Datenschutz-, Veröffentlichungs- und Informationsfreiheitsregelwerk der Semmelweis Universität

Datum des Inkrafttretens: 1. April 2026

Buch I: Datenschutzrichtlinie

Inhaltsverzeichnis

Präambel 5
1. ALLGEMEINE BESTIMMUNGEN 5
1.1. Ziel der Richtlinie ist wie folgt: 5
1.2. Geltungsbereich der Richtlinie 5
1.3. Anwendbare Rechtsvorschriften, Begriffe, Formulare 6
1.4. Grundsätze, Rechtsgrundlage und Zweck der Datenverarbeitung 6
1.5. Integrierter Datenschutz, Durchführung einer Datenschutz-Folgenabschätzung 10
1.6. Durchsetzung der Datenschutzgrundsätze und Gewährleistung der Rechenschaftspflicht... 11
1.7. Vorschriften zur Datenverarbeitung und Datensicherheit im Rahmen der Verwaltungsabläufe 13
1.8. Allgemeine Zwecke der Datenverarbeitung, Dokumente zur Datenverarbeitung, Verzeichnisse 15
1.9. Erfassung der Datenverarbeitungsvorgänge 15
1.10. Datenübermittlung und Aufzeichnung der übermittelten Daten 16
1.11. Datenschutzerklärungen und deren Aufzeichnung 17
1.12. Verfügungsregister 19
1.13. Registrierung von Auftragsverarbeitern, gemeinsamen Verantwortlichen und Datenverarbeitungsvorgängen 20
1.14. Datenschutzvorfälle und deren Erfassung 20
1.15. Die lokalen Datenschutzbeauftragten und ihr Verzeichnis 22
2. Gewährleistung der Rechte der betroffenen Personen im Zusammenhang mit der Datenverarbeitung 22
2.1. Gewährleistung der Rechte der betroffenen Person 22
2.2. Unterrichtung der betroffenen Personen 23
2.3. Gewährleistung des Rechts auf Änderung und Berichtigung der Daten 24
2.4. Gewährleistung des Rechts auf Löschung der Daten 25
2.5. Gewährleistung des Rechts auf Einschränkung der Datenverarbeitung 25
2.6. Gewährleistung des Rechts auf Datenübertragbarkeit 26
2.7. Gewährleistung des Rechts auf Widerspruch gegen die Datenverarbeitung 26
2.8. Gewährleistung des Rechts auf Auskunft 27
2.9. Prüfung der Rechtsgrundlagen der Datenverarbeitung 27
2.10. Verarbeitung besonderer Daten 29
2.11. Gewährleistung der Verhinderung von Datenlecks 30
3. Das Datenschutzsystem der Universität 30
3.1. Der Datenschutzbeauftragte 30
3.2. Das Zentrum für Datenschutz und Patientenrechte (ABK) 32

3.3. Benennung des lokalen Datenschutzbeauftragten, dessen Aufgaben 33
3.4. Das System der Datenschutzkontrolle..... 34
4. Unterstützung der datenverarbeitenden Organisationseinheiten der Universität bei der Einhaltung der Vorschriften 35
5. Datenschutzbestimmungen im Zusammenhang mit wissenschaftlicher Forschung 36
6. Schlussbestimmungen 39
7. Anhänge 39

Präambel

Die Semmelweis-Universität (im Folgenden: Universität) handelt gemäß dem Gesetz CCIV von 2011 über das nationale Hochschulwesen (im Folgenden: Nftv.), dem Gesetz CXII von 2011 über das Recht auf informationelle Selbstbestimmung und die Informationsfreiheit (im Folgenden: Infotv.) das Gesetz CLIV von 1997 über das Gesundheitswesen (im Folgenden: Eütv.), das Gesetz XLVII von 1997 über die Verarbeitung und den Schutz von Gesundheitsdaten und damit verbundenen personenbezogenen Daten (im Folgenden: Eüak.) sowie auf der Grundlage der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (im Folgenden: Verordnung) werden die Regeln für die Datenverarbeitung an der Universität wie folgt festgelegt.
Die Vorschriften der Semmelweis-Universität über Datenschutz, Offenlegung und Anträge auf Zugang zu Daten von öffentlichem Interesse, Buch I: Datenschutzordnung (im Folgenden: Vorschriften über Datenschutz, Offenlegung und Anträge auf Zugang zu Daten von öffentlichem Interesse (AKK), Buch I: Datenschutzordnung (ASZ), Ordnung) ist gemäß den Bestimmungen der Verordnung auszulegen und anzuwenden. Zur Förderung einer einheitlichen Auslegung und Anwendung leistet das Zentrum für Datenschutz und Patientenrechte (im Folgenden: ABK) Unterstützung.

1. ALLGEMEINE BESTIMMUNGEN

1.1. Ziel der Richtlinie ist wie folgt:

Artikel 1

(1) Festlegung der Regeln für die Datenverarbeitung durch die Universität als Verantwortlicher.

1.2. Geltungsbereich der Richtlinie

Artikel 2

(1) Der Geltungsbereich dieser Richtlinie erstreckt sich
   a) auf alle Daten, die nach den einschlägigen Rechtsvorschriften als personenbezogene Daten eingestuft werden;
   b) auf die Universität und alle ihre Organisationseinheiten, in denen personenbezogene Daten verarbeitet werden;
   c) auf alle Personen, die personenbezogene Daten verarbeiten oder im Rahmen ihrer Tätigkeit an der Universität Kenntnis von personenbezogenen Daten erlangen.

(2) Der Geltungsbereich dieser Richtlinie erstreckt sich nicht auf die von der Universität unterhaltenen Einrichtungen, die im Eigentum der Universität stehenden Gesellschaften sowie auf Organisationen mit eigener Rechtspersönlichkeit, die unter Beteiligung der Universität tätig sind oder mit dem Betrieb der Universität in Verbindung stehen (im Folgenden „Organisation“), jedoch unterstützt die Universität als Träger, Eigentümer oder

Beteiligter dieser Organisationen diese und erwartet, dass sie ihr eigenes Datenschutzsystem unter Berücksichtigung dieser Richtlinie ausbauen.

1.3. Anwendbare Rechtsvorschriften, Begriffe, Formulare

Artikel 3

(1) Die in dieser Richtlinie verwendeten Begriffe entsprechen den in den geltenden Rechtsvorschriften definierten Begriffen.

(2) Im Sinne dieser Richtlinie:

a) Organisationseinheiten, die zur Benennung eines lokalen Datenschutzbeauftragten verpflichtet sind: die im Verzeichnis der Organisationseinheiten der Organisations- und Betriebsordnung der Universität als Stufe I eingestuften Organisationseinheiten, die Organisationseinheiten der Patientenversorgung (Kliniken und die András-Pető-Abteilung für Rehabilitation und Gesundheitsversorgung), sowie unter den sonstigen in die Stufe I eingestuften Organisationen die Studentische Selbstverwaltung der Universität und die Doktoranden-Selbstverwaltung.

(3) Die Verwendung der im Formulararchiv veröffentlichten Formulare – gemäß den festgelegten Dateninhalten – ist verpflichtend.

1.4. Grundsätze, Rechtsgrundlage und Zweck der Datenverarbeitung

Artikel 4

(1) Die Universität führt ihre Datenverarbeitungsaktivitäten auf der Grundlage der in Artikel 5 Absatz (1) der Verordnung festgelegten Grundsätze durch, nämlich der Grundsätze der Rechtmäßigkeit, der Fairness und der Transparenz, der Zweckbindung, der Datenminimierung und der begrenzten Speicherdauer, der Richtigkeit sowie der Gewährleistung der Integrität und Vertraulichkeit.

(2) Die Universität ergreift – im Einklang mit dem in Artikel 25 der Verordnung verankerten Grundsatz des eingebauten und standardmäßigen Datenschutzes – geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass die Datenverarbeitung durch die Universität im Einklang mit den geltenden Vorschriften erfolgt.

(3) Alle Organisationseinheiten der Universität sorgen dafür, dass die Universität in der Lage ist, die Einhaltung der Grundsätze und der Vorschriften zur Datenverarbeitung nachzuweisen (Grundsatz der Rechenschaftspflicht).

(4) Bei Tätigkeiten, die mit der Verarbeitung personenbezogener Daten verbunden sind, nimmt die betreffende Organisationseinheit die dem für die Datenverarbeitung Verantwortlichen obliegenden Aufgaben gemäß den vom Datenschutzbeauftragten festgelegten Richtlinien wahr.

(5) Die Universität verarbeitet personenbezogene Daten nur dann, wenn

a) die betroffene Person ihre Einwilligung zur Verarbeitung ihrer personenbezogenen Daten zur Erreichung eines bestimmten Zwecks erteilt hat;

b) [1]die Datenverarbeitung zur Erfüllung eines Vertrags erforderlich ist, bei dem die betroffene Person eine der Vertragsparteien ist, oder zur Durchführung von Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person vor Abschluss des Vertrags getroffen werden;

c) [2]die Datenverarbeitung ist zur Erfüllung einer für den Verantwortlichen geltenden rechtlichen Verpflichtung erforderlich;

d) [3]die Datenverarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich;

e) [4]die Datenverarbeitung ist zur Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder im Rahmen der Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) [5]die Datenverarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, es sei denn, die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, haben Vorrang vor diesen Interessen, insbesondere wenn die betroffene Person ein Kind ist.

(6) Sonderdaten dürfen verarbeitet werden, wenn

a) [6]die betroffene Person ihre ausdrückliche Einwilligung zur Verarbeitung besonderer personenbezogener Daten für einen oder mehrere bestimmte Zwecke erteilt hat, es sei denn, das Unionsrecht oder das Recht eines Mitgliedstaats sieht vor, dass das allgemeine Verbot der Verarbeitung besonderer Daten nicht durch die Einwilligung der betroffenen Person aufgehoben werden kann;

b) [7]die Datenverarbeitung erforderlich ist, damit der für die Verarbeitung Verantwortliche oder die betroffene Person ihren Verpflichtungen aus den Rechtsvorschriften über Beschäftigung sowie soziale Sicherheit und sozialen Schutz nachkommen und ihre spezifischen Rechte ausüben kann, sofern das Unionsrecht oder das Recht der Mitgliedstaaten, das angemessene Garantien zum Schutz der Grundrechte und Interessen der betroffenen Person vorsieht, sowie ein nach dem Recht des Mitgliedstaats geltender Tarifvertrag dies zulassen;

c) [8]die Datenverarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich, sofern die betroffene Person aufgrund ihrer körperlichen oder rechtlichen Handlungsunfähigkeit nicht in der Lage ist, ihre Einwilligung zu erteilen;

d) [9]die Datenverarbeitung erfolgt im Rahmen der rechtmäßigen Tätigkeit einer Stiftung, eines Vereins oder einer sonstigen gemeinnützigen Organisation mit politischen, weltanschaulichen, religiösen oder Interessenvertretungszwecken sowie

[1] VERORDNUNG Artikel 6 Absatz (1) lit. b)
[2]VERORDNUNG Artikel 6 Absatz (1) lit. c)
[3]VERORDNUNG Artikel 6 Absatz (1) lit. d)
[4]VERORDNUNG Artikel 6 Absatz (1) lit. e)
[5]VERORDNUNG Artikel 6 Absatz (1) lit. f)
[6]VERORDNUNG Artikel 9 Absatz (2) lit. a)
[7]VERORDNUNG Artikel 9 Absatz (2) lit. b)
[8]VERORDNUNG Artikel 9 Absatz (2) lit. c)
[9]VERORDNUNG Artikel 9 Absatz (2) lit. d)

gewerkschaftlichen Zielen unter Einhaltung angemessener Garantien, vorausgesetzt, dass die Datenverarbeitung ausschließlich aktuelle oder ehemalige Mitglieder dieser Einrichtung oder Personen betrifft, die im Zusammenhang mit den Zielen der Organisation in regelmäßiger Verbindung zu ihr stehen, und dass die personenbezogenen Daten ohne die Einwilligung der betroffenen Personen nicht Personen außerhalb der Organisation zugänglich gemacht werden;

e) [10]die Datenverarbeitung ist für Zwecke der präventiven Gesundheitsversorgung oder der Gesundheitsfürsorge am Arbeitsplatz, zur Beurteilung der Arbeitsfähigkeit des Arbeitnehmers, zur Erstellung einer medizinischen Diagnose, zur Erbringung von Gesundheits- oder Sozialleistungen oder -behandlungen oder zur Verwaltung von Gesundheits- oder Sozialsystemen und -diensten erforderlich, und zwar auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder im Rahmen eines Vertrags mit einem Angehörigen der Gesundheitsberufe;

f) [11]die Datenverarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit erforderlich, wie beispielsweise zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung der medizinischen Versorgung, die Gewährleistung eines hohen Qualitäts- und Sicherheitsniveaus bei Arzneimitteln und Medizinprodukten, und erfolgt auf der Grundlage von EU-Recht oder Recht eines Mitgliedstaats , das angemessene und konkrete Maßnahmen zur Gewährleistung der Rechte und Freiheiten der betroffenen Person vorsieht, insbesondere in Bezug auf die berufliche Schweigepflicht;

g) [12]Die Datenverarbeitung ist für Zwecke der Archivierung im öffentlichen Interesse, für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke erforderlich, und zwar auf der Grundlage von Rechtsvorschriften der Union oder der Mitgliedstaaten, die im Verhältnis zum angestrebten Ziel stehen, den wesentlichen Inhalt des Rechts auf den Schutz personenbezogener Daten wahren und angemessene und konkrete Maßnahmen zur Gewährleistung der Grundrechte und Interessen der betroffenen Person vorsehen.

(7) [13]Der betroffene Personen ist vor der Erhebung der Daten darüber zu informieren, auf welcher Rechtsgrundlage die Datenverarbeitung gemäß den Artikeln 13 und 14 der Verordnung erfolgt. Dies geschieht durch die Veröffentlichung einer Datenschutzerklärung.

(8) [14]Auf der Grundlage der Einwilligung, wenn die betroffene Person freiwillig, ausdrücklich, in Kenntnis der Sachlage und unmissverständlich ihre Einwilligung zur Verarbeitung der sie betreffenden Daten erteilt.

a) Die Einwilligung erstreckt sich auf alle Datenverarbeitungsvorgänge, die zum selben Zweck oder zu denselben Zwecken durchgeführt werden.

[10]VERORDNUNG Artikel 9 Absatz (2) lit. h)
[11]VERORDNUNG Artikel 9 Absatz (2) lit. i)
[12]VERORDNUNG Artikel 9 Absatz (2) lit. j)
[13]VERORDNUNG Artikel 12 Absatz (1)
[14]VERORDNUNG Artikel 7

b) Bei einer Datenverarbeitung, die mehreren Zwecken dient, muss die Einwilligung für jeden einzelnen Verarbeitungszweck gesondert erteilt werden.

c) Mit der Einwilligung darf nur eine Datenverarbeitung durchgeführt werden, bei der die Einhaltung der Anforderungen an die vorherige Unterrichtung und die Freiwilligkeit nachweisbar sind. Die Freiwilligkeit kann nicht nachgewiesen werden, wenn die Einwilligung zu einer Datenverarbeitung, die ausschließlich den Interessen der Universität dient, in einem Unterordnungsverhältnis, massenhaft, in einem bestimmten Personenkreis und ausnahmslos von den betroffenen Personen erteilt wurde.

d) Die Einwilligung kann in jeder Form erteilt werden, bei der die betroffene Person identifizierbar ist und die Tatsache der Einwilligung festgehalten wird;

e) Eine Einwilligung darf nicht mündlich oder telefonisch erteilt werden

f) Die Einwilligung kann insbesondere erteilt werden:

fa) schriftlich (mit Unterschrift der betroffenen Person);

fb) nach individueller Identifizierung der betroffenen Person (z. B. durch Identifizierung über das Studienverwaltungssystem) auf elektronischem Wege, sofern die Einwilligung dokumentiert (protokolliert) wird;

fc) auf elektronischem Wege in einer Nachricht, die von der bei der betreffenden Universität registrierten E-Mail-Adresse der betroffenen Person gesendet wird, sofern die unveränderte Aufzeichnung und Aufbewahrung der Nachricht gewährleistet ist.

(9) Der lokale Datenschutzbeauftragte führt über die von den betroffenen Personen erteilten Einwilligungen ein Verzeichnis mit folgenden Angaben:

a) Name und Aktenzeichen des Datenverarbeitungsregisters,

b) Aktenzeichen der Einwilligung zur Datenverarbeitung,

c) die personenbezogenen Identifikationsdaten der betroffenen Person,

d) Zeitpunkt der Erteilung der Einwilligung zur Datenverarbeitung,

e) Aktenzeichen der Datenschutzerklärung,

f) Zeitpunkt des Widerrufs der Einwilligung zur Datenverarbeitung.

(10)[15] Mitarbeiter, die in den Organisationseinheiten der Universität Daten verarbeiten, sind gemäß Artikel 8 Abs. (4) des Gesetzes I von 2012 über das Arbeitsgesetzbuch, dem Eütv. und dem Eüak sowie anderen Vorschriften, die eine Geheimhaltungspflicht vorschreiben, verpflichtet, die im Rahmen ihrer Tätigkeit erlangten personenbezogenen Daten ohne zeitliche Begrenzung geheim zu halten. Die Geheimhaltungspflicht erstreckt sich nicht auf die Offenlegung von Daten von öffentlichem Interesse und auf die gesetzlich festgelegten Auskunfts- und Informationspflichten in Bezug auf Daten, die aus Gründen des öffentlichen Interesses öffentlich sind, sowie auf Beschwerden und Meldungen von öffentlichem Interesse.

(11)[16] Neue Mitarbeiter der Universität erhalten bei ihrem Dienstantritt – als Teil des Einarbeitungspakets – eine grundlegende Einweisung in den Datenschutz. Die weitere

[15]Gesetz Nr. I von 2012, § 8 Abs. (4), Gesetz Nr. CLIV von 1997 über das Gesundheitswesen, § 25, und Gesetz Nr. C von 2012 über das Strafgesetzbuch, Artikel 219

[16]VERORDNUNG Artikel 39 Absatz (1) lit. b)

Aus- und Fortbildung wird vom ABK organisiert. Über die Schulungen der Mitarbeiter führt der lokale Datenschutzbeauftragte ein Verzeichnis mit folgenden Angaben:

a) Name der an der Schulung teilnehmenden Person,

b) Datum der Grundschulung,

c) Datum der Fortbildung.

1.5. Integrierter Datenschutz, Durchführung einer Datenschutz-Folgenabschätzung

Artikel 5

(1) [17]Auf Antrag des lokalen Datenschutzbeauftragten führt die ABK vor Beginn einer neuen Datenverarbeitung (insbesondere bei Einsatz neuer Datenverarbeitungstechnologien), sofern diese voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt, eine Folgenabschätzung durch, um zu prüfen, wie sich der geplante Datenverarbeitungsvorgang auf den Schutz personenbezogener Daten auswirkt.

(2) Die ABK ist verpflichtet, bei der Durchführung der Datenschutz-Folgenabschätzung den fachlichen Rat des Datenschutzbeauftragten einzuholen.

(3) Die Folgenabschätzung ist in den folgenden Fällen durchzuführen:

a) bei einer systematischen und umfassenden Bewertung bestimmter persönlicher Merkmale natürlicher Personen, die auf einer automatisierten Datenverarbeitung – einschließlich der Profilerstellung – beruht und auf der Entscheidungen beruhen, die für die natürliche Person rechtliche Auswirkungen haben oder sie in ähnlicher Weise erheblich beeinträchtigen,

b) bei der groß angelegten, systematischen Überwachung öffentlicher Orte, beispielsweise beim Einsatz elektronischer Überwachungssysteme (Kameras), die diese Voraussetzungen erfüllen;

c) bei der Verarbeitung einer großen Anzahl von Gesundheitsdaten und anderen besonderen Daten; bei Datenverarbeitungen, die in dem von der Aufsichtsbehörde geführten Verzeichnis aufgeführt sind, das eine Datenschutz-Folgenabschätzung vorschreibt.

d) Sollte die Datenschutz-Folgenabschätzung ergeben, dass die geplante Datenverarbeitung – mangels Maßnahmen zur Risikominderung – tatsächlich mit einem hohen Risiko verbunden wäre, konsultiert der Datenschutzbeauftragte vor der Verarbeitung personenbezogener Daten die Aufsichtsbehörde.

(4) Die Universität sorgt kontinuierlich dafür, dass ihre internen Vorschriften, Arbeitsanweisungen und Verträge den Datenschutzbestimmungen entsprechen. Vor der Veröffentlichung von Vorschriften, Anweisungen (interne Regelungsdokumente), Arbeitsanweisungen und Musterverträgen ist in Fragen der Verarbeitung personenbezogener Daten die Stellungnahme des ABK einzuholen. Bei der Ermächtigung zur Erlassung von Richtlinien und Anweisungen ist, sofern relevant, auf die Ermächtigung durch die Verordnung hinzuweisen.

[17]VERORDNUNG Artikel 25 und Artikel 35

1.6. Durchsetzung der Datenschutzgrundsätze und Gewährleistung der Rechenschaftspflicht

Artikel 6

(1) [18]Die Universität darf personenbezogene Daten verarbeiten, wenn:

a) die Datenverarbeitung gesetzlich vorgeschrieben ist (obligatorische Datenverarbeitung). Eine solche Datenverarbeitung betrifft insbesondere die Datenverarbeitung im Zusammenhang mit der Hochschulbildung, der Beschäftigung, der öffentlichen Bildung oder der Erbringung von Gesundheitsdienstleistungen.

b) Die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Eine solche Datenverarbeitung ist insbesondere dann gegeben, wenn sie zur Erfüllung einer gesetzlich vorgeschriebenen Verpflichtung (z. B. Datenübermittlung) unbedingt erforderlich ist.

c) Die betroffene Person hat ihre Einwilligung zur Datenverarbeitung gemäß den Punkten0 4 Absatz (8) lit. (1)a) -(1)c) erteilt. Eine solche Datenverarbeitung umfasst insbesondere die Verarbeitung von Daten im Zusammenhang mit dem Versand von Newslettern auf der Grundlage einer freiwilligen Anmeldung, der Teilnahme an verschiedenen Veranstaltungen und Gewinnspielen, dem Ausfüllen von Fragebögen oder der Teilnahme an wissenschaftlichen Forschungsvorhaben.

d) Die Datenverarbeitung ist zur Erfüllung eines Vertrags erforderlich, bei dem die betroffene Person eine der Vertragsparteien ist, oder sie ist erforderlich, um auf Wunsch der betroffenen Person vor Abschluss des Vertrags Maßnahmen zu ergreifen. Eine solche Datenverarbeitung kann insbesondere im Rahmen einer von einer Universität angebotenen, freiwillig in Anspruch genommenen Dienstleistung erfolgen.

e) Die Datenverarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich.

f) Die Datenverarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, es sei denn, die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, haben Vorrang vor diesen Interessen, insbesondere wenn die betroffene Person ein Kind ist.

(2) [19]Die Universität ergreift bei der Verarbeitung personenbezogener Daten zur Durchsetzung der Grundsätze der Datenverarbeitung folgende Maßnahmen:

a) [20]Im Interesse der Rechtmäßigkeit, der Fairness und der Transparenz: Die Verarbeitung personenbezogener Daten muss rechtmäßig und fair sowie für die betroffene Person transparent erfolgen. Bei der Verarbeitung personenbezogener Daten müssen natürlichen Personen die Rechtsgrundlage, die Art und Weise sowie der Umfang der Erhebung und Nutzung ihrer personenbezogenen Daten sowie die Möglichkeit und die Art und Weise des Zugriffs auf diese Daten transparent gemacht werden. Um sicherzustellen, dass die Verarbeitung personenbezogener Daten für die betroffene Person transparent ist, führt der lokale Datenschutzbeauftragte für jeden Verarbeitungszweck unter ein Verarbeitungsverzeichnis, erstellt für jede darin erfasste

[18] VERORDNUNG Artikel 5 Absatz (2), Artikel 5 Absatz (1) und Artikel 6
[19] VERORDNUNG Artikel 5 Absatz (2), Artikel 5 Absatz (1) und Artikel 6
[20]VERORDNUNG Artikel 5 Absatz (1) lit. a)

Datenverarbeitung eine Datenschutzerklärung, die er auf der Unterseite seiner Organisationseinheit registriert und öffentlich sowie uneingeschränkt zugänglich macht.

b) [21]Zweckbindung: Die Erhebung personenbezogener Daten darf nur zu festgelegten, eindeutigen und rechtmäßigen Zwecken erfolgen. Personenbezogene Daten dürfen nicht in einer Weise verarbeitet werden, die mit diesen Zwecken unvereinbar ist.

c) [22]Datenminimierung: Personenbezogene Daten müssen im Hinblick auf die Zwecke der Datenverarbeitung angemessen und relevant sein und dürfen sich auf das Notwendige beschränken.

d) [23]Richtigkeit: Personenbezogene Daten müssen richtig und auf dem neuesten Stand sein, d. h., es müssen alle angemessenen Maßnahmen getroffen werden, um unrichtige personenbezogene Daten im Hinblick auf die Zwecke der Datenverarbeitung unverzüglich zu löschen oder zu berichtigen.

e) [24]Begrenzte Speicherdauer: Die Speicherung personenbezogener Daten muss in einer Form erfolgen, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es zur Erreichung der Zwecke der Datenverarbeitung erforderlich ist; eine Speicherung personenbezogener Daten über diesen Zeitraum hinaus darf nur erfolgen, wenn die Datenverarbeitung auch danach nachweislich erforderlich ist. Um sicherzustellen, dass die Speicherung personenbezogener Daten auf die erforderliche Dauer beschränkt bleibt, legt die Universität für jede Datenverarbeitung in ihrer Aktenverwaltungsordnung eine Frist für die Löschung der Daten fest und trägt diese Frist in ihr Datenverarbeitungsregister ein.

f) Integrität und Vertraulichkeit: Die Verarbeitung personenbezogener Daten muss so erfolgen, dass durch geeignete technische und organisatorische Maßnahmen die angemessene Sicherheit der personenbezogenen Daten gewährleistet ist, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor versehentlichem Verlust, Zerstörung oder Beschädigung der Daten.

g) [25]Rechenschaftspflicht: Die ABK leistet praktische Unterstützung bei der Gestaltung der von der Datenverarbeitung betroffenen Prozesse gemäß den Vorgaben dieser Richtlinie, um die Konformität sicherzustellen. Der Datenschutzbeauftragte überprüft gemäß dem jährlichen Arbeitsplan, die ABK hingegen im Laufe des Jahres im Zusammenhang mit den einzelnen Fällen kontinuierlich die Erfüllung der Datenschutzanforderungen. Der ABK verschafft sich anhand der von den lokalen Datenschutzbeauftragten erstellten jährlichen Selbstkontrollprotokolle regelmäßig einen Überblick über den aktuellen Stand der Konformität.

[21]VERORDNUNG Artikel 5 Absatz (1) lit. b)
[22]VERORDNUNG Artikel 5 Absatz (1) lit. c)
[23]VERORDNUNG Artikel 5 Absatz (1) lit. d)
[24]VERORDNUNG Artikel 5 Absatz (1) lit. e)
[25]VERORDNUNG Artikel 5 Absatz (2)

1.7. Vorschriften zur Datenverarbeitung und Datensicherheit im Rahmen der Verwaltungsabläufe

Artikel 7

(1) [26]Die Mitarbeiter der Universität sind gemäß den Bestimmungen des Informationsgesetzes, der Verordnung und dieser Richtlinie verpflichtet, Unterlagen, die personenbezogene Daten enthalten, außerhalb der Arbeitszeit – und soweit möglich auch während der Arbeitszeit – in einem verschlossenen Schrank aufzubewahren. Auf dem Schreibtisch und an anderen Orten im Büro dürfen amtliche Unterlagen nur zum Zweck der Arbeitsausübung und während der Dauer der Arbeit aufbewahrt werden.

(2) [27]In Unterlagen, die personenbezogene Daten enthalten und sich im Besitz des Sachbearbeiters oder im Archiv befinden, dürfen außer dem Sachbearbeiter und dessen Vorgesetztem keine anderen Personen Einsicht nehmen, es sei denn, dies ist gesetzlich zulässig oder es wird in einer an den Sachbearbeiter gerichteten Anfrage nachgewiesen, dass dies zur Erfüllung seiner dienstlichen Aufgaben erforderlich ist.

(3) [28]Ohne gesetzliche Ermächtigung dürfen die Daten nur mit Einwilligung der betroffenen Person an Dritte weitergegeben werden. Wenn die betroffene Person der Weitergabe ihrer Daten an eine andere Stelle nicht zustimmt, ist sie darüber zu informieren, dass ihrem Antrag in diesem Fall nicht oder nicht vollständig entsprochen werden kann.

(4) Bei der Datenübermittlung innerhalb der Universität ist der Datenanforderer in jedem Fall verpflichtet, den Zweck und die Rechtsgrundlage der Datenanforderung nachzuweisen. Die Datenübermittlung darf erst nach Prüfung dieser Angaben erfolgen.

(5) [29]Bei der Ausübung des Einsichtsrechts durch die betroffene Person oder deren Vertreter ist so vorzugehen, dass dadurch die Rechte anderer nicht verletzt werden (personenbezogene oder geschützte Daten, die sich auf andere Personen beziehen, sind zu schwärzen oder auf andere Weise unkenntlich zu machen). Ebenso ist bei der Anfertigung von Kopien oder Auszügen vorzugehen.

(6) [30]Für die sichere Aufbewahrung der in Absatz (1) aufgeführten Unterlagen ist der Sachbearbeiter verantwortlich, bei dem sich diese bei Arbeitsende befinden. Über andere Aspekte hinaus sind aus datenschutzrechtlichen Gründen die Räume, in denen gemeinsam genutzte Drucker oder Kopierer betrieben werden, unter Berücksichtigung der Anforderungen an die Datensicherheit zu nutzen.

(7) [31]Über die sonstigen Aspekte hinaus sind aus datenschutzrechtlichen Gründen die Räume, in denen Computer oder Arbeitsplätze betrieben werden, so zu nutzen, dass sie den Anforderungen des Datenschutzes, des Brandschutzes und der IT-Sicherheit entsprechen. Der Sachbearbeiter ist verpflichtet, den Computer und die damit verbundenen Datenträger so zu handhaben und aufzubewahren, dass schutzbedürftige Daten nicht von Unbefugten eingesehen werden können. Er ist ferner verpflichtet, nach Arbeitsende den Arbeitsplatz – mit Ausnahme der Arbeitsplätze, die ständig eingeschaltet und online bleiben müssen –

[26]VERORDNUNG Artikel 5 Absatz (1) lit. f)
[27]VERORDNUNG Artikel 5 Absatz (1) lit. f)
[28]VERORDNUNG Artikel 6 Absatz (1)
[29]VERORDNUNG Artikel 5 Absatz (1) lit. f)
[30]VERORDNUNG Artikel 32
[31]VERORDNUNG Artikel 5 Absatz (1) lit. f)

auszuschalten und die Tür abzuschließen.

(8) [32]Unterlagen, die personenbezogene Daten enthalten, dürfen – außer zur Erfüllung dienstlicher Aufgaben – nur mit Genehmigung des unmittelbaren Vorgesetzten aus den Räumlichkeiten der Universität entfernt werden. Auch in diesem Fall ist der Sachbearbeiter verpflichtet, dafür zu sorgen, dass die Unterlagen nicht verloren gehen, beschädigt oder vernichtet werden und dass ihr Inhalt nicht in die Hände Unbefugter gelangt.

(9) [33]Daten, die zur Erreichung des Zwecks der Datenverarbeitung nicht mehr erforderlich sind, sowie Daten, für die der Zweck der Datenverarbeitung weggefallen ist oder sich geändert hat, sind – im Einklang mit den Bestimmungen der Aktenverwaltungsordnung – unverzüglich oder nach Ablauf der vorgeschriebenen Aufbewahrungsfrist zu vernichten. Auch für die Vernichtung sonstiger Unterlagen, die personenbezogene Daten enthalten, ist unter Einhaltung der erforderlichen Sicherheitsmaßnahmen zu sorgen.

(10) [34]Die Zugriffsberechtigungen für die einzelnen Register und Datenverarbeitungen sind vom Leiter der Organisationseinheit unter Aufschlüsselung nach Person und Aufgabenbereich im Einklang mit den Bestimmungen der Informationssicherheitsrichtlinie festzulegen.

(11) [35]In einem auf Antrag oder auf Initiative der betroffenen Person eingeleiteten Verfahren gelten die für die Durchführung des Verfahrens erforderlichen personenbezogenen Daten – sofern die Datenverarbeitung auf der Einwilligung der betroffenen Person beruht – als eingewilligt.

(12) [36]Für die auf einer Einwilligung beruhende Datenverarbeitung ist die schriftliche Einwilligung der betroffenen Person einzuholen (die ihre zur Identifizierung geeigneten Daten enthält, sowie seine Erklärung, dass er auf der Grundlage der vom Datenverantwortlichen veröffentlichten und ihm zur Kenntnis gebrachten Datenschutzerklärung (Bezeichnung der Datenschutzerklärung und Angabe des Zugriffsorts) freiwillig seine Einwilligung zur Verarbeitung seiner darin genannten personenbezogenen Daten durch den Datenverantwortlichen für den darin genannten Zweck und auf der darin genannten Rechtsgrundlage erteilt.

(13) [37]Im Rahmen der Bearbeitung eines Vorgangs dürfen nur solche personenbezogenen oder besonderen Daten verarbeitet werden, die für den jeweiligen Vorgang unbedingt erforderlich sind und deren Zweckbindung nachweisbar ist. Die Daten dürfen ausschließlich zur Bearbeitung des jeweiligen Vorgangs verwendet werden und dürfen – sofern das Gesetz nichts anderes vorsieht – nicht mit anderen Verfahren und Daten verknüpft werden.

(14) [38]Zur Gewährleistung der Datenqualität dürfen personenbezogene Daten nur aus einem gültigen amtlichen Ausweis, der zur Identifizierung der betroffenen Person geeignet ist, erfasst werden; besondere Daten dürfen nur mit schriftlicher Einwilligung der betroffenen Person erfasst werden.

---

[32]VERORDNUNG Artikel 5 Absatz (1) lit. f)
[33]VERORDNUNG Artikel 32
[34]VERORDNUNG Artikel 32
[35]VERORDNUNG Artikel 6 Absatz (1)
[36]VERORDNUNG Artikel 7
[37]VERORDNUNG Artikel 5 Absatz (1) lit. b)
[38]VERORDNUNG Artikel 5 Absatz (1) lit. d)

(15) [39]Bei der Datenerhebung und der weiteren Datenverarbeitung ist auf die Richtigkeit, Vollständigkeit und Aktualität der personenbezogenen Daten zu achten, damit die Rechte der betroffenen Personen nicht beeinträchtigt werden.

(16) [40]Personenbezogene und besondere Daten, die nicht in die Akten aufgenommen, sondern in papiergebundenen Aufzeichnungen festgehalten werden, sind – um ihre weitere Verwendung zu verhindern – so zu gestalten, dass sie nicht mehr zur Identifizierung geeignet sind. Arbeitskopien, die im Rahmen des EDV-Verfahrens entstanden sind, sowie beschädigte oder aus anderen Gründen überflüssig gewordene Kopien sind zu vernichten.

1.8. Allgemeine Zwecke der Datenverarbeitung, Dokumente zur Datenverarbeitung, Verzeichnisse

Artikel 8

(1) [41]Die Universität führt je nach den unterschiedlichen Zwecken der Datenverarbeitung Datenverarbeitungen zu Verwaltungs- und Registrierungszwecken durch.

(2) Die in dieser Richtlinie vorgeschriebenen Verzeichnisse und Dokumente werden vom lokalen Datenschutzbeauftragten geführt und erstellt. Für die Vollständigkeit der Verzeichnisse sowie für die Richtigkeit und Aktualität der darin enthaltenen Daten ist der Leiter der Organisationseinheit verantwortlich, die den lokalen Datenschutzbeauftragten benannt hat.

1.9. Erfassung der Datenverarbeitungsvorgänge

Artikel 9

(1) [42] Die Verarbeitung personenbezogener Daten an der Universität erfolgt nach Eintragung in das Verzeichnis der Datenverarbeitungsvorgänge gemäß Artikel 30 der Verordnung.

(2) Das Verzeichnis der Datenverarbeitungsvorgänge wird von der Universität als Verantwortlicher dezentral über die lokalen Datenschutzbeauftragten geführt und aufbewahrt.

(3) Der Leiter der Organisationseinheit, die den Datenbestand zu Registrierungszwecken verwaltet, meldet die Einrichtung eines neuen Datenbestands vor Beginn der Tätigkeit dem ABK. Stellt der ABK oder der Datenschutzbeauftragte im Rahmen seiner Tätigkeit fest, dass die Verarbeitung personenbezogener Daten die Führung eines Registers erfordert, informiert er den Leiter der Organisationseinheit darüber und leistet methodische Unterstützung bei der Erfüllung der mit dem Register verbundenen Aufgaben.

(4) Das Verzeichnis der Datenverarbeitungen muss die Erfassung der Datenverarbeitungen aller organisatorischen Einheiten gemäß der internen Gliederung der Organisationseinheit enthalten. Die Organisationseinheit überprüft durch in die Prozesse integrierte Selbstkontrollen und der ABK durch jährliche Kontrollen die inhaltliche Richtigkeit und Aktualität der veröffentlichten Verzeichnisse. Die Organisationseinheit ergänzt und ändert

[39]VERORDNUNG Artikel 5 Absatz (1) lit. d)
[40]VERORDNUNG Artikel 5 Absatz (1) lit. f)
[41]VERORDNUNG Artikel 6
[42]VERORDNUNG Artikel 30

das Datenverarbeitungsregister bei Bedarf. Bei Beendigung der Datenverarbeitung archiviert die Organisationseinheit das Datenverarbeitungsregister; bei Aufnahme einer neuen Datenverarbeitung erstellt sie ein neues Datenverarbeitungsregister.

(5) Die Organisationseinheiten, die zur Benennung eines lokalen Datenschutzbeauftragten verpflichtet sind, veröffentlichen das Verzeichnis auf ihrer Website im XLS-Format.

(6) Ein Muster für das Verzeichnis der Datenverarbeitung ist in der Formularsammlung verfügbar.

1.10. Datenübermittlung und Aufzeichnung der übermittelten Daten

Artikel 10

(1) [43]Personenbezogene Daten dürfen nur an Personen weitergegeben werden, die den Zweck und die Rechtsgrundlage der Datenverarbeitung ausdrücklich angegeben haben und die aufgrund gesetzlicher Bestimmungen zur Kenntnisnahme der Daten berechtigt sind.

(2) Die Datenübermittlung ist zu protokollieren, damit festgestellt werden kann, welche Daten der für die Datenverarbeitung Verantwortliche an wen, auf welcher Rechtsgrundlage und wann übermittelt oder bereitgestellt hat (z. B. im Rahmen der innerstaatlichen Rechtshilfe usw.). Ist die Eintragung eines neuen Eintrags in das Verzeichnis gerechtfertigt, bei dem die Rechtsgrundlage nicht eindeutig ist, prüft die ABK auf individuelle Anfrage des lokalen Datenschutzbeauftragten die Rechtsgrundlage und die Rechtmäßigkeit der Datenübermittlung und nimmt Stellung zur Durchführbarkeit der Datenübermittlung.

(3) Das Register wird vom lokalen Datenschutzbeauftragten für jede Organisationseinheit geführt.

(4) Für die Rechtmäßigkeit der Datenübermittlung haftet der Leiter der Organisationseinheit gegenüber der betroffenen Person hinsichtlich der von ihm verwalteten Daten.

(5) Kann die Datenübermittlung nicht rechtmäßig erfolgen oder hat der Antragsteller die für die Entscheidung über den Antrag erforderlichen Informationen auch nach Aufforderung nicht angegeben, ist die Datenübermittlung abzulehnen.

(6) Die Verweigerung der Datenübermittlung ist dem Antragsteller schriftlich unter Angabe der Gründe mitzuteilen.

(7) Die betroffene Person ist im Rahmen des auf ihren Antrag hin eingeleiteten Verfahrens mangels einer gesetzlichen Ermächtigung zur Datenübermittlung – im Hinblick auf ihre besonderen Daten schriftlich – aufzufordern, zu erklären, ob sie der Übermittlung ihrer personenbezogenen Daten zustimmt, sofern zur Erledigung ihrer Angelegenheit die Einholung von Informationen bei einer anderen Stelle erforderlich ist.

(8) Die betroffene Person hat das Recht, Auskunft über die Verarbeitung ihrer personenbezogenen Daten zu verlangen; ferner kann sie die Berichtigung ihrer personenbezogenen Daten oder – mit Ausnahme der obligatorischen Datenverarbeitung – deren Löschung oder Sperrung verlangen. Anträge auf Auskunft über die Datenverarbeitung sind, sofern die gesetzlichen Voraussetzungen vorliegen, innerhalb von höchstens 30 Tagen, nach Möglichkeit jedoch vorrangig zu bearbeiten.

[43] VERORDNUNG Artikel 5 Absatz (2)

(9) Die Weitergabe personenbezogener Daten, die Erteilung von Auskünften sowie die Verknüpfung verschiedener Datenverarbeitungen sind nur zulässig, wenn die betroffene Person ihre Einwilligung erteilt hat oder dies gesetzlich vorgeschrieben oder erlaubt ist und die Voraussetzungen für die Datenverarbeitung in Bezug auf jede einzelne personenbezogene Daten erfüllt sind.

(10) Der lokale Datenschutzbeauftragte überprüft das Verzeichnis der Datenübermittlungen bis zum 31. Dezember jedes Jahres, nimmt gegebenenfalls Änderungen vor und erstellt ein Protokoll über die Überprüfung. Das Protokoll wird der ABK bis zum 10. Januar des auf das betreffende Jahr folgenden Jahres auf elektronischem Wege übermittelt.

(11) Die ABK veröffentlicht das Muster des gemäß Artikel 30 der Verordnung erstellten Verzeichnisses der Datenübermittlungen sowie das Muster des für die Überprüfung des Verzeichnisses erforderlichen Protokolls im Formulararchiv.

1.11. Datenschutzerklärungen und deren Aufzeichnung

Artikel 11

(1) [44]Werden personenbezogene Daten über die betroffene Person bei dieser selbst erhoben, informiert der für die Datenverarbeitung Verantwortliche die betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten; wurden die Daten nicht bei der betroffenen Person erhoben, so erfolgt die Unterrichtung innerhalb einer angemessenen Frist nach Erhalt der Daten, spätestens jedoch innerhalb eines Monats, in Form einer Datenschutzerklärung.

(2) Die Universität verwendet zwei Arten von Datenschutzerklärungen:

a) eine allgemeine Datenschutzerklärung als Zusammenfassung der Datenverarbeitungsaktivitäten der Universität (vorbereitet von: ABK, herausgegeben von: Rektor, Kanzler und dem Vorsitzenden des Klinischen Zentrums),

b) spezifische Datenschutzerklärungen als Beschreibung der einzelnen, nach Zweck abgegrenzten Datenverarbeitungsvorgänge (Erstellung: lokaler Datenschutzbeauftragter, Herausgeber: Leiter der Organisationseinheit, die zur Benennung eines lokalen Datenschutzbeauftragten verpflichtet ist).

(3) [45]Die allgemeine Datenschutzerklärung enthält:

a) den Namen und die Anschrift der Universität,

b) den Namen und die Kontaktdaten des Vertreters der Universität,

c) die Kontaktdaten des Datenschutzbeauftragten der Universität,

d) den Zweck der Verarbeitung der von der Universität verarbeiteten personenbezogenen Daten,

e) die Rechtsgrundlagen für die Verarbeitung der von der Universität verwalteten Daten,

f) die Hauptkategorien der von der Universität verarbeiteten personenbezogenen Daten,

g) die Hauptgruppen der von der Datenverarbeitung betroffenen Personen,

h) die allgemeine Verarbeitungs- und Aufbewahrungsdauer der von der Universität verwalteten Daten,

[44] VERORDNUNG Artikel 13 und 14
[45] VERORDNUNG Artikel 13

i) die allgemeinen organisatorischen und technischen Maßnahmen, die die Universität zum Schutz der Daten ergreift,

j) etwaige Datenschutzvorfälle und Risiken, die im Rahmen der Datenverarbeitung durch die Universität auftreten können, sowie die Maßnahmen zur Bewältigung dieser Risiken,

k) die Empfänger der von der Universität regelmäßig erbrachten Dienstleistungen im Zusammenhang mit personenbezogenen Daten ,

l) die Kategorien der im Rahmen der Datenverarbeitungstätigkeiten der Universität eingesetzten gemeinsamen Verantwortlichen und Auftragsverarbeiter sowie die Art ihrer Tätigkeiten.

(4) [46]Die allgemeinen Datenschutzerklärungen nach Gruppen von betroffenen Personen

a) über die Verarbeitung von Mitarbeiterdaten,

b) die Verarbeitung von Daten von Studierenden,

c) die Verarbeitung von Gesundheitsdaten,

d) die Datenverarbeitung zu Forschungszwecken,

e) die Datenverarbeitung, die Persönlichkeitsrechte im Sinne gesonderter Rechtsvorschriften betrifft

(5) [47]Die individuellen Datenschutzerklärungen enthalten zusätzlich zu den Bestimmungen in Abs. (3) den Zweck der Verarbeitung der personenbezogenen Daten, die von der Universität

a) für den jeweiligen Zweck verarbeiteten personenbezogenen Daten,

b) die Rechtsgrundlage für die Verarbeitung der für den jeweiligen Zweck verarbeiteten Daten,

c) die Kategorien der für den jeweiligen Zweck verarbeiteten personenbezogenen Daten,

d) die Gruppen von betroffenen Personen, die von der Datenverarbeitung für den jeweiligen Zweck betroffen sind,

e) die allgemeine Dauer der Verarbeitung und Speicherung der verarbeiteten Daten,

f) die allgemeinen organisatorischen und technischen Maßnahmen, die im Interesse der Datensicherheit getroffen werden,

g) die bei der Datenverarbeitung für den jeweiligen Zweck möglicherweise auftretenden Datenschutzvorfälle, Risiken und die zur Bewältigung dieser Risiken getroffenen Maßnahmen,

h) die Empfänger der Datenübermittlungen im Rahmen der Datenverarbeitung für den jeweiligen Zweck,

i) die Bezeichnung und die Tätigkeit der gemeinsamen Verantwortlichen und Auftragsverarbeiter, die im Rahmen der Datenverarbeitung für den jeweiligen Zweck eingesetzt werden.

(6) [48]Die Universität stellt den betroffenen Personen Informationen über ihre Datenverarbeitungsaktivitäten in Form von Datenschutzhinweisen zur Verfügung, die auf der Website veröffentlicht werden.

[46] VERORDNUNG Artikel 13
[47] VERORDNUNG Artikel 13
[48] VERORDNUNG Artikel 5 Absatz (2)

a) Die allgemeinen Datenschutzhinweise werden vom ABK auf der Startseite der Website der Universität veröffentlicht.

b) Die individuellen Datenschutzerklärungen sind auf der Startseite der Website der Organisationseinheit, die zur Benennung eines lokalen Datenschutzbeauftragten verpflichtet ist, zu veröffentlichen; auf der Website der Generaldirektion für Recht und Verwaltung (im Folgenden: JIF) ist ein Link zu diesen Datenschutzerklärungen anzubringen.

(7) [49]Über die Veröffentlichung der individuellen Datenschutzerklärungen ist ein Verzeichnis mit folgenden Angaben zu führen

a) das Aktenzeichen der Datenschutzerklärung,

b) Titel der Datenschutzerklärung,

c) Zeitpunkt der Veröffentlichung der Datenschutzerklärung,

d) Datum des Außerkrafttretens bzw. der Änderung der Datenschutzerklärung.

(8) [50]Der lokale Datenschutzbeauftragte überprüft das Verzeichnis der einzelnen Datenschutzerklärungen bis zum 31. Dezember jedes Jahres, nimmt gegebenenfalls Änderungen vor und erstellt ein Protokoll über das Ergebnis der Überprüfung. Das Protokoll wird der ABK bis zum 10. Januar des auf das betreffende Jahr folgenden Jahres auf elektronischem Wege übermittelt.

(9) Die ABK veröffentlicht das Muster des Verzeichnisses sowie das Muster des Protokolls, das für die Überprüfung des Verzeichnisses erforderlich ist, im Formulararchiv.

1.12. Verfügungsregister

Artikel 12

(1) [51]Der lokale Datenschutzbeauftragte informiert die betroffene Person über die ihr gemäß den Artikeln 15 bis 22 der Verordnung zustehenden Rechte

a) Auskunft,

b) Zugriff,

c) Berichtigung,

d) Einschränkung,

e) Löschung/Recht auf Vergessenwerden,

f) Datenübertragbarkeit,

g) Widerspruch,

h) Einwilligung

– aufgeschlüsselt nach Organisationseinheiten – ein Verzeichnis der Erledigungen.

(2) Der lokale Datenschutzbeauftragte überprüft das Verzeichnis der Verfügungen bis zum 31. Dezember jedes Jahres, nimmt gegebenenfalls Änderungen vor und erstellt ein Protokoll über das Ergebnis der Überprüfung. Das Protokoll und seine Anhänge werden bis zum 10. Januar des auf das betreffende Jahr folgenden Jahres elektronisch an die ABK übermittelt.

[49] VERORDNUNG Artikel 5 Absatz (2)
[50]VERORDNUNG Artikel 5 Absatz (1) lit. d)
[51] VERORDNUNG Artikel 5 Absatz (2)

(3) Die ABK veröffentlicht das Muster des Verzeichnisses sowie das Muster des Protokolls, das für die Durchführung der Überprüfung des Verzeichnisses erforderlich ist, im Formulararchiv.

1.13. Registrierung von Auftragsverarbeitern, gemeinsamen Verantwortlichen und Datenverarbeitungsvorgängen

Artikel 13

(1) Die von der Universität abgeschlossenen Verträge über die Datenverarbeitung, die gemeinsame Datenverwaltung und die Datenverarbeitung durch Dritte werden im Rahmen der rechtlichen Begutachtung auch von der ABK begutachtet.

(2) Über die Verträge gemäß Absatz (1) führt der ABK ein Verzeichnis, das Folgendes enthält
   a) den Namen, die Anschrift und den Namen des Vertreters des Auftragsverarbeiters, des gemeinsamen Verantwortlichen und der den Auftrag zur Datenverarbeitung erteilenden Organisation;
   b) den Namen und die Kontaktdaten des Datenschutzbeauftragten des Auftragsverarbeiters, des gemeinsamen Verantwortlichen oder der Organisation, die die Datenverarbeitung in Auftrag gibt;
   c) den Zweck der Datenverarbeitung und der Auftragsverarbeitung;
   d) die Rechtsgrundlage für die Verarbeitung der zum Zweck der Datenverarbeitung verarbeiteten Daten;
   e) die Kategorien der personenbezogenen Daten, die zum Zweck der Datenverarbeitung verarbeitet werden;
   f) die Gruppen von betroffenen Personen, die von der Datenverarbeitung betroffen sind;
   g) den Geltungsbereich der Vereinbarung über die Datenverarbeitung;
   h) die betroffene Organisationseinheit der Universität.

(3) Für die Datenverarbeitung ist eine Vereinbarung gemäß Artikel 28 der Verordnung, für gemeinsame Verantwortliche eine Vereinbarung gemäß Artikel 30 der Verordnung als Nebenvertrag zum Rahmenvertrag abzuschließen. Ein Muster hierfür veröffentlicht der ABK im Formulararchiv.

1.14. Datenschutzvorfälle und deren Erfassung

Artikel 14

(1) [52]Die Mitarbeiter sind verpflichtet, den Verdacht auf festgestellte Datenschutzvorfälle (im Folgenden: Vorfall) – innerhalb von 24 Stunden nach Bekanntwerden – dem lokalen Datenschutzbeauftragten (in dessen Abwesenheit dem Leiter der Organisationseinheit) zu melden.

(2) Der lokale Datenschutzbeauftragte meldet den festgestellten Vorfall – spätestens 36 Stunden nach Bekanntwerden des Vorfalls – schriftlich dem Datenschutzbeauftragten und dem Informationssicherheitsbeauftragten.

[52] VERORDNUNG Artikel 33

(3) Bei Nichteinhaltung der Frist erstellt der Leiter der betroffenen Organisationseinheit einen Bericht an den Rektor und den Kanzler, die nach Einholung der Stellungnahme des Datenschutzbeauftragten über das weitere Vorgehen entscheiden.

(4) [53]Die Universität führt – über den Datenschutzbeauftragten – ein Verzeichnis zum Zweck der Überprüfung der im Zusammenhang mit dem Vorfall getroffenen Maßnahmen sowie zur Unterrichtung der betroffenen Personen, das den Umfang der betroffenen personenbezogenen Daten, den Kreis und die Anzahl der vom Vorfall betroffenen Personen, den Zeitpunkt, die Umstände und die Auswirkungen des Vorfalls sowie die zu seiner Behebung ergriffenen Maßnahmen und sonstige in den Rechtsvorschriften zur Datenverarbeitung festgelegte Angaben.

(5) [54]Der Datenschutzbeauftragte entscheidet innerhalb von 48 Stunden nach der Meldung, ob die Universität im Zusammenhang mit dem Vorfall einer Meldepflicht unterliegt. Falls die Universität gegenüber der Datenschutzbehörde meldepflichtig ist, bereitet der Datenschutzbeauftragte den Bericht so für die Entscheidung durch den Rektor und den Kanzler vor, dass die Meldung innerhalb von 72 Stunden erfolgen kann.

(6) [55]Bei der Risikoanalyse des Vorfalls prüft der Datenschutzbeauftragte:

a) die Art des Datenschutzvorfalls,

b) den Kreis der betroffenen Personen und deren ungefähre Anzahl,

c) die Kategorien und die ungefähre Anzahl der von dem Vorfall betroffenen Daten,

d) den Namen und die Kontaktdaten des lokalen Datenschutzbeauftragten oder eines anderen Ansprechpartners, der weitere Informationen bereitstellt,

e) die wahrscheinlichen Folgen des Vorfalls,

f) die getroffenen oder geplanten Maßnahmen zur Behebung des Vorfalls, einschließlich gegebenenfalls Maßnahmen zur Milderung etwaiger nachteiliger Folgen des Vorfalls.

(7) Die für die Meldung des Vorfalls an den Datenschutzbeauftragten, dessen Bewertung, die Entscheidung über die Vorfallbewältigung, die Meldung des Vorfalls an die Aufsichtsbehörde sowie die Unterrichtung der betroffenen Personen über den Vorfall erforderlichen Formulare veröffentlicht die ABK im Formulararchiv.

(8) [56]Der Datenschutzbeauftragte meldet – gemäß der Entscheidung des Rektors und des Kanzlers – den Vorfall innerhalb von 72 Stunden nach Bekanntwerden an die Aufsichtsbehörde, sofern der Datenschutzvorfall voraussichtlich ein Risiko für die Rechte der betroffenen Person darstellt.

(9) [57]Wenn der Datenschutzvorfall voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person darstellt, informiert die Universität – gemäß der Entscheidung des Rektors – die betroffene Person unverzüglich, spätestens jedoch innerhalb von 30 Tagen.

(10) Der lokale Datenschutzbeauftragte überprüft das von ihm geführte Verzeichnis der Vorfälle bis zum 31. Dezember jedes Jahres, nimmt gegebenenfalls Änderungen vor und

[53] VERORDNUNG Artikel 5 Absatz (2)
[54] VERORDNUNG Artikel 33 Absatz (1)
[55] VERORDNUNG Artikel 33 Absatz (3) Artikel 39 Absatz (19) lit. d)
[56] VERORDNUNG Artikel 33 Absatz (1)
[57] VERORDNUNG Artikel 34

erstellt ein Protokoll über das Ergebnis der Überprüfung, das er bis zum 10. Januar des auf das betreffende Jahr folgenden Jahres auf elektronischem Wege an den ABK übermittelt.

(11) Die ABK veröffentlicht das Muster für das Verzeichnis zur Vorfallbearbeitung sowie für das zur Überprüfung des Verzeichnisses erforderliche Protokoll im Formulararchiv.

1.15. Die lokalen Datenschutzbeauftragten und ihr Verzeichnis

Artikel 15

(1) Der Leiter einer Organisationseinheit, der gemäß Artikel 3 Abs. (2) zur Benennung verpflichtet ist, hat die ABK innerhalb von 8 Tagen über die Benennung des lokalen Datenschutzbeauftragten sowie über den Widerruf der Benennung zu informieren.

(2) Die ABK führt ein Verzeichnis der lokalen Datenschutzbeauftragten.

(3) Das Verzeichnis enthält:

a) den Namen der Organisationseinheit,

b) den Namen, die Position und die Kontaktdaten des lokalen Datenschutzbeauftragten,

c) das Datum der Ernennung bzw. des Widerrufs der Ernennung des lokalen Datenschutzbeauftragten.

2. Gewährleistung der Rechte der betroffenen Personen im Zusammenhang mit der Datenverarbeitung

2.1. Gewährleistung der Rechte der betroffenen Person

Artikel 16

(1) Die Universität unterstützt die Ausübung der Rechte der betroffenen Person. Zur Ausübung ihrer Rechte muss die betroffene Person bei Einreichung des Antrags ihre Identität und ihre Berechtigung nachweisen. Wird der Antrag nicht von der berechtigten Person gestellt oder kann der Antragsteller nicht identifiziert werden, ist der Antrag abzulehnen. Der Antrag ist unter Verwendung des Formulars einzureichen, das im Anhang der Richtlinie enthalten ist und auf der Website des JIF für jedermann uneingeschränkt zugänglich ist.

(2) Der Antrag kann elektronisch an die E-Mail-Adresse adatvedelem@semmelweis.hu oder per Post an das Zentrum für Datenschutz und Patientenrechte der Semmelweis-Universität, 1428 Budapest, Postfach 2, eingereicht werden.

(3) Wurde der Antrag bei einer anderen Organisationseinheit der Universität eingereicht, ist er innerhalb von drei Werktagen an das ABK weiterzuleiten.

(4) Ist der Antrag unvollständig, fordert das ABK den Antragsteller innerhalb von 8 Tagen zur Vervollständigung auf. Die Frist zur Vervollständigung wird nicht in die 8-tägige Weiterleitungsfrist sowie in die für die Bearbeitung des Antrags vorgesehene 30-tägige Frist eingerechnet.

(5) Die ABK leitet den Antrag zusammen mit ihrer Stellungnahme zur Berechtigung des Antragstellers und zur Durchführbarkeit des Antrags innerhalb von 8 Arbeitstagen an die für die Bearbeitung des Antrags zuständige Organisationseinheit weiter.

(6) Der Leiter der Organisationseinheit informiert die betroffene Person 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 bei Bedarf um weitere zwei Monate verlängert werden. Zur Fristverlängerung sind sowohl der ABK als auch die an der Bearbeitung des Antrags beteiligte Organisationseinheit berechtigt.

(8) Über die Fristverlängerung informiert der Leiter der Organisationseinheit die betroffene Person sowie gleichzeitig die ABK innerhalb eines Monats nach Eingang des Antrags unter Angabe des Grundes für die Verzögerung. Hat die betroffene Person den Antrag auf elektronischem Wege gestellt, so ist die Benachrichtigung nach Möglichkeit auf elektronischem Wege zu übermitteln, es sei denn, die betroffene Person wünscht etwas anderes.

(9) Der Leiter der für die Prüfung des Antrags zuständigen Organisationseinheit informiert den Antragsteller und gleichzeitig die ABK innerhalb eines Monats nach Eingang des Antrags schriftlich und unter Angabe von Gründen über die Ablehnung des Antrags.

(10) Der lokale Datenschutzbeauftragte führt ein Verzeichnis über die eingegangenen Anträge sowie deren Erledigung oder Ablehnung. Das Verzeichnis enthält:

a) die Aktenzeichen,
b) die Identitätsdaten des Antragstellers,
c) den Gegenstand des Antrags und die Art des betroffenen Rechts,
d) das Datum des Eingangs des Antrags,
e) die Erledigung des Antrags und den Zeitpunkt der Erledigung,
f) den Grund und den Zeitpunkt der Ablehnung des Antrags,
g) die Dauer der Bearbeitung des Antrags.

2.2. Unterrichtung der betroffenen Personen

Artikel 17

(1) [58]Um die betroffenen Personen angemessen zu informieren, veröffentlicht die Universität zu jeder Datenverarbeitung eine Datenschutzerklärung.

(2) Die Datenschutzerklärung enthält zusätzlich zu den im Verzeichnis der Verarbeitung personenbezogener Daten festgehaltenen Angaben Informationen darüber, dass die betroffene Person

a) das Recht hat, eine Bestätigung und Auskunft über die über ihn verarbeiteten Daten zu erhalten,
b) auf welche Weise er die ihm im Zusammenhang mit der Datenverarbeitung zustehenden Rechte ausüben kann,
c) er vom Datenverantwortlichen Zugang zu den ihn betreffenden personenbezogenen Daten, deren Berichtigung, Löschung oder Einschränkung der Verarbeitung verlangen sowie der Verarbeitung dieser personenbezogenen Daten widersprechen kann,
d) er kann vom Verantwortlichen die Datenübertragbarkeit seiner Daten verlangen,
e) seine Einwilligung zur Datenverarbeitung jederzeit widerrufen, wobei die Rechtmäßigkeit der vor dem Widerruf – auf der Grundlage der Einwilligung – durchgeführten Datenverarbeitung davon unberührt bleibt,

[58] VERORDNUNG Artikel 15

f) er kann zum Schutz seiner 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) ob Sie zur Bereitstellung der personenbezogenen Daten verpflichtet sind und welche möglichen Folgen die Nichtbereitstellung der Daten haben kann.

(3) Im Falle einer Datenverarbeitung auf der Grundlage einer gesetzlichen Bestimmung, der Erfüllung einer Aufgabe im öffentlichen Interesse oder im Rahmen der Ausübung öffentlicher Gewalt, der Erfüllung einer rechtlichen Verpflichtung der Universität, einer vertraglichen Verpflichtung, eines berechtigten Interesses der Universität oder eines Dritten sowie des berechtigten Interesses der betroffenen Person erfolgt die Information durch die Universität auf elektronischem Wege; Die Universität stellt die Informationen auf ihrer zentralen Website zur Verfügung. Die Universität informiert die betroffenen Personen bei jeder Datenverarbeitung über den Ort, an dem die Informationen zur Datenverarbeitung abrufbar sind.

(4) Bei einer Datenverarbeitung auf der Grundlage der Einwilligung der betroffenen Person ist die Datenschutzerklärung der betroffenen Person – durch Übergabe, postalische Zustellung oder per E-Mail – zu übermitteln, und ein Dokument, das den Erhalt bestätigt, ist zusammen mit den Datenverarbeitungsunterlagen aufzubewahren. Die Unterrichtung der betroffenen Person muss – im Interesse einer transparenten Unterrichtung, Kommunikation und der Umsetzung geeigneter Maßnahmen zur Ausübung der Rechte der betroffenen Person – vor der Erhebung der Daten bei der betroffenen Person erfolgen. Stammen die Daten nicht von der betroffenen Person, muss diese innerhalb von 30 Tagen darüber unterrichtet werden.

(5) Die Verantwortung für die Unterrichtung liegt beim Leiter der Organisationseinheit, die zur Benennung eines lokalen Datenschutzbeauftragten verpflichtet ist.

2.3. Gewährleistung des Rechts auf Änderung und Berichtigung der Daten

Artikel 18

(1) Im Rahmen der Gewährleistung des Rechts auf Berichtigung hat die betroffene Person das Recht, auf ihren Antrag hin zu verlangen, dass die Universität die sie betreffenden personenbezogenen Daten unverzüglich und ohne ungerechtfertigte Verzögerung ändert oder berichtigt. Unter Berücksichtigung des Zwecks der Datenverarbeitung hat die betroffene Person das Recht, die Vervollständigung unvollständiger personenbezogener Daten zu verlangen – unter anderem durch eine ergänzende Erklärung.

(2) Die Änderung oder Löschung von Gesundheitsdaten darf nur so erfolgen, dass die ursprünglich erfassten Daten lesbar bleiben.

(3) Für die Berichtigung der Daten ist der Leiter der für die Datenverarbeitung zuständigen Organisationseinheit verantwortlich.

2.4. Gewährleistung des Rechts auf Löschung der Daten

Artikel 19

(1) Im Rahmen der Gewährleistung des Rechts auf Löschung der Daten hat die betroffene Person das Recht, auf ihren Antrag hin zu verlangen, dass die Universität unverzüglich prüft, ob
   a) die Verarbeitung der personenbezogenen Daten für den Zweck, für den sie erhoben oder anderweitig verarbeitet wurden, noch erforderlich ist,
   b) ob die betroffene Person ihre Einwilligung, die die Grundlage für die Datenverarbeitung bildet, widerrufen hat und ob eine andere Rechtsgrundlage für die Datenverarbeitung vorliegt,
   c) die betroffene Person Widerspruch gegen die Datenverarbeitung eingelegt hat und kein vorrangiger Rechtsgrund für die Datenverarbeitung vorliegt,
   d) ob die Datenverarbeitung zum Zwecke der direkten Werbung erfolgte und die betroffene Person Widerspruch gegen die Datenverarbeitung eingelegt hat,
   e) ob die personenbezogenen Daten unrechtmäßig verarbeitet wurden,
   f) ob die personenbezogenen Daten aufgrund der Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen, die dem für die Datenverarbeitung Verantwortlichen nach dem für ihn geltenden Unionsrecht oder dem Recht eines Mitgliedstaats obliegt,
   g) ob die Erhebung der personenbezogenen Daten im Zusammenhang mit dem Angebot von Diensten der Informationsgesellschaft erfolgte.

(2) Sofern die Voraussetzungen für die Löschung der Daten vorliegen, führt die Universität deren Löschung gemäß der Anordnung der betroffenen Person unverzüglich durch.

(3) Sofern die Datenverarbeitung gesetzlich vorgeschrieben ist und eine entsprechende Ermächtigung vorliegt, informiert der für die Datenverarbeitung Verantwortliche die betroffene Person – gleichzeitig mit der Ablehnung des Antrags – darüber.

(4) Die Verantwortung für die Löschung der Daten liegt beim Leiter der für die Datenverarbeitung zuständigen Organisationseinheit.

2.5. Gewährleistung des Rechts auf Einschränkung der Datenverarbeitung

Artikel 20

(1) Im Rahmen der Gewährleistung des Rechts auf Einschränkung der Datenverarbeitung hat die betroffene Person das Recht, auf ihren Antrag hin zu verlangen, dass die Universität die Datenverarbeitung in den folgenden Fällen unverzüglich einschränkt:
   a) Wenn die betroffene Person die Richtigkeit der personenbezogenen Daten bestreitet, gilt die Einschränkung für den Zeitraum, der es dem für die Datenverarbeitung Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen,
   b) wenn die Datenverarbeitung unrechtmäßig ist und die betroffene Person der Löschung der Daten widerspricht und stattdessen die Einschränkung ihrer Verwendung beantragt hat,

c) der für die Datenverarbeitung Verantwortliche die personenbezogenen Daten für die Zwecke der Datenverarbeitung nicht mehr benötigt, die betroffene Person diese jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt,

d) die betroffene Person hat gegen die Datenverarbeitung Widerspruch eingelegt; in diesem Fall gilt die Einschränkung so lange, bis festgestellt ist, ob die berechtigten Gründe des für die Datenverarbeitung Verantwortlichen Vorrang vor den berechtigten Gründen der betroffenen Person haben.

(2) Die Universität handelt – sofern die Voraussetzungen für eine Einschränkung der Datenverarbeitung vorliegen – unverzüglich gemäß den Anweisungen der betroffenen Person.

(3) Die Verantwortung für die Einschränkung der Datenverarbeitung liegt beim Leiter der für die Datenverarbeitung zuständigen Organisationseinheit.

2.6. Gewährleistung des Rechts auf Datenübertragbarkeit

Artikel 21

(1) Im Rahmen der Gewährleistung des Rechts auf Datenübertragbarkeit hat die betroffene Person das Recht, auf ihren Antrag hin zu verlangen, dass die Universität unverzüglich prüft, ob

a) die Datenverarbeitung zur Erfüllung eines Vertrags erforderlich ist, bei dem die betroffene Person eine der Vertragsparteien ist, oder zur Durchführung von Maßnahmen erforderlich ist, die auf Antrag der betroffenen Person vor Abschluss des Vertrags getroffen werden, oder

b) auf der Grundlage der Einwilligung der betroffenen Person erfolgt.

(2) Sofern die Voraussetzungen für die Datenübertragbarkeit gegeben sind, stellt die Universität der betroffenen Person unverzüglich und gemäß deren Anweisungen

a) die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung stellen

b) die Daten direkt an den von der betroffenen Person benannten Datenverantwortlichen übermittelt.

(3) Die Verantwortung für die Übermittlung der Daten liegt beim Leiter der für die Datenverarbeitung zuständigen Organisationseinheit.

2.7. Gewährleistung des Rechts auf Widerspruch gegen die Datenverarbeitung

Artikel 22

(1) Im Rahmen der Gewährleistung des Rechts auf Widerspruch gegen die Datenverarbeitung hat die betroffene Person das Recht, auf ihren Antrag hin von der Universität ohne ungerechtfertigte Verzögerung prüfen zu lassen, ob das Recht auf Widerspruch gegen die Datenverarbeitung geltend gemacht werden kann, d. h.

a) ob die Datenverarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse erforderlich war,

b) ob die Datenverarbeitung zur Wahrung der berechtigten Interessen des für die Datenverarbeitung Verantwortlichen oder eines Dritten erforderlich war.

(2) Sind die Voraussetzungen für die Geltendmachung des Widerspruchsrechts gegen die Datenverarbeitung gegeben und liegt keine andere Rechtsgrundlage für die Datenverarbeitung vor, so stellt die Universität die Datenverarbeitung gemäß der betreffenden Bestimmung unverzüglich ein.
(3) Für die Einstellung der Datenverarbeitung ist der Leiter der für die Datenverarbeitung zuständigen Organisationseinheit verantwortlich.

2.8. Gewährleistung des Rechts auf Auskunft

Artikel 23

(1) Aufgrund des Rechts auf Auskunft ist die betroffene Person berechtigt, vom Verantwortlichen Auskunft darüber zu erhalten, ob ihre personenbezogenen Daten verarbeitet werden, und falls eine solche Verarbeitung stattfindet, hat sie das Recht auf Auskunft über die personenbezogenen Daten sowie über folgende Informationen:
   a) die Kategorien der personenbezogenen Daten der betroffenen Person;
   b) die Zwecke der Datenverarbeitung;
   c) die Empfänger oder Kategorien von Empfängern, denen die personenbezogenen Daten offengelegt wurden oder offengelegt werden, einschließlich insbesondere Empfänger in Drittländern sowie internationale Organisationen;
   d) die geplante Dauer der Speicherung der personenbezogenen Daten oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
   e) er kann vom Verantwortlichen die Berichtigung, Löschung oder Einschränkung der Verarbeitung der ihn betreffenden personenbezogenen Daten verlangen und gegen die Verarbeitung dieser personenbezogenen Daten Widerspruch einlegen;
   f) er hat das Recht, eine Beschwerde bei der Aufsichtsbehörde einzureichen;
   g) sofern die Daten nicht bei der betroffenen Person erhoben wurden, alle verfügbaren Informationen über ihre Herkunft;
   h) die Tatsache einer automatisierten Entscheidungsfindung gemäß Artikel 22 Absätze (1) und (4) der Verordnung, einschließlich Profiling, sowie zumindest in diesen Fällen die angewandte Logik und verständliche Informationen darüber, welche Bedeutung diese Datenverarbeitung hat und welche zu erwartenden Folgen sie für die betroffene Person hat.
(2) Erfolgt eine Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation, hat die betroffene Person das Recht, über die entsprechenden Garantien gemäß Artikel 46 der Verordnung informiert zu werden.
(3) Für die Gewährleistung des Rechts auf Auskunft ist der Leiter der für die Datenverarbeitung zuständigen Organisationseinheit verantwortlich.

2.9. Prüfung der Rechtsgrundlagen der Datenverarbeitung

Artikel 24

(1) [59]Die Universität überprüft jedes Jahr die Dokumentation aller im Datenverarbeitungsregister erfassten Verarbeitungen personenbezogener Daten, um sicherzustellen, dass die darin enthaltenen Daten gemäß den gesetzlichen Bestimmungen und den Vorschriften der Universität verarbeitet wurden, dass die entsprechende Rechtsgrundlage für die Datenverarbeitungen weiterhin besteht und dass die betreffenden Daten auf einer angemessenen Rechtsgrundlage verarbeitet werden. Der Leiter der Organisationseinheit handelt hinsichtlich der Rechtsgrundlage der Datenverarbeitung gemäß den methodischen Richtlinien des ABK.

(2) Bei der Überprüfung jeder Datenverarbeitung muss die Rechtsgrundlage der Datenverarbeitung festgestellt werden und geprüft werden, ob die Dokumentation, die die für die Datenverarbeitung erforderliche Rechtsgrundlage belegt, vorliegt. Bei der Feststellung der Rechtsgrundlage leistet der ABK bei Bedarf Unterstützung.

(3) [60]Rechtsgrundlagen für die Datenverarbeitung der Universität und erforderliche Unterlagen:

a) Datenverarbeitung auf der Grundlage der Einwilligung der betroffenen Person: Einwilligung der betroffenen Person oder ihres gesetzlichen Vertreters, die eine freiwillige und eindeutige Willensbekundung der betroffenen Person enthält, die auf einer angemessenen Aufklärung (Zweck, Rechtsgrundlage, Dauer der Datenverarbeitung, Name und Anschrift des Verantwortlichen sowie Name und Anschrift des Auftragsverarbeiters und die mit der Datenverarbeitung verbundenen Tätigkeiten) beruht und mit der die betroffene Person ihre unmissverständliche Einwilligung zur Verarbeitung der sie betreffenden personenbezogenen Daten – entweder umfassend oder in Bezug auf bestimmte Vorgänge – erteilt;

b) Datenverarbeitung, die zur Erfüllung eines mit der betroffenen Person geschlossenen oder noch abzuschließenden Vertrags erforderlich ist: der mit der betroffenen Person geschlossene Vertrag – Erklärung zum Vertragsabschluss (wobei im Vertrag die erforderliche Datenverarbeitung angegeben ist oder auf einem separaten Blatt dargelegt wird, zur Erfüllung welcher Vertragsbestimmung die Datenverarbeitung erforderlich ist);

c) Datenverarbeitung, die zur Erfüllung einer rechtlichen Verpflichtung des für die Datenverarbeitung Verantwortlichen erforderlich ist: genaue Bezeichnung der Rechtsvorschrift, die die Datenverarbeitung vorschreibt oder erforderlich macht;

d) Datenverarbeitung, die zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich ist: Wurde die Interessenabwägung durchgeführt?

da) Was ist der Zweck der Datenverarbeitung?

db) ist die Verarbeitung personenbezogener Daten zur Erreichung des Zwecks der betroffenen Person oder einer anderen natürlichen Person unbedingt erforderlich,

dc) ob alternative Lösungen zur Verfügung stehen, mit denen der beabsichtigte Zweck ohne die Verarbeitung personenbezogener Daten erreicht werden kann,

dd) die möglichst genaue Definition des berechtigten Interesses,

[59] VERORDNUNG Artikel 5 Absatz (1) lit. a), Artikel 6
[60]VERORDNUNG Artikel 6

de) welche personenbezogenen Daten und für welchen Zeitraum die Verarbeitung aufgrund des berechtigten Interesses erforderlich ist,

df) welche Interessen die andere Partei haben könnte, die die Datenverarbeitung auf der Grundlage der Interessen der anderen Partei rechtmäßig rechtfertigen;

e) Datenverarbeitung, die zur Erfüllung einer Aufgabe im öffentlichen Interesse oder im Rahmen der Ausübung öffentlicher Befugnisse, die dem Verantwortlichen übertragen wurden, erforderlich ist: genaue Bezeichnung und Wortlaut der Rechtsvorschrift, die das öffentliche Interesse oder die dem Verantwortlichen übertragenen öffentlichen Befugnisse als maßgebliches festlegt, sowie die aus diesen Befugnissen abgeleitete Notwendigkeit der jeweiligen Datenverarbeitung;

f) [61]erforderlich zur Wahrung der berechtigten Interessen des für die Datenverarbeitung Verantwortlichen oder eines Dritten: Wurde die Interessenabwägung durchgeführt,

fa) Ist die Verarbeitung personenbezogener Daten zur Erreichung des Zwecks des für die Datenverarbeitung Verantwortlichen oder eines Dritten unbedingt die Verarbeitung personenbezogener Daten unbedingt erforderlich ist,

fb) Gibt es alternative Lösungen, mit denen der beabsichtigte Zweck ohne die Verarbeitung personenbezogener Daten erreicht werden kann,

fc) die möglichst genaue Bestimmung des berechtigten Interesses,

fd) Was ist der Zweck der Datenverarbeitung?

fe) welche personenbezogenen Daten für wie lange im Rahmen des berechtigten Interesses verarbeitet werden müssen,

ff) welche Interessen die andere Partei haben könnte, die die Datenverarbeitung auf der Grundlage der Interessen der anderen Partei rechtmäßig rechtfertigen.

(4) [62]Bei der Dokumentation der auf einer Einwilligung beruhenden Datenverarbeitung ist zu prüfen, ob

a) ob Unterlagen zur Untermauerung der Rechtsgrundlage vorliegen und ob deren Einholung rechtmäßig erfolgte,

b) die Einwilligung die geeignete Rechtsgrundlage für die Datenverarbeitung war,

c) die Einwilligung in geeigneter Form erteilt wurde,

d) die betroffene Person vor Erteilung der Einwilligung angemessen informiert wurde.

(5) Die Universität gewährleistet durch den uneingeschränkten Download des auf ihren Websites verfügbaren Formulars „ANTRAG AUF AUSÜBUNG DER RECHTE DER BETROFFENEN“ das Recht der betroffenen Person, ihre frühere Einwilligung zu widerrufen, zu ändern oder einzuschränken.

(6) Für die Prüfung der Rechtsgrundlage der Datenverarbeitung ist der lokale Datenschutzbeauftragte verantwortlich.

2.10. Verarbeitung besonderer Daten

Artikel 25

[61] VERORDNUNG Artikel 6 Absatz (1) lit. f), Präambel Absatz (69)
[62] VERORDNUNG Artikel 7

(1) Die Universität verarbeitet besondere Daten ausschließlich, wenn eine der in Artikel 9 Absatz (2) der Verordnung genannten Voraussetzungen vorliegt.

(2) [63]Bei der Verarbeitung besonderer Kategorien personenbezogener Daten prüft der lokale Datenschutzbeauftragte bei jeder Datenverarbeitung, ob die auf Einwilligung beruhende Datenverarbeitung gemäß den Datenschutzvorschriften erfolgt ist. Hinsichtlich der Rechtskonformität der Datenverarbeitung ist die Stellungnahme des ABK maßgebend.

2.11. Gewährleistung der Verhinderung von Datenlecks

Artikel 26

(1) [64] Die Universität wendet geeignete Verfahren zur Verhinderung, Erkennung, Meldung und Untersuchung von Datenlecks an.

(2) Die Universität ergreift gemäß den Vorgaben der Informationssicherheitsrichtlinie die folgenden Maßnahmen, um die Weitergabe personenbezogener Daten zu verhindern:

a) Es überprüft die fortwährende Vertraulichkeit, Integrität, Verfügbarkeit und Widerstandsfähigkeit der Systeme und Dienste, die zur Verarbeitung personenbezogener Daten verwendet werden,

b) prüft die Fähigkeit, im Falle eines physischen oder technischen Vorfalls den Zugriff auf personenbezogene Daten und die Verfügbarkeit der Daten rechtzeitig wiederherzustellen,

c) legt im Rahmen der IT-Sicherheit ein Verfahren zur regelmäßigen Prüfung, Bewertung und Beurteilung der Wirksamkeit der technischen und organisatorischen Maßnahmen fest, die zur Gewährleistung der Sicherheit der Datenverarbeitung getroffen wurden,

d) führt eine Risikoanalyse durch, um ein angemessenes Sicherheitsniveau festzulegen und die Risiken zu ermitteln, die durch die versehentliche oder unrechtmäßige Vernichtung, den Verlust, die Veränderung, die unbefugte Offenlegung oder den unbefugten Zugriff auf übermittelte, gespeicherte oder auf andere Weise verarbeitete personenbezogene Daten entstehen, sowie den dadurch verursachten Schaden zu bestimmen.

3. Das Datenschutzsystem der Universität

3.1. Der Datenschutzbeauftragte

Artikel 27

(1) [65]Der Kanzler ernennt im Einvernehmen mit dem Rektor aus den Reihen des JIF – mit juristischem Abschluss sowie mindestens 3 Jahren Berufserfahrung im Bereich des Datenschutzes – – zum Datenschutzbeauftragten ernennt – im Wege eines Auswahlverfahrens oder bis zur Entscheidung über das Auswahlverfahren durch Beauftragung –, um die Aufgaben des Datenschutzbeauftragten der Universität als Verantwortlicher und Auftragsverarbeiter wahrzunehmen.

[63] VERORDNUNG Artikel 9
[64] VERORDNUNG Artikel 32
[65] VERORDNUNG Artikel 37 Absätze (5) und (6)

(2) [66] Die Universität stellt sicher, dass der Datenschutzbeauftragte in alle Angelegenheiten, die die Verwaltung und Verarbeitung personenbezogener Daten betreffen, in angemessener Weise und rechtzeitig einbezogen werden kann. Zur Erfüllung seiner Aufgaben ist er berechtigt, Einsicht in die von den Organisationseinheiten verwalteten Daten zu nehmen und Daten von den Organisationseinheiten anzufordern.

(3) Die Universität stellt dem Datenschutzbeauftragten die Ressourcen zur Verfügung, die für die Erfüllung seiner Aufgaben, den Zugriff auf personenbezogene Daten und Datenverarbeitungsvorgänge sowie für die Aufrechterhaltung seiner Fachkenntnisse erforderlich sind.

(4) [67]Der Datenschutzbeauftragte darf im Zusammenhang mit der Wahrnehmung seiner Aufgaben von niemandem Weisungen entgegennehmen. Der Datenschutzbeauftragte ist unmittelbar der obersten Leitung der Universität gegenüber rechenschaftspflichtig.

(5) [68]Der Datenschutzbeauftragte unterliegt im Zusammenhang mit seiner Tätigkeit einer zeitlich unbegrenzten Geheimhaltungspflicht, unabhängig vom Bestehen des Rechtsverhältnisses.

(6) Zu den Aufgaben des Datenschutzbeauftragten gehören insbesondere:

a) Er informiert den für die Datenverarbeitung Verantwortlichen oder den Auftragsverarbeiter und berät ihn fachlich,

b) auf der Grundlage eines jährlichen Arbeitsplans die Umsetzung der rechtlichen Steuerungsinstrumente im Bereich des Datenschutzes sowie die Einhaltung der Vorschriften zu überprüfen, worüber er dem Rektor und dem Kanzler jährlich in Form eines Berichts Rechenschaft ablegt,

c) überwacht fachlich die datenschutzbezogene Schulung der Mitarbeiter,

d) gibt auf Anfrage fachliche Beratung zur Datenschutz-Folgenabschätzung und überwacht die Durchführung der Folgenabschätzung,

e) arbeitet mit der Aufsichtsbehörde zusammen,

f) fungiert in Angelegenheiten der Datenverarbeitung – einschließlich der Vorabkonsultation – als Ansprechpartner gegenüber der Aufsichtsbehörde und führt gegebenenfalls auch in anderen Fragen Konsultationen mit ihr durch,

g) wirkt an der integrierten Risikobewertung der Universität bei der Ermittlung von Datenschutzrisiken mit,

h) unterbreitet im Rahmen seiner Beratungstätigkeit Vorschläge für die Themen der Schulungen zum Thema Datenschutz.

i) [69]unterstützt die betroffene Person bei der Ausübung ihrer Rechte und veranlasst den für die Datenverarbeitung Verantwortlichen, die zur Prüfung und Behebung der Beschwerde erforderlichen Maßnahmen zu ergreifen.

j) Der Datenschutzbeauftragte erstellt auf der Grundlage der Informationen der Organisationseinheiten bis zum 15. Dezember jedes Jahres – erstmals im Jahr 2025 – einen Jahresbericht für den Rektor und den Kanzler zur Bewertung der Datenschutzaktivitäten der Universität mit folgendem Inhalt:

[66] VERORDNUNG Artikel 39
[67] VERORDNUNG Artikel 38 Absatz (3)
[68] VERORDNUNG Artikel 38 Absatz (5)
[69] VERORDNUNG Artikel 38 Absatz (4), Artikel 25/M des Informationsgesetzes

ja) Anzahl und Art der laufenden oder im Berichtsjahr abgeschlossenen Verfahren vor den Datenschutzbehörden sowie die wichtigsten Erkenntnisse daraus,

jb) Anzahl, Art und wichtigste Erkenntnisse zu Rechtsstreitigkeiten im Zusammenhang mit Datenschutzfragen,

jc) Fortschritte bei Projekten zur Einhaltung der Datenschutzvorschriften,

jd) Darstellung der Maßnahmen im Zusammenhang mit dem Aufbau eines Netzwerks lokaler Datenschutzbeauftragter,

je) allgemeine Bewertung der Datenschutzaktivitäten der Universität.

jf) Überblick über Informationen im Zusammenhang mit der Bearbeitung von Datenanfragen von öffentlichem Interesse, Art und Typen der Datenanfragen von öffentlichem Interesse sowie die Einhaltung der Fristen.

(7) Der Datenschutzbeauftragte ist berechtigt,

a) jede Datenverarbeitung, die in den Geltungsbereich dieser Richtlinie fällt, zu überprüfen und alle Räumlichkeiten zu betreten, in denen Datenverarbeitung stattfindet,

b) Auskünfte und Erläuterungen zu jeder Datenverarbeitung, die in den Geltungsbereich dieser Richtlinie fällt, einzuholen,

c) mit Beratungs- und Genehmigungsrecht an allen Gremien der Universität und ihrer Organisationseinheiten teilzunehmen, in denen Themen auf der Tagesordnung stehen, die in seinen Zuständigkeitsbereich fallen.

d) im Rahmen seiner Zuständigkeit Datenschutzaufrufe, Datenschutzabmahnungen sowie Datenschutzdurchführungsanweisungen gemäß Teil I.1 Artikel 3 Abs. (4) Buchstabe e der Organisations- und Betriebsordnung der Universität zu erlassen;

e) konkrete Maßnahmen beim Rektor, Kanzler oder den Vorsitzenden des klinischen Zentrums, in dem er Maßnahmen der Leitung vorschlägt, wenn auf der Grundlage der in den normativen Regelungsdokumenten festgelegten Bestimmungen weitere Maßnahmen erforderlich werden könnten, die nicht in den Zuständigkeitsbereich des Datenschutzbeauftragten fallen und einen Fachbereich, eine Organisationseinheit oder einen oder mehrere Mitarbeiter betreffen.

3.2. Das Zentrum für Datenschutz und Patientenrechte (ABK)

Artikel 28

(1) Das ABK arbeitet als Organisationseinheit des JIF unter der Leitung des Generaldirektors des JIF und unter der fachlichen Aufsicht des Datenschutzbeauftragten.

(2) Das ABK wird vom Direktor für Datenschutz und Patientenrechte geleitet.

(3) Die Aufgabe des ABK im Bereich der Regulierung besteht darin:

a) die regelmäßige Überprüfung der Vorschriften zur Datenverarbeitung und Datensicherheit sowie die Sicherstellung ihrer Aktualität,

b) die Erstellung der in dieser Richtlinie festgelegten Formulare und deren Veröffentlichung im Formulararchiv,

c) die Mitwirkung und fachliche Beratung der Organisationseinheiten bei der Erstellung und Aktualisierung der datenschutzrelevanten Teile von Vorschriften, die auch Regeln zur Datenverarbeitung enthalten.

(4) Die Aufgaben des ABK im Bereich der Beratung:
   a) [70]Richtlinien bereitstellt und individuelle Beratung für die lokalen Datenschutzbeauftragten und die Leiter der Organisationseinheiten hinsichtlich der Praxis der universitätsinternen Verfahren im Zusammenhang mit dem Datenschutz und den Patientenrechten (Datenschutzerklärungen, Patienteninformationen, Bearbeitung von Beschwerden im Zusammenhang mit der Datenverarbeitung, Datenweitergabe, Führung der Dokumentation) anbietet,
   b) Erstellung methodischer Leitfäden,
   c) Unterstützung des Informationssicherheitsbeauftragten der Universität durch datenschutzrechtliche Beratung bei den in seinen Zuständigkeitsbereich fallenden Genehmigungs- und Zulassungsverfahren.

(5) [71]Aufgabe des ABK ist es, Beschwerden im Zusammenhang mit der Datenverarbeitung im Rahmen der Beschwerdeverfahren zu untersuchen.

(6) Die Aufgabe des ABK im Rahmen der Kontrolle:
   a) Bei Meldung oder Feststellung einer unrechtmäßigen Datenverarbeitung beteiligt er sich an deren Untersuchung und leistet Unterstützung bei deren Beendigung,
   b) er führt die Kontrolle der Tätigkeiten der Organisationseinheiten und der lokalen Datenschutzbeauftragten im Zusammenhang mit Datenschutzaufgaben durch.

(7) Die Aufgaben des ABK bei der Organisation von Schulungen:
   a) Erstellung von Schulungsthemen auf der Grundlage der Vorschläge des Datenschutzbeauftragten,
   b) Erstellung von Schulungsunterlagen zum Datenschutz für neue Mitarbeiter auf der Grundlage der Schulungsthemen,
   c) Organisation der Schulung der lokalen Datenschutzbeauftragten,
   d) im Falle von Gesetzesänderungen die Organisation von Informationsveranstaltungen, je nach Art und Umfang der Änderungen.

(8) Das ABK wirkt gemäß der Vertragsordnung der Universität an der Begutachtung von Verträgen mit, die den Datenschutz sowie die Verarbeitung personenbezogener Daten betreffen.

(9) Die Mitarbeiter des ABK sind zur Erfüllung ihrer Aufgaben berechtigt, Einsicht in die von den Organisationseinheiten verwalteten Daten zu nehmen und Daten von den Organisationseinheiten anzufordern. Die Mitarbeiter des ABK unterliegen im Zusammenhang mit dieser Tätigkeit einer zeitlich unbegrenzten Geheimhaltungspflicht, unabhängig vom Bestehen eines Rechtsverhältnisses.

3.3. Benennung des lokalen Datenschutzbeauftragten, dessen Aufgaben

Artikel 29

(1) Der Leiter einer Organisationseinheit, der zur Benennung eines lokalen Datenschutzbeauftragten verpflichtet ist, ist für die Datenverarbeitungsaktivitäten der von ihm geleiteten Organisationseinheit(en) verantwortlich.

[70] Geändert durch: Senatsbeschluss Nr. 31/2026 vom 25. März, Artikel 12. Gültig ab dem: 1. April 2026
[71] Geändert durch: Senatsbeschluss Nr. 31/2026 vom 25. März, Artikel 12. Gültig ab dem: 1. April 2026

(2) Der Leiter der Organisationseinheit, der zur Benennung eines lokalen Datenschutzbeauftragten verpflichtet ist,
   a) ernennt den lokalen Datenschutzbeauftragten und
   b) überprüft in regelmäßigen Abständen anhand von Berichten dessen Tätigkeit,
   c) entscheidet nach Ablauf der vorgeschriebenen Aufbewahrungsfrist über die weitere Speicherung oder Vernichtung der gespeicherten Daten.

(3) Als lokalen Datenschutzbeauftragten ist eine Person zu benennen, die über fachliche Eignung und insbesondere über fundierte Kenntnisse des Datenschutzrechts und der Datenschutzpraxis verfügt sowie zur Erfüllung der gesetzlich vorgeschriebenen Aufgaben geeignet ist.

(4) Der lokale Datenschutzbeauftragte
   a) sorgt für die Erstellung, Führung, Veröffentlichung und Überprüfung der Aufzeichnungen und Datenschutzhinweise der Organisationseinheit im Zusammenhang mit der Datenverarbeitung und informiert den ABK gemäß den Bestimmungen dieser Richtlinie über das Ergebnis der Überprüfung;
   b) organisiert die Datenschutzschulung der mit der Datenverwaltung und Datenverarbeitung befassten Personen in der Organisationseinheit,
   c) wirkt auf Anfrage des ABK bei der Beantwortung von Beschwerden mit, die sich auf die von der Organisationseinheit durchgeführte Verarbeitung personenbezogener Daten beziehen,
   d) [72]stellt auf Anfrage der ABK Informationen über die von ihm untersuchten Beschwerden im Zusammenhang mit der Datenverarbeitung, über Datenanfragen sowie über die getroffenen Maßnahmen zur Verfügung,
   e) informiert den Datenschutzbeauftragten über den Verdacht auf einen Datenschutzvorfall,
   f) stellt der JIF Daten zur Beantwortung von Anfragen von öffentlichem Interesse zur Verfügung, die bei der Organisationseinheit eingegangen sind oder dort vorliegen.

(5) Ist kein lokaler Datenschutzbeauftragter benannt, so werden die in dieser Richtlinie festgelegten Aufgaben des lokalen Datenschutzbeauftragten vom Leiter der zur Benennung befugten Organisationseinheit wahrgenommen.

3.4. Das System der Datenschutzkontrolle

Artikel 30

(1) [73]Der Rektor, der Kanzler und der Vorsitzende des Klinischen Zentrums überprüfen über den Datenschutzbeauftragten und den ABK die Umsetzung der Rechtsvorschriften zur Datenverarbeitung und zum Datenschutz. Der Datenschutzbeauftragte erstellt bis zum 1. Februar jedes Jahres einen Jahresbericht für den Rektor, den Kanzler und den Vorsitzenden des Klinischen Zentrums über den aktuellen Stand des Datenschutzes.

(2) Die Organisationseinheiten überprüfen ihre eigenen Datenverarbeitungsprozesse und deren Konformität im Rahmen einer in die Prozesse integrierten Selbstkontrolle.

[72] Geändert durch: Senatsbeschluss Nr. 31/2026 vom 25. März, Artikel 12. Gültig ab dem: 1. April 2026
[73] VERORDNUNG Artikel 39, Artikel 5 Absatz (2)

(3) Die lokalen Datenschutzbeauftragten überprüfen bis zum 31. Dezember jedes Jahres die von ihnen geführten Verzeichnisse sowie die veröffentlichten Datenschutzerklärungen und unterrichten den ABK gemäß den Bestimmungen dieser Richtlinie bis zum 10. Januar des auf das betreffende Jahr folgenden Jahres über das Ergebnis dieser Überprüfung.

(4) Der Datenschutzbeauftragte überprüft auf der Grundlage eines jährlichen Prüfplans, ob die Organisationseinheiten der Universität
   a) ihren Verpflichtungen im Zusammenhang mit dem Schutz personenbezogener Daten nachkommen, insbesondere
      aa) der Informationspflicht gegenüber den betroffenen Personen sowie
      ab) ihrer Verpflichtungen zur Gewährleistung des Auskunftsrechts der betroffenen Personen sowie
      ac) die Verpflichtungen zur Gewährleistung der Rechte der betroffenen Personen.
   b) ob sie ihren Verpflichtungen im Zusammenhang mit Datenschutzvorfällen nachkommen,

(5) Der Datenschutzbeauftragte erstellt ein Protokoll über die Überprüfung und ergreift folgende Maßnahmen:
   a) Bei Feststellung von Mängeln fordert er den Leiter der betroffenen Organisationseinheit innerhalb von 15 Tagen auf, innerhalb einer Frist von 15 Tagen Abhilfemaßnahmen zu ergreifen,
   b) führt nach Ablauf der Frist zur Ergreifung von Maßnahmen innerhalb von 30 Tagen eine Nachkontrolle durch, um die Umsetzung der Maßnahmen zu überprüfen.
   c) Innerhalb von 15 Tagen nach der Nachkontrolle überprüft er die Umsetzung der Maßnahme und informiert den Kanzler im Falle des Ausbleibens oder der nicht ordnungsgemäßen Durchführung der Maßnahme mit der Aufforderung, Maßnahmen zu ergreifen.

(6) Die ABK prüft die von den lokalen Datenschutzbeauftragten erstellten jährlichen Überprüfungsprotokolle und leistet bei Mängeln durch einen vom Generaldirektor für Recht und Verwaltung benannten Mitarbeiter Unterstützung, um die Einhaltung der Vorschriften sicherzustellen.

(7) Die Kontrollbehörde handelt bei datenschutzrechtlichen Prüfungen gemäß den für sie geltenden Vorschriften.

4. Unterstützung der datenverarbeitenden Organisationseinheiten der Universität bei der Einhaltung der Vorschriften

Artikel 31

(1) Der Generaldirektor der JIF hat zur Förderung der Datenschutzkonformität einen Mitarbeiter mit eigenständigem Aufgabenbereich benannt, der in Zusammenarbeit mit dem lokalen Datenschutzbeauftragten der Organisationseinheit gemäß einem vom Generaldirektor der JIF – nach vorheriger Absprache mit dem Direktor des ABK – festgelegten Zeitplan den Organisationseinheiten methodische Unterstützung leistet
   a) bei der Erstellung der Datenschutzdokumentation und deren inhaltlich korrekter Führung (Datenschutz-Eignungsaudit),

b) zur Überprüfung der operativen Konformität der Organisationseinheiten gemäß den von der Datenschutzbehörde festgelegten fachlichen methodischen Vorgaben (Datenschutz-Betriebsaudit),

c) zur Gewährleistung des in dieser Richtlinie vorgeschriebenen Datenschutzbewusstseins auf Vorschlag des Datenschutzbeauftragten und gemäß den vom ABK festgelegten Schulungsthemen Datenschutzschulungen durchführt und eine Einstufungsprüfung für die vom Leiter der Organisationseinheit benannten Mitarbeiter durchführt,

d) er berichtet dem Generaldirektor der JIF regelmäßig über den aktuellen Stand der Compliance-Unterstützungsmaßnahmen.

e) Der benannte Mitarbeiter informiert den zuständigen lokalen Datenschutzbeauftragten über seine Erreichbarkeit und den Zeitplan für die Schulung.

(2) Die JIF veröffentlicht auf ihrer Website einen methodischen Leitfaden

a) zur Verarbeitung von Mitarbeiterdaten,

b) die Verarbeitung von Studierenden-Daten,

c) zur Verarbeitung von Gesundheitsdaten,

d) Aufgaben im Zusammenhang mit der Verarbeitung von Daten, die durch gesonderte Rechtsvorschriften geschützte Persönlichkeitsrechte betreffen, sowie

e) die Maßnahmen zur Unterstützung der Einhaltung von Eignungs- und Betriebsprüfungen sowie zur Gewährleistung des Datenschutzbewusstseins durch entsprechende Schulungen,

f) zur Förderung der Einhaltung der Datenschutzvorschriften durch die unterhaltsberechtigten Einrichtungen

(3) Die Anwendung der Leitfäden ist für Personen und Organisationen, die in den Geltungsbereich der Richtlinie fallen, verbindlich und wird von den unter ihrer Trägerschaft stehenden Einrichtungen erwartet.

5. Datenschutzbestimmungen im Zusammenhang mit wissenschaftlicher Forschung

Artikel 32

(1) Die Semmelweis-Universität unterstützt die selbstständige und gemeinschaftliche wissenschaftliche Forschungstätigkeit der Universitätsangehörigen – insbesondere, aber nicht ausschließlich der Forscher, Dozenten, Studierende und Doktoranden – (im Folgenden: Forscher) bei ihren eigenständigen und gemeinschaftlichen wissenschaftlichen Forschungsaktivitäten (im Folgenden: wissenschaftliche Forschung); die Universität ermöglicht – in begründeten Fällen – den Zugriff auf und die Verarbeitung von Daten, die zur Identifizierung von Personen geeignet sind, zum Zwecke der wissenschaftlichen Forschung.

(2) Sofern im Rahmen der wissenschaftlichen Forschung personenbezogene Daten verarbeitet werden, ist der Forschungsleiter für die uneingeschränkte Einhaltung der in den Rechtsvorschriften und den internen Regelungen der Universität festgelegten Datenschutz- und Datensicherheitsvorschriften verantwortlich.

(3) Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken darf nur auf der Grundlage eines schriftlich festgelegten und von der Ethikkommission

schriftlich genehmigten Forschungsplans (im Folgenden: Forschungsplan) erfolgen, der vom Forschungsleiter und dem Leiter der von der Datenverarbeitung betroffenen Organisationseinheit genehmigt wurde. Die Organisationseinheit führt ein Verzeichnis der genehmigten Forschungsprojekte.

(4) Der Forscher darf im Rahmen der wissenschaftlichen Forschung ausschließlich Daten aus nachgewiesenen Quellen verarbeiten, die den berufsethischen Normen, den nationalen und internationalen Rechtsvorschriften sowie den internen Vorschriften der Universität (im Folgenden: alle Vorschriften) entsprechen. Für den Nachweis der Herkunft der Daten ist der Forscher verantwortlich.

(5) Der Forscher darf im Rahmen der wissenschaftlichen Forschung personenbezogene Daten ausschließlich

a) mit einer Berechtigung, die allen Vorschriften entspricht;

b) für den im Forschungsplan festgelegten Zweck und in dem für den Forschungszweck erforderlichen Umfang;

c) für den Zeitraum, der zur Erreichung der im Forschungsplan festgelegten Ziele erforderlich ist;

d) in einer Form, bei der personenbezogene Daten durch Anonymisierungs- oder Pseudonymisierungsverfahren von den zur Identifizierung geeigneten Daten getrennt sind

verarbeiten.

(6) Im Rahmen wissenschaftlicher Forschung dürfen von den gespeicherten Daten keine Kopien angefertigt werden, die personenbezogene Daten enthalten.

(7) Im Falle der Anonymisierung personenbezogener Daten ist der Forschungsleiter verpflichtet, dafür zu sorgen, dass eine echte Anonymisierung gemäß den gesetzlichen Bestimmungen durchgeführt wird und dass die Anonymisierung unumkehrbar ist.

(8) Im Falle der Pseudonymisierung personenbezogener Daten ist der Forschungsleiter verpflichtet, dafür zu sorgen, dass eine echte Pseudonymisierung gemäß den gesetzlichen Bestimmungen durchgeführt wird. Weitere Informationen, die eine Rückidentifizierung natürlicher Personen ermöglichen, dürfen dem Forscher nur dann übermittelt werden, wenn die Rechtsgrundlage der wissenschaftlichen Forschung in der Einwilligung der betroffenen Person auf der Grundlage einer vorherigen Aufklärung besteht oder die Rückidentifizierung in glaubwürdiger Weise im lebenswichtigen Interesse der betroffenen Person erfolgt.

(9) Der Forschungsleiter ist verpflichtet, dafür zu sorgen, dass die im Rahmen der wissenschaftlichen Forschung verwendeten personenbezogenen Daten nicht für andere Forschungszwecke verwendet werden, es sei denn, die Rechtsgrundlage der wissenschaftlichen Forschung ist die auf Aufklärung beruhende Einwilligung der betroffenen Person.

(10) Gelangt im Zusammenhang mit der wissenschaftlichen Forschung ein personenbezogenes Datum in unzulässiger Weise in den Besitz eines Forschers, so sperrt dieser die Daten und benachrichtigt unverzüglich den Forschungsleiter sowie den Datenschutzbeauftragten der Universität.

(11) Die Gewährleistung eines angemessenen Schutzniveaus im Zusammenhang mit der wissenschaftlichen Forschung liegt in der Verantwortung des Forschungsleiters.

(12) Bei der Einrichtung des Schutzes ist darauf zu achten, dass technische, organisatorische, programmtechnische und rechtliche Maßnahmen sowie solche Mittel eingesetzt werden, die den Schutzgegenstand vor schädlichen Einflüssen und Absichten aus verschiedenen Gefahrenquellen auf der Grundlage des verfügbaren Wissens am wirksamsten fördern bzw. gewährleisten.

(13) Ein Forscher darf im Rahmen der wissenschaftlichen Forschung nur dann an der Verarbeitung personenbezogener Daten mitwirken, wenn er vom Forschungsleiter in den einschlägigen fachlichen, datenschutzrechtlichen und datensicherheitstechnischen Vorschriften geschult wurde.

(14) Der Forschungsleiter kann für die Durchführung der Schulung und hinsichtlich ihres Inhalts die fachliche Unterstützung des Generaldirektors für Informatik sowie des Datenschutzbeauftragten der Universität in Anspruch nehmen.

(15) Es liegt in der Verantwortung des Forschungsleiters, sicherzustellen, dass der Forscher vor der Teilnahme an der wissenschaftlichen Forschung eine entsprechende fachliche Schulung sowie eine Schulung zu Datenschutz und Datensicherheit erhält – unter besonderer Berücksichtigung der Pseudonymisierung und Anonymisierung von Daten. Der Forschungsleiter führt ein Verzeichnis über die durchgeführten Schulungen und bewahrt dieses Verzeichnis 10 Jahre lang auf.

(16) Über die in Absatz (13) vorgeschriebene Schulung führt der Forschungsleiter ein Verzeichnis, das folgende Angaben enthalten muss

a) den Ort der Unterweisung,

b) Name und Unterschrift der Person(en), die die Schulung durchgeführt hat(haben),

c) die in der Schulung behandelten Themen und die wichtigsten Feststellungen,

d) die Namen und Unterschriften der Teilnehmer an der Schulung.

(17) Auch in Bezug auf personenbezogene Daten, die im Rahmen der wissenschaftlichen Forschung bekannt werden, sind die Datenschutzvorschriften einzuhalten, insbesondere die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO) festgelegten

a) Grundsätze des Datenschutzes;

b) die Vorschriften für die Führung von Aufzeichnungen über Datenverarbeitungsvorgänge sowie über einzelne Datenübermittlungen und einzelne Datenübertragungen;

c) Bestimmungen zur Erstellung und Veröffentlichung einer Datenschutzerklärung; sowie

d) die Vorschriften zur Datensicherheit.

(18) Für die Führung des Verzeichnisses der Datenverarbeitungsvorgänge im Zusammenhang mit personenbezogenen Daten, die im Rahmen der wissenschaftlichen Forschung verwendet werden, erteilt der Generaldirektor für Rechts- und Verwaltungsangelegenheiten methodische Richtlinien.

(19) Wird die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken von einem Studierenden oder Doktoranden der Universität durchgeführt, so tritt an die Stelle des Forschungsleiters in den Bestimmungen dieser

Verordnung der Betreuer des Studierenden oder Doktoranden, und bei der Datenverarbeitung sind auch die besonderen Bestimmungen der Studien- und Prüfungsordnung sowie der Promotionsordnung anzuwenden.

(20) Beruht die wissenschaftliche Forschung auf einer internationalen oder nationalen Zusammenarbeit, so ist hinsichtlich der mit der Forschung verbundenen Datenverarbeitung zudem die zwischen den beteiligten Parteien geschlossene Datenschutzvereinbarung maßgeblich.

6. Schlussbestimmungen

Artikel 33

(1) Der Senat der Semmelweis-Universität hat auf der Grundlage der in Buch I, Teil I.1, Artikel 19 Abs. (10) Buchstabe d der Organisations- und Geschäftsordnung erteilten Ermächtigung die Verordnung über Datenschutz, Offenlegung und Anträge auf Zugang zu Daten von öffentlichem Interesse, Buch I, Datenschutzverordnung, mit seinem Beschluss Nr. 88/2025 (25. September) verabschiedet.

(2) Die Datenschutz-, Veröffentlichungs- und Vorschriften für Anträge auf Zugang zu Daten von öffentlichem Interesse, Buch I: Datenschutzvorschriften, treten am 2. Oktober 2025 in Kraft.

(3) Gleichzeitig mit dem Inkrafttreten dieser Richtlinie werden die durch den Senatsbeschluss Nr. 107/2022 (19. Dezember) verabschiedeten und durch die Senatsbeschlüsse Nr. 118/2024 (16. Dezember), 54/2023 (29. Juni) und 6/2025 (23. Januar) geänderte „Verordnung über Datenschutz, Offenlegung und Anträge auf Zugang zu Daten von öffentlichem Interesse“, Buch I: Datenschutzverordnung, außer Kraft gesetzt.

7. Anhänge

Anhang Nr. 1: Arten von Registern, Datenschutzerklärungen und Protokollen, die vom lokalen Datenschutzbeauftragten geführt werden
Anhang Nr. 2: Prüfpfad

1. Anhang: Arten von Registern, Datenschutzerklärungen und Protokollen, die vom lokalen Datenschutzbeauftragten geführt werden

A) Verzeichnis der Datenverarbeitungsvorgänge – das Verzeichnis gemäß Artikel 30 der Verordnung, das nach Art der Datenverarbeitungsvorgänge zu führen ist:

1. berufliche Tätigkeiten
2. wissenschaftliche Forschungstätigkeiten
3. Tätigkeiten im Bereich Personalwesen
4. Verwaltungsaktivitäten (Wirtschaft, Sekretariat, Kommunikation)

B) Datenschutzerklärungen im Zusammenhang mit dem Verzeichnis der Datenverarbeitungsvorgänge

C) Weitere Verzeichnisse:

1. Verzeichnis der Datenschutzerklärungen
2. Verzeichnis der Datenübermittlungen
3. Register der Einwilligungen der betroffenen Personen
4. Verfügungsregister
5. Schulungsregister
6. Verzeichnis der Datenschutzvorfälle

D) Protokolle

1. Protokoll über die vorgeschriebene Führung der Register
2. Protokoll zur Selbstkontrolle

Anhang Nr. 2: Prüfpfad

2/A. Zentrum für Datenschutz und Patientenrechte[74]

	Schritte des Prozesses	Schritte der Vorbereitung	Verantwortungsebenen					Als Ergebnis des Prozesses entstandenes Dokument
			Zuständiger	Prüfer	Art der Kontrolle	Genehmigender	Art der Genehmigung	
1.	Freigabe von Patientendaten	Prüfung der Durchführbarkeit des Antrags	Beauftragter Mitarbeiter der ABK	Leiter der ABK	Prüfung des Dokuments, Unterschrift	Leiter der ABK	Unterschrift	Antwortdokument
2.	Durchführung einer Folgenabschätzung	Prüfung der Notwendigkeit einer neuen Datenverarbeitung, Rücksprache mit dem Datenschutzbeauftragten	Leiter der betroffenen Organisationseinheit, lokaler Datenschutzbeauftragter	Leiter der ABK, Datenschutzbeauftragter	Analyse der Daten	Leiter der ABK	Unterschrift	Dokument zur Folgenabschätzung
3.	Mitwirkung bei der Untersuchung der Bearbeitung von Patientenbeschwerden auf Anfrage der Direktion für Prozessvertretung	Stellungnahme zu einem vom Direktorium für Rechtsvertretung eingereichten Antrag durch den	vom ABK benannten Mitarbeiter	Leiter der ABK	Prüfung des Dokuments, Unterschrift	Leiter der ABK	Unterschrift	Antwortdokument an die Direktion für Prozessvertretung
4.	Bearbeitung von Datenschutzbeschwerden auf Organisationsebene	Unterstützung auf Anfrage, Stellungnahme zu einem bestimmten Fall	Beauftragter Mitarbeiter der ABK	Leiter der ABK	Prüfung des Dokuments, Unterschrift	Leiter der ABK	Unterschrift	Antwortdokument
5.	Erstellung von Richtlinien	Vorschlag zur Veröffentlichung der Richtlinien	Beauftragter Mitarbeiter der ABK	Leiter der ABK	Prüfung des Dokuments, Unterschrift	Leiter der ABK	Unterschrift	Leitfaden

[74] Geändert durch: Senatsbeschluss Nr. 31/2026 vom 25. März, Artikel 12. Gültig ab dem: 1. April 2026

	Schritte des Prozesses	Schritte der Vorbereitung	Verantwortungsebenen					Als Ergebnis des Prozesses entstandenes Dokument
			Zuständiger	Prüfer	Art der Kontrolle	Genehmigender	Art der Genehmigung	
6.	Kontaktpflege zu den Patientenrechtsvertretern	Treffen gemäß Arbeitsplan und nach Bedarf	Leiter der ABK	n.n.	Prüfung des Dokuments, Unterschrift	Leiter der ABK	Unterschrift	Erinnerungen
7.	Führung von Registern	Einrichtung und fortlaufende Einführung von Registern	Beauftragter Mitarbeiter der ABK	Leiter der ABK	Prüfung des Dokuments, Unterschrift	Leiter der ABK	Unterschrift	Eintragung mit Unterschrift zur Bestätigung der durchgeführten Prüfung
8.	Stellungnahme zu Verträgen zum Thema Datenschutz sowie zur Verarbeitung personenbezogener Daten	Prüfung von Verträgen	Beauftragter Mitarbeiter der ABK	Leiter der ABK	Prüfung des Dokuments, Unterschrift	Leiter der ABK	Unterschrift	datenschutzrechtlich konformer Vertragsentwurf
9.	Überprüfung der Konformität der Datenschutzmaßnahmen der Universität	Prüfung der von den lokalen Datenschutzbeauftragten erstellten Jahresberichte, fortlaufende Aktivitäten während des Jahres, Prüfung der Konformität der eingegangenen Dokumente	Beauftragter Mitarbeiter der ABK	Leiter der ABK	Rechenschaftslegung	Leiter der ABK	Annahme des Berichts	Bericht über das Ergebnis der Konformitätsprüfung

2/B. Datenschutzbeauftragter

	Schritte des Verfahrens	**Schritte der Vorbereitung**	**Verantwortungsebenen**					**Als Ergebnis des Prozesses erstelltes Dokument**
			Auftraggeber	**Prüfer**	**Art der Kontrolle**	**Genehmigender**	**Art der Genehmigung**	
1.	Information und Beratung	Kennenlernen des jeweiligen Sachverhalts, Erarbeiten einer Stellungnahme	Datenschutzbeauftragter	k. A.	k. A.	k. A.	Unterschrift	Antwortschreiben an den Anfragenden
2.	Überprüfung der Umsetzung der rechtlichen Steuerungsinstrumente im Bereich des Datenschutzes	Planung und Durchführung der Aufgaben des jährlichen Arbeitsplans	Datenschutzbeauftragter	k. A.	k. A.	k. A.	Unterschrift	Jahresbericht an den Rektor und den Kanzler
3.	Überprüfung der Datenverarbeitungsaktivitäten	Durchführung von Aufgaben gemäß dem Jahresarbeitsplan	Datenschutzbeauftragter	k. A.	Zwischenbericht	k. A.	Unterschrift	Informationsblatt für den Rektor und den Kanzler
4.	Umgang mit Datenschutzvorfällen	Erkennung und Bewertung eines Vorfalls,	lokaler Datenschutzbeauftragter/Datenverantwortlicher, Leiter der vom Vorfall betroffenen Organisationseinheit	Datenschutzbeauftragter	Analyse von Daten und Informationen	Rektor, Kanzler	Unterschrift	Meldung zur Bearbeitung des Vorfalls, Unterrichtung des Rektors und des Kanzlers, gegebenenfalls Meldung an die Aufsichtsbehörde
5.	Kontaktpflege und Zusammenarbeit mit der Aufsichtsbehörde	Erfassung und Auswertung der für den jeweiligen Fall relevanten Informationen,	Datenschutzbeauftragter	k. A.	k. A.	Rektor, Kanzler	Unterschrift	Bericht

	Schritte des Verfahrens	**Schritte der Vorbereitung**	**Verantwortungsebenen**					**Als Ergebnis des Prozesses erstelltes Dokument**
			Auftraggeber	**Prüfer**	**Art der Kontrolle**	**Genehmigender**	**Art der Genehmigung**	
		Erfüllung der Meldepflicht						