/seine Verfügbarkeit und den Zeitplan für die Schulung.
- (2) JIF veröffentlicht einen methodischen Leitfaden auf seiner Website
- a) die Verarbeitung der Daten der Beschäftigten,
  - b) die Verarbeitung der Daten der Studierenden,
  - c) die Verwaltung von Gesundheitsdaten,
  - d) Aufgaben im Zusammenhang mit der Verarbeitung von Daten, die durch besondere Rechtsvorschriften geschützte personenbezogene Daten betreffen, und
  - e) über Mittel zur Unterstützung der Einhaltung der Vorschriften durch Angemessenheits- und Betriebsprüfungen und Schulungen zur Gewährleistung des Datenschutzbewusstseins,
  - f) die Förderung der Einhaltung des Datenschutzes bei den vorbehaltenen Einrichtungen
- (3) Die Anwendung der Leitlinien ist für Personen und Organisationen, die unter diese Regelung fallen, obligatorisch und wird von den von ihr erfassten Einrichtungen erwartet.

## 5. Anhänge

Anhang 1: Arten von Aufzeichnungen, Informationsvermerken und Protokollen, die vom örtlichen Datenschutzbeauftragten geführt werden

Anhang 2: Prüfpfad

1. Anhang ...: Arten von Aufzeichnungen, Informationsvermerken und Protokollen, die vom örtlichen Datenschutzbeauftragten geführt werden
  
- A) Datenverarbeitungsregister - das in Artikel 30 der Verordnung genannte, zu führende Register (nach Art der Verarbeitungstätigkeit):
  1. pädagogische Aktivitäten:
  2. wissenschaftliche Forschungstätigkeiten
  3. Arbeits- und Humanressourcenaktivitäten
  4. Verwaltungstätigkeiten (Wirtschaft, Sekretariat, Kommunikation)
  
- B) Hinweise zur Datenverwaltung im Zusammenhang mit dem Verarbeitungsregister
  
- C) für weitere Aufzeichnungen:
  1. Informationsregister zur Datenverwaltung
  2. Datenübertragungsregister
  3. Register der Beiträge der beteiligten Parteien
  4. Dispositionsregister
  5. Bildungsregister
  6. Aufzeichnung von Datenschutzvorfällen
  
- D) Protokoll
  1. eine Aufzeichnung über die vorgeschriebene Führung von Aufzeichnungen
  2. Selbstinspektionsbericht

Anhang 2: Prüfpfad

2/A. Zentrum für Datenschutz und Patientenrechte

	Prozessschritte	Vorbereitungsschritte	Verantwortungsebenen					das aus dem Prozess resultierende Dokument
			Task-Manager	Überprüfung	Art der Überprüfung	Zulassung	Art der Zulassung	
1	Freigabe von Patientendaten	die Prüfung der Zulässigkeit eines Antrags	Beauftragte/r Mitarbeiter/in der ABK	Leiter/in der ABK	Dokumentenkontrolle, Unterschrift	Leiter/in der ABK	Unterschrift	Antwortdokument
2	eine Folgenabschätzung vorzunehmen	Bewertung der Notwendigkeit einer neuen Verarbeitung, Konsultation des Datenschutzbeauftragten	Leiterin/Leiter der betreffenden Dienststelle, örtlicher Datenschutzbeauftragter	Leiter/in der ABK, DPO	Datenanalyse	Leiter/in der ABK	Unterschrift	Dokument zur Folgenabschätzung
3	zentralisierte Bearbeitung von Patientenbeschwerden	Prüfung einer Überweisung im Rahmen des entsprechenden Verfahrens, an dem ein klinisches Zentrum beteiligt ist	Beauftragte/r Mitarbeiter/in der ABK	Leiter/in der ABK	Dokumentenkontrolle, Unterschrift	Leiter/in der ABK, Präsident/in des Klinikums	Unterschrift	Antwortdokument
4	Bearbeitung von Beschwerden auf organisatorischer Ebene	Unterstützung auf Anfrage, Stellungnahme zu einer bestimmten Angelegenheit	Beauftragte/r Mitarbeiter/in der ABK	Leiter/in der ABK	Dokumentenkontrolle, Unterschrift	Leiter/in der ABK	Unterschrift	Antwortdokument
5	Ausarbeitung von Richtlinien	Vorschlag für die Veröffentlichung von Richtlinien	Beauftragte/r Mitarbeiter/in der ABK	Leiter/in der ABK	Dokumentenkontrolle, Unterschrift	Leiter/in der ABK	Unterschrift	Antwortdokument
6	Kontaktaufnahme mit Patientenvertretern	geplante und Ad-hoc-Sitzungen	Leiter/in der ABK	n.a.	Dokumentenkontrolle, Unterschrift	Leiter/in der ABK	Unterschrift	Erinnerungsschreiben
7	Aktenführung	Einrichtung und laufende Durchführung von Registern	Beauftragte/r Mitarbeiter/in der ABK	Leiter/in der ABK	Dokumentenkontrolle, Unterschrift	Leiter/in der ABK	Unterschrift	ein Protokoll mit einer Unterschrift, die die

	Prozessschritte	Vorbereitungsschritte	Verantwortungsebenen				das aus dem Prozess resultierende Dokument	
			Task-Manager	Überprüfung	Art der Überprüfung	Zulassung		Art der Zulassung
								Durchführung der Kontrolle bestätigt
8	Abgabe von Stellungnahmen zu Verträgen über den Datenschutz und die Verarbeitung personenbezogener Daten	Prüfung der Verträge	Beauftragte/r Mitarbeiter/in der ABK	Leiter/in der ABK	Dokumentenkontrolle, Unterschrift	Leiter/in der ABK	Unterschrift	ein Vertragsentwurf, der den Datenschutzanforderungen entspricht
9	Überwachung der Einhaltung des Datenschutzes an der Universität	Prüfung der von den örtlichen behördlichen Datenschutzbeauftragten erstellten Jahresprotokolle, der laufenden Tätigkeiten im Laufe des Jahres, Prüfung der Angemessenheit der eingegangenen Unterlagen	Beauftragte/r Mitarbeiter/in der ABK	Leiter/in der ABK	Berichterstattung	Leiter/in der ABK	Annahme der Berichte	Bericht über die Ergebnisse der Konformitätsbewertung

2/B. Datenschutzbeauftragter

	Prozessschritte	Vorbereitungsschritte	Verantwortungsebenen					das aus dem Prozess resultierende Dokument
			Task-Manager	Überprüfung	Art der Überprüfung	Zulassung	Art der Zulassung	
1	Information und Beratung	sich über den Fall informieren, einen Standpunkt entwickeln	die/der Datenschutzbeauftragte	n. a.	n. a.	n.a.	Unterschrift	Antwortschreiben an den Antragsteller
2	Überwachung der Durchsetzung von datenschutzbezogenen Rechtsinstrumenten	Planung und Durchführung der Aufgaben des Jahresarbeitsplans	die/der Datenschutzbeauftragte	n. a.	n. a.	n.a.	Unterschrift	jährliche Unterrichtung der Rektorin/des Rektors und der Kanzlerin/des Kanzlers
3	Überwachung der Datenverarbeitungstätigkeiten	Durchführung von Aufgaben im Rahmen des jährlichen Arbeitsplans	die/der Datenschutzbeauftragte	n. a.	Halbjahresbericht	n. a.	Unterschrift	Informationsschreiben für den Rektor und den Kanzler
4	Umgang mit Datenschutzverletzungen	Erkennung und Bewertung von Vorfällen,	örtlicher Datenschutzbeauftragter/Datenverantwortlicher, Leiter der vom Vorfall betroffenen Abteilung	die/der Datenschutzbeauftragte	Analyse von Daten und Informationen	Die Rektorin/der Rektor, die Kanzlerin/der Kanzler	Unterschrift	Bericht über das Management von Zwischenfällen, Unterrichtung des Rektors und des Kanzlers, Berichterstattung an die Aufsichtsbehörde, falls erforderlich
5	Verbindung und Zusammenarbeit mit der Aufsichtsbehörde	Sammlung und Analyse relevanter Informationen zu einem Fall, Einhaltung der	die/der Datenschutzbeauftragte	n. a.	n. a.	Die Rektorin/der Rektor, die Kanzlerin/der Kanzler	Unterschrift	Berichterstattung

	Prozessschritte	Vorbereitungsschritte	Verantwortungsebenen					das aus dem Prozess resultierende Dokument
			Task-Manager	Überprüfung	Art der Überprüfung	Zulassung	Art der Zulassung	
		Berichtspflichten						