DIE SPITÄLER DER SCHWEIZ
LES HÔPITAUX DE SUISSE
GLI OSPEDALI SVIZZERI

Leitfaden und Checklisten

Anwendung EU-Datenschutzgesetzgebung auf Spitäler[1] mit Sitz in der Schweiz

Inhaltsverzeichnis

[1] Der Begriff Spitäler wird im vorliegenden Leitfaden als Sammelbegriff für jede Art von Spitälern, Kliniken und vergleichbaren Institutionen verwendet.

Geschäftsstelle · Lorrainestrasse 4A · 3013 Bern
T 031 335 11 11 · F 031 335 11 70
geschaeftsstelle@hplus.ch · www.hplus.ch

Dieser Leitfaden enthält eine allgemeine Darstellung zur Anwendung der EU-Datenschutz-gesetzgebung auf Spitäler mit Sitz in der Schweiz. Er erhebt keinen Anspruch auf Vollständigkeit und vermag eine auf den Einzelfall bezogene vertiefte Analyse nicht zu ersetzen. Dessen Anwendung erfolgt auf eigenes Risiko. Bei Unsicherheit empfiehlt sich die Beiziehung eines Datenschutzspezialisten bzw. einer Datenschutzspezialistin.

Vorgehenshinweise: Lesen Sie den Leitfaden sorgfältig durch und beantworten Sie anschliessend unter Einbezug der Ausführungen im Leitfaden die Fragen in den Checklisten auf Seiten 10 und 11. Der Leitfaden ist so aufgebaut, dass er die Voraussetzungen für eine Anwendung der EU-Daten-schutzgesetzgebung zuerst allgemein erklärt und anschliessend spezielle Ausführungen mit Blick auf die Spitäler macht.

Literatur und Materialien:
- EHMANN EUGEN/SELMAYR MARTIN (Hrsg.), DS-GVO, Datenschutzrundverordnung, Kommentar, München 2017.
- KÜHLING JÜRGEN/BUCHNER BENEDIKT (Hrsg.), Datenschutz-Grundverordnung, Kommentar, München 2017.
- PETER CHRISTIAN, DSGVO und E-DSG fordern Schweizer Spitäler, Praxen, Heime und Spitex in: Jusletter 26. Februar 2018
- Einführungserwägungen zur Datenschutzgrundverordnung (siehe Kapitel 2).

1 Ausgangslage

Am 25. Mai 2018 wird die neue EU-Datenschutzgesetzgebung in Kraft treten. Diese gilt in erster Linie für Datenverarbeitungen innerhalb der EU. Jedoch enthält sie Normen, die dazu führen, dass auch Datenverarbeitungen durch Institutionen, die ihren Sitz ausserhalb der EU haben (z.B. in der Schweiz), unter die EU-Datenschutzgesetzgebung fallen können. Fällt eine Datenverarbeitung in den Anwendungsbereich der EU-Datenschutzgesetzgebung, spielt es keine Rolle, ob diese durch eine natürliche oder juristische Person oder durch Behörden jeglicher Hierarchiestufen erfolgt (in der Schweiz Bund, Kantone oder Gemeinden). Die EU-Datenschutzgesetzgebung ist in diesem Fall stets anwendbar.

Ist die EU-Datenschutzgesetzgebung anwendbar, sieht sie für bestimmte Fälle eine Pflicht vor, in der EU eine Vertretung zu benennen. Diese Pflicht gilt allerdings nur für natürliche und juristische Personen; Behörden und öffentliche Stellen sind davon ausgenommen.
Fällt eine Datenverarbeitung unter die EU-Datenschutzgesetzgebung, gilt es zu beachten, dass bei unrechtmässigen Datenverarbeitungen, bei Nichtbefolgung der Anweisung einer EU-Datenschutzaufsichtsbehörde oder bei Nichtbeachtung der Pflicht, in der EU eine Vertretung zu bestellen, hohe Geldbussen drohen können. Je nach Verstoss betragen diese bis zu EUR 10 oder EUR 20 Mio. bzw. bei Unternehmen bis zu 2 bzw. 4% des gesamten weltweit erzielten Jahresumsatzes des vergangenen Geschäftsjahres – je nachdem, welcher Betrag höher ist.

2 Neue EU-Datenschutzgesetzgebung

Die neue EU-Datenschutzgesetzgebung umfasst verschiedene Erlasse. Von übergeordneter Bedeutung sind insbesondere die folgenden zwei Verordnungen:

- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. L 119/1 vom 4.5.2016

  ⇨ diese Verordnung wird in der Regel mit DSGVO oder EU-DSGVO abgekürzt.

- Vorschlag für eine Verordnung des europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation (Verordnung über Privatsphäre und elektronische Kommunikation), [COM(2017) 10 final]

  ⇨ bei dieser Verordnung liegt die definitive Version noch nicht vor.

Obwohl bei der EU-Verordnung über Privatsphäre und elektronische Kommunikation die definitive Version noch nicht vorliegt, ist zurzeit davon auszugehen, dass diese zusammen mit der DSGVO am **25. Mai 2018 in Kraft treten** und ab diesem Zeitpunkt unmittelbar gelten wird.

3 Anwendungsvoraussetzungen

Damit die EU-Datenschutzgesetzgebung auf Institutionen mit Sitz ausserhalb der EU - und damit auch in der Schweiz - Anwendung findet, müssen mehrere Voraussetzungen erfüllt sein. Die nachfolgenden Ausführungen zeigen, um welche Voraussetzungen es sich handelt und wie sich diese prüfen lassen.

3.1 Verarbeitung personenbezogener Daten

Rechtsgrundlagen:
- Art. 1 Abs. 1 i.V. m. Art. 2 Abs. 1 und Art. 4 Ziff. 1, 2, 4 DSGVO
- Einführungserwägungen DSGVO, Ziff. 14 und 26

Eine Voraussetzung, die für eine Anwendung der EU-Datenschutzgesetzgebung stets erfüllt sein muss, ist das Vorliegen einer **(1) Verarbeitung (2) personenbezogener Daten (3) über natürliche Personen**.

(1) Verarbeitung: Der Begriff «Verarbeiten» ist sehr weit gefasst und umfasst praktisch jeden Umgang mit personenbezogenen Daten – z.B. das Erheben, Erfassen, Ordnen, Speichern, Verändern, Abfragen, Verwenden, die Bekanntgabe, die Verknüpfung oder das Löschen von personenbezogenen Daten. Ob die Verarbeitung automatisiert oder in anderer Weise erfolgt, spielt keine Rolle. Ebenfalls eine Form der Verarbeitung stellt das «Profiling» dar. Beim «Profiling» werden personenbezogene Daten automatisiert verarbeitet, wobei das Ziel darin besteht, bestimmte persönliche Aspekte der Person, über die Daten bearbeitet werden, wie z.B. die Gesundheit, die Arbeitsleistung, den Aufenthaltsort, die persönlichen Vorlieben oder die wirtschaftlichen Verhältnisse zu analysieren oder vorauszusagen.

(2) Personenbezogene Daten: Als (2.1) personenbezogene Daten gelten alle Informationen, die sich auf eine (2.2) identifizierte oder identifizierbare (2.3) natürliche Person beziehen.

(2.1) Der **Begriff der personenbezogenen Daten** ist weit zu verstehen und umfasst alle Informationen, die Inhalte aufweisen, die sich auf eine natürliche Person beziehen. Die EU-Datenschutzgesetzgebung unterscheidet folgende zwei Arten personenbezogener Daten:

- ***normale personenbezogene Daten*** - z.B. Name, Anschrift, Geburtsdatum, Telefonnummer
  ⇨ die Verarbeitung dieser Art personenbezogener Daten ist aus datenschutzrechtlicher Sicht in der Regel bedingt heikel.
- ***besondere Kategorien personenbezogener Daten*** – z.B. Gesundheitsdaten, Daten aus denen sich die rassische und ethnische Herkunft, die politische Meinung, die religiöse Gesinnung, die sexuelle Orientierung oder die Zugehörigkeit zu einer Gewerkschaft ergeben. Ebenfalls darunter fallen genetische und biometrische Daten, sofern diese zur eindeutigen

Identifizierung einer natürlichen Person dienen ⇨ die Verarbeitung dieser personenbezogenen Daten ist in der Regel heikel bis sehr heikel. Entsprechend sind bei deren Verarbeitung stets hohe bis sehr hohe Datenschutzanforderungen zu beachten.

(2.2) **Identifiziert und identifizierbar:** Eine Person ist identifiziert oder identifizierbar:

- ***identifiziert*** ist eine Person, wenn sich ihre Identität unmittelbar aus den Daten selbst ergibt z.B. aus Ausweispapieren.
- ***identifizierbar*** ist eine Person, wenn sich ihre Identität aus dem Kontext der Daten oder durch Kombination mit weiteren Daten ergibt - z.B. die Zuordnung der Person zu einer Kennzeichnung wie einem Namen, einer Kennnummer, zu Standortdaten, zu einer IP-Adresse oder aber zu einem oder mehreren besonderen Merkmalen, die sich aus der physischen, genetischen, wirtschaftlichen, kulturellen oder sozialen Identität der Person ergeben.

(3) Natürliche Person: = jeder Mensch als Träger von Rechten und Pflichten. Das Gegenteil sind juristische Personen im Sinne von Personenvereinigungen wie z.B. ein Verein, eine Aktiengesellschaft, eine GmbH oder eine öffentlich-rechtliche Anstalt. Die EU-Datenschutzgesetzgebung erfasst nur die Verarbeitung personenbezogener Daten über natürliche Personen. Eine Ausnahme findet sich allerdings für das Anbieten und Nutzen von Kommunikationsdiensten. In deren Rahmen erfasst die EU-Datenschutzgesetzgebung auch die Verarbeitung personenbezogener Daten über juristische Personen.

Fokus Spitäler:
Spitäler verarbeiten regelmässig besondere Kategorien personenbezogener Daten in Form von Gesundheitsdaten. Entsprechend gelten für sie erhöhte Datenschutzanforderungen. Damit erfüllen sie die erste Voraussetzung für die Anwendbarkeit der EU-Datenschutzgesetzgebung «die Verarbeitung personenbezogener Daten» stets.

3.2 Weitere Voraussetzungen

Damit die EU-Datenschutzgesetzgebung auf eine Institution mit Sitz in der Schweiz Anwendung findet, muss neben dem Vorliegen einer Verarbeitung personenbezogener Daten mindestens eine weitere Voraussetzung erfüllt sein. Um welche weiteren Voraussetzungen es sich handelt, findet sich nachfolgend ausgeführt:

3.2.1 Niederlassung in der EU

Rechtsgrundlagen:
- Art. 3 Abs. 1 DSGVO
- Einführungserwägungen DSGVO, Ziff. 22

Verfügt eine Institution mit Sitz in der Schweiz über eine **(1) Niederlassung** in der EU, findet die EU-Datenschutzgesetzgebung **(2) im Rahmen der Tätigkeit dieser Niederlassung** Anwendung.

(1) Niederlassung: Nach der EU-Datenschutzgesetzgebung liegt eine Niederlassung vor, wenn in der EU (1.1) eine feste Einrichtung besteht, von der aus (1.2) eine Tätigkeit effektiv und tatsächlich stattfindet.

- ***(1.1) Feste Einrichtung*** = liegt vor, wenn sie einen gewissen Grad an Beständigkeit hat - mobile Geschäftsstätten oder Messestände sind keine festen Einrichtungen.
- ***(1.2) Effektiv und tatsächlich stattfindende Tätigkeit*** = irgendwie geartete menschliche Aktivitäten – Serverstandorte oder Briefkastenfirmen erfüllen diese Voraussetzung nicht.

Nur wenn beide Voraussetzungen erfüllt sind, liegt eine Niederlassung im Sinne der EU-Datenschutzgesetzgebung vor. Ob die Niederlassung eigene Rechtspersönlichkeit hat, spielt keine Rolle. Es kann sich bei Niederlassungen somit auch um interne Abteilungen wie Rechenzentren, die Buchhaltung oder Produktionsstätten sowie aber auch Zweigstellen oder Agenturen handeln.

(2) Im Rahmen der Tätigkeit dieser Niederlassung: Die Verarbeitung der personenbezogenen Daten muss im Rahmen der Tätigkeit der jeweiligen Niederlassung in der EU stattfinden. Um diese Voraussetzung zu erfüllen, muss die effektive Verarbeitung allerdings nicht zwingend in der EU stattfinden. Veranschaulichen lässt sich das an folgendem Beispiel: Findet die Verwaltung der Kundendaten einer EU-Niederlassung durch den Mutterkonzern in den USA statt, findet diese Verarbeitung zwar ausserhalb der EU aber im Rahmen der Tätigkeit der Niederlassung in der EU statt.

Fokus Spitäler:
Es ist durchaus denkbar, dass gewisse Spitäler – insbesondere in Grenzkantonen – über eine Niederlassung im grenznahen Ausland verfügen – z.B. in Form eines spezialisierten Röntgeninstituts oder Labors. Grenzkantone wie Aargau, Basel-Stadt, Genf, Graubünden, Jura, Neuenburg, St. Gallen, Schaffhausen, Thurgau, Tessin, Waadt und Wallis sollten die Frage nach der Niederlassung in der EU daher sorgfältig prüfen.

3.2.2 Anbieten von Waren und Dienstleistungen

Rechtsgrundlagen:
- Art. 3 Abs. 2 lit. a DSGVO
- Einführungserwägungen DSGVO, Ziff. 23

Die EU-Datenschutzgesetzgebung findet Anwendung, wenn eine Institution mit Sitz in der Schweiz, Daten von **(1) Personen, die sich in der EU befinden**, verarbeitet, sofern sie diesen Personen **(2) Waren oder Dienstleistungen (3) anbietet**.

(1) Personen, die sich in der EU befinden: Die Personen müssen sich zum Zeitpunkt der fraglichen Datenbearbeitung in der EU befinden. Dabei spielt es keine Rolle, ob die Personen Unionsbürger (Staatsbürger eines Mitgliedstaats) sind oder in der EU Wohnsitz haben. Auch Personen, die aus Drittländern stammen und sich nur vorübergehend in der EU aufhalten (z.B. Expats, Austauschschüler oder Reisende), befinden sich nach der EU-Datenschutzgesetzgebung während ihrem Aufenthalt in der EU.

(2) Waren und Dienstleistungen: Was unter Waren und Dienstleistungen zu verstehen ist, definiert die EU-Datenschutzgesetzgebung nicht. Der Begriff der **Waren** lässt sich jedoch unter Einbezug anderweitiger EU-Gesetzgebung als alle beweglichen körperlichen Gegenstände, die einen Geldwert haben und Gegenstand von Handelsgeschäften sein können, definieren. Darunter fallen neben herkömmlichen Handelswaren auch Energieträger (Öl, Gas, Strom), Saatgut, Tiere, Abfälle, Kunstgegenstände oder Träger immaterieller Güter (z.B. Ton- und Bildträger). Der Begriff der **Dienstleistungen** ist nach Ansicht der Literatur weit zu verstehen. Er umfasst insbesondere auch jede Art von Internet-Dienstleistungen wie z.B. im Internet buchbare Reisen, Cloud-Angebote, das Anbieten von Apps, Social Media-Angebote oder Streaming Dienste.

(3) Anbieten: Mit Blick auf das Anbieten ist kein aktives Handeln der anbietenden Institution notwendig. Auch das passive Bereithalten eines Angebots kann ein Angebot im Sinne der EU-Datenschutzgesetzgebung darstellen. Allerdings ist davon auszugehen, dass das blosse Zugänglichmachen einer Website in der Union kein Angebot im Sinne der EU-Datenschutzgesetzgebung darstellt. Andere Faktoren wie die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich sind oder die Erwähnung von Kunden oder

Nutzern, die sich in der EU befinden, können dagegen Indizien für ein Angebot darstellen. Mit Blick auf die Schweiz kann die Verwendung einer Landessprache, die gleichzeitig auch in einem oder mehreren Mitgliedstaaten gebräuchlich ist (Deutsch in Deutschland und Österreich, Französisch in Frankreich und Italienisch in Italien) allerdings kaum als solches Indiz gelten. Wenn die Website die Leistungen jedoch auch in Euro anbietet oder als Referenzen Kunden aus dem EU-Raum angibt, kann dies als Anbieten im Sinne der EU-Datenschutzgesetzgebung verstanden werden. Irrelevant ist, ob das Angebot entgeltlich erfolgt. Auch unentgeltliche Angebote (z.B. Internet-Dienstleistungen wie die Google-Suchmaschine, Google Maps, Social Media oder andere Gratisdienste) sind von der EU-Datenschutzgesetzgebung erfasst.

Fokus Spitäler:
Spitäler sollten prüfen, ob sie medizinische oder kosmetische Produkte, Medizingeräte, Gesundheits-Apps oder ähnliches anbieten (auch unentgeltlich) und falls ja, ob sie diese Produkte auch Personen, die sich in der EU befinden, anbieten – z.B. weil sie die Produkte auch in EURO anbieten oder in einer oder mehreren Sprachen eines Mitgliedstaats (Ausnahmen sind Deutsch, Französisch und Italienisch - da es sich dabei um Landesprachen der Schweiz handelt).
Wenn eine Person aus dem EU-Raum sich in einem Schweizer Spital behandeln lässt, entspricht dies nicht einem Anbieten von Waren und Dienstleistungen an Personen, die sich in der EU befinden. Die Behandlung und die damit verbundenen Datenverarbeitungen finden in der Schweiz statt und unterliegen daher der schweizerischen Datenschutzgesetzgebung. Dies gilt auch für den Fall, dass im Anschluss an die Behandlung dem Hausarzt der behandelten Person, der seine Praxis in einem EU-Mitgliedstaat hat, Austrittsberichte oder der Krankenversicherung der betroffenen Person mit Sitz in einem EU-Mitgliedstaat Rechnungen übersendet werden.
Es ist jedoch darauf hinzuweisen, dass die Prüfung der Voraussetzung «Anbieten von Waren und Dienstleistungen an Personen, die sich in der EU befinden» Grauzonen aufweist und eine abschliessende Beantwortung der Sachlage zurzeit nicht möglich ist. Verlässliche Antworten wird es erst geben, wenn dazu Entscheide von Datenschutzaufsichtsbehörden und Gerichten der EU-Mitglied-staaten ergangen sind.

3.2.3 Verhaltensbeobachtung (Tracking und Profiling)

Rechtsgrundlagen:
- Art. 3 Abs. 2 lit. b DSGVO
- Einführungserwägungen DSGVO, Ziff. 24

Die EU-Datenschutzgesetzgebung findet Anwendung, wenn eine Institution mit Sitz in der Schweiz Daten über natürliche Personen verarbeitet, um **(1) das Verhalten dieser Personen zu beobachten**, sofern **(2) das Verhalten in der EU stattfindet**.

(1) Verhalten von Personen beobachten: Diese Regelung bezieht sich ausschliesslich auf Datenverarbeitungen, die dem Beobachten der Internetaktivitäten einer natürlichen Person dienen (Tracking) - inklusive der nachfolgenden Verwendung von Techniken zur Erstellung eines Profils der betroffenen Person anhand dessen sich deren Vorlieben oder Verhaltensweisen analysieren oder voraussagen lassen (Profiling). Nicht erfasst sind somit andere Beobachtungsformen wie z.B. Satelliten- oder Drohnenaufnahmen.

Damit ein Beobachten vorliegt, muss dieses eine bestimmte Dauer und eine gewisse Intensität aufweisen. Vorgehensweisen, die zum Vornherein als einmalige und punktuelle Handlungen ausgestaltet sind, stellen kein Beobachten im Sinne der EU-Datenschutzgesetzgebung dar. Gleichzeitig ist für das Vorliegen eines Beobachtens aber auch keine flächendeckende oder systematische Überwachungstätigkeit erforderlich. Insbesondere der Einsatz von Analyse-Tools wie Cookies oder Social Plugins (z.B. Like-Button von Facebook) sowie der Einsatz von Value-

Added Services führen stets zum Vorliegen eines Beobachtens im Sinne der EU-Datenschutzgesetzgebung.

Mit Blick auf Webseiten, die Tracking und Profiling Tools verwenden, ist davon auszugehen, dass es für ein Beobachten im Sinne der EU-Datenschutzgesetzgebung nicht darauf ankommt, ob sich die Webseite konkret an Personen, die sich in der EU befinden, wendet (wie beim Anbieten von Waren und Dienstleistungen – siehe Punkt 3.2.2 oben). Damit wird jeder Webseitenanbieter, der entsprechende Tools einsetzt, von der EU-Datenschutzgesetzgebung erfasst, sofern sich die Nutzer im Zeitpunkt des Besuchs der Webseite in der EU befinden und die eingesetzten Tracking und Profiling Tools zu einer Verarbeitung personenbezogener Daten führen.

(2) Verhalten findet in EU statt: Das Verhalten findet in der EU statt, wenn sich die von der Beobachtung betroffenen Personen während der Nutzung des Internets physisch innerhalb der EU befinden. Dies lässt sich jeweils anhand der IP-Adresse des Endgeräts der betroffenen Person feststellen.

Fokus Spitäler:
Die IT-Abteilungen der Spitäler sollten prüfen, inwiefern im Rahmen der spitaleigenen Homepage der Einsatz von Tracking- und Profiling-Instrumenten erfolgt. Ein entsprechender Einsatz könnte zur Anwendbarkeit der EU-Datenschutzgesetzgebung führen. Erfolgt ein entsprechender Einsatz, empfiehlt sich eine Prüfung, inwiefern der Verzicht auf Tracking- und Profiling-Instrumente möglich ist. Eine weitere Möglichkeit besteht darin, Besucher mit einer IP-Adresse aus dem EU-Raum mittels Geo-Lokalisierungstools vom Tracking und Profiling auszunehmen.

4 Benennung eines Vertreters in der EU

Rechtsgrundlagen:
- Art. 4 Ziff. 17, Art. 27 sowie Art. 83 Abs. 4 lit. a DSGVO
- Einführungserwägungen DSGVO, Ziff. 80

Steht fest, dass die EU-Datenschutzgesetzgebung auf die Verarbeitung personenbezogener Daten einer Institution mit Sitz in der Schweiz Anwendung findet, kann eine Pflicht bestehen, in der EU eine Vertretung zu benennen. Die Aufgabe dieser Vertretung besteht darin, die Institution bei den sich aus der EU-Datenschutzgesetzgebung ergebenden Pflichten zu vertreten und den von der Verarbeitung betroffenen Personen in der EU und den EU-Datenschutzaufsichtsstellen als Ansprechpartner zu dienen.

Eine Pflicht zur Benennung einer solchen Vertretung besteht allerdings nur für natürliche und juristische Personen mit Sitz ausserhalb der EU. **Behörden und öffentliche Stellen** eines nicht EU-Mitgliedstaats sind davon ausgenommen. Um zu bestimmen, ob eine Behörde oder öffentliche Stelle im Sinne der EU-Datenschutzgesetzgebung vorliegt, ist in erster Linie danach zu fragen, ob die betroffene Einheit Aufgaben der öffentlichen Verwaltung wahrnimmt bzw. die Verarbeitung der personenbezogenen Daten zu öffentlichen Zwecken erfolgt.

Besteht eine Pflicht zur Benennung einer Vertretung in der EU, hat die Benennung schriftlich zu erfolgen. Selbst wenn eine Datenverarbeitung in mehreren Mitgliedstaaten erfolgt, reicht es aus, wenn eine Vertretung bestimmt wird. Allerdings muss sich diese in einem der Mitgliedstaaten, in dem eine Datenverarbeitung erfolgt, befinden. Als Vertreter kommen natürliche oder juristische Personen in Form von Rechtsanwaltskanzleien, Treuhandunternehmen oder bei Konzernen auch konzerninternen Vertretungen im jeweiligen Mitgliedstaat in Frage.

Die Pflicht zur Benennung einer solchen Vertretung besteht allerdings auch für natürliche und juristische Personen mit Sitz ausserhalb der EU nicht uneingeschränkt. Sie entfällt, wenn alle drei der nachfolgenden Voraussetzungen erfüllt sind:

- die Verarbeitung der personenbezogenen Daten erfolgt nur **(1) gelegentlich**
  und
- sie umfasst keine **(2) umfangreiche** Verarbeitung besonderer Kategorien personenbezogener Daten und keine umfangreiche Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten
  und
- ihre Art, ihr Zweck und ihr Umfang bieten **(3) voraussichtlich kein Risiko für die Rechte und Freiheiten** der von der Verarbeitung betroffenen Personen

(1) gelegentlich: gelegentlich ist eine Verarbeitung, wenn sie nicht regelmässig erfolgt und nicht Bestandteil des Kerngeschäfts der jeweiligen Institution darstellt.

(2) umfangreich: umfangreich ist eine Verarbeitung, wenn sie eine grosse Menge an Daten oder Datenanalysen von hoher Intensität umfasst. Die Verarbeitung besonderer Kategorien personenbezogener Daten bzw. die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten führen somit nicht automatisch zu einer Verpflichtung zur Benennung einer Vertretung in der EU. Eine solche besteht nur, wenn es sich um eine umfangreiche oder intensive Verarbeitung entsprechender Daten handelt. Allerdings dürfte die Verarbeitung dieser beiden Datenkategorien verbreitet zu einem voraussichtlichen Risiko für die Rechte und Freiheiten der betroffenen Personen führen und damit von der dritten Voraussetzung erfasst sein.

(3) voraussichtlich kein Risiko für Rechte und Freiheiten: wenn zwar ein Risiko nicht völlig ausgeschlossen werden kann, dieses aber bei genauerer Betrachtung gering erscheint.

Bei Missachtung der Pflicht zur Benennung eines Vertreters in der EU kann eine Geldbusse von bis zu 10 Mio. EUR oder im Fall eines Unternehmens von bis zu 2% seines gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres (je nach dem welcher Betrag höher ist) drohen.

Allerdings wird es in vielen Fällen nicht einfach sein, die Frage nach der Pflicht zur Benennung eines solchen Vertreters eindeutig zu beantworten. Sei dies, weil es unklar ist, ob eine Institution eine Behörde oder öffentliche Stelle im Sinne der EU-Datenschutzgesetzgebung darstellt oder weil sich Schwierigkeiten bei der Prüfung der vorgenannten Ausschlusskriterien ergeben. Es wird daher Aufgabe der Gerichte und Datenschutzaufsichtsstellen der EU-Mitgliedstaaten sein, hier eine zielführende Praxis zu entwickeln. Bis dahin wird eine gewisse Rechtsunsicherheit bestehen.

Fokus Spitäler:
Nach dem schweizerischen Datenschutzrecht gelten Spitäler, soweit sie einen kantonalen oder kommunalen Leistungsauftrag erfüllen, als öffentliche Organe des jeweiligen Kantons bzw. der jeweiligen Gemeinde.
Mit Blick auf die EU-Datenschutzgesetzgebung ist unklar, wie sich der Begriff «Behörden und öffentliche Stellen» in der Umsetzung definiert. Es gibt jedoch aus dem deutschen Recht Hinweise, dass eine mit der Schweiz vergleichbare Lösung denkbar ist. Spitäler, die einen Leistungsauftrag haben und die Voraussetzungen für eine Anwendbarkeit der EU-Datenschutzgesetzgebung erfüllen, werden in der Tendenz somit davon ausgehen können, dass sie auch unter der EU-Datenschutzgesetzgebung als «Behörden und öffentliche Stellen» gelten und für sie entsprechend keine Pflicht zur Benennung einer Vertretung in der EU besteht. Es ist jedoch ausdrücklich darauf hinzuweisen, dass eine abschliessende Beantwortung dieser Frage zurzeit nicht möglich ist.
Spitäler, die über keine Leistungsaufträge verfügen und die Voraussetzungen für eine Anwendbarkeit der EU-Datenschutzgesetzgebung erfüllen, sollten sämtliche Voraussetzungen für die Benennung einer Vertretung in der EU prüfen. Sie stellen weder unter der schweizerischen noch der EU-Datenschutzgesetzgebung «Behörden oder öffentliche Stellen» dar.

5 Mögliche Vorgehensweisen bei Anwendbarkeit der EU-Datenschutzgesetzgebung

Ist davon auszugehen, dass die EU-Datenschutzgesetzgebung anwendbar ist, sind folgende Vorgehensweisen denkbar:

1. Wurden in **Checkliste A** die **Fragen 1 und 2** mit **JA** beantwortet, findet die EU-Datenschutz-gesetzgebung auf die Datenverarbeitungen im Rahmen der Tätigkeit der Niederlassung in der EU stets Anwendung. Diese Verarbeitungen sind gemäss der EU-Datenschutzgesetzgebung auszugestalten. Eine Vertretung in der EU muss in diesem Fall nicht bestimmt werden, da sich die Niederlassung in der EU befindet und damit in der EU eine Ansprechperson besteht.

2. Wurden in **Checkliste A** die **Fragen 1 und 3** oder die **Fragen 1 und 4** mit **JA** beantwortet, sind folgende Vorgehensweisen denkbar:

   2.1 Festlegen, welche Datenverarbeitungen betroffen sind und prüfen, ob sich diese so ausgestalten lassen, dass sie nicht mehr unter die EU-Datenschutzgesetzgebung fallen.

   2.2 Falls dies nicht möglich oder erwünscht ist, ***in einem ersten Schritt*** prüfen, welche Verarbeitungen betroffen sind und diese entsprechend der EU-Datenschutzgesetzgebung ausgestalten. Die Anwendbarkeit der EU-Datenschutzgesetzgebung bedeutet in der Regel nicht, dass eine Verarbeitung nicht mehr zulässig ist, sondern lediglich, dass die Verarbeitung die Anforderungen der EU-Datenschutzgesetzgebung erfüllen muss. Die sonstigen Datenverarbeitungen der Institution richten sich nach wie vor nach dem schweizerischen Datenschutzrecht. Allerdings dürfte eine Abgrenzung nicht immer einfach sein und im Rahmen des Einsatzes von Analyse-Tools wie Cookies oder Social Plugins (z.B. Like-Button von Facebook) sowie des Einsatzes von Value-Added Services dürfte eine Anwendung der EU-Datenschutzgesetzgebung mehrheitlich gegeben sein. ***In einem zweiten Schritt*** ist zu prüfen, inwiefern eine Vertretung in der EU zu benennen ist (⇨ Checkliste B).

Bei Unsicherheiten empfiehlt sich jedenfalls die Beiziehung eines Datenschutzexperten oder einer Datenschutzexpertin.

6 Checklisten

Die nachfolgenden Checklisten dienen als Orientierungshilfe und können eine konkrete Analyse des Einzelfalls nicht ersetzen. Ihre Anwendung erfolgt auf eigenes Risiko. Bei Unsicherheit empfiehlt sich die Beiziehung eines Datenschutzspezialisten bzw. einer Datenschutzspezialistin.

I. Anwendbarkeit der EU-Datenschutzgesetzgebung (Checkliste A)

Nr.	Fragen	Ref. LF*	Antwort	
			JA	NEIN
1.	Findet eine Verarbeitung personenbezogener Daten statt?	3.1	❑	❑
2.	Findet die Datenverarbeitung im Rahmen der Tätigkeit einer Niederlassung in der EU statt?	3.2.1	❑	❑
3.	Findet die Datenverarbeitung im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen an Personen, die sich in der EU befinden, statt?	3.2.2	❑	❑
4.	Findet die Datenverarbeitung zwecks Beobachtens des Internetverhaltens von Personen, die sich in der EU befinden, statt?	3.2.3	❑	❑

* Ref. LF = Referenz Leitfaden

Je nach Antwortkombination gestaltet sich die Sachlage wie folgt:

- Kann Frage 1 mit NEIN beantwortet werden, gelangt die EU-Datenschutzgesetzgebung NICHT zur Anwendung und es kann auf die Beantwortung der Fragen 2 bis 4 verzichtet werden.

- Muss Frage 1 und mindestens eine der Fragen 2 bis 4 mit JA beantwortet werden, gelangt die EU-Datenschutzgesetzgebung für die jeweiligen Datenverarbeitungen zur Anwendung.

- Kann Frage 1 mit JA und können die Fragen 2 bis 4 alle mit NEIN beantwortet werden, gelangt die EU-Datenschutzgesetzgebung NICHT zur Anwendung. In diesem Fall richtet sich die gesamte Datenverarbeitung nach der schweizerischen Datenschutzgesetzgebung.

II. Benennung eines Vertreters in der EU (Checkliste B)

Nr.	Fragen	Ref. LF*	Antwort	
			JA	NEIN
1.	Ist Ihre Institution eine Behörde oder öffentliche Stelle?	4.	❑	❑
2.	Erfolgt die Verarbeitung personenbezogener Daten regelmässig?	4.	❑	❑
3.	Findet eine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten oder personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten statt?	4.	❑	❑
4.	Führt die Datenverarbeitung unter Berücksichtigung ihrer Art, ihres Umfangs und ihres Zwecks voraussichtlich zu einem Risiko für die Rechte und Freiheiten von natürlichen Personen?	4.	❑	❑

* Ref. LF = Referenz Leitfaden

Je nach Antwortkombination gestaltet sich die Sachlage wie folgt:

- Lässt sich Frage 1 mit JA beantworten, kann auf die Beantwortung der Fragen 2 bis 4 verzichtet werden und es besteht KEINE Pflicht zur Benennung einer Vertretung in der EU.

- Muss Frage 1 mit NEIN und die Fragen 2 bis 4 alle mit JA beantwortet werden, besteht EINE Pflicht zur Benennung einer Vertretung in der EU.

- Muss Frage 1 mit NEIN und können die Fragen 2 bis 4 alle mit NEIN beantwortet werden, besteht KEINE Pflicht zur Benennung einer Vertretung in der EU.

- Muss Frage 1 mit NEIN beantwortet werden und weisen die Fragen 2 bis 4 sowohl JA- als auch NEIN-Antworten auf, bedarf es jedenfalls einer eingehenderen Betrachtung des Einzelfalls.