Datenschutzkonzept UAK am UKS

Klara Dauber, betriebliche Datenschutzbeauftragte
Universitätsklinikum des Saarlandes, Homburg

Inhaltsverzeichnis

Datenschutzkonzept UAK am UKS

1. Tätigkeitsbeschreibung und Hintergrund

Die UAK ist mit Beschluss des Aufsichtsrats des UKS vom 29.04.2021 eingesetzt und beauftragt worden, in Unterstützung der Kontrollaufgabe des Aufsichtsrates die Missbrauchs-verdachtsfälle am UKS umfassend und in einem übergreifenden gesellschaftlichen Sinne aufzuarbeiten, wobei die Betroffenen und ihre Geschichte im Mittelpunkt der Aufarbeitung stehen und in den Aufarbeitungsprozess einbezogen werden sollen. Aufgabe der UAK ist insbesondere, durch Beiziehung aller erforderlichen Akten/Unterlagen möglichst alle Verdachtsfälle zu erfassen und zu beurteilen, Fragen ggf. angezeigter Entschädigungsleistungen zu klären, Täterstrategien nachzugehen, die Organisations- und Regelstrukturen am UKS zu analysieren und auf dieser Basis Empfehlungen für eine verbesserte Prävention gegen sexuellen Missbrauch und eine gute Compliance am UKS nach Maßgabe heutiger „best practice“ abzugeben. Dabei hat der Aufsichtsrat des UKS der UAK Unabhängigkeit bei ihrer Arbeit und bei der Veröffentlichung ihrer Ergebnisse zugesichert. Die UAK ist selbständig tätige, dem Aufsichtsrat zuzuordnende Arbeitseinheit und damit auch Organ des UKS.

2. Glossar / Begriffsbestimmungen und Abkürzungen

Begriffsbestimmungen

personenbezogene Daten / pbD

Das sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Auftragsverarbeiter

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet.

Betroffene

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

Verantwortlicher

Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel dieser Verarbeitung entscheidet.

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

Patientenakte
Sind die gesammelten Unterlagen und Aufzeichnungen eines Behandlungsteams über einen Patienten. Dazu gehören die Anamnese, Diagnosen, Notizen über Untersuchungen, Untersuchungsergebnisse, Therapiemaßnahmen, Operationen, Befunde, Aufklärungen, Einwilligungen und der Arztbriefe. Patientendaten sind Gesundheitsdaten, Art. 9 Abs. 1 DSGVO.

Zusatzakten
Sind personenbezogene Daten, der Kinderschutzgruppe am UKS, die ein Zusatz zur stationären Patientenakte darstellen und in Papierform von der Kinderschutzgruppe geführt werden. Teilweise enthält die Zusatzakte Doppelungen aus der Patientenakte, vor allem werden darin aber die Umstände zu dem konkreten Kindermissbrauchsverdacht festgehalten, die nicht in diesem Umfang in der stationären Akte enthalten sind.

Akten
Akten sind Unterlagen, Dokumente etc. die nicht notwendigerweise einen Patientenbezug aufweisen, diesen aber aufweisen können.

Abkürzungen

UKS
Universitätsklinikum des Saarlandes

UAK
Unabhängige Aufarbeitungs- Kommission

SDSG
Saarländisches Datenschutzgesetz

EU DSGVO / DSGVO
Europäische Datenschutzgrundverordnung (EU-DSGVO)

KJP
Kinder und Jugendpsychiatrie

MA
Mitarbeitende

TOM
Technisch Organisatorische Maßnahmen

pbD
personenbezogene Daten

MS Office
Bürosoftware der Firma Microsoft (Textverarbeitung, Tabellenkalkulation, Präsentationen)

MS Teams
Kollaborations-Software der Firma Microsoft – vorrangig für Videotelefonie verwendet.

3. Zwecke der Verarbeitung

1. Umfassende übergreifende Aufarbeitung der Missbrauchsverdachtsfälle am Universitätsklinikum des Saarlandes (UKS) über die juristische Aufklärung hinaus in einem übergreifenden gesellschaftlichen Sinne
2. Aufarbeitung mit den Betroffenen/ Schaffen eines Verständigungsprozesses
3. Initiieren von Entschädigungszahlungen
4. Angebot gezielter Unterstützung für Betroffene
5. Untersuchung des institutionellen Umgangs des UKS mit Betroffenen und deren Familien
6. Untersuchen der Rechtslage bezüglich des Informationsaustausches zwischen öffentlichen Stellen im Falle des Verdachts pädosexueller Verhaltensweisen und falls erforderlich Vorschläge zur Gesetzesänderung machen, um das Schutzniveau für Kinder und Jugendliche zu erhöhen
7. Analyse der Täterstrategien
8. Prävention von pädokriminellem Verhalten
9. Schaffen von größtmöglicher Transparenz
10. Organisationsanalyse, prüfen ob Handlungsbedarf oder Verbesserungsbedarf besteht
11. Veröffentlichen von Ergebnissen

4. Umfang der Verarbeitung

1. Patientenakten der Kinder und Jugendpsychiatrie (KJP), die einen Bezug zu M. S aufweisen. Aktenführende Stelle UKS.
2. Zusatzakten der Kinderschutzgruppe des UKS, soweit diese einen Bezug zu verdachtsfällen sexuellen Missbrauchs am UKS aufweisen. Aktenführende Stelle UKS.
3. Personalakten des M. S. Aktenführende Stelle UKS.
4. Ermittlungs- und Strafakten von M. S/ andere Strafakten/Polizeiliche Akten Aktenführende Stelle Staatsanwaltschaft, Polizei.
5. Unterlagen des Justiziariats, der Ärztlichen Direktion und Unterlagen anderer Stellen am UKS (Dezernate etc.) mit Bezug zu den Missbrauchsverdachtsfällen. Aktenführende Stelle UKS.
6. Veröffentlichungen in Presse/Medien
7. Berichte und Unterlagen des Sonderermittlers Schnur. Aktenführende Stelle Staatskanzlei.
8. Privatleben M. S. – Judoclub- Täterstrategien herausfinden
9. Akten/Protokolle des Parlamentarischen Untersuchungsausschusses des saarländischen Landtages zu den Missbrauchsverdachtsfällen am UKS, Aktenführende Stelle: Landtag des Saarlandes.
10. Kontaktdaten Betroffener, die sich mit der UAK in Verbindung setzen
11. Bankverbindungsdaten für Entschädigungszahlungen

5. Organisationsstruktur und Verantwortlichkeiten

1. Die unabhängige Aufarbeitungskommission (Kommission) ist eine öffentliche Stelle nach § 2 Abs. 2 BDSG und in ihrer Gesamtheit als eigener Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO anzusehen.
   Sie entscheidet selbst über Art und Umfang der Verarbeitung personenbezogener Daten, also darüber, welche personenbezogenen Daten und Datenkategorien sie für die Erfüllung ihres Auftrags benötigt und wie sie mit diesen Daten mit Blick auf die weitere Verarbeitung und die Erfüllung ihrer Aufgabe umgeht. Insbesondere der Arbeitsauftrag stellt hierzu klar, dass die Kommission unabhängig und weisungsfrei agiert und sowohl die Organisation ihrer inneren Abläufe, die Setzung thematischer Schwerpunkt als auch die Veröffentlichung der Ergebnisse selbst verantwortet. Hierbei trägt die Kommission insbesondere auch die Verantwortung für die Rechtmäßigkeit ihres Handelns, insbesondere dafür, dass ihr Handeln den Anforderungen des Datenschutzes genügt und die Rechte Dritter nicht verletzt werden. Dies gilt auch für die Veröffentlichung der Untersuchungsergebnisse.
   Dass der Arbeitsauftrag der Kommission durch den Aufsichtsrat vorgegeben ist, steht ihrer Qualifikation als Verantwortlicher i.S.d. Art. 4 Nr. 7 DSGVO nicht entgegen. Durch die Zusicherung von Unabhängigkeit und Weisungsfreiheit geht die Erfüllung dieses Arbeitsauftrags mit einer Autonomie einher, die der Kontrolle des Aufsichtsrates (bzw. des UKS) entzogen ist.

2. Die Kommission ist zusammen mit dem UKS als gemeinsam Verantwortliche i.S.d. Art. 26 DSGVO zu qualifizieren. Denn eine gemeinsame Verantwortlichkeit kann selbst dann vorliegen, wenn nicht jeder Beteiligte Zugang zu den personenbezogenen Daten hat. Ausreichend ist es bereits, wenn einer der Beteiligten die Datenverarbeitung unmittelbar beeinflusst oder jedenfalls von der Datenverarbeitung selbst profitiert und dadurch an der Entscheidung über die Zwecke und Mittel der Verarbeitung teilnimmt. Insofern müssen die Beteiligungsbeiträge bei der gemeinsamen Verantwortung nicht gleichwertig sein.

   Übertragen auf den vorliegenden Sachverhalt bedeutet dies, dass der Aufsichtsrat des UKS, als Organ des UKS gem.§ 4 Satzung des Universitätsklinikums des Saarlandes, hier unterschiedliche Beiträge bei der Zweck- und Mittelentscheidung i.S.d. Art. 26 DSGVO leistet. Durch die Definition des Arbeitsauftrags gibt der Aufsichtsrat des UKS den für die Kommission verbindlichen Rahmen vor und bestimmt damit abschließend die Verarbeitungszwecke. Indem der Aufsichtsrat des UKS im Arbeitsauftrag darüber hinaus auch Vorgaben hinsichtlich der beizuziehenden Akten und Unterlagen macht (und jedenfalls die UKS-internen Akten der Kommission zu einem späteren Zeitpunkt zur Verfügung stellen wird), beteiligt sich der Aufsichtsrat des UKS auch an der Entscheidung über die Mittel der Verarbeitung. Auch ist das UKS als öffentliche Stelle nach § 2 Abs. 2 BDSG anzusehen.

   Alle Beiträge sowohl des UKS als auch der Kommission stehen dabei unter dem gemeinsamen, übergeordneten Interesse an einer Aufarbeitung der bisher bekannten Missbrauchsverdachtsfälle am UKS, um hierdurch dem Versprechen nach

größtmöglicher Transparenz nachzukommen und mit geeigneten Maßnahmen künftig dafür Sorge zu tragen, dass der Schutz vor sexuellem Missbrauch insbesondere von Kindern am UKS gewährleistet ist.

3. Datenschutzbeauftragte
   Die gemeinsame Datenschutzbeauftragte der UAK und des UKS ist Frau Ass. Jur. Klara Sophia Dauber.

6. Datenschutzziele

Die UAK verpflichtet sich darauf, dass …

- die rechtlichen Pflichten durch die einschlägigen Datenschutzgesetze eingehalten werden.
- personenbezogene Daten nur auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.
- die Betroffenen hinreichend über die Verarbeitung ihrer personenbezogenen Daten informiert werden.
- die personenbezogenen Daten nur für den benötigten Zweck genutzt werden.
- nur personenbezogene Daten gesammelt werden, welche auch für den Prozess erforderlich sind.
- die personenbezogenen Daten so geschützt werden, das unbefugte Dritte diese nicht manipulieren können.
- personenbezogene Daten nur für die Dauer des Zweckes aufbewahrt oder verarbeitet werden und anschließend sofort vernichtet bzw. gelöscht werden, wenn sie nicht mehr erforderlich sind.
- personenbezogene Daten so geschützt werden, dass diese nicht von unbefugten Dritten abgeschöpft oder eingesehen werden können.
- personenbezogene Daten vor unbeabsichtigter Zerstörung oder Verlust geschützt werden.
- die Dokumentation über den Prozess vorhanden ist bzw. zeitnah erstellt werden kann, um Auskunft geben zu können.

7. Anfallende Datenkategorien und Kategorien betroffener Personen

Kategorien betroffener Personen

Folgende Kategorien betroffener Personen sind Gegenstand des Untersuchungsauftrags:

- Beschäftigte
- Auszubildende und Praktikanten
- ehemalige Arbeitnehmer
- freie Mitarbeiter

- Vorstand, Dezernatsleiter, Klinikdirektoren
- Angehörige von Beschäftigten
- Angehörige von Betroffenen
- Interessenten
- Lieferanten und Dienstleister
- Geschäftspartner
- externe Berater
- Besucher
- Pressevertreter
- Patienten
- Mitglieder des Judoclubs und ehemalige Mitglieder des Judoclubs

Kategorien personenbezogener Daten

Folgende Kategorien personenbezogener Daten sind oder könnten im Lauf der Untersuchung Gegenstand der Verarbeitung sein:

- Adressen
- Alter / Geburtsdatum
- Arbeitszeitdaten
- Audiodaten
- Bankverbindung; inkl. Zahlungsverkehr
- Behandlungsdaten
- Beschäftigtendaten (Qualifikationen)
- Bilddaten
- Hobbys
- E-Mails
- Gesundheitsdaten
- Mitarbeiterbewertungen / -beurteilungen
- Namen
- Personal- und Identifikationsnummern
- Reisebuchungs- und Reiseabrechnungsdaten
- Straftaten / strafrechtliche Ermittlungsdaten / strafrechtliche Verurteilungen
- Telekommunikationsabrechnungsdaten
- Telekommunikationsverbindungsdaten
- Telefonnummern
- Vertragsdaten
- Zahlungsdaten
- Zugangsdaten

8. Maßnahmen zum Umgang mit Datenschutzvorfällen

Datenschutz Richtlinie - Datenpanne

Es wurde am UKS ein Prozess zur Meldung einer Datenpanne erarbeitet, der auch für die UAK übernommen wird. Die erforderlichen Dokumente und Beschreibung des Ablaufs stehen jedem Mitarbeiter im Intranet zur Verfügung, so dass eine erforderliche Meldung rasch erfolgen kann. Die Datenschutzbeauftragte ist immer vorab zu informieren.

Erkennen von Datenschutzvorfällen

Es findet eine technische Überwachung der IT-Infrastruktur sowie eine technisch eingerichtete und bei Bedarf mögliche Überwachung der Zugriffe auf besonders sensible Daten und dem Erfassen und Auswerten über Log Systemen statt.

Datenschutz-Vorfallbehandlung

Der Ablauf zur Meldung einer Datenpanne ist vorhanden und läuft wie folgt:

- Überblick über die Situation gewinnen
- Abstimmung mit dem Datenschutzbeauftragten und ggf. mit den Verantwortlichen
- Maßnahmen treffen um Leib und Leben zu schützen
- Sofortmaßnahmen treffen, um den Vorfall einzudämmen
- Dokumentation des Vorfalls:
  - Betroffene Daten und Personenkategorien
  - Anzahl Betroffener und der Datensätze
  - Beschreibung der wahrscheinlichen Folgen
  - Beschreibung der ergriffenen und vorgeschlagenen Maßnahmen
  - Ggf. Maßnahmen für die Abmilderung der möglichen negativen Folgen
- Sicherung der Beweismittel
- Behebung des Schadens und Aufnahme des regulären Betriebs
- Nachbereitung um die Ursachen zu ermitteln und konkrete Verbesserungen erarbeiten
- Ermitteln, ob eine gesetzliche Meldepflicht besteht und welche Vorgaben und Fristen hierbei eingehalten werden müssen
- Die Meldung sollte innerhalb von 72 Std. erfolgen

Die Mitarbeiterinnen und Mitarbeiter haben die Möglichkeit eine Datenschutzverletzung nach Art. 33 DS-GVO“ formlos / Formblattunterstützt an den DSB zu melden.
Die weitere Vorgehensweise wird dann umgehend abgestimmt.

Bewertung der Wirksamkeit der getroffenen Maßnahmen

Die getroffenen Maßnahmen von Datenschutzvorfällen müssen auf ihre Wirksamkeit hin geprüft werden.

9. Rechtsgrundlagen

Bedingt durch die organisatorische Angliederung der Kommission als Institution an den Aufsichtsrat, die Aufgaben des Aufsichtsrates wahrnimmt, leiten sich auch die datenschutzrechtlichen Befugnisse von denen des Aufsichtsrates ab.

Dies hat zur Konsequenz, dass als alleinige Rechtsgrundlagen für die durch die Kommission durchgeführte Datenverarbeitung zum einen eine Einwilligung der Betroffenen nach Art. 6 Abs. 1 lit. a DSGVO sowie zum anderen Art. 6 Abs. 1 lit. e DSGVO ist.
Danach ist eine Verarbeitung personenbezogener Daten durch die Kommission nur rechtmäßig, wenn sie zur Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
Da es sich bei den zu verarbeitenden Daten insbesondere um Gesundheitsdaten und somit eine besondere Kategorie von Daten i.S.d. Art. 9 Abs. 1 DSGVO handelt, wird für die Verarbeitung lediglich die Einwilligung gem. Art. 9 Abs. 2 lit. a DSGVO oder Art. 9 Abs. 2 lit. g DSGVO i.V.m. § 7 Abs. 1 SDSG herangezogen.
Bei der praktischen Ausfüllung dieses Erlaubnistatbestandes und der gebotenen Abwägung wird berücksichtigt, dass die Kommission vom Aufsichtsrat eingesetzt wurde, um letztlich Aufgaben des Aufsichtsrates wahrzunehmen. Wenn auch nicht ausdrücklich, so hat doch der Aufsichtsrat seine Befugnisse im Zusammenhang mit der Aufarbeitung der Missbrauchsverdachtsfälle auf die Kommission übertragen. Die durch die Kommission beabsichtigte Datenverarbeitung erfolgt daher alleine zur Wahrnehmung von Aufgaben, die eigentlich dem Aufsichtsrat als Kontrollgremium des UKS obliegen. Insofern ist es logisch zwingend, dass die Befugnisse der Kommission bei allen Datenverarbeitungen nicht über die Befugnisse einer legitimierten Datenverarbeitung durch den Aufsichtsrat des UKS hinausgehen dürfen und zu den Datenverarbeitungsbefugnissen des Aufsichtsrates streng akzessorisch sind. Erforderlich i.S.d. Art. 6 Abs. 1 lit. e DSGVO ist daher maximal die Datenverarbeitung, die auch der Aufsichtsrat zulässigerweise durchführen dürfte.

Zum Zwecke der Aufarbeitung der sexuellen Missbrauchsverdachtsfälle am UKS wird die UAK alle erforderlichen Akten am UKS beiziehen. Dies wird auf der Rechtsgrundlage von Art. 9 Abs. 2 lit. a DSGVO erfolgen, sowie einer Entbindung von der ärztlichen Schweigepflicht.

Die Rechtsgrundlagen im Einzelnen

1. Patientenakten der Kinder und Jugendpsychiatrie (KJP), die einen Bezug zu M. S aufweisen, Patientenakten auf die sich der Untersuchungsauftrag des Aufsichtsrates des UKS erstreckt und Personalakten des M. S. Aktenführende Stelle UKS.

   Die datenschutzrechtliche Zulässigkeit der Verwendung der beim UKS geführten Aktenbestände (Patientenakten, Personalakte des Herrn S) wird durch § 4 Abs. 2 SDSG legitimiert, zumindest solange, wie sich die Datenverarbeitung im Rahmen der von § 7 Abs. 1 SDSG erwähnten Aufsichts- und Kontrolltätigkeit bewegt.
   Eine weitergehende Analyse der Akten wird nur mit der Einwilligung der Betroffenen nach Art. 6 Abs. 1 lit. a DSGVO in die Verarbeitung ihrer pbD möglich sein. Zusätzlich wird auch eine Entbindung von der ärztlichen Schweigepflicht nach § 203 StGB notwendig sein.

2. Zusatzakten der Kinderschutzgruppe des UKS, soweit diese einen Bezug zu Verdachtsfällen sexuellen Missbrauchs am UKS aufweisen und vom

Untersuchungsauftrages des Aufsichtsrates des UKS erfasst sind. Aktenführende Stelle UKS.

Die datenschutzrechtliche Zulässigkeit wird durch § 4 Abs. 2 SDSG legitimiert, zumindest solange, wie sich die Datenverarbeitung im Rahmen der von § 7 Abs. 1 SDSG erwähnten Aufsichts- und Kontrolltätigkeit bewegt. Eine weitergehende Analyse der Zusatzakten wird nur mit der Einwilligung der Betroffenen nach Art. 6 Abs. 1 lit. a DSGVO in die Verarbeitung ihrer pbD möglich sein. Zusätzlich wird auch eine Entbindung von der ärztlichen Schweigepflicht nach § 203 StGB notwendig sein.

3. Dokumente/Unterlagen die im Rahmen der Aufklärung der Verdachtsfälle sexuellen Missbrauchs erzeugt wurden und die am UKS lagern oder auf Speichermedien gespeichert sind. Aktenführende Stelle UKS.

   Die datenschutzrechtliche Zulässigkeit wird durch § 4 Abs. 2 SDSG legitimiert, zumindest solange, wie sich die Datenverarbeitung im Rahmen der von § 7 Abs. 1 SDSG erwähnten Aufsichts- und Kontrolltätigkeit bewegt.
   Zusätzlich muss die ursprüngliche Verarbeitung, genauer die Erhebung rechtmäßig gewesen sein.
   Sollten die Dokumente oder Unterlagen unter die ärztliche Schweigepflicht fallen, ist ein Entbinden von der ärztlichen Schweigepflicht hier nicht notwendig, siehe Argumentation Punkt 6.

4. Ermittlungs- und Strafakten von M. S. Aktenführende Stelle Staatsanwaltschaft, Polizei

   Für Datenerhebungen bei Dritten bedarf es sowohl einer legitimen Erhebungsbefugnis auf Seiten der Aufarbeitungskommission als auch einer legitimen Übermittlungsbefugnis auf Seiten der übermittelnden Stelle.
   Akten und Unterlagen, die sich ausschließlich mit der Person des Herrn S beschäftigen unterfallen wegen des Todes nicht den datenschutzrechtlichen Beschränkungen. Andere in der Akte erwähnte Namen von Personen müssen geschwärzt werden.

5. Andere Strafakten, Polizeiliche Akten. Aktenführende Stelle Staatsanwaltschaft, Polizei.

   Für Datenerhebungen bei Dritten bedarf es sowohl einer legitimen Erhebungsbefugnis auf Seiten der Aufarbeitungskommission als auch einer legitimen Übermittlungsbefugnis auf Seiten der übermittelnden Stelle.

   Bei einem Übermittlungsersuchen an eine andere öffentliche Stelle trägt gem. § 6 Abs. 1 SDSG grundsätzlich die übermittelnde Stelle die Verantwortung für die Zulässigkeit der Übermittlung. Erfolgt die Übermittlung aufgrund eines Ersuchens einer öffentlichen Stelle, trägt diese die Verantwortung. Die empfangende Stelle hat in dem

Ersuchen jedoch der übermittelnden Stelle, die für die Prüfung der Zulässigkeit der Übermittlung erforderlichen Angaben detailliert darzulegen.

Hier kann eine Verarbeitung pbD durch die UAK auf § 474 Abs. 2 S. 1 Nr. 1 StPO gestützt werden, allerdings mit der Einschränkung, dass die pbD nur zu dem Zwecke der Entschädigungszahlung verarbeitet werden dürfen. Die Verarbeitung ist auf die personenbezogenen Daten beschränkt, die zum Zwecke repressive Gefahrenabwehr verarbeitet werden.

6. Unterlagen des Justiziariats des UKS mit Bezug auf Missbrauchsverdachtsfälle. Aktenführende Stelle UKS.

   Die datenschutzrechtliche Zulässigkeit wird durch § 4 Abs. 2 SDSG legitimiert, zumindest solange, wie sich die Datenverarbeitung im Rahmen der von § 7 Abs. 1 SDSG erwähnten Aufsichts- und Kontrolltätigkeit bewegt. **Sollten diese Unterlagen der ärztlichen Schweigepflicht unterliegen wird eine Entbindung von der ärztlichen Schweigepflicht nicht notwendig sein.**

   Bei der Übermittlung der Patientenakte an einen Arzt der UAK würden wir zwar davon ausgehen, dass § 203 Abs. 1 StGB grundsätzlich tatbestandlich erfüllt ist. Jedoch könnte eine die Rechtswidrigkeit ausschließende Offenbarungsbefugnis gegeben sein, wenn es sich bei dem externen Arzt der UAK um eine mitwirkende Person im Sinne des § 203 Abs. 3 S. 2 StGB handelt.

   Nach § 203 Abs. 3 Satz 2 StGB handeln zur Verschwiegenheit verpflichtete Personen dann nicht rechtswidrig, wenn sie fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist.

   Es könnte rechtlich vertretbar sein, diese Voraussetzungen hier als gegeben anzusehen.

   In Abgrenzung zu den berufsmäßig tätigen Gehilfen und den in Vorbereitung auf den Beruf tätigen Personen (§ 203 Abs. 3 Satz 1) werden von dem Begriff der sonstigen mitwirkenden Personen diejenigen erfasst, die zwar an der beruflichen oder dienstlichen Tätigkeit der schweigepflichtigen Person mitwirken, also in diese Tätigkeit in irgendeiner Weise eingebunden werden und Beiträge dazu leisten, ohne allerdings in die Sphäre des Berufsgeheimnisträgers eingegliedert zu sein (BT-Drs. 18/11936 S. 22 f.).

   Eine Offenbarung von fremden Geheimnis an diese Mitwirkenden ist nach § 203 Abs. 3 Satz 2 StGB gerechtfertigt, soweit dies für die Inanspruchnahme der Tätigkeit der mitwirkenden Person erforderlich ist. Damit darf der Berufsgeheimnisträger Geheimnisse insoweit mitteilen, als dies für die Übertragung der Tätigkeit und damit die externe Mitwirkung notwendig ist (Schönke/Schröder § 203 Rn. 51). Nicht

entscheidend ist dagegen, ob die Hinzuziehung des externen Mitwirkenden, dem gegenüber das fremde Geheimnis offenbart wird, für die Ausübung der Tätigkeit des Berufsgeheimnisträgers erforderlich ist. D.h. es kommt gerade nicht auf die Frage an, ob die Auslagerung der fraglichen Tätigkeit gerade wegen einer besonderen Fachkunde des Beauftragten in Betracht gezogen wird und auch nicht darauf, ob der Beauftragte die ausgelagerte Tätigkeit besser als der Auftrag gebende Berufsgeheimnisträger durchführen kann. Nach dem Willen des Gesetzgebers soll eine Hinzuziehung externer Dritter schon aus rein wirtschaftlichen Gründen zulässig sein (BT-Drs.18/11936 S. 17 f.).

Wenn zwar Maßstab für die Erforderlichkeit nicht die Tätigkeit des Berufsgeheimnisträgers, sondern die der Beauftragung zugrundeliegenden vertraglichen Abreden sind, verlangt § 203 Abs. 3 Satz 2 StGB gleichwohl eine Konnexität zwischen der Tätigkeit des Berufsgeheimnisträgers und der übertragenen Tätigkeit. Danach muss die Mitwirkung des Externen unmittelbar mit der beruflichen Tätigkeit des Geheimnisträgers, ihrer Vorbereitung, Durchführung, Auswertung oder Verwaltung zusammenhängen. Eine solche Konnexität liegt nach h.E. auch bei der Auslagerung von über § 203 StGB geschützten Tätigkeiten zur Erfüllung ordnungsrechtlicher Pflichten des Berufsgeheimnisträgers vor, wenn und soweit die Erfüllung dieser Pflichten unmittelbar aus der beruflichen Tätigkeit der schweigepflichtigen Person herrührt.

Für eine Hinzuziehung eines externen Arztes zur Erledigung dieser Tätigkeit spricht bereits dessen fachliche Expertise. Darüber hinaus erscheint die Mitwirkung eines objektiven Dritten zur Bewältigung dieser Aufgabe erforderlich.

7. Berichte und Unterlagen des Sonderermittlers Schnur oder sonstige Akten der Staatskanzlei zu Verdachtsfällen sexuellen Missbrauchs am UKS. Aktenführende Stelle Staatskanzlei.

   Eine Weitergabe der Berichte und Unterlagen des Sonderermittlers Schnur erfolgt auf der Rechtsgrundlage der rechtsaufsichtslichen Beratungsfunktion der Staatskanzlei, nach §§ 4 Abs. 2 SDSG, 7 Abs. 1 SDSG.
   Polizeiliche Unterlagen aus dem Präventivbereich dürfen nicht aufgrund dieser Rechtsgrundlage verarbeitet werden. Hier kann eine Verarbeitung durch die UAK auf § 474 Abs. 2 S. 1 Nr. 1 StPO gestützt werden, allerdings mit der Einschränkung, dass die pbD nur zu dem Zwecke der Entschädigungszahlung verarbeitet werden dürfen und sich die Rechtsgrundlage nur die Weitergabe der Akten (nicht den Bericht) des Sonderermittlers bezieht.
   Zudem muss gem. § 479 Abs. 5 Nr. 1 StPO die zuständige Staatsanwaltschaft der Weitergabe dieser Akten zustimmen.

Weitere Unterlagen der Staatskanzlei zu den Verdachtsfällen sexuellen Missbrauchs am UKS dürfen der Rechtsgrundlage der rechtsaufsichtslichen Beratungsfunktion der Staatskanzlei, nach §§ 4 Abs. 2 SDSG, 7 Abs. 1 SDSG an die UAK übergeben werden.

Unterlagen die im Rahmen der Kontaktaufnahme von Betroffenen mit der Staatskanzlei, namentlich Herrn Brocher, entstanden sind können aufgrund einer fortgeltenden konkludenten Einwilligung der Betroffenen in die Verarbeitung Ihrer personenbezogenen Daten im Rahmen der Aufklärung der Verdachtsfälle sexuellen Missbrauchs am UKS an die UAK übermittelt werden.

8. Privatleben M. S – Judoclub- Täterstrategien herausfinden

   Keine Rechtsgrundlage. Man könnte den Judo Club bitten auf seine Mitglieder zuzugehen, um deren datenschutzrechtliche Einwilligung bitten und gleichzeitig die UAK vorstellen.

9. Akten/Protokolle des Parlamentarischen Untersuchungsausschusses des saarländischen Landtages zu den Missbrauchsverdachtsfällen am UKS, Aktenführende Stelle: Landtag des Saarlandes.

   Eine Einsichtnahme in den öffentlichen Teil der Protokolle des Untersuchungsausschusses ist ohne weitere Rechtsgrundlage möglich.

   Eine Einsichtnahme in den nicht öffentlichen Teil der Protokolle wird mit der Einwilligung der Mitglieder des parlamentarischen Untersuchungsausschusses nach Art. 6 Abs. 1 a DSGVO gewährt. Der Aufsichtsrat des UKS stellt eine Anfrage an den Landtag mit dem Inhalt, dass mit Einwilligung der Ausschussmitglieder die Übermittlung der nicht öffentlichen Protokolle an die UAK erfolgen soll.

10. Die Einbindung des Ärztlichen Personals der UAK mit Einwilligung der Betroffenen

    Kann nur durch die informierte Einwilligung der Betroffenen legitimiert werden. Hier ist zu beachten, dass auch eine Entbindung von der ärztlichen Schweigepflicht erforderlich ist.
    Beim diesbezüglichen Erstkontakt mit den Betroffenen wird die Kontaktaufnahme durch das UKS mit der Bitte um Einwilligung in die Datenverarbeitung durch die Aufarbeitungskommission, verbunden mit dem Hinweis, dass die Akte an das Ärztliches Personal der UAK zur Auswertung übermittelt werden soll, erfolgen. Der Prozess wird gegenüber den Betroffenen transparent dargelegt.

11. Die Einbindung des Ärztlichen Personals der UAK bei der Betreuung einer Telefonhotline für die Betroffenen

Das Ärztliches Personal der UAK soll für die UAK eine Telefonhotline betreuen, bei der sich Betroffene telefonisch melden können. Hierbei wird die Einwilligung der Betroffenen nach Art. 9 Abs. 2 a DSGVO eingeholt.

10. Technisch Organisatorische Maßnahmen

Die Verantwortlichen der UAK und des UKS haben abgestimmt, dass die TOM im Grunde denen des UKS entsprechen. Dazu haben die gemeinsam für die Verarbeitung Verantwortlichen vereinbart, dass die vorhandenen TOM des UKS auch für die UAK übernommen werden.
Die Umsetzung richtet sich damit nach der laufenden Dokumentation der TOM des UKS und wird hier nur referenzierend als Anlage aufgenommen.
Dies bedeutet, dass die UAK in Sachen Daten-Back-Up, Virenschutz und Protokollierung den gleichen Anforderungen und Umsetzungen unterliegt wie das UKS.
Es gilt die jeweils gültige Fassung und Version der TOM des UKS bzw. die ergänzenden IT-Hinweise des UKS.

Bei Abweichungen zu höher notwendigen Anforderungen von Datenschutzgesetzen oder behördlichen Anforderungen werden Empfehlungen vom Datenschutzbeauftragten ausgesprochen. Daraus werden Maßnahmen abgeleitet, mit der UAK durchgesprochen und die Umsetzung begleitet. Die erfolgten Maßnahmen sind zu dokumentieren und es erfolgt eine jährliche Überprüfung.

Unabhängig davon gelten für die UAK folgende spezielle technische Möglichkeiten schon jetzt, ergänzend zu denen des UKS:

Bestimmten Mitgliedern der UAK wird, auf Anforderung, ein vom UKS eingerichteter Laptop bereitgestellt, damit keine private Hardware verwendet werden muss.
Zudem wird jedem Mitglied der UAK ein virtueller Rechner innerhalb des Campus zur Verfügung gestellt, der über die UKS Bestandsinfrastruktur verfügt (AD-Kennung, Mail-Postfach, Netzlaufwerksnutzung, notwendige lokale Software). Um auf den jeweiligen Rechner von außen zu gelangen, wird es Remote-Zugänge auf Basis von Citrix mit Zwei-Faktor-Authentifizierung über Smartphone-PIN geben. Damit ist auch eine sichere Verbindung und die grundsätzlichen Datenschutzvorgaben des UKS berücksichtigt.
Zur Ablage aller Informationen – unabhängig, ob sie von Kliniken und Dezernaten oder den sechs Mitarbeitern selbst abgelegt werden – stellt das UKS einen zentralen Datenspeicher zur Verfügung, der für jeden einzelnen als Netzlaufwerk unter Windows sichtbar ist.
Nach Festlegung involvierter UKS-Fachbereiche erhalten dortige Ansprechpartner Zugriff auf einen „gekapselten“ Teil dieses Zentralspeichers, um im Auftrag ihrer Abteilung dort angeforderte Daten abzulegen (der MA sieht nur die Dokumente, die er selbst abgelegt hat). Zu einem der UAK festgelegten Datum werden diese Zugänge dann für diese Mitarbeiter gesperrt, so dass nur noch die Mitglieder der UAK auf den gesamten Datenpool zugreifen können. Sollte sich im Nachhinein die Notwendigkeit weiterer Datenlieferungen ergeben, lässt sich das auf unterschiedliche Arten leicht lösen.

Für das Arbeiten der UAK wird auf den o.g. virtuellen Rechnern Software wie MS Office und das Recherchetool Lookeen zur Verfügung gestellt.

Auf Basis dieses Konzeptes ergibt sich folgende Zusammenstellung an IT-Komponenten für die Arbeit der UAK-Mitglieder:

- Persönliche Kennungen (beinhaltet Computeranmeldung, E-Mails, Teams, Speicherbereich, CITRIX-Remotezugang mit Zwei-Faktor-Authentifizierung)
- 6 Arbeitsplatz-PCs (als VM, für die Remotearbeit von zu Hause und/oder aus dem Büro Campus SB) mit jeweils folgender Software
    - MS Office (Word, Excel, Outlook)
    - MS Teams für Videokonferenzen inkl. Webcam/Headset
    - Recherchetool Lookeen
- Zentraler Speicherbereich, mit speziellem Zugangskonzept, zur Wahrung der Datentrennung.
- Ein zentrales Backup der Arbeitsumgebung (Laufzeit max. 2 Monate in die Vergangenheit. D.h. wenn nach 3 Monaten ein Datenverlust auffallen würde, wäre kein Backup mehr möglich.)

11. Schriftliche Dokumentation

Die UAK führt ein Verzeichnis aller Verarbeitungstätigkeiten.
Das Verarbeitungsverzeichnis wird regelmäßig auf Vollständigkeit und Aktualität hin geprüft. Es beinhaltet Beschreibungen der Verarbeitungstätigkeiten und muss die gesetzlichen Anforderungen der DSGVO erfüllen:

- Name und Kontaktdaten des Verantwortlichen
- Zwecke der Verarbeitung für jeden Prozess
- Beschreibung der Kategorien betroffener Personen
- Kategorien personenbezogener Daten
- Kategorien der Empfänger
- Drittländer, wohin Daten übertragen werden
- Fristen der Löschung

Die gesetzlich geforderten allgemeinen technischen und organisatorischen Maßnahmen werden nur bei Abweichungen zu den geltenden Sicherheitsmaßnahmen, welche ebenfalls dokumentiert werden, näher beschrieben.
Bei Prozessen, bei denen pbD von Dienstleistern verarbeitet werden, müssen diese Dienstleister ihr Verarbeitungsverzeichnis für diese Prozesse auf Anforderung zur Verfügung stellen.

Daneben werden folgende Punkte in den einzelnen Verarbeitungstätigkeiten geprüft:

- Rechtmäßigkeit der Verarbeitung
- Möglichkeit der Pseudonymisierung und Anonymisierung

Das UKS ergänzt sein Verzeichnis der Verarbeitungstätigkeiten entsprechend. Ein Muster einer Beschreibung einer Verarbeitungstätigkeit befindet sich in Anlage C.

12. Betroffenenrechte

Betroffene können ihre Rechte gegenüber beiden Verantwortlichen geltend machen.

Betroffene haben jederzeit die Möglichkeit Kontakt aufzunehmen, um ihre Betroffenenrechte wahrnehmen zu können. Diese sind das Recht auf Auskunft, das Recht auf Löschung, Einschränkung und Berichtigung sowie das Recht auf Daten-Portabilität.

Dabei stehen folgende Meldewege zur Verfügung:

- E-Mail
- Postalisch
- Telefonisch
- Persönlich

Die Kontaktinformationen stehen öffentlich im Internet zur Verfügung oder (soweit bekannt) wurden den Betroffenen übermittelt. Damit ist eine leichte Erreichbarkeit gegeben.

Authentifizierung: Die betroffene Person muss eindeutig authentifiziert sein. Ungerechtfertigte Betroffenenanfragen durch Scheinidentitäten sind zu verhindern.
Bei nicht schriftlicher Anfrage wird den Betroffenen mitgeteilt, diese Anfrage über den schriftlichen Weg (Mail u/o Webformular) einzureichen.

Bei Erhalt einer Betroffenenanfrage wird dem Betroffenen der Erhalt der Anfrage mitgeteilt. Es wird geprüft, ob die Anfrage beantwortet werden darf bzw. ob die Anfrage umgesetzt werden kann oder ob andere rechtliche Gründe dem entgegenstehen. Bei Bedarf wird der zuständige Datenschutzbeauftragte zusätzlich hinzugezogen. Die eingegangene Betroffenenanfrage wird dann innerhalb von einem Monat fristgerecht beantwortet. Bei negativer Anfrage wird dem Anfragesteller ebenfalls die Information zugestellt, dass dieser die Information nicht erhalten darf oder das seine Anfrage nicht begründet ist.

13. Datenlöschung

Die personenbezogenen Daten werden nach Ablauf der Aufbewahrungsfristen und nach Ende der Zweckbestimmungen umgehend gelöscht. Die Aufbewahrungsfrist beträgt drei Jahre nach Abschluss der Tätigkeit der UAK.
Die Unterlagen, welche die UAK verarbeitet, sind gem. DIN 66399 in Gänze als Daten der Sicherheitsstufe 5 (sensibel / geheim) und höher einzustufen. Diese unterliegen der Schutzklasse 3 und wenn man das Schutzstufenkonzept der Aufsichtsbehörde Niedersachsen hinzuzieht der Schutzstufe D und E (Gefahr der Beeinträchtigung von Ansehen, Gesundheit, Vermögen des Betroffenen).
Somit erfolgt die Vernichtung bei elektronisch verarbeiteten Unterlagen in einem digitalen Verfahren, bei Daten in Papierform durch einen geeigneten Shredder bzw. über eine Datenschutztonne und anschließender Entsorgung durch einen zertifizierten Dienstleister.

14. Prüfung / Bewertung & Verbesserung der datenschutzrechtlichen Umsetzung

Internes Audit

Es erfolgt ggf. ein Audit zur Überprüfung der Umsetzung der Anforderungen der DSGVO. Das Ergebnis dieses Audits wird schriftlich festgehalten und dokumentiert den Status über den Stand des Datenschutzes im Bereich der UAK.
Beim Audit sollten stichprobenartige Kontrollen von Dokumenten und Räumlichkeiten vorgenommen werden. Daneben existiert ein vordefinierter Katalog an Punkten, welche ebenfalls im Zuge des Audits geprüft werden.

Externes Audit

Externe Dienstleister, welche personenbezogene Daten verarbeiten, müssen regelmäßig auf Einhaltung der vertraglich festgelegten Punkte geprüft werden. Diese Überprüfung erfolgt im Laufe bzw. spätestens mit dem Abschluss der Zusammenarbeit und ist zu dokumentieren. Dies kann z.B. durch ein Audit geschehen, oder durch entsprechende eigen erstellte Nachweise des Dienstleisters bspw. Dokumentation / Berichte des eigenen DSB, Zertifikate oder vergleichbare Unterlagen.

Nichtkonformität und Korrekturmaßnahmen

Bei Nichtkonformität mit Gesetzen bei der Verarbeitung von pers. bez. Daten werden diese Prozesse eingestellt. Der Prozess wird geprüft und wenn möglich Korrekturmaßnahmen eingeleitet, um diesen Prozess Datenschutzkonform weiterzuführen.

Fortlaufende Verbesserung

Die getroffenen Maßnahmen müssen regelmäßig auf Ihre Effektivität hin geprüft und bei Bedarf verbessert werden.

15. Webseite

Die UAK wird eine Webseite betreiben, bzw. eine Unterseite des Webauftritts der UKS durch das UKS betreiben lassen.
Wesentliche Inhalte der Webseite werden sein:

- Allgemeine Beschreibung der Aufgabenstellung der UAK und Zielsetzung
- Allgemeine Erreichbarkeit der UAK (Mail, Telefon, Postalisch, Webformular*)
- Erreichbarkeit der telefonischen Betreuung durch das Ärztliches Personal der UAK, incl. die Aufklärung über die Einbindung des Ärztliches Personal der UAK
- Laufende Berichterstattung zum Stand der Aufarbeitung
- Darstellung der Betroffenenrechte
- Abbildung der Informationspflichten der UAK (Art 13/14 DSGVO)
- Darstellung der gemeinsamen Verantwortlichkeit, Art. 26 Abs. 2 S. 2 DSGVO

*: Das Kontaktformular wird so aufgesetzt, dass es einem Betroffenen möglich ist, auch eine pseudonyme Anfrage zu stellen. Das wird dadurch erreicht, dass die Angabe von Namen oder Anschrift oder Mailadresse oder Telefon als freiwillig / optional dargestellt wird.
Zur Sicherstellung der Erreichbarkeit für Rückfragen oder der Beantwortung von Fragen ist jedoch zwingend einer der Kontaktkanäle Mailadresse u/o Telefonnummer zu nennen.
Bereits auf der Webseite sollte Betroffen darauf hingewiesen werden, dass die Kontaktaufnahme durch Sie selbst nur auf freiwilliger Basis in Form einer aufgeklärten Einwilligung erfolgt. Diese Einwilligungen müssen datenschutzkonform erfolgen, dies bedeutet, dass die in Art. 7 DSGVO genannten Punkte eingehalten werden:

- Freiwilligkeit
- Nachweisbarkeit der Einwilligung
- Leicht verständlich
- Möglichkeit des Widerrufs
- Kopplungsverbot

16. Öffentliche Veranstaltungen

Die UAK beabsichtigt eine Auftaktveranstaltung, die der Öffentlichkeit zugänglich sein soll. Die Mitglieder der UAK werden sich bei dieser Auftaktveranstaltung vorstellen und auch die Arbeit der Aufarbeitungskommission darstellen. Eine weitere Verarbeitung von pbD ist bei der Auftaktveranstaltung nicht geplant.

17. Abschlussbericht / Tätigkeitsbericht

In dem von der UAK vorzulegenden Abschlussbericht werden keine auf einzelne Personen beziehbare Daten und Namen wiedergegeben, es sei denn, die Betroffenen sind ausdrücklich damit einverstanden oder der Name einer Person ist im Zusammenhang mit den Missbrauchsverdachtsfällen beim UKS schon öffentlich bekannt.

Anlagen

Anlage A: Absichtserklärung der gemeinsam Verantwortlichen

Zwischen
Dem Universitätsklinikum des Saarlandes
– im Folgenden „Verantwortlicher A“ –
und
Der Unabhängigen Aufarbeitungskommission
– im Folgenden „Verantwortlicher B“ –
Der Verantwortliche A und der Verantwortliche B werden im Folgenden auch einzeln als „Absichtserklärende“ oder gemeinsam als die „Absichtserklärenden“ bezeichnet.

§ 1 Gegenstand der Absichtserklärung
(1) Die Absichtserklärenden schließen diese Vereinbarung (im Folgenden „Absichtserklärung““) zwischen gemeinsam Verantwortlichen im Hinblick auf die Verarbeitung personenbezogener Daten im Rahmen der Erfüllung des Auftrages der Unabhängigen Aufarbeitungskommission mit dem Aufsichtsratsbeschluss vom 26.04.2021 (im Folgenden „Aufsichtsratsbeschluss“). Nachdem die Absichtserklärenden gemeinsam die Zwecke der und die Mittel zu den nachstehend beschriebenen Verarbeitungsvorgängen (im Folgenden „Verarbeitungsvorgänge“) festgelegt haben, betrachten sie sich als gemeinsam für die Verarbeitung Verantwortliche im Sinne von Art. 26 der Datenschutzgrundverordnung (im Folgenden „DS-GVO“).
(2) Zur Klarstellung wird festgehalten, dass hinsichtlich jeglicher Verarbeitungen, die außerhalb des Anwendungsbereichs dieser Absichtserklärung fallen, jede der Absichtserklärenden als Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO allein verantwortlich und voll haftbar bleibt, und dass insoweit keinerlei Verantwortlichkeiten oder Verpflichtungen einer Absichtserklärende gegenüber der jeweils anderen Absichtserklärende bestehen.
(3) Die vorliegende Absichtserklärung enthält die wechselseitigen Verantwortlichkeiten und Verpflichtungen der Absichtserklärenden hinsichtlich der Verarbeitungsvorgänge. Sollten die Bestimmungen dieser Absichtserklärung zu denen des Aufsichtsratsbeschlusses in Widerspruch stehen, gehen die erstgenannten vor, wenn und soweit die Verantwortlichkeiten und Verpflichtungen der Absichtserklärenden hinsichtlich der Verarbeitungsvorgänge betroffen sind. Unbeschadet dessen sind die Absichtserklärenden darüber einig, dass keine der Absichtserklärenden für die Erfüllung ihrer Verantwortlichkeiten im Rahmen dieser Absichtserklärung eine Vergütung verlangen kann, sondern dass derlei Ansprüche vollständig von den Vergütungsvereinbarungen aus dem Aufsichtsratsbeschluss abgedeckt werden.
(4) Soweit in dieser Absichtserklärung nichts Abweichendes bestimmt ist, haben die hierin verwendeten Begriffe die Bedeutung, die ihnen in Art. 4 DS-GVO zugeschrieben wird.

§ 2 Grundsätze für die Verarbeitung und Einzelheiten der Verarbeitungsvorgänge
(1) Die Absichtserklärenden sichern einander zu und gewährleisten, dass sämtliche personenbezogenen Daten in Übereinstimmung mit den Bestimmungen dieser Absichtserklärung und der anwendbaren Datenschutzgesetze erhoben und weiter verarbeitet werden, insbesondere im Einklang mit den in Art. 5 DS-GVO niedergelegten Grundsätzen für die Verarbeitung personenbezogener Daten. Sollte eine der

Absichtserklärenden der Ansicht sein, dass die jeweils andere Absichtserklärende im Rahmen der Ausführung der vorliegenden Absichtserklärung deren Bestimmungen oder die anwendbaren Datenschutzgesetze verletzt, wird sie diese andere Absichtserklärende unverzüglich darüber in Kenntnis setzen.
(2) Im Rahmen der Verarbeitungsvorgänge werden die Absichtserklärenden sämtliche personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format verarbeiten.
(3) Keine der Absichtserklärenden wird Kopien oder Duplikate der unter dieser Absichtserklärung verarbeiteten personenbezogenen Daten anfertigen, wenn dies nicht für die Verarbeitungsvorgänge (einschließlich Daten-Backups) oder zwecks Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich ist.
(4) Die Einzelheiten der Verarbeitungsvorgänge nach dem Muster in Anlage C dargestellt. Diese Einzelheiten enthalten eine umfassende Darstellung von Art, Zweck und Gegenstand der Verarbeitungsvorgänge, die Kategorien der von den Verarbeitungsvorgängen betroffenen Personen und der Art der verarbeiteten personenbezogenen Daten. Zusätzlich werden die Absichtserklärenden in Anlage A jeden Schritt der Verarbeitungsvorgänge beschreiben und dabei festhalten, (a) welche der Absichtserklärenden für welchen dieser Schritte verantwortlich zeichnet und (b) auf welcher Rechtsgrundlage die einzelnen Verarbeitungsvorgänge beruhen.
(5) Wenn dies wegen einer Veränderung der Verarbeitungsvorgänge selbst und/oder aufgrund einer Änderung oder Ergänzung des Aufsichtsratsbeschlusses erforderlich wird, werden die Absichtserklärenden die Festlegungen in Anlage A entsprechend anpassen. Angesichts der Verpflichtungen der Absichtserklärenden als gemeinsam für die Verarbeitung Verantwortliche, ist jede der Absichtserklärenden dafür verantwortlich, die jeweils andere Absichtserklärende darüber zu unterrichten, wenn sie eine Anpassung der Festlegungen in Anlage C für notwendig erachtet. Unbeschadet dessen wird jede der Absichtserklärenden regelmäßig, zumindest aber einmal jährlich, prüfen, ob die Festlegungen in Anlage A die dann aktuellen Verarbeitungsvorgänge widerspiegeln.
(6) Die Absichtserklärenden weisen hiermit dem Verantwortlichen B die Befugnis zu, Entscheidungen hinsichtlich der Verarbeitungsvorgänge mit Wirkung für alle gemeinsam für die Verarbeitung Verantwortlichen umzusetzen. Hierdurch wird der Verantwortliche B für alle Absichtserklärenden im Hinblick auf die Verarbeitungsvorgänge zur Hauptniederlassung in der Europäischen Union. Danach ist die federführende Aufsichtsbehörde hinsichtlich der Verarbeitungsvorgänge die Aufsichtsbehörde das unabhängige Datenschutzzentrum des Saarlandes.

§ 3 Ort der Datenverarbeitung; Übermittlung in Drittländer und das Vereinigte Königreich

(1) Die Absichtserklärenden werden personenbezogene Daten ausschließlich an ihrem eigenen oder dem Sitz ihrer befugten Auftragsverarbeiter verarbeiten. Danach werden sämtliche Verarbeitungsvorgänge grundsätzlich in den Mitgliedsstaaten der Europäischen Union oder in einem anderen Staat ausgeführt, der Absichtserklärende des Vertrags über den Europäischen Wirtschaftsraum ist.
(2) Jede Verarbeitung personenbezogener Daten außerhalb von EU/EWR ist nur bei vorheriger Vereinbarung zwischen den Absichtserklärenden und nur dann zulässig, wenn die Voraussetzungen der Art. 44 ff. DS-GVO eingehalten werden.
(3) Für die Zwecke der vorliegenden Absichtserklärung wird das Vereinigte Königreich von Großbritannien und Nordirland als Drittland betrachtet, um die Risiken eines „Brexits“ zu

vermindern. Aus diesem Grund ist jede Datenverarbeitung im Vereinigten Königreich nur dann erlaubt, wenn angemessene Garantien im Sinne des Art. 46 DS-GVO zur Absicherung vereinbart werden.

§ 4 Rechte der betroffenen Personen

Ist die Arbeit des Verantwortlichen B beendet, wird der Verantwortliche A bezüglich der Betroffenenrechte verantwortlich sein.

(1) Die Absichtserklärenden werden den betroffenen Personen die Informationen gemäß Art. 13, 14 DS-GVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache mitteilen.

(2) Die Absichtserklärenden geben den Verantwortlichen B als Anlaufstelle für die betroffenen Personen an. Die Absichtserklärenden sind sich dabei gleichwohl bewusst, dass die betroffenen Personen desungeachtet ihre Rechte bei und gegenüber jeder der Absichtserklärenden geltend machen können. Aus diesem Grunde hat der Verantwortliche B den Verantwortlichen A unverzüglich über jede Beschwerde, Mitteilung oder Anfrage zu unterrichten, die er direkt von einer betroffenen Person hinsichtlich dessen oder deren personenbezogener Daten erhält, ohne auf jene Anfrage zu antworten. Der Verantwortliche A wird dem Verantwortlichen B die notwendige Unterstützung im Hinblick auf jede Beschwerde, Mitteilung oder Anfrage einer betroffenen Person zuteilwerden lassen.

(3) Der Verantwortliche B wird der betroffenen Person bestätigen, ob sie betreffende personenbezogene Daten im Rahmen der Verarbeitungsvorgänge verarbeitet werden. Soweit dies der Fall ist, wird der Verantwortliche B der betroffenen Person die Informationen gemäß Art. 15 Abs. 1 DS-GVO sowie eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, gemäß Art. 15 Abs. 3 DS-GVO zur Verfügung stellen.

(4) Der Verantwortliche B wird mit der gebotenen Sorgfalt jede Anfrage einer betroffenen Person hinsichtlich (a) der Berichtigung ihrer vermeintlich unrichtigen personenbezogenen Daten, (b) der Löschung ihrer personenbezogenen Daten, (c) der Einschränkung der Verarbeitung ihrer personenbezogenen Daten oder (d) des Rechts dieser betroffenen Person auf Datenportabilität untersuchen. Nach Abschluss der Untersuchung wird der Verantwortliche B entscheiden, ob die Anfrage begründet ist oder nicht, und welche der Absichtserklärenden oder ob beide Absichtserklärenden verpflichtet ist bzw. sind, die personenbezogenen Daten zu berichtigen oder zu löschen, oder ihre Verarbeitung einzuschränken, oder der betroffenen Person das Recht auf Datenportabilität zu gewähren. Der Verantwortliche B wird den Verantwortlichen A entsprechend informieren.

(5) Wenn eine Anfrage betreffend die Löschung personenbezogener Daten begründet ist, oder nach Kündigung oder Auslaufen des Aufsichtsratsbeschlusses werden die Absichtserklärenden die betreffenden oder sämtliche personenbezogenen Daten löschen. Wenn die Datenschutzgesetze, denen eine Absichtserklärende unterliegt, es dieser Absichtserklärende verbieten, sämtliche oder Teile der personenbezogenen Daten zu löschen, muss diese Absichtserklärende garantieren, dass (a) die Vertraulichkeit dieser personenbezogenen Daten gewahrt bleibt, (b) sie die personenbezogenen Daten nicht mehr aktiv verarbeitet und (c) sie diese personenbezogenen Daten löschen wird, sobald die gesetzliche Verpflichtung, die Daten nicht zu löschen, nicht mehr besteht. Jede Absichtserklärende wird ein Protokoll über die Löschung personenbezogener Daten aufsetzen, welches der jeweils anderen Absichtserklärende auf Anfrage bereitzustellen ist.

§ 5 Gemeinsame Zusicherungen der Absichtserklärenden

(1) Die Absichtserklärenden haben bevollmächtigte Vertreter und deren Stellvertreter als alleinige Ansprechpartner für sämtliche Kommunikation betreffend die Verarbeitungsvorgänge bestimmt. Zurzeit sind die folgenden Personen als bevollmächtigter Vertreter und dessen Stellvertreter aufseiten des Verantwortlichen A bestimmt:
Bevollmächtigter Vertreter: der Vorstand des UKS
Aufseiten des Verantwortlichen B sind der bevollmächtigte Vertreter und dessen Stellvertreter:
Bevollmächtigter Vertreter:
Herr Jörg Ziercke
Stellvertreterin:
Frau Dr. Christine Hohmann-Dennhardt
Die Absichtserklärenden werden einander sofort schriftlich über jeden Wechsel in der Person des bevollmächtigten Vertreters oder dessen Stellvertreter unterrichten und einen Ersatz benennen. Bis eine solche Mitteilung die jeweils andere Absichtserklärende erreicht hat, bleiben die benannten Personen berechtigt, Nachrichten der jeweils anderen Absichtserklärende entgegenzunehmen und an diese gerichtete Nachrichten gelten als ordnungsgemäß übermittelt.
(2)Jegliche Kommunikation zwischen den Absichtserklärenden erfolgt in Textform oder schriftlich durch die hierzu nach der vorliegenden Absichtserklärung berechtigten Personen. Mündliche Mitteilungen werden unverzüglich in Textform oder schriftlich bestätigt.
(3) Mitarbeiter beider Absichtserklärenden: (a) die Zugang zu personenbezogenen Daten haben, haben sich einer Verpflichtung zur Vertraulichkeit unterworfen oder unterliegen einer gesetzlichen Geheimhaltungspflicht; (b) dürfen personenbezogene Daten nur nach Weisung der anstellenden Absichtserklärende verarbeiten, wenn nicht eine anderweitige gesetzliche Verpflichtung zur Verarbeitung besteht; und (c) werden regelmäßig, zumindest aber einmal im Jahr, im Hinblick auf die Verpflichtungen der Absichtserklärenden unter der vorliegenden Absichtserklärung , den Datenschutzgesetzen und insbesondere der DS-GVO geschult.
(4) Auf Anfrage werden die Absichtserklärenden einander im Falle von Ermittlungen oder Anfragen einer Aufsichtsbehörde unterstützen, wenn und soweit sich diese Ermittlung oder Anfrage auf die Verarbeitungsvorgänge bezieht. Die Absichtserklärenden unternehmen die erforderlichen Schritte, um jegliche Verpflichtungen im Zusammenhang mit einer solchen Ermittlung oder Anfrage einzuhalten. Unabhängig von einer Unterstützungsanfrage werden die Absichtserklärenden einander in jedem Falle über jegliche derartige Ermittlung oder Anfrage einer Aufsichtsbehörde unterrichten.
(5) Die Absichtserklärenden werden einander unverzüglich, in keinem Fall später als 24 Stunden, nachdem sie eine Verletzung des Schutzes personenbezogener Daten festgestellt haben, hierüber unterrichten. Diese Mitteilung muss die Informationen gemäß Art. 33 Abs. 3 DS-GVO oder, wenn die mitteilende Absichtserklärende nicht in der Lage ist, diese Informationen innerhalb der 24-Stunden-Frist zur Verfügung zu stellen, zumindest eine Erklärung enthalten zu (a) den Gründen für dieses Unvermögen, (b) dem zu erwartenden zusätzlichen Zeitraum bis zur Vervollständigung der Informationen und (c) soweit vorhanden, dem Einfluss dieses Unvermögens auf die ergriffenen Maßnahmen zur Abmilderung der nachteiligen Auswirkungen dieser Verletzung des Schutzes personenbezogener Daten. Sollte eine Absichtserklärende wegen eines Risikos für die

Rechte und Freiheiten natürlicher Personen gesetzlich dazu verpflichtet sein, Informationen bereitzustellen (insbesondere, aber nicht ausschließlich nach Art. 33, 34 DS-GVO), hat die jeweils andere Absichtserklärende die verpflichtete Absichtserklärende nach besten Kräften bei der Erfüllung ihrer Informationspflichten zu unterstützen. Soweit möglich, soll jede Kommunikation mit der zuständigen Aufsichtsbehörde und/oder den betroffenen Personen im Zusammenhang mit einer Verletzung des Schutzes personenbezogener Daten vor ihrer Absendung zwischen den Absichtserklärenden abgestimmt werden.
(6) In Anbetracht der Art der Verarbeitungsvorgänge und unter Berücksichtigung der Bestimmungen des Art. 35 DS-GVO stimmen die Absichtserklärenden darin überein, dass eine Datenschutz-Folgenabschätzung erforderlich könnte. Die Absichtserklärenden werden miteinander kooperieren und sich im Rahmen einer dann notwendigen Datenschutz-Folgenabschätzung und/oder einer vorherigen Konsultation der Aufsichtsbehörde, zu der die Absichtserklärenden nach Art. 36 DS-GVO im Hinblick auf eine solche Datenschutz-Folgenabschätzung gesetzlich verpflichtet sind, unterstützen, wenn künftige Änderungen der Verarbeitungsvorgänge aufzeigen, dass die Verarbeitungsvorgänge voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben.

§ 6 Technische und organisatorische Maßnahmen
(1) Vor Beginn der Verarbeitung haben die Absichtserklärenden die in Anlage B genannten technischen und organisatorischen Maßnahmen umzusetzen und diese während der Laufzeit der vorliegenden Absichtserklärung aufrechtzuerhalten. Hierbei handelt es sich (a) um Maßnahmen zur Sicherstellung der Einhaltung der Rechte der betroffenen Personen und (b) um technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme zu gewährleisten. Dabei müssen der Stand der Technik, die Implementierungskosten und die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen berücksichtigt werden.
(2) Weil die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und technologischen Fortentwicklungen unterliegen, ist es den Absichtserklärenden erlaubt, alternative und angemessene Maßnahmen umzusetzen, wenn hierdurch der Sicherheitsstandard der in Anlage C spezifizierten Maßnahmen nicht unterschritten wird.
(3) Unbeschadet dessen ist eine Absichtserklärende zur Umsetzung weiterer Maßnahmen verpflichtet, wenn sich herausstellt, dass (a) die in Anlage C spezifizierten Maßnahmen angesichts des technischen Fortschritts und technologischer Fortentwicklungen nicht länger angemessen im Sinne des obigen Absatzes 1 sind und/oder (b) ein Audit oder eine Untersuchung durch eine Aufsichtsbehörde ergeben hat, dass die Maßnahmen in Anlage B unzureichend sind.
(4) Jede der Absichtserklärenden wird jegliche Änderungen im vorstehenden Sinne dokumentieren und der jeweils anderen Absichtserklärende eine Kopie der solcherart ergänzten oder aktualisierten technischen und organisatorischen Maßnahmen zur Verfügung stellen.

§ 7 Weitere Verantwortliche; Einschaltung von Auftragsverarbeitern
(1) Die Absichtserklärenden erkennen an, dass keinen weiteren Verantwortlichen durch Beitritt zu dieser Absichtserklärung Zugriff auf die bis zu diesem Zeitpunkt als Teil der

Verarbeitungsvorgänge verarbeiteten personenbezogenen Daten gewährt werden darf. Die Absichtserklärenden sind weiter darüber einig, dass, sofern sie einen weiteren Verantwortlichen in künftige Verarbeitungsvorgänge einbeziehen wollten, dies (a) eine Ergänzungsvereinbarung sowohl zum Aufsichtsratsbeschluss als auch zu dieser Absichtserklärung , (b) eine sorgfältige Durchführung des in § 2 Abs. 5 niedergelegten Prozesses und (c) eine aktualisierte Information an die betroffenen Personen im Sinne des § 4 Abs. 1 erforderlich machen würde.
(2) Eine Absichtserklärende darf nicht ohne vorherige Zustimmung der jeweils anderen Absichtserklärende einen Auftragsverarbeiter hinsichtlich der Verarbeitungsvorgänge einsetzen. Die Absichtserklärenden erteilen einander hiermit die Erlaubnis, die nachstehend benannten Auftragsverarbeiter für die dort jeweils bezeichneten Verarbeitungsvorgänge einzusetzen:
Klicken Sie hier, um Text einzugeben.
(3) Setzt eine Absichtserklärende einen Auftragsverarbeiter ein, muss sie diesem Verpflichtungen zu Datenschutz, Vertraulichkeit und Datensicherheit auferlegen, die (a) den Anforderungen der Art. 28, 29 DS-GVO genügen und (b) zumindest so streng ausfallen wie die in dieser Absichtserklärung niedergelegten. § 3 Abs. 2 und 3 gelten entsprechend.
(4) Eine Absichtserklärende muss der jeweils anderen Absichtserklärende schriftlich mitteilen, wenn sie beabsichtigt einen neuen Auftragsverarbeiter einzusetzen. Wenn die informierte Absichtserklärende der einsetzenden Absichtserklärende innerhalb von 30 Tagen ab Erhalt dieser Mitteilung schriftlich in nachvollziehbarer Weise ihre Ablehnung des vorgeschlagenen Einsatzes mitteilt, werden die Absichtserklärenden nach Treu und Glauben eine beidseits akzeptable Alternativlösung aushandeln.
(5) Erfüllt ein Auftragsverarbeiter seine Verpflichtungen im Hinblick auf die Verarbeitungsvorgänge nicht, so hat die einsetzende Absichtserklärende gegenüber der jeweils anderen Absichtserklärende vollumfänglich für die Einhaltung der Verpflichtungen des Auftragsverarbeiters einzustehen.
(6) Die Absichtserklärenden sind darüber einig, dass die Erbringer von Hilfsleistungen keine Auftragsverarbeiter im Sinne der Datenschutzgesetze sind; dies betrifft insbesondere Transportdienstleistungen von Post- oder Kurierdiensten, Geldtransportleistungen, Telekommunikationsleistungen, Sicherheitsdienste und Reinigungsleistungen. Unbeschadet dessen werden die Absichtserklärenden mit solchen Dienstleistern übliche Vertraulichkeitsvereinbarungen abschließen.

§ 8 Auditrechte

(1) Jede Absichtserklärende hat das Recht, die Einhaltung dieser Absichtserklärung aufseiten der jeweils anderen Absichtserklärende zu überprüfen, wenn dies erforderlich ist, um (a) einer Verpflichtung gegenüber einer Aufsichtsbehörde ordnungsgemäß nachzukommen oder (b) sich selbst davon zu überzeugen, dass die jeweils andere Absichtserklärende nach einem Datenschutzvorfall ihre Abläufe an die Bestimmungen dieser Absichtserklärung angepasst hat.
(2) Wenn und soweit eine solche Überprüfung Vor-Ort-Inspektionen erfordert, sollen diese gewöhnlich während der üblichen Geschäftszeiten und ohne unnötige Störungen des Betriebsablaufs stattfinden. Die Absichtserklärende, die eine Überprüfung durchführt, wird die jeweils andere Absichtserklärende mit einer angemessenen Frist im Vorwege über sämtliche mit der Überprüfung verbundenen Umstände unterrichten.
(3) Eine Absichtserklärende darf einen Dritten mit der Durchführung der Überprüfung beauftragen. In einem solchen Fall ist der Dritte schriftlich auf die strikte Wahrung von

Geheimhaltung und Vertraulichkeit zu verpflichten, wenn nicht der Dritte einer beruflichen Verschwiegenheitsflicht unterliegt.

§9 Anordnungsklarstellung
Die Absichtserklärenden erklären, einer durchsetzbaren oder vollziehbaren Anordnung der Aufsichtsbehörde ordnungsgemäß nachzukommen und die vertretungsberechtigten Personen der Absichtserklärenden und Ihre für den kritischen Verarbeitungsvorgang verantwortlichen Personen auf die Umsetzung der Anordnung zu verpflichten.

§ 10 Sonstige Bestimmungen

(1) Änderungen oder Ergänzungen der vorliegenden Absichtserklärung sind nur wirksam, wenn sie schriftlich abgefasst wurden.
(3) Wenn eine Bestimmung dieser Absichtserklärung von dem zuständigen Gericht für unwirksam oder nicht durchsetzbar erklärt wird, bleiben die übrigen Bestimmungen uneingeschränkt wirksam.
(4) Diese Absichtserklärung tritt mit Unterschrift der Absichtserklärenden in Kraft. Sie gilt, ungeachtet des Endes des Tätigkeitszeitraumes der UAK solange bis sämtliche personenbezogenen Daten von den Absichtserklärenden und/oder sämtlichen eingesetzten Auftragsverarbeitern gelöscht worden sind und tritt sodann automatisch außer Kraft.

Die Absichtserklärenden haben diese Absichtserklärung durch ordnungsgemäß bevollmächtigte Vertreter an dem unten angegebenen Datum abgeschlossen.
Klicken Sie hier, um Text einzugeben
(Ort, Datum)
Klicken Sie hier, um Text einzugeben

Anlage B: Technische und organisatorische Maßnahmen des UKS

Zum Zeitpunkt der Niederlegung dieses Datenschutzkonzeptes gelten die folgend TOM:

Technische und Organisatorische Maßnahmen (TOMs) nach DS-GVO / BDSG neu

In diesem Dokument sind die technischen und organisatorischen Maßnahmen (TOMs) des Universitätsklinikums des Saarlandes (UKS) dokumentiert, die zur Gewährleistung von Datenschutz und Datensicherheit getroffen worden sind.

1. Vertraulichkeit (Art 32 Abs. 1 lit. B DSGVO)

1.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen

- Für die Serverräume
  - Manuelles Schließsystem
  - Türen mit Knauf an der Außenseite
  - Automatisches Zugangskontrollsystem
  - Chipkartensystem
  - Alarmanlage
- Für das Zentrum für Informations- und Kommunikationstechnik (ZIK)
  - Manuelles Schließsystem
  - Automatisches Zugangskontrollsystem
  - Chipkartensystem
  - Alarmanlage
- Für die Kliniken und die Verwaltung
  - Manuelles Schließsystem
  - Z.T. automatisches Zugangskontrollsystem (z.B. Labore)

Organisatorische Maßnahmen

- Dokumentierte Schlüsselvergabe
- Mitarbeiter / Besucherausweise
- Besucher nur in Begleitung durch Mitarbeiter in sensiblen Bereichen
- Rücknahme von Zugangsmitteln nach Ablauf der Berechtigung
- Sorgfalt bei Auswahl des Reinigungsdienstes (Tochterunternehmen)

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Technische Maßnahmen

- BIOS-Schutz (separates Passwort)
- Login mit Benutzername und Passwort
- Verschlüsselung von Festplatten in PCs und Notebooks
- Verschlüsselung von mobilen Datenträgern
- Automatische Desktopsperre
- Einsatz von Firewalls

- Einsatz und regelmäßige Aktualisierung zentraler und dezentraler Virenschutz-Programmen
- Einsatz von Spam-Filtern
- Einsatz von VPN oder Citrix bei Remote-Zugriffen
- 2-Faktor Authentifizierung bei Remotezugriffen

Organisatorische Maßnahmen

- Erstellen von Benutzerprofilen
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Passwortrichtlinie
- Umgehende Sperrung von Berechtigungen beim Ausscheiden von Mitarbeitern

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Technische Maßnahmen

- Datenschutztonne für Papierabfälle
- Aktenschredder (mindestens Stufe 3)
- Physische Löschung von Datenträgern vor Wiederverwendung
- Externe datenschutzkonforme Entsorger für Papier und Datenträger
- Protokollierung von Zugriffen auf Anwendungen und Daten

Organisatorische Maßnahmen

- Rollen und Berechtigungskonzept
- Festgelegte Abläufe zur Genehmigungserteilung, Kontrolle und Entzug von Berechtigungen
- Restriktive Vergabe von Administrator-Berechtigungen
- Datenschutztresor

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Technische Maßnahmen

- Trennung von Produktiv-, Test- und Entwicklungssystem
- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Logisch Mandantentrennung (softwareseitig)

Organisatorische Maßnahmen

- Umfangreiches Berechtigungskonzept

2. Pseudonymisierung und Verschlüsselung (Art 32 Abs. 1 lit. a DSGVO)

Maßnahmen zur Pseudonymisierung und Verschlüsselung der personenbezogenen Daten.

Technische Maßnahmen

- Anzeige von Anfangsbuchstaben von Patienten zur Info von Angehörigen in der Notaufnahme
- Manuelle Verschlüsselung sensibler Daten in einzelnen Diensten

Organisatorische Maßnahmen

- Pseudonymisierung bzw. Anonymisierung klinischer Daten zur Nutzung in der Forschung

3. Integrität (Art 32 Abs. 1 lit. b DSGVO)

3.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen

- Einsatz von VPN für Remotezugänge bzw. Site-to-Site-Tunneln
- Verschlüsselte Datenübertragung beim Mailversand und im Web
- Sichere Behälter beim Transport von Akten in das Scanzentrum

Organisatorische Maßnahmen

- Verbot der unverschlüsselten E-Mail-Nutzung für personenbezogene Daten
- Dokumentation der Empfänger von Daten

3.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Technische Maßnahmen

- Protokollierung der Eingabe, Änderung und Löschung von Daten

Organisatorische Maßnahmen

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung durch überwiegend individuelle Benutzernamen

4. Verfügbarkeit und Belastbarkeit (Art 32 Abs. 1 lit. b und c DSGVO)

4.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, einschließlich Maßnahmen zur Wiederherstellung bei physischen oder technischen Zwischenfällen.

Technische Maßnahmen

- Unterbrechungsfreie Stromversorgung (USV)
- Notstromversorgung über Dieselaggregate
- Feuer- und Rauchmeldeanlagen
- Brandfrühsterkennung und Löschsystem in den Serverräumen
- Klimatisierung von Server- und Verteilerräumen
- Überwachung von Temperatur und Feuchtigkeit in den Serverräumen
- Synchrone Datenspiegelung in zwei Serverräumen
- Virtuelle Servercluster über zwei Serverräumen
- RAID-Systeme
- Alarmmeldung bei unberechtigtem Zutritt zu Serverräumen
- Einsatz von Firewalls und Virenscannern

- Patchmanagement

Organisatorische Maßnahmen

- Backup & Recovery-Konzept
- Zentrale Datenhaltung mit regelmäßiger Datensicherung
- Aufbewahrung von Datensicherung an zwei getrennten Orten
- Kontrolle der Sicherungsvorgänge
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Bestehe eines Notfallplans

5. Verfahren zur regelmäßigen Überprüfung und Evaluierung (Art 32 Abs. 1 lit. d DSGVO)

5.1 Datenschutz-Management

Sonstige Maßnahmen, vor allem organisatorische Maßnahmen zum Schutz personenbezogener Daten.

Technische Maßnahmen

- Portale für Verfahrensbeschreibungen und Dokumente im Bereich Informationssicherheit

Organisatorische Maßnahmen

- Interne Datenschutzbeauftragte (DSB)
- Interner Beauftragter für Informationssicherheit (ISB)
- Etablierung eines Informationssicherheitsmanagementsystems (ISMS)
- Regelmäßige Schulung der Mitarbeiter zum Datenschutz und zur IT-Sicherheit
- Regelmäßige Sensibilisierung der Mitarbeiter durch E-Mails und bei gemeinsamen Begehungen des Datenschutzes und der Informationssicherheit
- Datenschutz-Folgeabschätzung (DSFA) für kritische Systeme
- Regelmäßige interne und externe Penetrationstests
- KRITIS-Audit alle zwei Jahre

5.2 Incidet-Respond-Management

Sonstige Maßnahmen zum Umgang mit Datenschutzzwischenfällen.

Technische Maßnahmen

- Einsatz von Firewalls mit regelmäßiger Aktualisierung
- Einsatz von Spamfiltern mit regelmäßiger Aktualisierung
- Einsatz von Virenscannern mit regelmäßiger Aktualisierung
- IDS?

Organisatorische Maßnahmen

- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Einbindung von DSB und ISB bei Sicherheitsvorfällen und Datenpannen
- Dokumentation von Sicherheitsvorfällen und Datenpannen im Ticketsystem und bei schweren Vorfällen in umfangreicher Textform

5.3 Datenschutzfreundliche Voreinstellungen

Maßnahmen, die gewährleisten, dass Voreinstellungen den Interessen der Betroffenen gerecht werden (privacy by default).

Technische Maßnahmen

- Einfache Ausübung des Wiederrufrechts des Betroffenen durch technische Maßnahmen

Organisatorische Maßnahmen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Umsetzung datenschutzfreundlicher Voreinstellungen

5.4 Auftragskontrolle (Outsourcing an Dritte)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Technische Maßnahmen

-

Organisatorische Maßnahmen

- Auswahl des Auftragnehmers unter Datenschutz- und Datensicherheitsaspekten
- Abschluss eines Auftragsverarbeitungsvertrages
    - Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
    - Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer
    - Schriftliche Weisungen an den Auftragnehmer
    - Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
    - Regelung zum Einsatz von Subunternehmern
    - Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Vorabkontrolle des Auftragsverarbeiters, insbesondere vorherige Prüfung der Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen

Anlage C: Muster für ein Verzeichnis der Verarbeitungstätigkeiten/ Beschreibung einer Verarbeitungstätigkeit

2 Angaben zur Verarbeitungstätigkeit

2.1 Organisatorische Angaben

2.1.1 Ansprechpartner / Verfahrensverantwortliche

Vollständiger Name (n)	
Klinik/Organisationseinheit	
Straße Hausnummer	
PLZ / Ort	
Telefon	
Telefax	
E-Mail-Adresse	
Internet-Adresse	

2.1.2 Zeitangaben

Datum der Einführung	
Datum der Erstbeschreibung	
Datum der letzten Änderung	

2.2 Zweck der Verarbeitung

2.2.1 Bezeichnung des Verfahrens

2.2.2 Zweckbestimmung

2.3 Rechtsgrundlage

2.3.1 Verarbeitung von Daten, die nicht zu besonderen Kategorien gemäß Art. 9 Abs. 1 DS-GVO zählen (Art. 6 DS-GVO)

Bitte ankreuzen	**Rechtsgrundlage DS-GVO**
	Einwilligung (Art. 6 Abs. 1 lit. a)
	Zur Vertragserfüllung notwendig (Art. 6 Abs. 1 lit. b)
	Zur Erfüllung einer rechtlichen Verpflichtung, welcher der Verantwortliche unterliegt, erforderlich (Art. 6 Abs. 1 Lit c)
	Erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 6 Abs. 1 lit. d)
	Verarbeitung liegt im öffentlichen Interesse oder erfolgt in Ausübung öffentlicher Gewalt (Art. 6 Abs. 1 lit. e)
	Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen nicht (Art. 6 Abs. 1 lit. f)

2.3.2 Verarbeitung besondere Kategorien personenbezogener Daten (Art. 9 DS-GVO)

Bitte ankreuzen	Rechtsgrundlage DS-GVO	Ergänzende national-gesetzliche Regelung
	Einwilligung (Art. 9 Abs. 2 lit. a)	
	Patientenbehandlung (Art. 9 Abs. 2 lit. h)	
	Weitergabe von Daten an Mit-/ Nachbehandler (Art. 9 Abs. 2 lit. h)	
	Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben Art. 9 Abs. 2 lit. c)	
	Abrechnung von Leistungen (Art. 9 Abs. 2 lit. f)	
	Qualitätssicherung der Patientenversorgung (Art. 9 Abs. 2 Lit i)	
	Gesetzlich geregelte Krankheitsregister (Art. 9. Abs. 2 lit. h)	
	Gesundheitsstatistik des Bundes und der Länder (Art. 9 Abs. 2 lit. j in Verbindung mit Art. 89 Abs. 1)	
	Arbeitsmedizinische Untersuchung (Art. 9 Abs. 2 Lit h in Verbindung mit Art. 9. Abs. 3)	
	Untersuchung durch Gesundheitsamt (Art. 9. Abs. 2 Lit i)	
	Impfungen in Schule usw. durch Ämter (Art. 9. Abs. 2 Lit i)	
	Verteidigung der behandelnden Person vor Gericht (Art. 9 Abs. 2. lit. f)	
	Wissenschaftliche u. historische Forschung (Art. 9 Abs. 2 lit. j in Verbindung mit Art. 89 Abs. 1)	
	Gesetzlich vorgeschriebene Archivierung zu hist. Zwecken (Art. 9 Abs. 2 lit. j in Verbindung mit Art. 89 Abs. 1)	
	Verarbeitung von seitens der betroffenen Person öffentlich zugänglich gemachten Daten (Art. 9 Abs. 2 lit. e)	

2.4 Beschreibungen der Kategorien betroffener Personen und der Kategorien personenbezogener Daten

2.4.1 Beschreibung der Kategorien betroffener Personen

Kategorien betroffener Personen	Beschreibung
Patienten	
Mitarbeiter, Angestellte, Rentner, Bewerber, Auszubildende, Praktikanten, gewerbliche Mitarbeiter	
Lieferanten sowie andere Geschäftspartner, sofern diese zur Erfüllung der in Abschnitt 2.2.2 genannten Zwecke erforderlich sind	
Kunden, Mitarbeiter von Kunden	

2.4.2 Beschreibung der Kategorien personenbezogener Daten

Kategorien personenbezogener Daten	Beschreibung
Daten der Patientenbehandlung	
Angaben zur Person (des Betroffenen)	
Mitarbeiter als Anwender der Software	

2.5 Kategorien von Empfängern

2.5.1 Interne Empfänger

Empfänger	**Rechtsgrundlage**

2.5.2 Externe Empfänger

Empfänger	**Rechtsgrundlage**

2.6 Übermittlungen an ein Drittland oder an eine internationale Organisation

Name des Drittstaates	
Empfänger oder Kategorien von Empfängern	
Art der Daten oder Datenkategorien	
Rechtsgrundlage	
Angabe der geeigneten Garantien	

2.7 Fristen für die Löschung

Kategorien personenbezogener Daten	**Löschfristen**

2.8 Getroffene technische und organisatorische Maßnahmen gemäß Art. 32 Abs. 1 DS-GVO (hier kann auf die TOMs des ZIK verwiesen werden, Abweichungen müssen jedoch beschrieben werden)

2.8.1 Pseudonymisierung personenbezogener Daten

Kategorien betroffener Personen	**Verfahrensbeschreibung**

2.8.2 Verschlüsselung personenbezogener Daten

Kategorien betroffener Personen	**Verfahrensbeschreibung**

2.8.3 Sicherstellung von Verfügbarkeit

Kategorien betroffener Personen	**Verfahrensbeschreibung**

2.8.4 Beschreibung des Verfahrens zur Gewährleistung um den Zugang zu personenbezogenen Daten bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Kategorien betroffener Personen	**Verfahrensbeschreibung**

2.8.5 Sicherstellung von Integrität

Kategorien betroffener Personen	**Verfahrensbeschreibung**

2.8.6 Sicherstellung von Vertraulichkeit

Kategorien betroffener Personen	**Verfahrensbeschreibung**

Anlage D: Muster für die „Meldung einer Datenpanne“

Meldung einer Datenpanne
Art. 33 der Datenschutzgrundverordnung schreibt eine Meldung im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden, nachdem die Verletzung bekannt wurde an die zuständige Aufsichtsbehörde vor, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Um das zu beurteilen benötigt die UAK und das UKS Ihre Unterstützung. Bitte melden Sie gleich, wenn Sie eine Datenpanne bemerken und füllen Sie diese Fragen aus und geben es an den Datenschutzbeauftragten weiter. Die UAK und das UKS müssen - falls eine Meldung erforderlich sein sollte - die Meldefrist von 72 Stunden einhalten!

- Verantwortlicher (Firma und Anschrift):
- Abteilung / Fachbereich:
- Wer meldet: Name, Vorname
- Telefon für Rückfragen
- Was ist passiert (kurze Beschreibung mit Details):
- Zeitraum bzw. Zeitpunkt des Vorfalls:
- Wann wurde es festgestellt:
- Welche Datenkategorien sind betroffen. Bitte hier aufzählen:

Um welche Verletzung des Schutzes personenbezogener Daten handelt es sich?
Eine Verletzung der Sicherheit, die zu folgendem führt:

☐ Vernichtung von pbD unbeabsichtigte oder unrechtmäßige

☐ Verlust von pbD unbeabsichtigte oder unrechtmäßige

☐ Veränderung pbD unbeabsichtigte oder unrechtmäßige

☐ Offenlegung unbefugt

☐ Zugang unbefugt

(Art. 4 Nr. 12 DSGVO - Verletzung des Schutzes personenbezogener Daten - eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden).

- Anzahl der betroffenen Personen, deren Rechte verletzt wurden:
- Mit welchen Folgen / Risiken muss aus Sicht der betroffenen Personen gerechnet werden:
- Welche technischen und organisatorischen Maßnahmen bestanden:

- Welche zusätzlichen technischen und organisatorischen Maßnahmen wurden getroffen:
- Wurden die Betroffenen benachrichtigt:
- Wenn ja, wann und durch wen:

Vielen Dank für Ihre Unterstützung.

Die UAK, das UKS & der Datenschutzbeauftragte

Anlage E: Muster Informationspflicht Kontaktaufnahme zur UAK über Webseite

Informationspflicht und Hinweise zum Datenschutz UAK / UKS

Für die durch uns verarbeiteten personenbezogenen Daten (Kontaktformular) erteilen wir gem. Art. 13 und 14 DSGVO den Betroffenen folgende Informationen:

Verarbeitende Stelle		**UAK & UKS**
Vertreter des Verantwortlichen		Für die UAK: der Vorsitzende der UAK Für die UKS: der Vorstand - siehe Impressum
Datenschutzbeauftragter		Ass. jur. Klara Dauber Datenschutzbeauftragte Datenschutz@uks.eu
Verarbeitungszwecke		Registrierung von Betroffenen zur Kontaktaufnahme.
Rechtsgrundlagen		Die Verarbeitung erfolgt auf Basis einer Einwilligung durch die betroffene Person gem. Art 6 Abs. 1 lit. a DSGVO.
Berechtigtes Interesse		Eine Erhebung der Daten erfolgt nicht auf Basis eines berechtigten Interesses.
Empfänger der Daten		Die erhobenen Daten werden ausschließlich bei der UAK gespeichert und nur für die Aufarbeitung der Missbrauchsverdachtsfälle verwendet.
Übermittlung der Daten in Drittstaaten		Eine Weitergabe der erhobenen personenbezogenen Daten in Drittstaaten oder internationale Organisationen findet nicht statt.
Dauer der Speicherung		Die Verarbeitung der Daten erfolgt für die Dauer der Einsetzung der UAK und werden nach Abschluss der Aufarbeitung nach drei Jahren gelöscht.
Betroffenenrechte		Betroffene haben das Recht auf Auskunft, Löschen, Sperren ihrer personenbezogenen Daten, sowie das Recht der Einschränkung der Verarbeitung und das Widerspruchsrecht. Zur Wahrung Ihrer o.a. Betroffenenrechte wenden sie sich bitte schriftlich (postalisch oder E-Mail) an die o.a. verarbeitende Stelle.
Beschwerderecht bei der Aufsichtsbehörde		Ergänzend steht Ihnen das Recht auf Beschwerde zu. Solche richten Sie bitte an die zuständige Datenschutzbehörde: *Unabhängiges Datenschutzzentrum Saarland* *Fritz-Dobisch-Str. 12* *66111 Saarbrücken* Tel. 0681 94781-0 Fax 0681 94781-2 poststelle@datenschutz.saarland.de
Widerrufbarkeit von Einwilligungen		Sie haben das Recht Ihre Einwilligung mit Wirkung für die Zukunft zu widerrufen. Diese senden Sie bitte schriftlich (postalisch oder E-Mail) an die o.a. verarbeitende Stelle.
Automatisierte Entscheidungsfindung und Profiling		Mit den erhobenen personenbezogenen Daten wird keine automatisierte Entscheidungsfindung betrieben, noch werden die Daten zu einer Profilbildung herangezogen oder genutzt.
Weiterverarbeitung der Daten zu anderen als den ursprünglichen Zwecken.		Aktuell ist eine Verarbeitung / Verwendung zu anderen als den o.a. Zwecken nicht beabsichtigt. Werden weitere Zwecke erkannt und sollen diese genutzt werden, so wird sich die verarbeitende Stelle mit dem Betroffenen in Verbindung setzen und zu diesen weiteren Zwecken aufklären und ggf. ergänzende Einwilligungen einholen.

Stand 16.09.2021

Anlage F: Muster Webformular – Kontaktaufnahme zur UAK

Anmerkung: Auf der Webseite wird der Betroffene um seine Einwilligung in die Verarbeitung seiner personenbezogenen Daten gebeten, Art. 6 Abs. 1 lit. a DSGVO. Die Einwilligungserklärung erfolgt mit dem Hinweis des Widerrufes, siehe Ausführungen zur Webseite, Punkt 14.

Vielen Dank für Ihr Interesse an der Tätigkeit der Unabhängigen Aufarbeitungs- Kommission / UAK.

Wir freuen uns, dass Sie mit uns Kontakt aufnehmen wollen und sich persönlich oder institutionell an der Aufarbeitung der Vorfälle im Zusammenhang mit den Missbrauchsverdachtsfällen am UKS beteiligen.

Nutzen Sie dafür das untenstehende Formular oder kontaktieren Sie uns telefonisch unter +49 (0) 68xxx xxxx – xx oder unser Ärztliches Personal der UAK/ unter +49 (0) 68xxx xxxx.

Sie können auch jederzeit ein Gespräch mit uns vereinbaren – dieses werden vertraulich behandelt.

Um einen Kontakt herstellen zu können ist mindestens die Mitteilung/Nennung eines Kontakt-Kanals (E-Mail oder Telefon) erforderlich.

Vorname:	Nachname:
_____	_____
E-Mail:	Telefon:
_____@_____	_____
Ihr Kennwort:	
_____	
Ihre Nachricht:	
_____ …	
Die obigen Angaben erfolgen freiwillig. *Sofern Sie möchten, dass wir Kontakt zu Ihnen aufnehmen ist jedoch die Angabe mindestens eines Kontaktkanals erforderlich.*	