HAMMERMANN EHLERS ALBERT
RECHTSANWÄLTE IN PARTNERSCHAFT

HAMMERMANN EHLERS ALBERT • Karl-Liebknecht-Straße 25 • 03046 Cottbus

NAEMI-WILKE-STIFT
Dr.-Ayrer-Straße 1-4
03172 Guben

12. czerwca 2023
sz770

Nasz znak: EH-211/23
Projekt - NAEMI-WILKE-STIFT

Krótkie sprawozdanie z oceny ochrony danych osobowych

Podział

PETER ALBERT *
Rechtsanwalt
Fachanwalt für Arbeitsrecht
Fachanwalt für Miet- & WEG-Recht

BENJAMIN EHLERS *
Rechtsanwalt
Fachanwalt für Steuerrecht
Fachanwalt für Handels- & Gesellschaftsrecht

FALK HAMMERMANN **
Rechtsanwalt
Fachanwalt für Bau- & Architektenrecht
Fachanwalt für Miet- & WEG-Recht

ANTJE GERDES *
Rechtsanwältin
Mediatorin
Fachanwältin für Familienrecht

CLAUDIA NAPIERALSKI **
Rechtsanwältin
Fachanwältin für Strafrecht

MARTA SZATARSKA LL.M *
Rechtsanwältin
Fachanwältin für Transport- & Speditionsrecht
Radca Prawny

AG Cottbus PR 54 CB

Deutsche Bank AG
BIC: DEUTDEDB160

Geschäftskonto
IBAN: DE95 1207 0024 0304 3486 00

Anderkonto
IBAN: DE97 1207 0024 0015 6851 00

VR Bank Lausitz eG
BIC: GENODEF1FWA

Geschäftskonto
IBAN: DE67 1806 2678 0006 2318 29

KANZLEI COTTBUS *

Karl-Liebknecht-Straße 25 (ggü. Staatstheater)
D-03046 Cottbus

T 0355 - 479 20 10
F 0355 - 479 20 11
E info@hea-rechtsanwalt.de

KANZLEI POTSDAM **

Mies-van-der-Rohe-Straße 2
D-14469 Potsdam

T 0331 - 505 87 69
F 0331 - 505 89 86
E potsdam@hea-rechtsanwalt.de

Skróty

Skrót	wyjaśnienie
ust.	ustęp
TFUE	Traktat o funkcjonowaniu UE
art.	artykuł
UODO	Ustawa o ochronie danych osobowych
RODO	Ogólne rozporządzenie o ochronie danych osobowych
mot.	motyw RODO
UE	Unia Europejska
zg.	zgodnie
Konst.	Konstytucja
dot.	dotyczy
UOPI	Ustawa o ochronie przed infekcjami
w zw. z	w związku z
dosł.	littera łacińska - litera
z dal. dow.	z dalszymi dowodami
nr na marg.	numer na marginesie
zd.	zdanie
KS	Kodeks Socjalny
m.in.	między innymi
p.w.	przede wszystkim
por.	porównaj
np.	na przykład
nr	numer

Literatura

Paal/Pauly, DS-GVO BDSG, 3. nakład 2021
BeckOK Datenschutzrecht, Wolff/Brink, 43. edycja, stan: 01.02.2023
Thüsing, Beschäftigtendatenschutz und Compliance, 3. nakład 2021

I. Przyczyny udzielenia zlecenia

Fundacja Naemi Wilke Stift (dalej szpital) zleciła nam doradztwo prawne w zakresie planowanego rozwoju infrastruktury medycznej w zakresie współpracy pomiędzy szpitalem w Guben, ośrodkiem opieki medycznej również w Guben (dalej MVZ) oraz pogotowiem ratunkowym w Gubinie (zwanego dalej pogotowiem ratunkowym). W szczególności należy wyjaśnić kwestie prawa korporacyjnego dotyczące nowego MVZ, który ma zostać utworzony, a także ogólne kwestie ochrony danych dotyczące współpracy trzech podmiotów.

To krótkie sprawozdanie ma na celu rzucić światło na ogólne aspekty planowanego projektu związane z ochroną danych osobowych.

II. Rzeczywista sytuacja wyjściowa

W ramach niniejszej oceny przyjmujemy następującą - abstrakcyjnie przedstawioną - sytuację wyjściową:
Planowana jest współpraca trzech niezależnych prawnie firm, których działalność skupiać się będzie na opiece medycznej nad pacjentami w ogólnym tego słowa znaczeniu. Na szczególną uwagę zasługuje forma prawna szpitala, który w świetle prawa cywilnego pełni funkcję fundacji kościelnej oraz fakt, że dwie spółki mają siedzibę w Niemczech (kraj związkowy Brandenburgia), a trzeci podmiot w Polsce.

Współpraca powinna przebiegać w ten sposób, by pacjenci – niezależnie od tego, do którego z trzech podmiotów są przyjmowani po raz pierwszy – mieli dostęp do oferty usług wszystkich zaangażowanych podmiotów. W tym celu konieczne będzie przekazywanie danych pacjentów pomiędzy trzema podmiotami których definicja zostanie omówiona w dalszej części. Te działania dotyczące przetwarzania powinny być przedmiotem oceny ochrony danych, choć prawdopodobnie istnieje wiele sytuacji przetwarzania, które wymagają oddzielnego rozpatrzenia każdego indywidualnego przypadku.

III. Sytuacja początkowa w świetle prawa o ochronie danych

Biorąc pod uwagę lokalizacje trzech podmiotów (Niemcy i Polska), należy spodziewać się przetwarzania danych w UE.

Od 25 maja 2018 r. przepisy RODO regulują, w jakim zakresie mogą być przetwarzane dane osobowe w UE.

RODO jako europejski akt prawny będący rozporządzeniem wywołuje zgodnie z Art. 288 ust. 2 TFUE, bezpośrednie skutki we wszystkich państwach członkowskich UE i nie wymaga (np. w

przeciwieństwie do dyrektyw unijnych) jakiejkolwiek implementacji do krajowej podstawy prawnej. RODO jest zatem jednolitą podstawą prawną przetwarzania danych osobowych na terenie UE.

Tylko dzięki tak zwanym klauzulom otwierającym w RODO istnieje co najmniej selektywny zakres dla krajowych ustawodawców w zakresie tworzenia krajowych przepisów o ochronie danych, które nie mogą być sprzeczne z wymogami RODO. Takie krajowe podstawy prawne należy zatem rozpatrywać indywidualnie.

IV. Definicje

W celu zapewnienia jednolitego rozumienia pojęć zawartych w przepisach o ochronie danych osobowych, warto omówić te najistotniejsze w odpowiedni zwiezły sposób.

- **Dane osobowe (Art. 4 lit. 1 RODO)**

Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (w dalszej części „osobie, której dane dotyczą".) Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

- **Dane dotyczące zdrowia**

Dane dotyczące zdrowia oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia(por. art. 4 lit.15 RODO).

- **Przetwarzanie**

Przetwarzanie w roz. art. 4 lit. 2 RODO oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie

- **Administrator**

Zgodnie z art. 4 lit. 7 RODO Administrator oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

Uwaga: Zgodnie z art. 24 RODO odpowiedzialność Administratora obejmuje w szczególności:

- zgodność z przepisami RODO
- podjęcie odpowiednich środków ochronnych
- wykazanie tego.

- **Podmiot przetwarzający**

Podmiot przetwarzający w roz. Art. 4 lit. 8 ROD oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Z kolei odpowiedzialną jest osoba decydująca o celu i sposobach przetwarzania, czyli klient.

V. Obowiązki Administratora

Każdy z trzech podmiotów musi przestrzegać obowiązków jako osoba odpowiedzialna za ochronę danych we własnej firmie oraz w związku z planowanym projektem. Te powinny początkowo zostać opisane jedynie w sposób abstrakcyjny, a następniej omówione bardziej szczegółowo w odniesieniu do planowanej współpracy.

Należy podkreślić prawne zasady przetwarzania danych uregulowane w art. 5 RODO, obowiązki informacyjne wynikające z art. 13 RODO oraz obowiązek wyznaczenia inspektora ochrony danych (m.in. art. 37 RODO).

1. **Zasady przetwarzania danych**

Każda z zaangażowanych firm jest zobowiązana przestrzegać zasad przetwarzania danych ujednoliconych w art. 5 RODO.
Są to:

- legalność przetwarzania według zasad dobrej wiary; przejrzystość (art. 5 ust. 1 lit. a) RODO)
- Ograniczenie celu (art. 5 ust. 1 lit. b) RODO)
- Minimalizacja danych (art. 5 ust. 1 lit. c) RODO)
- Dokładność (art. 5 ust. 1 lit. d) RODO)
- Ograniczenie przechowywania (art. 5 ust. 1 lit. e) RODO)
- Integralność i poufność (art. 5 ust. 1 lit. f) RODO)
- rozliczalność (art. 5 ust. 2 RODO)

Zasady te dotyczą wszystkich operacji przetwarzania danych i muszą być przestrzegane niezależnie od tego, jakie kategorie danych są przetwarzane. Szczególne znaczenie mają zasady określone w artykule 5 ustęp 1 lit. a) i b) RODO, których należy przestrzegać w planowanym projekcie, w szczególności przy przekazywaniu danych pomiędzy poszczególnymi podmiotami.

Istotne znaczenie ma zasada celowości, która legitymizuje przetwarzanie danych (por. Paal/Pauly/Frenzel RODO art. 5 ust. 23). Zgodnie z art. 5 ust. 1 lit. b RODO dane osobowe muszą być „zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie mogą być dalej przetwarzane w sposób niezgodny z tymi celami". Cel określa zatem powód, dla którego dane osobowe są przetwarzane. W rezultacie cel przetwarzania danych jest stałym punktem, na którym oparte są np. konieczność przetwarzania, podstawa prawna zgodnie z Art. 6 ust. 1 DSGVO, a także obowiązki informacyjne zgodnie z Art. 13 i nast. (por. RODO BeckOK/Schantz art. 5 ust. 13).

Zasada ograniczenia celu obejmuje również dalsze przetwarzanie przez osoby inne niż ta, która zebrała dane, dlatego też zbierający jest zobowiązany do przekazania zamierzonych celów także kolejnym użytkownikom (por. Paal/Pauly/Frenzel RODO art. 5 pkt 29).

Wskazane jest zatem, aby osoby zaangażowane skupiły się na wcześniejszym ustaleniu celów przetwarzania, aby na tej podstawie przygotować wszystkie dalsze kroki.

2. Obowiązki informacyjne

- Obowiązki informacyjne w przypadku zbierania danych od osoby, której dane dotyczą (art. 13 RODO)
- Obowiązki informacyjne w przypadku gromadzenia danych od strony trzeciej (art. 14 RODO).

Jeżeli dane osobowe są zbierane od osoby, której dane dotyczą, osoba odpowiedzialna jest zobowiązana do poinformowania osoby, której dane dotyczą, o danych określonych w art. 13 i 14 RODO w momencie ich zbierania (w tym imię i nazwisko oraz dane kontaktowe osoby odpowiedzialnej, w stosownych przypadkach jej przedstawiciela, cele przetwarzania i podstawa prawna).

3. Wymagania dotyczące dokumentacji

Zgodnie z Art. 30 ust. 1 RODO Administrator jest zobowiązany do rejestrowaia wszystkich czynności przetwarzania danych osobwowych. Ma to na celu między innymi umożliwienie organowi nadzorczemu szybkiego wglądu w procesy przetwarzania w firmie.

Ponieważ oczekuje się, że wszystkie podmioty będą przetwarzać szczególne kategorie danych (głównie dane dotyczące zdrowia), obowiązek prowadzenia rejestrów czynności będzie dotyczył wszystkich zaangażowanych osób i nie będzie zbędny w świetle art. 30 ust. 5 RODO.

4. Ocena skutków dla ochrony danych

Ponadto w przypadku ryzykownych operacji przetwarzania konieczne będzie również przeprowadzenie tak zwanej oceny skutków dla ochrony danych zgodnie z art. 35 RODO. Następnie należy przeprowadzić ocenę skutków planowanych operacji przetwarzania. Ma to zastosowanie, gdy forma przetwarzania, w szczególności z wykorzystaniem nowych

technologii, ze względu na charakter, zakres, okoliczności i cele przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

5. Powołanie Inspektora Ochrony Danych

Zgodnie z Art. 37 ust.1 RODO obowiązek wyznaczenia inspektora ochrony danych istnieje w każdym przypadku, w którym:

- przetwarzanie odbywa się przez organ lub podmiot publiczny, z wyjątkiem sądów, o ile działają one w ramach swoich czynności administrayjnych (por. art. 37 ust. 1 lit. a) RODO),
- główna działalność administratora lub podmiotu przetwarzającego polega na prowadzeniu procesu przetwarzania, które ze względu na swój rodzaj, zakres i/lub cel wymagają szeroko zakrojonego, regularnego i systematycznego monitorowania osób, których dane dotyczą (por. art. 37 ust. 1 lit. b) RODO) lub
- główna działalność osoby odpowiedzialnej lub podmiotu przetwarzającego polega na szeroko zakrojonym przetwarzaniu szczególnych kategorii danych zgodnie z art. 9 RODO lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa zgodnie z art. 10 RODO (por. art. 37 ust. 1) (c) RODO).

W dwóch ostatnich przypadkach nacisk kładziony jest na podstawową działalność administratora, która – aby powstał obowiązek wynikający z tych przepisów – musi polegać na realizacji procesu przetwarzania danych osobowych.

W tym kontekście motyw 97 RODO pokazuje, że pojęcie „głównej działalności" administratora odnosi się do jego głównych czynności, a nie do procesu przetwarzania, które mają charakter jedynie działalności dodatkowej.
Ponadto Art. 37 ust.4 zdanie 1 RODO zawiera klauzulę otwierającą przepisy krajowe państw członkowskich. Niemiecki ustawodawca wykorzystał tę klauzulę otwierającą w § 38 ust. 1 UODO. Zgodnie z tym osoba odpowiedzialna i podmiot przetwarzający powinni powołać inspektora ochrony danych w uzupełnieniu do przepisów RODO, jeżeli spełniony jest jeden z poniższych warunków:

- zatrudniają zwykle co najmniej 20 osób na stałe przy zautomatyzowanym przetwarzaniu danych osobowych;
- przeprowadzają przetwarzanie podlegające ocenie skutków dla ochrony danych zgodnie z Art. 35 RODO; lub
- przetwarzają dane osobowe w ramach prowadzonej działalności w celu transmisji, transmisji anonimowej lub w celu badania rynku lub opinii.

VI. Prawa osób, których to dotyczy

Prawa osób, których to dotyczy, nie są przedmiotem niniejszej opinii i dlatego należy o nich wspomnieć jedynie w celu ogólnego zrozumienia.

Termin prawa osób, których dane dotyczą, oznacza prawa osób, których dane podlegają przetwarzaniu. Art. 12 i nast. RODO szczegółowo regulują prawa osób, których dane dotyczą.

Osobom, których dane dotyczą, przysługują następujące prawa w związku z przetwarzaniem danych:

• prawo do informacji (art. 15 RODO)
• prawo do sprostowania (art. 16 RODO)
• prawo do usunięcia danych (art. 17 RODO)
• prawo do ograniczenia (art. 18 RODO)
• prawo do przenoszenia danych (art. 20 RODO)
• prawo do sprzeciwu (art. 21 RODO)
• prawo do cofnięcia zgody (art. 7 ust. 3 RODO)
• prawo do niepodlegania zautomatyzowanej decyzj (art. 22 RODO)
• Prawo do odwołania się do organu nadzorczego (art. 77 RODO w zw. z § 19 UODO).

Celem tych praw, które wynikają również z obowiązków Administratora, jest ochrona zainteresowanej osoby w jej samostanowieniu informacyjnym (por. art. 2 ust. 1 w związku z art. 1 ust. 1 Konstytucji). Ponadto prawa osób, których to dotyczy, służą w szczególności zapewnieniu przepływu informacji i przejrzystości.

VII. Ogólne wymagania dotyczące przetwarzania danych osobowych

Każde przetwarzanie danych osobowych stanowi w szczególności ingerencję w podstawowe prawo do samostanowienia informacyjnego (art. 2 ust. 1 w zw. z art. 1 ust. 1 Konst.).Dlatego każde przetwarzanie danych osobowych wymaga podstawy prawnej, która ma formę zgody osoby zainteresowanej lub może wynikać z normy uprawniającej. Przetwarzanie danych bez podstawy prawnej jest zatem zabronione lub, mówiąc inaczej: Przetwarzanie danych osobowych zawsze wymaga zgody prawnej.

1. Podstawy prawne zgodnie z RODO

a) podstawa prawna (zezwolenie) do przetwarzania danych osobowych może istnieć w różnych wariantach, które są w dużej mierze uregulowane w art. 6 RODO

Zgodnie z tym przetwarzanie danych może być dozwolone w następujących okolicznosciach

- istnienie zgody (art. 6 ust. 1 zd. 1 lit. a) RODO)
- przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą (art. 6 ust. 1 zd. 1 lit. b) RODO)
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze (art. 6 ust. 1 zdanie 1 lit. c) RODO)
- Przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 zd. 1 lit. d) RODO)

- przetwarzanie jest niezbędne do wykonania zadania leżącego w interesie publicznym lub w ramach sprawowania władzy publicznej przekazanej Administratorowi (art. 6 ust. 1 S. 1 lit. e) RODO)
- przetwarzanie jest niezbędne do ochrony prawnie uzasadnionych interesów Administratora lub strony trzeciej, chyba że nadrzędny jest interes lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem (art. 6 ust 1 pkt 1 lit f) RODO).

To, które uprawnienia mogą być istotne, zależy od odpowiednich operacji przetwarzania lub danych, które mają być przetwarzane.

Exkurs: Zgoda

Pojęcie zgody jest również prawnie zdefiniowane przez prawo w art. 4 nr 11 RODO.
Zgodnie z tym zgoda to każde dobrowolne, świadome i jednoznaczne wyrażenie woli w konkretnym przypadku w formie oświadczenia lub innego wyraźnego działania potwierdzającego, że osoba, której dane dotyczą, wskazuje, iż wyraża zgodę na przetwarzanie swoich danych osobowych.

Do skutecznego wyrażenia zgody przed przetwarzaniem wymagane jest uprzednie, dobrowolne, świadome, konkretne i formalne oświadczenie osoby, której dane dotyczą, która jest zdolna do wyrażenia zgody na przetwarzanie danych osobowych (BeckOK DatenschutzR/Stemmer RODO art. 7 ust. 34).

W odniesieniu do planowanego przedsięwzięcia szczególne znaczenie będą miały wymogi dotyczące świadomego wyrażenia zgody, formy oraz – w indywidualnych przypadkach – możliwości wyrażenia zgody.

- Poinformowanie

Bycie poinformowanym odnosi się do obowiązku Administratora do poinformowania osoby zainteresowanej o punktach, o których mowa w Art. 13 RODO, aby umożliwić osobie wyrażającej zgodę ocenę zakresu jej oświadczenia. Wymóg bycia poinformowanym uwzględnia zatem zasadę przejrzystości zapisaną w art. 5 ust. 1 lit. a) RODO.

Uwaga: Jednym z głównych wyzwań stojących przed firmami zajmującymi się uzyskiwaniem formularzy zgody pacjentów będzie wcześniejsze opracowanie formularzy w celu spełnienia ustawowych wymogów informacyjnych. Jednym z celów przetwarzania, które należy określić, będzie w szczególności przekazywanie danych między trzema podmiotami.

W każdym razie znaczenie prawidłowej i pełnej informacji dla pacjenta jest już znane z codziennej praktyki klinicznej.

- Forma

Z prawnej definicji zgody można wywnioskować, że oświadczenie woli musi być złożone „jednoznacznie [...] w formie oświadczenia lub innej wyraźnej czynności potwierdzającej". Obejmuje to ustne, pisemne lub ostateczne oświadczenia woli (por. motyw 32, s. 2). Na przykład samo milczenie nie wystarczy (por. motyw 32, s. 3).

Istotne jest, aby każdy z podmiotów udowodnił, że oświadczenie woli faktycznie istniało. Ponieważ na Administratorze spoczywa ciężar udowodnienia istnienia zgody (por. art. 7 ust. 1 RODO, motyw 42 S. 1).

Uwaga: Zasadniczo zawsze należy uzyskać pisemną zgodę, o ile jest to możliwe. Jeżeli w wyjątkowych przypadkach oświadczenie o wyrażeniu zgody nie zostanie złożone na piśmie, to przynajmniej złożenie oświadczenia (z podaniem miejsca, daty, świadków) powinno zostać udokumentowane dla celów dowodowych. Oświadczenia ogólne lub blankietowe nie są w żadnym wypadku wystarczające.

Na koniec należy zauważyć, że oświadczenie o wyrażeniu zgody może zostać odwołane – przynajmniej ze skutkiem na przyszłość. Taka możliwość odwołania nie może być niepotrzebnie utrudniana osobie, której dane dotyczą (standardem są tu wymagania, jakie zostały postawione przy udzielaniu zgody).

---

b) W tym miejscu należy omówić specyfikę przetwarzania szczególnych kategorii danych objętych art.9 RODO.

Jednym z centralnych procesów przetwarzania danych w planowanym projekcie będzie przetwarzanie danych dotyczących zdrowia, które art. 9 DRODO nazywa „szczególną kategorią" danych osobowych.

W związku z pytaniem, w jakim zakresie przetwarzanie szczególnych kategorii danych jest dopuszczalne w świetle przepisów o ochronie danych, pojawia się teoretyczny spór, który nie został jeszcze ostatecznie wyjaśniony, dotyczący relacji między art. 9 RODO a art. 6 RODO. Niezależnie od szczegółów prawnych, jasnym jest, że Art. 9 RODO nakłada surowsze wymogi dotyczące zgodności przetwarzania z prawem niż Art. 6 RODO, ponieważ dane rejestrowane w tym procesie są szczególnie wrażliwe (por. motyw 51 s. 1) i dlatego zasługują na szczególną ochronę. W wyniku teoretycznej dyskusji należy stwierdzić, że przetwarzanie szczególnych kategorii danych osobowych może być uzasadnione jedynie na podstawie Art. 9 RODO.

Art. 9 RODO jest skonstruowany inaczej niż postanowienie o przetwarzaniu prostych danych osobowych (czyli: art. 6 RODO): O ile w tym przypadku przetwarzanie jest dopuszczalne i zgodne z prawem tylko pod pewnymi warunkami – w szczególności za zgodą – przetwarzanie szczególnych danych osobowych jest zabronione (por. Paal/Pauly/Fenzel RODO art. 9 ust. 1). Art. 9 ust. 2 RODO przewiduje wyjątki od zasady zakazu przetwarzania danych szczególnie wrażliwych.

Powodem tej konstrukcji prawnej jest szczególna potrzeba ochrony danych osobowych, które ze swej natury są szczególnie wrażliwe w odniesieniu do podstawowych praw i wolności i których przetwarzanie może wiązać się ze znacznym ryzykiem naruszenia wspomnianych podstawowych praw i wolności (por. motyw 51, s. 1).

Art. 9 ust. 2 RODO wymienia następujące warunki:

- zgoda(art. 9 ust. 2 lit a) RODO
- prawo ubezpieczeń społecznych i ochrony socjalnej (art. 9 ust. 2 lit b) RODO)
- przetwarzanie w celu ochrony żywotnych interesów (art. 9 ust. 2 lit c) RODO)
- Przetwarzanie wewnętrzne w określonym celu przez fundację, stowarzyszenie lub inną organizację non-profit o charakterze politycznym, światopoglądowym, religijnym lub związkowym (art. 9 ust. 2 lit d) RODO)
- osoba, której dane dotyczą, w sposób oczywisty upubliczniła dane (art. 9 ust. 2 lit. e) RODO)
- dochodzenie roszczeń (art. 9 ust. 2 lit. f) RODO)
- ważny interes publiczny (art. 9 ust. 2 lit. g RODO)
- przetwarzanie w celu indywidualnej opieki medycznej (art. 9 ust. 2 lit. h) RODO)
- przetwarzanie danych zdrowotnych w interesie publicznym (art. 9 ust. 2 lit. i RODO)
- Cele archiwalne, badawcze, statystyczne (art. 9 ust. 2 lit. j) RODO).

Aus denen in Art. 9 Abs. 2 DSGVO geregelten Ausnahmen von Absatz 1 (also von dem Verbot der Verarbeitung), kann jedoch keine grundsätzliche Erlaubnis allein beim Vorliegen einzelner Tatbestände abgeleitet werden (vgl. Paal/Pauly/Fenzel DS-GVO Art. 9 Rn.18).

Z zawartych w art. 9 ust. 2 RODO wyjątków nie można jednak uzyskać ogólnego zezwolenia (tj. z zakazu przetwarzania) uregulowanych, zwłaszcza jeśli spełnione są poszczególne warunki (por. Paal/Pauly/Fenzel RODO art. 9 nr .18). Oznacza to, że nawet w przypadku wystąpienia przypadków, o których mowa w Art. 9 ust.2 RODO, nie można z tego wywnioskować, że przetwarzanie danych jest zgodne z prawem.

Warunki uregulowane w art. 9 ust. 2 RODO mają raczej inną strukturę, ponieważ tylko niektóre wykluczają ważność zakazu na podstawie art. 9 ust. 1 RODO (por. Paal/Pauly/Fenzel RODO art. 9 ust.) a tym samym umożliwiają przetwarzanie danych. Dotyczy to stanu faktycznego, o którym mowa w Art. 9 ust. 2 lit. a), c), e) i f) RODO.

Inne warunki wymienione w Art. 9 ust. 2 RODO również wymagają dodania norm prawnych, czy to uzasadniających dopuszczalność przetwarzania (lit. b, g, h, i oraz j) i/lub gwarancje lub określających odpowiednie i konkretne środki (lit. b, d, g, h, i, j), por. Paal/Pauly/Fenzel RODO Art. 9 ust. 19.
Dla planowanego projektu oznacza to, że m.in. uzyskanie skutecznie prawnych oświadczeń zgody od zainteresowanych pacjentów będzie decydowało o legalności przetwarzania danych.

Eine Datenverarbeitung wird durch die drei beteiligten Akteure voraussichtlich ebenfalls (unmittelbar) erlaubt sein, wenn die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene

Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben (vgl. Art. 9 Abs. 2 lit. c) DSGVO).

Przetwarzanie danych będzie prawdopodobnie również (bezpośrednio) możliwe przez trzy zaangażowane podmioty, jeżeli jest ono niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, nie jest w stanie wyrazić zgody z przyczyn fizycznych lub prawnych (por. 9 ust. 2 lit. c RODO).

Natomiast odniesienie do wyjątków zawartych w art. 9 ust.2 lit b, g, h, i oraz j) RODO musi być uzupełnione o normy prawne (prawo krajowe), aby przetwarzanie danych było zgodne z prawem.

Podsumowując, można stwierdzić, że przetwarzanie danych dotyczących zdrowia przy wyrażeniu przez osobę, której dane dotyczą, ważnej i wyraźnej zgody, nie jest zabronione, lecz bezpośrednio dozwolone. Poza tym faktem należy wziąć pod uwagę strukturę Art. 9 RODO i, w razie potrzeby, zapoznać się z krajową podstawą prawną w celu zalegalizowania przetwarzania danych.

Bez szczegółowej wiedzy na temat poszczególnych procesów przetwarzania nie jest możliwe omówienie tutaj dalszych szczegółów. Te muszą zostać każdoraowo sprawdzone przy konkretnej sprawie.

2. Uprawnienia ustawowe zgodnie z prawem krajowym

W odniesieniu do planowanego projektu zezwolenia wynikające z krajowych podstaw prawnych mogą również uzasadniać dopuszczalność poszczególnych operacji przetwarzania poprzez wspomniane na wstępie klauzule otwierające RODO.

Wobec braku szczegółowej wiedzy na temat możliwych metod przetwarzania, krajowe podstawy prawne należy wymienić jedynie jako przykłady.

a) przepisy krajowe w Niemczech

Oprócz ogólnych przepisów RODO istnieją krajowe przepisy dotyczące ochrony danych, które mogą być ewentualnie stosowane w kontekście planowanego projektu.

- Federalna ustawa o ochronie danych (BDSG) i związkowe przepisy o ochronie danych

Do przepisów krajowych należy zreformowana wraz z wprowadzeniem RODO ustawa o ochronie danych osobowych UODO (nowa wersja) jako prawo uniwersalne które zgodnie z § 1 ust. 1 UODO ma zastosowanie zarówno do organów niepublicznych, jak i organów publicznych rządu federalnego i częściowo organom publicznym krajów związkowych.

Związkowe przepisy dotyczące ochrony danych istnieją również jako przepisy uniwersalne, których istnienie wynika z nakładających się kompetencji rządu federalnego i krajów

związkowych. Prawo ochrony danych podlega zatem kompetencjom legislacyjnym rządów federalnych lub związkowych, w zależności od treści.

Krajowe przepisy o ochronie danych regulują przy tym przetwarzanie danych przez władze państwowe i lokalne.

Oznacza to *(vgl. JuS 2006, 213 (214)):*

- Zgodnie z § 1 ust. 2 nr 1 BDSG pierwsze dwa ustępy federalnej ustawy o ochronie danych mają zastosowanie do federalnych organów publicznych.
- Władze krajów związkowych podlegają przepisom federalnym o ochronie danych, nawet jeśli wdrażają prawo krajowe.
- Zautomatyzowane przetwarzanie danych przez osoby fizyczne lub prawne zgodnie z prawem prywatnym podlega ostatecznie pierwszym i trzecim ustępom federalnej ustawy o ochronie danych zgodnie z § 1 ust. 2 nr 3 UODO.

Z czysto prawnego punktu widzenia UODO wchodzi w grę w odniesieniu do planowanego projektu. Z kolei Brandenburska ustawa o ochronie danych nie będzie miała większego znaczenia, ponieważ zaangażowane podmioty prawdopodobnie nie będą objęte zakresem tej związkowej ustawy o ochronie danych.

• Prawo kościelne o ochronie danych

Jako odpowiednia regulacja krajowa powinna być wymieniona ustawa o ochronie danych kościelnych zgodnie z ustawą o ochronie danych kościelnych (UODK).

Zakres organizacyjny tych przepisów obejmuje jednostki kościelne, do których należą kościelne korporacje, fundacje, instytucje, zakłady, zakłady i inne kościelne osoby prawne niezależnie od ich formy prawnej (por. § 3 ust. 1 lit. c UODK). Zgodnie z § 3 ust.2 UODK ustawa ta ma zastosowanie do przetwarzania danych osobowych, o ile odbywa się to w ramach działalności osoby odpowiedzialnej lub podmiotu przetwarzającego, niezależnie od tego, gdzie przetwarzanie ma miejsce, jeżeli odbywa się w kontekście lub w imieniu organu kościelnego.

Ponieważ szpital jest zorganizowany w formie prawnej fundacji kościelnej na mocy prawa cywilnego, Administrator lub jego zastępcy muszą w każdym przypadku przestrzegać UODK podczas przetwarzania danych osobowych.
Przepisy UODK są w wielu obszarach zbliżone do przepisów RODO. Np. rozdziały 1 (Przepisy ogólne), 2 (Zasady) czy 3 (Prawa osób, których dane dotyczą) ustawy zostały przyjęte w niemal niezmienionej formie z przepisów RODO.
W szczególności wymagania, które UODK nakłada na zgodność z prawem przetwarzania danych osobowych (por. § 6 ust. 1 KDG) są w dużej mierze porównywalne z wymogami RODO, zawierają one jedynie specyfikacje w odniesieniu do kontekstu kościelnego.

Istotne różnice można zauważyć przy ewentualnych karach pieniężnych, ponieważ władze kościelne są z nich zwolnione. Istnieją również inne różnice, na przykład w odniesieniu do wymogów dotyczących zgody (art. 8 KDG), które w KUODK są bardziej rygorystyczne niż w RODO. O ile zgoda ma być podstawą prawną przetwarzania danych osobowych (por. § 6 ust.

1 lit. b RODO), należy przestrzegać § 4 pkt 13 RODO i § 8 RODO. Zgodnie z tym skuteczne oświadczenie zgody wymaga m.in. formy pisemnej, która jest zbędna tylko w wyjątkowych przypadkach. W przypadku przetwarzania szczególnych kategorii danych osobowych zgoda musi również wyraźnie odnosić się do tych danych (por. § 8 ust. 4 UODK).
Tak zwana tajemnica danych jest wyraźnie uregulowana w § 5 UODK, ale nie w RODO. Tajemnica danych polega na tym, że osobom zajmującym się przetwarzaniem danych osobowych zabrania się ich przetwarzania bez upoważnienia, nawet po zakończeniu tej czynności. Osoby te muszą zobowiązać się na piśmie do zachowania poufności danych i przestrzegania odpowiednich przepisów o ochronie danych w momencie rozpoczęcia pracy.
Należy również zauważyć, że zgodnie z § 36 UODK wszystkie organy kościelne w rozumieniu § 3 ustęp 1 lit. a) UODKmuszą wyznaczyć na piśmie inspektora ochrony danych firmy. Organy kościelne w rozumieniu § 3 ust. 1 lit. b) i c) UODK wyznaczają na piśmie zakładowego inspektora ochrony danych, jeżeli

a) zwykle co najmniej dziesięć osób jest stale zaangażowanych w przetwarzanie danych osobowych,
b) główna działalność Administratora lub podmiotu przetwarzającego polega na wykonywaniu operacji przetwarzania, które ze względu na swój charakter, zakres lub cel wymagają szeroko zakrojonego, regularnego i systematycznego monitorowania osób, których dane dotyczą, lub
c) główna działalność Administratora lub podmiotu przetwarzającego polega na szeroko zakrojonym przetwarzaniu szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa na podstawie art. 12.

W kontekście planowanego projektu trzeba będzie zatem uwzględnić specyfikę kościelnego prawa ochrony danych, zgodnie z którym muszą być spełnione różne wymogi dotyczące zgodności przetwarzania z prawem w zależności od operacji przetwarzania, kategorii danych, które mają być przetwarzane lub danych podmiotów, których one dotyczą.

- Ustawy o szpitalach

Art. 9 ust. 2 RODO zawiera różne klauzule otwierające w odniesieniu do przetwarzania danych wrażliwych w sektorze zdrowia, z których ustawodawca krajowy w Niemczech skorzystał między innymi w przepisach niektórych krajów związkowych dotyczących szpitali.

- §§ 27 i następne Brandenburskiej ustawy o rozwoju szpitali (BUORS)

Zgodnie z § 27 ust. 1 BUORS obok RODO obowiązuje brandenburska ustawa o ochronie danych, o ile niniejsza ustawa lub inne przepisy szczególne regulujące przetwarzanie danych pacjentów przez szpitale nie stanowią inaczej.

§ 28 BUORS zawiera standard zezwoleń na przetwarzanie danych pacjentów w celu leczenia pacjentów, w tym niezbędnej dokumentacji.

Exkurs: dane pacjentów

Chociaż RODO zawiera definicję danych zdrowotnych jako danych szczególnie wrażliwych, pojęcie danych pacjenta nie zostało szczegółowo zdefiniowane.

Zgodnie z § 27 ust.2 BUORS dane pacjenta to „wszystkie indywidualne informacje dotyczące okoliczności osobistych lub faktycznych

1. konkretnych lub możliwych do zidentyfikowania pacjentów z sektora szpitalnego
2. ich krewnych i inne osób powiązanych oraz
3. innych osóby trzecich,

o których szpital dowiedział się w związku z leczeniem szpitalnym, dziennym lub ambulatoryjnym.

- Pozostałe podstawy prawne właściwe dla danego obszaru

Z przepisów ustawy socjalnej oraz ustawy o ochronie przed infekcjami mogą wynikać dalsze krajowe przepisy obszarowe dla sektora zdrowia.

b) przepisy krajowe w Polsce

Ustawodawca krajowy w Polsce skorzystał z klauzul otwierających zawartych w RODO jedynie w ograniczonym zakresie.

Mimo, że niektóre polskie przepisy zostały częściowo zreformowane po wejściu w życie RODO i w niektórych miejscach mogą stanowić uzupełnienie, to zmienione przepisy nie mają wpływu na rozważaną tutaj tematykę przetwarzania danych zdrowotnych, dlatego nie ma powodu obawiać się zaostrzenia przepisów polskiego prawa krajowego.

VIII. Konkretne problemy w związku z planowaniem ochrony

1. Kto jest odpowiedzialny za ochronę danych?

W ramach własnej działalności gospodarczej każdy z zaangażowanych podmiotów będzie odpowiedzialny za ochronę danych w rozumieniu art. 4 nr 7 RODO.

Jednak w odniesieniu do planowanego projektu możliwa jest również współodpowiedzialność (por. art. 4 nr 7 w związku z art. 26 ust. 1 zdanie 1 RODO).

Decydującą cechą współodpowiedzialności jest to, że zaangażowane strony wspólnie ustalają zarówno cel, jak i sposoby przetwarzania danych.

Ponieważ wymagania dotyczące współodpowiedzialności są stosunkowo niskie, nie ma potrzeby równego uprawnienia decyzyjnego i równych interesów wszystkich zaangażowanych stron ani nawet równoważnej odpowiedzialności w zakresie przetwarzania danych.

Zasadniczo wystarczy, aby każdy uczestnik miał wpływ na decyzję o celach i środkach przetwarzania. W rezultacie nawet każda z zaangażowanych stron może realizować różne cele zamierzonego przetwarzania danych.

Dla planowanego projektu ważne jest, że w przypadku wspólnej odpowiedzialności zgodnie z Art. 26 ust. 1 zdanie 2 RODO wymagana jest umowa między zaangażowanymi stronami. Przepis nie określa wprawdzie określonej formy takiej umowy, jednak forma tekstowa (w rozumieniu § 126b KC) jest wskazana. Ponadto zaleca się przynajmniej formę tekstową, ponieważ „istotne elementy umowy" muszą być udostępnione zainteresowanej osobie (por. art. 26 ust. 2 zd.2 RODO).

W odniesieniu do treści umowy decydujący jest faktycznie istniejący, a nie uzgodniony stosunek umowny.

Współadministratorzy ponoszą solidarną odpowiedzialność zgodnie z art. 82 ust. 2 zd. 1 ust. 4 RODO, dlatego osoba, której dane dotyczą, może żądać pełnego naprawienia szkody poniesionej przez każdą ze stron. Osoba odpowiedzialna, której dotyczy roszczenie, musi następnie poinformować pozostałe, tak by mogły one uczestniczyć w procesie naprawienia szkody.

Exkurs: Rozgraniczenie odpowiedzialności solidarnej – realizacja zamówienia.

Wspólna odpowiedzialność różni się od realizacji zamówienia tym, że wspólnie określa cel i sposoby przetwarzania danych. W przypadku tych ostatnich osoba odpowiedzialna określa cel i (zwykle także) środki, które ktoś inny wykonuje w zależności od instrukcji.

Uwaga: Jeżeli podmiot przetwarzający nie stosuje się do wskazań/poleceń osoby odpowiedzialnej oraz ustala cele i sposoby przetwarzania z naruszeniem przepisów RODO, jest on uważany za osobę odpowiedzialną w zakresie tego przetwarzania (por. art. 28 ust. 10 RODO).

Podstawowe rozważania i umowy będą zatem musiały zawierać również określenie kompetencji w zakresie określania celu i sposobów operacji przetwarzania danych.

---

2. Zasada celowości

Po określeniu celów przetwarzania w rozumieniu art. 5 ust. 1 lit. b) RODO w praktyce nie jest niczym niezwykłym, że istnieją następnie inne cele, dla których dane powinny być przetwarzane. Takie zmiany celu są możliwe pod pewnymi warunkami, ale w indywidualnych przypadkach mogą być problematyczne. Tym ważniejsze jest, aby cele przetwarzania zostały wcześniej szczegółowo opracowane.

Niezależnie od wymagań dotyczących dopuszczalności zmian celu, mają one wpływ na obowiązki informacyjne osoby odpowiedzialnej i, w razie potrzeby, dostosowanie katalogów/ewidencji czynności przetwarzania.

3. Obowiązki informacyjne

Właściwe wypełnienie obowiązków informacyjnych będzie kluczowym elementem planowanego projektu, aby przetwarzanie danych osobowych było w całości zgodne z prawem. W związku z tym należy zwrócić szczególną uwagę na opracowanie odpowiednich projektów informacji dla pacjentów, które muszą zawierać planowany projekt transferu danych pomiędzy zaangażowanymi podmiotami.

4. Ocena skutków dla ochrony danych

W przypadku szerokiego przetwarzania szczególnych kategorii danych osobowych zgodnie z art. 9 ust. 1 RODO, należy przeprowadzić ocenę skutków dla ochrony danych (patrz art. 35 ust. 3 lit. b) RODO. Obowiązek ten mógłby dotyczyć również planowanego przedsięwzięcia.

W szczególności przetwarzanie danych dotyczących zdrowia i pacjentów jako danych wrażliwych stwarza wysokie ryzyko dla ochrony tych danych.

5. Inspektor Ochrony Danych

W przypadku każdego z trzech podmiotów należy sprawdzić, czy istnieje obowiązek powołania inspektora ochrony danych na podstawie przepisów RODO lub UODO.

Obowiązek zgłoszenia wynikający z art. 37 ust. 1 lit. c RODO można rozważyć, jeżeli główna działalność osoby odpowiedzialnej polega między innymi na szeroko zakrojonym przetwarzaniu szczególnych kategorii danych w rozumieniu art. 9 ust.) RODO (np. dane dotyczące zdrowia). Może to mieć zastosowanie w szczególności do szpitali, laboratoriów lub praktyk lekarskich, które przetwarzają dane genetyczne, ale nie do indywidualnych praktyk lekarskich (por. motyw 91, s. 4).

Dla szpitala jako fundacji kościelnej obowiązek powołania inspektora ochrony danych będzie wynikał z ogólnokrajowego i obszarowego rozporządzenia § 36 UODK. Można przyjąć, że w tym wypadku szpital ma już inspektora ochrony danych.

6. Podstawy prawne przetwarzania danych

W związku z planowanym projektem przetwarzanie danych pacjentów jako danych dotyczących zdrowia będzie stanowiło filar oceny dopuszczalności operacji przetwarzania danych pod kątem ochrony danych.
W odniesieniu do obowiązujących podstaw prawnych dla odpowiednich procesów przetwarzania należy sprawdzić, które podstawy prawne mogą mieć zastosowanie.
Zgodnie z treścią punktu VII. właściwą podstawą prawną będzie zgoda pacjenta na przetwarzanie danych dotyczących jego zdrowia. W związku z tym należy zapoznać się i

przestrzegać przepisów UODK aby podmioty w kościelnych formach prawnych uzupełniały lub doprecyzowywały RODO.

Codzienność w systemie opieki zdrowotnej sprawia, że można spodziewać się przypadków, w których pacjent nie będzie mógł złożyć oświadczenia woli spełniającego wymogi skutecznej zgody (np. gdy pacjent jest nieprzytomny). W takich przypadkach brane są pod uwagę przesłanki zgodnie z Art. 9 ust. 2 lit. c) RODO. Wymaga to, aby dana osoba wyraziła zgodę, gdyby mogła. Warunkiem wstępnym przetwarzania danych, o którym mowa w ust. 1, jest zatem zgoda domniemana (por. Paal/Pauly/Frenzel RODO art. 9 ust. 29, z dalszymi odniesieniami). Osoba taka musi być przy tym ze względów fizycznych lub prawnych pozbawiona możliwości wyrażenia zgody (por. Paal/Pauly/Frenzel RODO art. 9 ust. 30).

Innym możliwym przykładem dotyczacym zgody jest Art. 9 (2) (h) RODO. Przetwarzanie danych wrażliwych jest dozwolone, jeżeli jest to niezbędne do celów ochrony zdrowia lub medycyny pracy, oceny zdolności pracownika do pracy, diagnostyki medycznej, opieki lub leczenia w ochronie zdrowia lub administrowania systemami i usługami w sektorze zdrowotnym lub społecznym.

7. Przekazywanie danych osobowych

Ponieważ przesyłanie danych jest formą przetwarzania danych, obowiązują te same zasady przetwarzania danych, o których mowa powyżej (art. 5 RODO), a także wymóg istnienia podstawy prawnej, która pozwala na ich przetwarzanie (art. 6 RODO itp.).

Przekazywanie danych osobowych między przedsiębiorstwami można zasadniczo podzielić na trzy kategorie:

- transmisja wewnątrz firmy lub pomiędzy firmami w grupie
- przekazywanie osobom trzecim
- przekazanie do usługodawcy związanego instrukcjami (podmiot przetwarzający).

Ze względu na brak konkretnej wiedzy na temat struktur, które mają powstać na gruncie prawa spółek, omówione zostaną tutaj tylko poszczególne aspekty przekazywania danych.

a) transmisja pomiędzy podmiotami

- transmisja danych w obrębie podmiotu

Przekazywanie danych pacjentów w ramach jednego podmiotu (np. między różnymi oddziałami szpitala) nie wydaje się być krytyczne w związku z planowanym projektem, o ile odbywa się ono zgodnie z zasadami przetwarzania zgodnie z Art. 5 RODO oraz wymaganym pozwoleniem w rozumieniu Art. 9 ust. 2 RODO W tym kontekście szczególną uwagę należy zwrócić na koncepcję ścisłego uprawmienia. W ramach podmiotu zorganizowanego w kościelną formę prawną należy również przestrzegać § 5 UODL, który reguluje obowiązek zachowania tajemnicy danych.

- Transmisja danych w ramach spółek grupy

Przesyłanie danych w ramach spółek należących do grupy jest bardziej ryzykowne. Ponieważ tego typu transmisja danych nie jest odrębnie uregulowana w RODO, z przepisów RODO nie można wywodzić tzw. przywileju grupowego, z którego wynikałaby ogólna dopuszczalność przesyłania danych w grupie (por. Thüsing, § 16 , pkt 3).

Z motywu 48 wynika jedynie szczególna cecha w odniesieniu do uzasadnionego interesu osoby odpowiedzialnej, który jest częścią grupy przedsiębiorstw lub grupy instytucji. Administratorzy ci mogą mieć prawnie uzasadniony interes w przekazywaniu danych osobowych w ramach grupy spółek do wewnętrznych celów administracyjnych, w tym przetwarzania danych osobowych klientów i pracowników.

W związku z przekazywaniem danych kwestia współodpowiedzialności może ponownie stać się istotna.

Głębsza dyskusja nie jest przedmiotem tej opinii, ponieważ wymaga to posiadania szczegółowej wiedzy w odniesieniu do przyszłej współpracy.

b) Przekazywanie osobom trzecim

Podstawowym pytaniem jest przede wszystkim to, kogo należy uważać za „stronę trzecią" w rozumieniu prawa o ochronie danych.

Definicja prawna Art. 4 nr 10 RODO opisuje stronę trzecią jako osobę fizyczną lub prawną, organ, instytucję lub inny organ, z wyjątkiem osoby, której dane dotyczą, Administratora, podmiotu przetwarzającego i osób, które podlegają bezpośredniej odpowiedzialności Administratora lub podmiotu przetwarzającego upoważnionego do przetwarzania danych osobowych. Przekazywanie danych między Administratorem, a stroną trzecią jest zawsze przekazaniem wymagającym zezwolenia w rozumieniu prawa o ochronie danych (por. Thüsing, § 16, ust. 13).

W szczególności należy rozważyć i sprawdzić przekazywanie danych stronom trzecim z siedzibą poza UE.

c) Forma przekazu

Przy wyborze formy transmisji należy zwrócić szczególną uwagę na ryzyko odpowiedzialności cywilnej, którą w przypadku utraty danych ponosi zasadniczo przekazujący/wysyłający dane.

Jeśli chodzi o różne formy przekazu, to pod uwag brane będą przede wszystkim formy cyfrowego/elektronicznego przekazu, a poczta tradycyjna będzie prawdopodobnie odgrywać rolę podrzędną.

W przypadku wszystkich cyfrowych ścieżek transmisji należy uwzględnić szczególną potrzebę ochrony danych zdrowotnych i zastosować odpowiednie szyfrowanie (zgodnie z aktualnym stanem techniki).

Podczas wysyłania wiadomości E-Mail nie wystarczy zaszyfrowanie wysyłanych załączników, jeśli można dokonać osobistego odniesienia z wiersza tematu lub tekstu E-Mail. W takim przypadku treść wiadomości E-Mail wraz z jej tematem powinna zostać opatrzona pseudonimem w takim stopniu, aby nie można było ustalić osób, których załącznik dotyczy.

Problemy mogą wystąpić przede wszystkim przy transmisji danych faksem, ponieważ największe ryzyko leży po stronie odbiorcy. Co do zasady nie będzie wiadome, z jakiej technologii korzysta odbiorca. W związku z tym co do zasady należy unikać przesyłania danych pacjentów za pomocą faksu.

Korzystając z usług w chmurze lub innych dostawców usług, należy zadbać o to, by byli to dostawcy, którzy działają zgodnie z przepisami RODO, najlepiej z siedzibą główną i lokalizacją serwerów w Niemczech lub przynajmniej w UE.

8. Koncepcje ochrony danych

Każda z zaangażowanych firm powinna mieć koncepcję ochrony danych, która dotyczy nie tylko ich własnej sytuacji biznesowej, ale także uwzględnia szczególną sytuację przetwarzania danym pomiędzy trzema podmiotami.

W szczególności należy uwzględnić koncepcję autoryzacji, która ma być poddana ścisłej ocenie, oraz udokumentować środki techniczne i organizacyjne (TOM), które mają zagwarantować bezpieczeństwo przetwarzania danych. Tzw. TOM mają być rejestrowane w rejestrach przetwarzania.

IX. Pytania i punkty do wyjaśnienia

Istotne kwestią pozostaje wyjaśnienie następujących zagadnień:

Jaka jest struktura odpowiedzialności między podmiotami (słowo kluczowe: wspólnie – ochrona danych – odpowiedzialność)? Jak zaprojektowane są struktury prawne między uczestnikami?
Jakie konkretne procesy przetwarzania danych osobowych są szczegółowo planowane?
Jakie cele przetwarzania są możliwe w ramach przetwarzania?
Określenie celów przetwarzania (Ważne: Samo istnienie podstawy prawnej przetwarzania danych nie oznacza, że cel został określony. Określenie celu to niejako „więcej” niż wymóg dotyczący podstawy przetwarzania.)
W jakiej formie powinien odbywać się głównie planowany transfer danych? Czy stosowane są już techniki szyfrowania? Jakie oprogramowanie powinno lub jest już używane? Czy w tym kontekście planowane są rozwiązania chmurowe?

Czy zaangażowane strony muszą wyznaczyć inspektora ochrony danych? Jeśli tak, czy można rozważyć powołanie wspólnego inspektora ochrony danych do nadzorowania całego projektu?

X. Wnioski

Reasumując, istnieje wiele podstaw prawnych ochrony danych, których należy przestrzegać, choć nie należy spodziewać się przeszkód, które całkowicie uniemożliwiłyby procesy przetwarzania danych w związku z planowanym projektem.
W tej mieszanej sytuacji wskazane będzie stosowanie jak najostrzejszych podstaw prawnych w zakresie przetwarzania danych osobowych, zwłaszcza danych dotyczących zdrowia, jak i samego pacjenta, jako standardu legalności procesów przetwarzania.

Benjamin Ehlers
Rechtsanwalt