KANCELARIA PREZESA RADY MINISTRÓW MINISTER –
CZŁONEK RADY MINISTRÓW

Michał Dworczyk

COA.WK.583.14.2019.NM

Warszawa, czerwca 2020 r.

Pan
Bartłomiej Chmielowiec

Rzecznik Praw Pacjenta

WYSTĄPIENIE POKONTROLNE

Przedstawiam Panu Ministrowi *Wystąpienie pokontrolne* (dalej: *Wystąpienie*) z kontroli przeprowadzonej[1] przez Kancelarię Prezesa Rady Ministrów w Biurze Rzecznika Praw Pacjenta[2] (dalej: BRPP, Biuro, Urząd lub jednostka) w zakresie *wybranych aspektów funkcjonowania Biura w latach 2018-2019 w związku z wejściem w życie rozporządzenia ws. ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO) oraz ustawy o ochronie danych osobowych (uodo).*

Podstawa prawna:
Art. 46 i 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[3] (dalej: *ustawa o kontroli*).

OTOCZENIE PRAWNE

W dniu 25 maja 2016 r. weszło w życie rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO). Do tego czasu podstawowym aktem prawnym regulującym kwestie ochrony danych osobowych w Unii Europejskiej była wydana ponad 20 lat wcześniej dyrektywa 95/46/WE[4]. W tym czasie globalizacja i postęp technologiczny istotnie zmieniły możliwości i metody przetwarzania danych osobowych, a skala ich wykorzystywania znacząco wzrosła. Wiązało się to także z licznymi ryzykami nadużyć i nieprawidłowości.

Okoliczności te spowodowały potrzebę zmiany modelu regulacji w zakresie ochrony danych osobowych. Podstawowym celem RODO było zagwarantowanie skuteczności tego systemu w zmieniającym się środowisku technologicznym, organizacyjnym i gospodarczym. Rozpoczęcie stosowania tego aktu 25 maja 2018 r. zmieniło zasady przetwarzania danych, zapewniając jednolity, spójny, efektywny i nowoczesny system ochrony danych na terenie Unii Europejskiej.

---

[1] Kontrolę przeprowadzili pracownicy Kancelarii Prezesa Rady Ministrów: Natalia Mikielska, główny specjalista, kierownik zespołu kontrolującego, Aneta Uśniacka, główny specjalista, członek zespołu kontrolującego oraz Roman Wójtowicz, główny specjalista, członek zespołu kontrolującego. Czynności kontrolne przeprowadzono od 5 grudnia 2019 r. do 31 stycznia 2020 r., w siedzibie Biura Rzecznika Praw Pacjenta w Warszawie, przy ul. Młynarskiej 46.

[2] BRPP działa na podst. ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz. U. z 2019 r., poz. 1127 t.j., ze zm.) – dalej: *ustawa o RPP*, zarządzenia Nr 3 Prezesa Rady Ministrów z 5 stycznia 2018 r. w sprawie nadania statutu BRPP (M.P. z 2018 r., poz. 53) oraz zarządzenia nr 1/2018 Rzecznika Praw Pacjenta z 12 stycznia 2018 r. w sprawie nadania Regulaminu organizacyjnego dla BRPP (ze zm.). Rzecznik jest centralnym organem administracji rządowej właściwym w sprawach ochrony praw pacjentów określonych w *ustawie o RPP* oraz w przepisach odrębnych. Do zakresu działania Rzecznika należy m.in.: prowadzenie postępowań wyjaśniających ws. dot. naruszeń praw pacjenta, prowadzenie postępowań ws. praktyk naruszających zbiorowe prawa pacjentów, ochrona praw pacjentów korzystających ze świadczeń zdrowotnych udzielanych przez szpital psychiatryczny, udział w sprawach cywilnych dot. naruszenia praw pacjenta, analiza skarg pacjentów w celu określenia zagrożeń i obszarów w systemie ochrony zdrowia wymagających naprawy. Rzecznik dysponuje uprawnieniem do przetwarzania danych osobowych, w tym szczególnej kategorii, niezbędnych do realizacji ustawowych zadań, przy zapewnieniu zabezpieczeń zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu danych (art. 47a *ustawy o RPP*).

[3] Dz. U. z 2020 r., poz. 224 t. j.

[4] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. ws. ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

RODO ustanowiło ogólne zasady ochrony danych osobowych, bez określenia szczegółowych metod i środków, które służyłyby ich realizacji. Zgodnie z zasadą rozliczalności to Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO. Musi on przy tym uwzględnić charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze.

Ponadto wspomniana regulacja wprowadziła instytucje prawne dotąd nieznane polskiemu sektorowi ochrony danych, zmodyfikowała poprzednio obowiązujące rozwiązania oraz przyjęła normy prawne zawierające wiele zwrotów niedookreślonych i klauzul generalnych, które wymagały wykładni. Z tego powodu rozpoczęcie stosowania RODO stanowiło duże wyzwanie dla wszystkich, których prawa i obowiązki akt ten uregulował[5]. Zarówno przed rozpoczęciem stosowania przepisów rozporządzenia, jak w późniejszym czasie w przestrzeni publicznej wyrażano wątpliwości dotyczące sposobu wywiązywania się z nałożonych na Administratorów obowiązków[6]. Choć rozporządzenie przewiduje wydawanie wytycznych i wskazówek zarówno na poziomie europejskim (przez Europejską Radę Ochrony Danych), jak i krajowym (przez Prezesa Urzędu Ochrony Danych Osobowych), to termin publikacji części z nich utrudniał odpowiednie przygotowanie jednostek do rozpoczęcia stosowania RODO[7].

Zmiana regulacji wpłynęła na sposób funkcjonowania niemal wszystkich podmiotów przetwarzających dane osobowe, zarówno prywatnych, jak i publicznych. W sektorze publicznym przetwarzanie danych osobowych co do zasady jest uprawnione w zakresie niezbędnym do wykonywania zadań państwa, realizacji uprawnień obywateli i sprawowania władzy publicznej w oparciu o przepisy prawa powszechnie obowiązującego. Z tego względu stosowaniu rozporządzenia nie sprzyjało zmieniające się otoczenie prawne, w tym związane z wejściem w życie tzw. ustawy wdrażającej RODO[8]. Wprowadziła ona zmiany w 162 ustawach z różnych obszarów, w tym z dziedziny prawa pracy i postępowania administracyjnego. Wymusiło to weryfikację oraz niejednokrotnie zmianę przyjętych przez Administratorów rozwiązań dotyczących w szczególności podstaw prawnych i zakresu przetwarzania danych[9].

Nowy model ochrony danych osobowych zabezpieczono istotnymi sankcjami, obejmującymi w szczególności administracyjne kary pieniężne, odpowiedzialność karną i cywilną. Górny limit kar pieniężnych dla jednostek sektora finansów publicznych wynosi do 100 tys. zł. Wyższe kary dla innych podmiotów przewiduje RODO, a mianowicie do 20 mln euro, a w przypadku przedsiębiorstw – do 4% ich całkowitego rocznego światowego obrotu. Dla zapewnienia skuteczności systemu ochrony danych osobowych ustawa o ochronie danych osobowych (uodo) przewidziała, w ramach odpowiedzialności karnej, w najwyższym wymiarze karę do 3 lat pozbawienia wolności. Wspomniane konsekwencje świadczą o znaczeniu ochrony danych i istotnie wzmacniają stosowanie nowych regulacji.

[5] *Wykonywanie obowiązków ABI, przyszłego inspektora ochrony danych, w świetle ogólnego rozporządzenia o ochronie danych*. Biuro GIODO, Warszawa, 2016 r.
[6] Np. wg badania EY przeprowadzonego wśród przedsiębiorców po roku od rozpoczęcia stosowania RODO dla większości z badanych (68%) przedsiębiorców i pracowników firm zaangażowanych we wdrażanie RODO przepisy były niejasne (Raport EY, *Rok z RODO. Stosowanie RODO w firmach – szanse i zagrożenia*, maj 2019 r.).
[7] Np. *Poradnik RODO dla pracodawców* opublikowano 4 października 2018 r. (https://uodo.gov.pl/pl/383/545).
[8] Ustawa z 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. z 2019 r., poz. 730).
[9] https://www.infor.pl/prawo/prawa-konsumenta/prawa-konsumenta/3584779,RODO-podsumowanie-2019-roku.html

OCENA KONTROLOWANEGO OBSZARU

W dniu rozpoczęcia stosowania RODO (25 maja 2018 r.) Biuro w znacznym zakresie było przygotowane do realizacji nowych zasad ochrony danych osobowych, pomimo obiektywnych trudności związanych ze zmieniającym się otoczeniem prawnym oraz nieugruntowaną praktyką w tym obszarze. W szczególności zaktualizowano dokumentację dot. zasad przetwarzania danych, zidentyfikowano procesy, w których dane są przetwarzane, przygotowano rejestr czynności przetwarzania (dalej: *Rejestr czynności*), opracowano klauzule informacyjne, przeprowadzono inwentaryzację umów cywilnoprawnych w zakresie powierzenia danych. Administratorowi Bezpieczeństwa Informacji powierzono funkcję Inspektora Ochrony Danych (dalej: IOD), a pracownikom zapewniono różne formy szkoleniowe w zakresie zmieniających się przepisów prawa. Ponadto obszar ochrony danych objęto audytami wewnętrznymi. Działania te sprzyjały prawidłowemu i bezpiecznemu przetwarzaniu danych w Urzędzie. Zapewnienie zgodności z przepisami RODO wymaga jednak stałego doskonalenia. Przyjęty w Biurze system ochrony danych po 1,5 roku od jego wdrożenia należy wzmocnić w celu zapewnienia kompleksowej i spójnej ochrony danych.

System ochrony danych osobowych w BRPP po 1,5 roku od rozpoczęcia stosowania RODO

- **[Inspektor Ochrony Danych]** Pozytywnie należy ocenić, że Rzecznik Praw Pacjenta (dalej: Rzecznik) zapewnił warunki dla prawidłowego i niezależnego wykonywania zadań przez Inspektora Ochrony Danych. O powołaniu i odwołaniu osób pełniących tę funkcję terminowo powiadamiano PUODO. Stopniowa realizacja opracowanego przez Inspektora planu (dalej: *Plan IOD*) służyła wzmocnieniu badanego obszaru. System ochrony danych powinien jednak w większym zakresie przewidywać realizację zadań Administratora przez wybranych pracowników Urzędu.
- **[zarządzanie ryzykiem]** Przeprowadzono analizę ryzyka obejmującą wszystkie procesy, w których przetwarzano dane osobowe. Nie stanowiła ona jednak punktu wyjścia dla przyjętych środków ochrony danych, ponieważ dokonano jej dopiero w 2019 r.
- **[rejestr czynności przetwarzania]** W Urzędzie prowadzono *Rejestr czynności,* obejmujący wszystkie procesy, w których dochodziło do przetwarzania danych. Dokonywano również jego przeglądów, jednak nie wyeliminowały one nieprawidłowości w *Rejestrze*, tj. niepełnych lub błędnych informacji.
- **[szkolenia]** Prawidłowo zarządzano wiedzą w zakresie ochrony danych. Pracownikom zapewniono różne formy szkoleniowe oraz dostęp do materiałów zwiększających znajomość zasad ochrony danych.
- **[upoważnienia]** Pracownicy posiadali upoważnienia do przetwarzania danych, jednak podstawa prawna większości z nich była nieprawidłowa. Rzecznik zapewnił przetwarzanie danych przez osoby upoważnione w 89% badanych przypadków (40 z 45 upoważnień). W pozostałym zakresie 4 wolontariuszy nie posiadało ważnego na dany rok upoważnienia, a 1 z upoważnień zostało wydane przez osobę nieuprawnioną. Ponadto prowadzone ewidencje upoważnień zawierały nieprawidłowe dane.
- **[powierzanie przetwarzania danych]** Powierzenie przetwarzania danych osobowych podmiotom zewnętrznym w większości (13 z 16 wymagających tego przypadków, tj. 81%) odbywało się na podstawie umów. Dokumenty te nie w pełni regulowały wymagane prawem warunki. W 3 przypadkach dot. konsultacji medycznych zastrzeżenia budzi powierzenie przetwarzania danych wyłącznie na podstawie upoważnienia. Umowy powierzenia były ewidencjonowane, ale rejestr obejmował tylko 62% z nich (8 z 13).

- **[klauzule informacyjne]** BRPP opracowało i stosowało klauzule informacyjne, które zawierały większość informacji określonych przepisami prawa. Sformułowano je jasnym i prostym językiem. Dokumenty te wymagają jednak uzupełnienia i uporządkowania.
- **[realizacja obowiązku informacyjnego]** W większości (87%) prawidłowo wywiązywano się z obowiązku informacyjnego w ramach ustawowych kompetencji Rzecznika, jak również w ramach zgody podmiotu danych (84%). Zastrzeżenia w tym zakresie dotyczą w szczególności nieprzekazania lub nieprawidłowego przekazania klauzuli informacyjnej uczestnikom konferencji oraz sformułowania nieprawidłowej treści zgody na przetwarzanie danych w ramach konkursu. Ponadto w Urzędzie przechowywano aplikacje kandydatów do pracy z 1 naboru o rok dłużej niż było to konieczne.
- **[realizacja praw podmiotów danych]** BRPP w 88% przypadków terminowo załatwiało wnioski podmiotów danych. Zastrzeżenia budzi udzielanie odpowiedzi na wnioski przez osoby działające bez upoważnienia, co było niezgodne z regulacjami wewnętrznymi.
- **[naruszenia ochrony]** Dokumentowano i ewidencjonowano zdarzenia dot. naruszeń ochrony danych. Nie stwierdzono przypadków wymagających zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych. Pozytywnie należy ocenić, że opracowano i udostępniono pracownikom *Dobre praktyki w zakresie troski o ochronę danych osobowych*. Zastrzeżenia budzi jednak, że w Urzędzie nie określono kiedy i przez kogo następuje stwierdzenie naruszenia ochrony danych, co utrudnia obliczanie terminu. W 3 przypadkach (z 10 badanych) nieprawidłowo zakwalifikowano incydenty jako zdarzenia niestanowiące naruszenia ochrony danych.
- **[dokumentacja przetwarzania]** Regulacje wewnętrzne normowały najważniejsze kwestie dotyczące ochrony danych, jednakże wymagają one doskonalenia w celu wyeliminowania braków i nieścisłości. Konieczne jest zintensyfikowanie prac nad przyjęciem nowych regulacji wewnętrznych, w szczególności, że słabości w procedurach zidentyfikowano w ramach audytów wewnętrznych i *Planu IOD*.
- **[audyty wewnętrzne]** Pozytywnie należy ocenić przeprowadzenie zarówno w 2018 r., jak i w 2019 r. zadań audytowych w zakresie ochrony danych osobowych. Stanowiły one niezależne źródło informacji dla Rzecznika o słabościach systemu kontroli zarządczej w badanym obszarze.

Wykaz skrótów, skrótowców i pojęć używanych w dokumencie:

Administrator – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

Administrator Bezpieczeństwa Informacji lub **ABI** – przed rozpoczęciem stosowania RODO podmiot powoływany przez Administratora w celu zapewniania przestrzegania przepisów o ochronie danych osobowych; od 25 maja 2018 r. jego miejsce zajął Inspektor Ochrony Danych;

czynności przetwarzania danych – zespół powiązanych ze sobą operacji (takich jak zbieranie, przechowywanie, modyfikowanie, przeglądanie), które można określić w sposób zbiorczy w związku z celem, w jakim te czynności są podejmowane (np. rekrutacja pracowników, zamówienia publiczne);

dane – dane osobowe;

dane szczególnej kategorii – dane *wrażliwe*, które podlegają szczególnym zasadom przetwarzania i ochrony, np. dotyczące zdrowia;

DG – Dyrektor Generalny BRPP;

DPIA – ocena skutków dla ochrony danych osobowych;

Grupa Robocza Art. 29 – Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych,

powierzenie przetwarzania danych – umocowanie przez Administratora innego podmiotu do przetwarzania danych osobowych w jego imieniu; przy powierzeniu danych o sposobie i celach ich przetwarzania decyduje Administrator, a nie podmiot przetwarzający;

przetwarzanie danych – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych, taka 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;

PUODO lub **organ nadzoru** – Prezes Urzędu Ochrony Danych Osobowych;

rejestr czynności – rejestr procesów przetwarzania danych osobowych, o którym mowa w art. 30 RODO. Obejmuje on najistotniejsze informacje dot. wskazanych procesów, np. cele przetwarzania, kategorie osób, danych osobowych oraz odbiorców. Za jego prowadzenie odpowiada Administrator;

RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. ws. ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz

powołana[10] jako niezależny europejski organ doradczy. Grupa ta została rozwiązana 25 maja 2018 r., a w jej miejsce powstała Europejska Rada Ochrony Danych;

IOD lub **Inspektor** – Inspektor Ochrony Danych, o którym mowa w art. 37 RODO, odpowiadający w szczególności za doradzanie Administratorowi i monitorowanie przestrzegania RODO w jednostce;

naruszenie ochrony danych – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

okres retencji – okres przechowywania danych nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;

podmiot danych – osoba, której dotyczą dane;

podmiot przetwarzający lub **procesor** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

uchylenia dyrektywy 95/46/WE[11];

ryzyko pierwotne – ryzyko przed podjęciem jakiegokolwiek działania w celu jego ograniczenia do poziomu akceptowalnego;

udostępnienie danych – przekazanie danych innemu Administratorowi; przy udostępnieniu danych o sposobie i celach ich przetwarzania decyduje Administrator, któremu dane przekazano;

substytucja – dalsze pełnomocnictwo do działania w imieniu mocodawcy, udzielone przez pełnomocnika mocodawcy;

substytut – dalszy pełnomocnik; osoba, której udzielono substytucji;

uodo – ustawa z 10 maja 2018 r. o ochronie danych osobowych[12];

upoważnienie do przetwarzania danych lub **upoważnienie** – dokument potwierdzający, że przetwarzanie danych odbywa się wyłącznie na polecenie Administratora.

OCENY I USTALENIA SZCZEGÓŁOWE

Przygotowanie Urzędu do wdrożenia RODO

1. Biuro było w znacznym zakresie przygotowane na rozpoczęcie stosowania z dniem 25 maja 2018 r. nowych zasad ochrony danych osobowych[13], mimo niesprzyjających okoliczności związanych ze zmieniającym się otoczeniem prawnym oraz kształtującą się praktyką w tym zakresie. BRPP posiadało system zarządzania bezpieczeństwem ochrony danych[14], na który składała się Polityka Bezpieczeństwa Danych Osobowych[15] (dalej: *Polityka BDO*) oraz Instrukcja Zarządzania Systemem Informatycznym[16] (dalej: *Instrukcja ZSI*). Dokumenty te regulowały najważniejsze zagadnienia[17]. W *Polityce BDO* unormowano najistotniejsze funkcje i zadania, tj. Administratora i IOD oraz pozostałych osób uczestniczących w procesie przetwarzania danych, jak również kwestie ich odpowiedzialności. W *Instrukcji ZSI* zawarto z kolei zasady oraz procedury zarządzania i administrowania systemami informatycznymi służącymi do przetwarzania danych[18].

W związku z rozpoczęciem stosowania RODO zaktualizowano dokumentację dot. zasad przetwarzania danych, na którą składała się w szczególności[19] *Polityka BDO* i *Instrukcja ZSI*[20]. W dokumentacji przewidziano najistotniejsze funkcje i zadania, procedury postępowania oraz narzędzia systemowe, takie jak rejestry i ewidencje służące zarządzaniu badanym obszarem.

W *Polityce BDO* ujęto zadania Administratora[21] wynikające z przepisów prawa dot. ochrony danych oraz kompetencje IOD – z wyjątkiem zadania pełnienia funkcji punktu kontaktowego dla organu nadzorczego (art. 39 ust. 1 lit. e RODO). Wyjaśniono[22], że powodem było przeoczenie, co nie wpływa jednak na zakres obowiązków IOD, ponieważ zadanie to wynika wprost z RODO. W procedurach ujęto także zadania i odpowiedzialności pozostałych osób, w tym Administratora Systemów Informatycznych, kierowników komórek, jak również wszystkich osób przetwarzających dane na polecenie Rzecznika.

---

[10] Na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w spr. ochrony osób fiz. w zakresie przetwarzania danych os. i swobodnego przepływu tych danych.
[11] Dz. Urz. UE L 119 z 4 maja 2016 r., str. 1 oraz Dz. Urz. UE L 127 z 23 maja 2018 r., str. 2.
[12] Dz.U. z 2019 r. poz. 1781 t. j.
[13] Uregulowanych w RODO i uodo.
[14] Zarządzenie nr 16/2018 Rzecznika Praw Pacjenta z 24 maja 2018 r. w sprawie wprowadzenia *Polityki Bezpieczeństwa Danych Osobowych w Biurze Rzecznika Praw Pacjenta, Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Biurze Rzecznika Praw Pacjenta oraz powołania IODO i wyznaczenia ASI* (dalej: *zarządzenie nr 16/2018*).
[15] Załącznik nr 1 do *zarządzenia nr 16/2018 – Polityka Bezpieczeństwa Danych Osobowych w Biurze Rzecznika Praw Pacjenta*.
[16] Załącznik nr 2 do *zarządzenia nr 16/2018 – Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Biurze Rzecznika Praw Pacjenta*.
[17] Podstawy prawne i zakres przetwarzanych danych, zarządzanie przetwarzaniem i bezpieczeństwem danych, zarządzanie uprawnieniami osób, zasady przetwarzania danych (w tym m.in. realizacji obowiązków informacyjnych; prowadzenia *Rejestru czynności*; realizacji praw osób, których dane dotyczą; powierzania i udostępniania danych innym podmiotom; zasady ochrony pomieszczeń oraz przetwarzania danych poza obszarem przetwarzania); formy przetwarzania danych; postępowanie w sytuacji podejrzenia bądź stwierdzenia naruszenia bezpieczeństwa danych.
[18] Procedury nadawania uprawnień do przetwarzania danych, stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem, zasady pracy użytkowników, tworzenie i przechowywanie kopii zapasowych, zasady przechowywania nośników zewnętrznych oraz kopii zapasowych, stosowane środki ochrony systemu, realizacji wymogów dot. rozliczalności operacji na danych osobowych, rejestrowanie zdarzeń w systemach i sieciach teleinformatycznych, a także procedury wykonywania napraw, przeglądów i konserwacji systemów oraz nośników danych.
[19] Szczegółowe regulacje dot. danych osobowych w poszczególnych procesach ujęto w odrębnych aktach wewnętrznych, tj. zarządzeniu Rzecznika Praw Pacjenta nr 25/2018 z 7 grudnia 2018 r. ws. określenia sposobu funkcjonowania infolinii (...) oraz zarządzeniu DG nr 32/2017 z 12 grudnia 2017 r. ws. wprowadzenia Regulaminu pracy (ze zm.).
[20] Przed wejściem w życie *zarządzenia nr 16/2018* obowiązywały zarządzenia nr 1/2016 Rzecznika Praw Pacjenta z 18 stycznia 2016 r. i nr 13/2018 z 13 kwietnia 2018 r.
[21] Zgodnie z § 6 pkt 17 *Polityki BDO* zadania Administratora są realizowane przez niego samodzielnie lub za pośrednictwem pracowników, zgodnie z kompetencjami określonymi w *Polityce* i odrębnych aktach wewnętrznych, czego przykładem były upoważnienia do wydawania upoważnień do przetwarzania danych.
[22] Pismo DG z 27 stycznia 2020 r., znak: RzPP-ODO.091.1.15.2019.

2. Przed rozpoczęciem stosowania RODO w Urzędzie zidentyfikowano procesy, w których dochodziło do przetwarzania danych. W efekcie przygotowano *Rejestr czynności* oparty na wzorze GIODO[23] oraz opracowano podstawowe klauzule informacyjne.

ABI we współpracy z kierownikami komórek organizacyjnych zidentyfikował procesy przetwarzania danych, a następnie utworzono *Rejestr czynności*. Dokonano inwentaryzacji umów, w ramach których dochodziło do przetwarzania danych, co nie zostało jednak udokumentowane. W Biurze nie stwierdzono przypadków przetwarzania danych bez podstawy prawnej albo niezgodnie z celami, dla których dane zostały zebrane. Przygotowano podstawowe klauzule informacyjne, które umieszczono w Internecie oraz przekazano pracownikom do stosowania. Przegląd przetwarzanych danych nie wykazał konieczności przekazania klauzul informacyjnych osobom, których dane pozyskano przed 25 maja 2018 r.

3. Rzecznik wywiązał się z obowiązku powołania Inspektora Ochrony Danych, tj. z dniem 25 maja 2018 r. funkcję tę powierzono dotychczasowemu Administratorowi Bezpieczeństwa Informacji. IOD umożliwiono wykonywanie obowiązków w sposób niezależny, niepowodujący ryzyka konfliktu interesów[24].

W strukturze organizacyjnej Urzędu od 1 stycznia 2018 r. przewidziano *samodzielne stanowisko ds. ochrony danych osobowych oraz realizacji innych określonych zadań*, które podlegało bezpośrednio Rzecznikowi Praw Pacjenta. W regulaminie organizacyjnym przewidziano, że do wspomnianego stanowiska stosuje się odpowiednio przepisy dot. komórek organizacyjnych, a do osoby pracującej na tym stanowisku – dyrektora. Osobie tej powierzono najpierw funkcję ABI, a od 25 maja 2018 r. – IOD.

4. Wszystkich pracowników zapoznano z obowiązującymi zasadami dot. ochrony danych, w szczególności poprzez szkolenia wewnętrzne i e-learning.

Pracownikom zapewniono wiedzę w zakresie zmian wynikających z RODO. Wszyscy zostali zapoznani ze zaktualizowaną *Polityką BDO* i *Instrukcją ZSI* oraz zobowiązani do ukończenia kursu dot. RODO dostępnego w systemie e-learningowym służby cywilnej[25]. IOD przeprowadził szkolenia wewnętrzne:

- dla Rzeczników Praw Pacjenta Szpitala Psychiatrycznego (dalej: RzPPSzP) – 13 kwietnia 2018 r.; w szkoleniu wzięło udział Kierownictwo BRPP;
- dla pracowników Urzędu – 7-8 czerwca 2018 r. (przeszkolono 71 z 90 zatrudnionych osób).

Wyjaśniono, że wcześniej pracownikom zapewniono wiedzę w ramach aktualizacji *Polityki BDO*. Ponadto DG oraz dwójka pracowników przed rozpoczęciem stosowania RODO uczestniczyli w szkoleniach zewnętrznych dot. nowego prawa ochrony danych osobowych.

5. Ochrona danych osobowych była przedmiotem audytów wewnętrznych prowadzonych w Urzędzie. Ponadto w ramach kontroli zarządczej uwzględniano ryzyka w tym zakresie, jednakże nie dokumentowano podejmowanych czynności.

W 2018 r. zrealizowano planowe zadanie audytowe dot. dostosowania BRPP do przepisów RODO. Audytor wykazał w nim, że do pełnej zgodności we wspomnianym zakresie wymagane jest podjęcie kilku rekomendowanych przez niego działań takich jak: wykonanie zoptymalizowanej analizy ryzyka oraz zaktualizowanie dokumentacji i rejestru czynności Zrealizowano również czynności sprawdzające dot. wydanych w 2017 r. rekomendacji w zakresie przetwarzania danych. Wyjaśniono, że zagrożenia w poszczególnych obszarach przetwarzania danych analizowane były w ramach kontroli zarządczej, co nie zostało jednak udokumentowane.

Stan wdrożenia RODO po 1,5 roku jego stosowania

6. **[Inspektor Ochrony Danych]** Rzecznik zapewnił funkcjonowanie IOD oraz umożliwił wykonywanie mu zadań w sposób niezależny[26]. Nie stwierdzono konfliktu interesów w ramach sprawowania jego funkcji[27]. Zagwarantowano ciągłość realizacji zadań IOD,

[23] GIODO 4 kwietnia 2018 r. opublikował wyjaśnienia i wskazówki dotyczące sposobu realizacji obowiązku prowadzenia rejestru czynności: https://archiwum.giodo.gov.pl/pl/1520281/10449.
[24] Zgodnie z art. 37 ust. 1 lit. a RODO, art. 9 pkt 1 uodo oraz art. 38 ust. 3 i 6 RODO.
[25] Kurs pn. *Przygotowanie do wdrożenia ogólnego rozporządzenia o ochronie danych osobowych (RODO).*
[26] Zgodnie z art. 37 ust. 1 lit. a RODO, art. 9 pkt 1 uodo oraz art. 38 ust. 3 RODO.
[27] Zgodnie z art. 38 ust. 6 RODO.

jednak efektywności działania obszaru ochrony danych nie sprzyjała czterokrotna zmiana osób pełniących tę funkcję. O zmianach terminowo[28] powiadamiano PUODO.

W kontrolowanym okresie funkcję IOD pełniły 4 osoby, w tym 3 pracowników[29] i 1 wykonawca zewnętrzny, świadczący usługi w okresie od 4 marca 2019 r. do czasu prowadzenia kontroli. Zmiany wynikały z odejścia z pracy albo długotrwałej nieobecności pracowników. Inspektorom zapewniono niezależność, która, zgodnie z art. 38 ust. 3 RODO, polegała na bezpośredniej podległości Rzecznikowi, braku instrukcji, jak również kar lub odwołania ze sprawowania funkcji. Choć Inspektorzy wykonywali także inne zadania (np. zw. z informatyzacją służby zdrowia), nie stwierdzono, aby wystąpił w tym zakresie konflikt interesów. W szczególności żaden z IOD nie zajmował stanowiska związanego z określaniem celów i sposobów przetwarzania danych[30]. Rzecznik pisemnie wyznaczał i odwoływał Inspektorów, o czym terminowo zawiadamiano PUODO[31].

7. IOD, sprawujący funkcję podczas kontroli KPRM, gwarantował poufność realizacji zadań, dysponował fachową wiedzą w dziedzinie ochrony danych oraz posiadał odpowiednie umiejętności do pełnienia powierzonej mu funkcji[32]. Zapewniono mu zasoby do wykonywania zadań oraz możliwość skutecznego, właściwego i niezwłocznego włączenia się we wszystkie procesy przetwarzania danych w jednostce[33]. W celu wsparcia IOD od 1 lutego 2019 r. w Urzędzie funkcjonował Zespół ds. Ochrony Danych Osobowych (dalej: *Zespół ODO*), jednak nie był on efektywnie wykorzystywany. System ochrony danych powinien w większym zakresie przewidywać realizację zadań Administratora przez jego pracowników. W szczególności, kiedy funkcję IOD powierzono wykonawcy zewnętrznemu.

Funkcję IOD w czasie prowadzenia kontroli sprawował od 4 marca 2019 r. wykonawca zewnętrzny na podstawie umowy o świadczenie usług. Rozwiązanie to przyjęto, ponieważ – jak wyjaśniono[34] – skala zadań realizowanych przez pracowników kompetentnych w tym zakresie uniemożliwiałaby pełnienie funkcji IOD w sposób należyty. Inspektor, który był radcą prawnym, posiadał wiedzę z zakresu ochrony danych osobowych, technologii informatycznych oraz służby zdrowia.

Z dniem 1 lutego 2019 r. powołano *Zespół ODO,* w skład którego oprócz IOD (przewodniczącego) wchodziło 2 pracowników Urzędu (członkowie zespołu). Wyznaczono ich ze względu na wiedzę z zakresu działań organizacyjnych i technicznych Biura oraz w dziedzinie ochrony praw pacjentów. Zakres zadań zespołu określono zarządzeniem Rzecznika[35], jednak jego członkowie nie mieli na stałe przypisanych obowiązków. W praktyce zadaniem członków zespołu było bieżące wsparcie IOD, m.in. w zakresie okresowej oceny zagrożeń ochrony danych, zarządzania w razie podejrzenia naruszenia ochrony danych oraz wypracowywania wniosków i propozycji dot. skutecznej ochrony danych. Członkowie *Zespołu ODO* nie prowadzili szkoleń ani nie wydawali upoważnień do przetwarzania danych, choć zadania te wynikały z zarządzenia dot. *Zespołu ODO*.

Zgodnie z zasadą rozliczalności określoną w art. 5 ust. 2 RODO, Administrator jest odpowiedzialny za zapewnienie zgodności z przepisami o ochronie danych i musi być w stanie to wykazać. IOD natomiast co do zasady powinien doradzać i monitorować wykonywanie tych obowiązków. Z tego względu należy poddać analizie zakres powierzonych przez Administratora zadań i rozważyć wzmocnienie roli *Zespołu ODO*. Takie działanie służyć będzie zapewnieniu prawidłowego funkcjonowania badanego obszaru, w tym ciągłości i terminowości realizacji zadań.

[28] Stosownie do art. 10 ust. 1, 3 i 6 oraz 158 ust. 1 uodo.
[29] W okresie od 25 maja 2018 r. do 4 marca 2019 r.
[30] *Wytyczne dotyczące inspektorów ochrony danych ('DPO')*, opracowane przez Grupę Roboczą Art. 29.
[31] W przypadku pierwszego IOD – osoby uprzednio pełniącej funkcję ABI – odwołano ją przed wymaganym terminem powiadomienia PUODO, stosownie do art. 158 ust. 1 uodo.
[32] Zgodnie z art. 37 ust. 5 i art. 38 ust. 5 RODO.
[33] Zgodnie z art. 38 ust. 1-2 RODO.
[34] Pismo DG z 20 grudnia 2019 r., znak: RzPP-ODO.091.1.4.2019.
[35] Zarządzenie nr 3/2019 Rzecznika Praw Pacjenta z 28 stycznia 2019 r. w sprawie określenia trybu funkcjonowania, zadań oraz sposobu wyznaczania członków *Zespołu ODO*.

8. Pozytywnie należy ocenić, że IOD w 2019 r. przeprowadził analizę dot. ochrony danych oraz opracował plan zadań. Zidentyfikowanie głównych obszarów wymagających poprawy oraz stopniowa realizacja *Planu IOD* służyły wzmocnieniu systemu przetwarzania danych w Urzędzie.

14 sierpnia 2019 r. Inspektor opracował, a Rzecznik zaakceptował, plan działań dot. organizacji systemu przetwarzania danych. *Plan IOD* uwzględniał najważniejsze zagadnienia w badanym obszarze. Realizację *Planu* przewidziano na okres od sierpnia 2019 r. do lutego 2020 r. Do 31 stycznia 2020 r. wykonano w całości 3 z 8 zadań, w tym przeprowadzono analizę ryzyka, i opracowano regulamin monitoringu. Do wykonania pozostało m.in. zakończenie prac nad przygotowanym w październiku 2019 r. projektem nowej *Polityki BDO*, wydanie nowych upoważnień i przeszkolenie pracowników (planowano na grudzień 2019 r., termin przesunięto na luty 2020 r.) oraz przeprowadzenie postępowań sprawdzających (planowano na styczeń-luty 2020 r.). Opóźnienia w realizacji *Planu* wynikały z realizacji innych zadań przez IOD.

9. Dane kontaktowe IOD były łatwo dostępne na stronie BIP Urzędu, choć nie zaktualizowano informacji w zakresie organizacji i rejestrów dotyczących danych osobowych. Nastąpiło to po zakończeniu badań kontrolnych.

Zapewniono łatwy dostęp do danych kontaktowych Inspektora zarówno w systemie wewnętrznym – dla pracowników, jak i w BIP Urzędu. Natomiast na stronie internetowej nie zaktualizowano informacji w zakresie organizacji i rejestrów dot. danych osobowych[36]. Wskazywały one, że w Urzędzie dalej funkcjonuje zlikwidowane 5 listopada 2018 r.[37] stanowisko ds. ochrony danych, które odpowiadało m.in. za rejestr zbiorów danych osobowych. Zmianę informacji uwzględniono w ramach planowanego uruchomienia nowej strony internetowej.

10. [analiza ryzyka naruszenia praw i wolności osób] Zastrzeżenia budzi, że analiza ryzyka dedykowana ochronie danych osobowych, która powinna być punktem wyjścia do przyjęcia właściwych środków ochrony, została po raz pierwszy przeprowadzona po 16 miesiącach od rozpoczęcia stosowania RODO, tj. w październiku 2019 r. Wyniki tej analizy nie zostały zatwierdzone przez Administratora, co nie sprzyjało realizacji zasady rozliczalności. Pozytywnie natomiast należy ocenić oszacowanie ryzyka z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania danych dla wszystkich procesów przetwarzania ujętych w *Rejestrze czynności.*

Analiza ryzyka dedykowana ochronie danych została sporządzona przez IOD we współpracy z Dyrektorem Departamentu Organizacyjno-Administracyjnego oraz Administratorem Systemów Informatycznych dopiero w październiku 2019 r. Dokument ten nie został zatwierdzony przez Administratora. Wyjaśniono[38], że powodem były trwające do grudnia 2019 r. prace dot. nowych form monitoringu, po zakończeniu których analiza miała zostać uzupełniona.

Analiza obejmowała w 19 procesach wszystkie 37 czynności przetwarzania danych osobowych z *Rejestru czynności.* Uwzględniała ona zagrożenia związane z wykorzystaniem 7[39] systemów informatycznych, wdrożonych przed rozpoczęciem stosowania RODO. W wynikach analizy ryzyka pojawiły się błędy w obliczeniach, które nie wpływały na działania podejmowane w odniesieniu do poziomu ryzyka.

11. [ocena skutków dla ochrony danych – DPIA] W kontrolowanym okresie nie prowadzono oceny skutków dla ochrony danych. Jej wykonanie, zgodnie z art. 35 ust. 1 RODO, jest konieczne przed rozpoczęciem przetwarzania danych, tj. w przypadku nowych operacji przetwarzania (rozpoczętych po 25 maja 2018 r.). Ocenę skutków przeprowadzono po okresie objętym kontrolą, tj. po 5 grudnia 2019 r. w związku z wprowadzeniem od 1 stycznia 2020 r. nowych operacji przetwarzania w zakresie monitoringu.

---

[36] https://rpp.gov.pl/statut-i-organizacja/ – regulamin organizacyjny i schemat organizacyjny, https://rpp.gov.pl/rejestry-i-ewidencje/rejestry-samodzielnego-stanowiska-ds-ochorny-danych-osobowych/ – rejestry m.in. zbiorów danych osobowych (data dostępu: 22 stycznia 2020 r.).

[37] Zgodnie z § 1 pkt 2 zarządzenia nr 24 Rzecznika Praw Pacjenta z 5 listopada 2018 r. zmieniającego zarządzenie w sprawie nadania Regulaminu organizacyjnego dla BRPP.

[38] Pismo DG z 16 stycznia 2020 r., znak RzPP-ODO-091.1.10.2019.

[39] EZD PUW, ITM Rejestr, eNOVA, Finanse Premium, NBE NBP, Kasa, Płatnik.

Zgodnie z art. 35 RODO ocena skutków dla ochrony danych jest wymagana, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Należy przy tym uwzględnić charakter, zakres, kontekst i cele takiego przetwarzania. Administrator musi ocenić skutki planowanych operacji przetwarzania dla ochrony danych przed rozpoczęciem przetwarzania. Wykonanie oceny od momentu rozpoczęcia stosowania RODO jest więc konieczne w przypadku wprowadzenia nowych kategorii danych, w tym z użyciem nowych technologii i przetwarzaniem na dużą skalę danych szczególnej kategorii. Również w przypadkach, gdy nastąpiła istotna zmiana przetwarzania danych.

Wyjaśniono[40], że nie prowadzono takiej oceny, ponieważ nie stwierdzono wysokiego poziomu ryzyka we wspomnianym zakresie, oraz nie zidentyfikowano procesów przetwarzania danych wymagających oceny w ramach wykazu PUODO z 2018 r.[41]. Ocenę przeprowadzono po okresie objętym kontrolą, tj. po 5 grudnia 2019 r. w związku z wdrożeniem od 1 stycznia 2020 r. nowych form monitoringu. Przy ocenie oparto się o wykaz PUODO z 2019 r.[42], w którym ujęto systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie (np. monitoring systemów poczty elektronicznej, oprogramowania, kart dostępowych itp. w zakładach pracy). Do przeprowadzenia oceny wykorzystano aplikację francuskiego organu nadzoru[43], którą zatwierdził PUODO[44].

12. [rejestr czynności przetwarzania] *Rejestr czynności* odpowiadał wzorowi określonemu w *Polityce BDO*, tj. uwzględniał wymogi art. 30 RODO[45] oraz zawierał informacje dodatkowe[46]. Pomimo jego dwukrotnej weryfikacji i aktualizacji, zawarte w nim informacje były niepełne i zawierały błędy oraz nie pozwalały na pełne monitorowanie operacji przetwarzania danych[47].

Rejestr czynności w imieniu Administratora prowadził IOD w formie elektronicznej na podstawie informacji od kierowników komórek. Obejmował on wszystkie procesy przetwarzania danych osobowych związanych z realizacją celów jednostki. W ramach procesów nie dochodziło do współadministrowania danymi, jak również do przekazywania danych do państw trzecich lub organizacji międzynarodowych. W styczniu 2019 r. *Rejestr czynności* zweryfikowano w ramach rocznego przeglądu, tj. zgodnie z § 14 ust. 5[48] *Polityki BDO,* a następnie we wrześniu 2019 r. *nieznacznie* zmodyfikowano w ramach *Planu IOD.* Kompleksowy przegląd rejestru przewidziano na styczeń-luty 2020 r. w ramach postępowań sprawdzających. *Rejestr czynności* zawierał nieprawidłowości w zakresie:

- podstawy prawnej, tj. w 14[49] czynnościach (z 37[50]) nie wpisano podstawy prawnej wynikającej z RODO, w tym podstawy przetwarzania danych szczególnej kategorii, w 27[51] nie podano konkretnego przepisu prawa krajowego, w 7[52] podano zbyt szeroką podstawę prawną[53];
- zgodności ze stanem faktycznym, tj. w 2 czynnościach błędnie podano termin usunięcia danych[54], w 6[55] błędnie wskazano podmiot przetwarzający, w 3[56] błędnie podano, że obowiązek informacyjny nie jest realizowany, w 7[57] nie wykazano przetwarzania danych w zbiorach papierowych, w 1[58] pominięto część kategorii osób, której czynność dotyczyła;

---

[40] Pismo DG z 20 stycznia 2020 r. znak: RzPP-ODO.091.1.12.1.2019.
[41] Komunikat z 17 sierpnia 2018 r. ws. wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. poz. 827).
[42] Komunikat z 17 czerwca 2019 r. ws. wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony (M. P. poz. 666).
[43] Commission Nationale de l'Informatique et des Libertes.
[44] https://uodo.gov.pl/pl/123/213.
[45] Zawierał: imię i nazwisko oraz dane kontaktowe Administratora; cel przetwarzania; opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych; kategorie odbiorców, którym dane zostały ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych; planowane terminy usunięcia danych, ogólny opis techniczny i organizacyjny środków bezpieczeństwa.
[46] Nazwa czynności przetwarzania; jednostka organizacyjna, która zgłosiła proces; jednostka organizacyjna, która bierze udział w procesie; podstawa prawna z RODO; podstawa prawna; źródło danych; nazwa systemu lub oprogramowania/zbiory papierowe; ocena skutków ochrony danych/DPIA; realizacja obowiązku informacyjnego.
[47] *Rejestr czynności* prowadzony jest m.in. w celu umożliwienia organowi nadzorczemu monitorowania prowadzonego przez Administratora przetwarzania (motyw 82 RODO).
[48] Przynajmniej raz w roku, nie później niż do 30 marca zawartość *Rejestru czynności* jest weryfikowana przez kierowników komórek na wezwanie IOD.
[49] W wierszach nr: 26, 1, 27, 28, 18, 21, 11 oraz 5, 6, 7, 8, 9, 10, 13.
[50] W dniu rozpoczęcia czynności kontrolnych *Rejestr czynności* zawierał 38 czynności. Jedna czynność (wiersz 25) została usunięta.
[51] W wierszach nr: 1, 2, 3, 4, 7, 8, 9, 10, 11, 12, 15, 16, 17, 18, 20, 21, 22, 26, 28, 29, 30, 32, 33, 35, 36, 37, 38.
[52] W wierszach nr: 30-33, 36, 37, 38.
[53] Podano właściwą podstawę prawną oraz dodatkowo przepis prawa, który nie miał zastosowania, tj. art. 10 RODO. *Przetwarzanie danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa (...) wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenie praw i wolności osób, których dane dotyczą.*
[54] Wiersze nr 26 i 27.Termin usunięcia danych nie odnosił się do okoliczności ustania celu przetwarzania lub cofnięcia zgody na przetwarzanie danych oraz wskazano, że logi przechowywane są przez czas nieokreślony zamiast 14 dni.
[55] W wierszach nr 11, 12, 15, 23, 30, 37.
[56] W wierszach nr 15, 16 i 26.
[57] W wierszach nr 31, 32, 33, 35, 36, 37, 38.
[58] Wiersz nr 13.

– kompletności informacji, tj. w 19[59] czynnościach nie podano kategorii danych z podziałem na dane zwykłe i dane szczególne, w 8 czynnościach[60] 38 pól nie zostało w ogóle uzupełnionych, a w 5 w 2 kolumnach wykazano informacje z sąsiedniej kolumny[61].

Ponadto te same 4 czynności zostały ujęte kilkakrotnie[62], co niekorzystnie wpływało na przejrzystość rejestru. Wyjaśniono[63], że błędy powstały w wyniku przeoczenia lub pomyłki i zostaną skorygowane. Wskazano, że kilkakrotne ujmowanie tych samych czynności w różnych wierszach wynikało ze zgłoszenia ich przez różne komórki organizacyjne, w związku ze specyfiką ich pracy. Liczba procesów w ramach modyfikacji *Rejestru czynności* zostanie jednak zmniejszona, a procesy uporządkowane. Wg Kontrolowanego wskazanie nazwy aktu prawnego, a nie konkretnego przepisu jest dopuszczalne, ponieważ RODO nie wymaga podawania w *Rejestrze czynności* informacji nt. podstawy prawnej.

Rejestr czynności powinien przejrzyście i kompleksowo prezentować operacje przetwarzania danych w Urzędzie, w tym pod względem zgodności z celami, jak i wymaganiami prawnymi. Określenie szczegółowej podstawy prawnej przetwarzania sprzyja zapewnieniu legalności przetwarzania, w szczególności gdy zadania wynikają z realizacji obowiązku prawnego ciążącego na Administratorze. Ponadto od jakości prowadzenia rejestru uzależniona jest sprawna realizacja wymogu współpracy z organem nadzorczym, tj. z PUODO[64].

13. [szkolenia pracowników] Pozytywnie należy ocenić zarządzanie wiedzą dot. ochrony danych. Pracownikom zapewniono różne formy szkoleniowe w związku z rozpoczęciem stosowania RODO. W 2019 r. ponownie przeszkolono RzPPSzP, a osoby pełniące szczególne zadania związane z ochroną danych (IOD i członków *Zespołu ODO*) skierowano na specjalistyczne szkolenia zewnętrzne. Nowo zatrudnieni pracownicy przed dopuszczeniem do przetwarzania danych byli szkoleni. W Urzędzie zapewniono dostęp do materiałów podnoszących świadomość dot. ochrony danych oraz zaplanowano dalsze szkolenia.

Odpowiednio na 31 grudnia 2018 r. i 5 grudnia 2019 r. przeszkolono 94% (133 z 142) i 96% (140 z 146) pracowników Urzędu. Wzięli oni udział, z wyjątkiem osób długotrwale nieobecnych, w co najmniej jednej formie szkolenia, tj. e-learningu, szkoleniu wewnętrznym lub wstępnym przy zatrudnieniu.

Oprócz szkoleń związanych z rozpoczęciem stosowania RODO, IOD przeprowadził szkolenie wewnętrzne dla Rzeczników Praw Pacjenta Szpitala Psychiatrycznego 24 października 2019 r. (przeszkolono 37 z 46 RzPPSzP). W *Planie IOD* ujęto kolejne szkolenia dla pracowników Biura.

Ponadto po zmianie przepisów 4 osoby brały udział w szkoleniach zewnętrznych, w tym 3 z nich – w studium dla Inspektorów Ochrony Danych (IOD i 2 członków Zespołu ODO).

W intranecie i na dysku wspólnym w przestrzeni dedykowanej ochronie danych zamieszczono m.in. prezentacje, klauzule informacyjne, akty prawne (w tym Politykę BDO) oraz inne materiały, służące podnoszeniu wiedzy w badanym obszarze.

[59] W wierszach nr 1, 2, 3, 4, 11, 12, 13, 15, 16, 17, 18, 19, 20, 21, 22, 26, 27, 28, 29.
[60] W wierszach nr 22, 31, 32, 33, 34, 35, 36, 38.
[61] Wiersze nr 5, 6, 24, 30, 37. W kolumnie dot. DPIA zawarto opis środków bezpieczeństwa, a w kolumnie dot. środków bezpieczeństwa – nazwę systemu lub oprogramowania.
[62] Czynność dot. rozpatrywania skarg i wniosków na podstawie KPA była wykazana dwukrotnie w wierszu 24 i 7. Czynność dot. rozliczeń z pracownikami ujęta w wierszu 25 obejmowała te same czynności przetwarzania, które zostały ujęte w 4 innych wierszach nr 3, 17, 19 i 20. Czynność dot. rozpatrywania wniosków kierowanych do Rzecznika w trybie art. 51 *ustawy o RPP* ujęta w wierszu 30 została powtórzona w wierszu 31. Również powołanie i odwołanie członków do wojewódzkiej komisji do spraw orzekania o zdarzeniach medycznych zamiast w jednym wierszu znalazło się w 3 czynnościach wymienionych w wierszu 36, 18 i 20.
[63] Pisma DG z 13 stycznia 2020 r., znak: RzPP-ODO.091.1.7.1.2019 oraz z 6 lutego 2020 r., znak: RzPP-ODO.091.1.21.2019.
[64] Zgodnie z art. 31 RODO *Administrator współpracuje z organem nadzorczym w ramach wykonywania przez niego swoich zadań*.

14. [upoważnienia do przetwarzania danych] Nieprawidłowym było niezaktualizowanie upoważnień do przetwarzania danych, pomimo upływu 1,5 roku od rozpoczęcia stosowania RODO. Podstawa prawna znacznej większości z nich od 25 maja 2018 r. była nieaktualna. W efekcie tylko 39 ze 145 pracowników Biura[65] (27%) posiadało upoważnienia z prawidłową podstawą prawną, tj. art. 29 RODO. Ponadto 6 upoważnień nie zaktualizowano także w przypadku zmiany ujętych w nich danych (dot. nazwiska/komórki organizacyjnej). W *Planie IOD* przewidziano wydanie nowych upoważnień w grudniu 2019 r., termin przesunięto na luty 2020 r.

> Art. 29 RODO nakazuje, by każda osoba działająca z upoważnienia Administratora i mająca dostęp do danych, przetwarzała je wyłącznie na polecenie Administratora. Zgodnie z art. 47a ust. 4 pkt 1 *ustawy o RPP* do przetwarzania danych dopuszczone są wyłącznie osoby pisemnie upoważnione.
>
> W Urzędzie przyjęto zasadę, że wszyscy pracownicy posiadają pisemne upoważnienia do przetwarzania danych osobowych, ponieważ każdy w ramach zadań służbowych przetwarza takie dane. Pomimo rozpoczęcia stosowania RODO osobom zatrudnionym przed tą datą nie wydano nowych upoważnień. Wskazano[66], że pracownicy działali zgodnie z art. 29 RODO, tj. na podstawie polecenia Administratora i skoro nie zmieniła się istota ich uprawnień do przetwarzania, upoważnienia zachowały swą moc. Ponadto 5 pracownikom nie wydano nowego upoważnienia pomimo zmiany nazwiska[67], a jednemu[68] pomimo zmiany organizacyjnej Urzędu. Wg Kontrolowanego[69], zmiana nazwiska nie wpływa na skuteczność wydanego polecenia przetwarzania danych. Z kolei ujęty w upoważnieniu zakres obowiązków pracownika odnosi się do zakresu aktualnego na dany moment, a nie obowiązującego przy wydawaniu upoważnienia. Najstarsze upoważnienia wydano z końcem 2010 r., i do 2016 r. nie wskazywano w nich stanowiska, komórki organizacyjnej[70] oraz zobowiązania do zachowania poufności. W *Planie IOD* uwzględniono wydanie nowych upoważnień po wprowadzeniu nowej *Polityki BDO* i przeprowadzeniu szkoleń dla pracowników, których termin przesunięto na luty 2020 r.

Po zmianie systemu ochrony danych osobowych oraz uchyleniu podstawy prawnej upoważnień, należało je zaktualizować[71]. Upoważnienia powinny precyzyjnie określać kto i w jakim zakresie jest uprawniony do przetwarzania danych. Z tego powodu należy je także aktualizować w przypadku zmiany danych dot. osoby oraz powierzonych jej zadań na określonym stanowisku.

15. RPP zapewnił w większości badanych przypadków (89%; 40 z 45), że dane były przetwarzanie przez osoby upoważnione w tym zakresie. Obszar zarządzania uprawnieniami do przetwarzania danych wymaga wzmocnienia, ponieważ w pozostałych spośród badanych upoważnień (11%) stwierdzono nieprawidłowości. Jedno z upoważnień podpisane zostało przez osobę nieuprawnioną, a 4 wolontariuszy przetwarzało dane bez ważnego upoważnienia. Było to niezgodne z art. 47a ust. 4 pkt 1 *ustawy o RPP* wymagającym, by Administrator dopuszczał do przetwarzania danych wyłącznie osoby pisemnie do tego upoważnione.

> Kontroli poddano 45 z 181 (25%) upoważnień do przetwarzania danych wykazanych w ewidencjach jako obowiązujące na 5 grudnia 2019 r.[72].
>
> Jedno upoważnienie[73] zostało wydane przez Zastępcę IOD, który działał bez upoważnienia Administratora. Z kolei w 2019 r. 4 wolontariuszy[74] przetwarzało dane bez ważnych upoważnień. Poprzednio obowiązujące wygasły z upływem terminu porozumień wolontariackich z końcem 2018 r., jednak osoby współpracujące z wolontariuszami były

---

[65] Z wyłączeniem Rzecznika jako Administratora danych.
[66] Pismo Zastępującego DG z 23 stycznia 2020 r., znak: RzPP-ODO.091.1.13.2019.
[67] Poz. 97, 107, 138, 202, 293 ewidencji upoważnień za lata 2010-2018 oraz poz. 17 ewidencji upoważnień z 2019 r.
[68] Poz. 203 ewidencji za lata 2010-2018.
[69] Pismo Zastępującego DG z 23 stycznia 2020 r., znak: RzPP-ODO.091.1.13.2019.
[70] Z wyjątkiem 2 upoważnień odpowiednio z 1 i 2 kwietnia 2014 r., znak RzPP-WSA.0132.9.2014.MK i RzPP-WSA.0132.10.2014.MK.
[71] Poradnik *RODO dla Administracji* opracowany 6 lutego 2019 r. przez Grupę Roboczą ds. Ochrony Danych Osobowych powołaną w Ministerstwie Cyfryzacji https://www.gov.pl/web/cyfryzacja/rodo-dla-administracji-odpowiedzi-na-27-pytan.
[72] Dobór próby celowy, z uwzględnieniem daty wydania oraz przedmiotu upoważnienia (zatrudnienie/inne zadania) i komórki organizacyjnej. Kryteria doboru: termin obowiązywania upoważnienia, ryzyko nieodwołania upoważnienia, zmiana danych dot. upoważnienia (nazwisko, stanowisko), wątpliwości dot. zawarcia umowy powierzenia. 20 z 45 badanych upoważnień (44%) sporządzono przed rozpoczęciem stosowania RODO, a 25 (56%) – po tym terminie.
[73] Upoważnienie z 27 lipca 2018 r., znak: RzPP-ODO.0132.96.2018.
[74] Dot. upoważnień znak: RzPP-ODO.0132.21.2018, RzPP-ODO.0132.23.2018, RzPP-ODO.0132.26.2018, RzPP-ODO.0132.105.2018.

przekonane o ich dalszym obowiązywaniu. Wyjaśniono[75], że porozumienia wolontariackie zapewniają zachowanie w tajemnicy danych pacjentów, co zabezpieczało interes Administratora. Ponadto w 1 przypadku omyłkowo nadano błędny znak upoważnienia[76].

Zapewnienie poufności realizacji zadań w porozumieniach wolontariackich jest procesem odrębnym od zarządzania uprawnieniami do przetwarzania danych. *Polityka BDO* w § 11 pkt 14 wymaga, by przed dopuszczeniem osoby do przetwarzania danych zweryfikować, czy posiada ona stosowne upoważnienie oraz złożyła oświadczenie o zachowaniu poufności. Ten obowiązek nie jest uzależniony od treści umów/porozumień.

16. Prawidłowemu zarządzaniu uprawnieniami nie sprzyjało wydawanie upoważnień dla wykonawców umów cywilnoprawnych, wolontariuszy i praktykantów na czas realizacji zadań, bez powiązania ich z konkretnymi umowami/porozumieniami. W 9 z 45 (20%) badanych upoważnień nie precyzowano terminu ich ważności. Powodowało to ryzyka m.in. w zakresie zapewnienia wiedzy osobom przetwarzającym nt. aktualnych zasad dot. ochrony danych, w szczególności w sytuacji gdy upoważnienia wydano przed rozpoczęciem stosowania RODO. Ponadto rodziło trudności w określeniu terminu ważności upoważnienia, przy czym z danych ujętych w ewidencji upoważnień również nie można było uzyskać informacji w tym zakresie. W ewidencji w takich sytuacjach nie podawano bowiem konkretnej daty ważności upoważnienia, a wpisywano na ogół *kontynuacja* albo *możliwość kontynuacji współpracy*.

W 9[77] upoważnieniach wydanych podmiotom zewnętrznym (wykonawcom umów cywilnoprawnych, wolontariuszom, praktykantom) nie podano nr/daty umowy albo porozumienia, ani nie określono terminu wykonywania zadań. Takie upoważnienia obowiązywały niejednokrotnie przez znaczny okres, np. jedno z upoważnień wydano w 2011 r., zatem obowiązywało 8 lat[78]. W ewidencji upoważnień za lata 2010-2018 w takich przypadkach wykazywano jako datę ustania upoważnienia *kontynuację* lub *możliwość kontynuacji współpracy*, a w ewidencji za 2019 r. nie podawano żadnych informacji. Od momentu wydania upoważnień niejednokrotnie dochodziło do przerw w wykonywaniu zadań, związanych z terminem podpisania kolejnej umowy/porozumienia, co nie było odnotowywane w rejestrze.

17. Wg Kontrolowanego[79] brak danych dot. umów/porozumień nie stanowi braku formalnego upoważnienia. Dokument ten świadczy o wydaniu przez Administratora polecenia do przetwarzania danych, którego szczegóły określają inne dokumenty oraz przepisy prawa. Wyjaśniono również, że upoważnienia tracą ważność w przypadku wygaśnięcia umowy i niepodjęcia dalszej współpracy z wykonawcą albo w sytuacji rezygnacji wolontariusza. Zaznaczono, że w przypadku zaprzestania świadczenia usług wolontarystycznych nie istnieje możliwość dalszego przetwarzania danych, ponieważ odbywa się ono wyłącznie w siedzibie BRPP. Kontrolowany zadeklarował, że praktyka ta zostanie zmieniona. Upoważnienia zostaną przypisane do konkretnych umów, porozumień i dokumentów (ze wskazaniem nr i daty obowiązywania).Zastrzeżenia budzi także sposób zapewnienia dostępu do danych w jednostkowym przypadku udzielenia przez pracownika Biura dalszego pełnomocnictwa procesowego (substytucji) do reprezentowania Rzecznika przed sądem w innym województwie. Przetwarzanie danych może odbywać się na podstawie upoważnienia lub – w przypadku przekazania danych – w ramach udostępnienia albo powierzenia. Administrator zanim zdecyduje, na jakiej podstawie przekaże innemu podmiotowi dane, powinien określić jego status w oparciu o analizę celu i sposobów przetwarzania. W badanym przypadku adwokatowi udzielono upoważnienia, natomiast wśród specjalistów prezentowane jest stanowisko, że Administratorem danych przetwarzanych przez adwokata jest kancelaria, spółka lub zespół adwokacki[80]. W takiej

[75] Pismo DG z 31 stycznia 2020 r., znak: RzPP-ODO.091.1.20.2019.
[76] Dot. poz. 11 ewidencji za 2019 r. (upoważnienie znak: RzPP-ODO.0132.26.2019 zamiast znak: RzPP-ODO.0132.27.2019).
[77] Poz. 81, 400, 405, 413, 416 ewidencji za lata 2010-2018 oraz 1 upoważnienie niezaewidencjonowane (z 30 sierpnia 2017 r.), i poz. 14, 23, 25 ewidencji z 2019 r.
[78] Upoważnienie z 1 lipca 2011 r., znak: RzPP-180-17-1/MBR/11 do przetwarzania danych w ramach umowy cywilnoprawnej.

sytuacji przetwarzanie danych odbywa się w ramach udostępnienia, a nie upoważnienia. Ponadto zakres tego upoważnienia był nieprawidłowy.

Jedno z upoważnień[81] wydano adwokatowi w ramach udzielonej substytucji do reprezentowania Rzecznika przed sądem. Wyjaśniono[82], że zdecydowano się na upoważnienie z uwagi na wykonywanie zawodu zaufania publicznego. BRPP zadeklarowało jednak, że praktyka ta zostanie zmieniona na rzecz powierzania przetwarzania danych. Ponadto zakres tego upoważnienia wykraczał poza realizowane zadania. Wskazano w nim na wykonywanie obowiązków służbowych w BRPP, pomimo że substytut nie był pracownikiem Biura, a jego zadaniem było reprezentowanie Rzecznika w sądzie. W ocenie BRPP[83], pojęcie pełnionych obowiązków służbowych powinno być rozumiane szeroko, bez względu na podstawę prawną realizacji obowiązków.

Z uwagi na zasadę minimalizacji danych (art. 5 ust. 1 pkt c RODO) nie można zgodzić się z Kontrolowanym co do szerokiej interpretacji zakresu upoważnienia. Dane muszą być ograniczone do zakresu niezbędnego dla celów przetwarzania, dlatego powinien być on precyzyjnie określony.

18. Ewidencje upoważnień do przetwarzania danych zawierały nieprawidłowe informacje.

Ewidencje upoważnień do przetwarzania danych były prowadzone oddzielnie za lata 2010-2018 i 2019 r. Decyzję o wprowadzeniu ewidencji na 2019 r. podjęto w związku z zaplanowanym na grudzień 2019 r. wydaniem nowych upoważnień pracownikom BRPP. 10[84] z 45 badanych upoważnień (22%) zaewidencjonowanych jako obowiązujące na 5 grudnia 2019 r. było nieaktualnych. Ponadto ewidencje zawierały następujące braki i niezgodności:

- w ewidencji za lata 2010-2018 błędnie wykazano 1 upoważnienie, którego faktycznie nie wydano[85], 1 upoważnienia nie ujęto[86], dwukrotnie wykazano 35 takich samych pozycji, 2 razy wskazano błędną[87] datę wydania upoważnienia[88] i 1 raz – imię osoby upoważnionej[89];
- w ewidencji za 2019 r. nie zachowano ciągłości numeracji (pominięto poz. 15), w 14 przypadkach nie ujęto informacji nt. daty ustania upoważnienia (w tym 4 wygasłych upoważnień)[90]. Ponadto w 4 przypadkach[91] nie podano informacji dot. identyfikatora w systemie informatycznym. Wyjaśniono[92], że ewidencję uzupełniono o informacje dot. obowiązywania upoważnień, a identyfikatorów nie podano, ponieważ nie zostały nadane.

19. [przetwarzanie danych bez umowy powierzenia] Nie zapewniono należytej ochrony danych przetwarzanych w imieniu Administratora, co było niezgodnie z art. 28 ust. 3 RODO[93] oraz przyjętą *Polityką BDO*[94]. W przypadku 3 umów cywilnoprawnych[95] (z 16 wymagających powierzenia przetwarzania, tj. 19%) dane osobowe przetwarzano bez umowy powierzenia, jedynie na podstawie upoważnienia do przetwarzania danych. Ponadto jedna z komórek Urzędu nie ujęła w *rejestrze udostępnień* danych przekazanych w ramach jednej z umów.

---

[79] Pismo Zastępującego DG z 23 stycznia 2020 r., znak: RzPP-ODO.091.1.13.2019.
[80] *Ogólne rozporządzenie o ochronie danych (RODO). Poradnik dla radców prawnych i adwokatów* przygotowany przez [redacted] i Wspólnicy. Wersja zaktualizowana wg stanu na 1 czerwca 2019 r.
[81] Upoważnienie z 10 października 2018 r., znak: RzPP-DPR-WPZ.0132.1.2018.
[82] Pismo DG z 6 lutego 2020 r., znak: RzPP-ODO.091.1.21.2019.
[83] Pismo Zastępującego DG z 23 stycznia 2020 r., znak: RzPP-ODO.091.1.13.2019.
[84] Poz. 2, 361, 363, 366, 395, 409 ewidencji upoważnień za lata 2010-2018 oraz 4, 12, 23, 25 ewidencji upoważnień z 2019 r.
[85] Upoważnienie z 17 stycznia 2011 r. – poz. 65 ewidencji upoważnień za lata 2010-2018.
[86] Upoważnienie z 30 sierpnia 2017 r., bez znaku.
[87] Pismo Zastępującego DG z 23 stycznia 2020 r., znak: RzPP-ODO.091.1.13.2019.
[88] Poz. 203 i 407 ewidencji upoważnień do przetwarzania danych osobowych za lata 2010-2018.
[89] Poz. 357 ewidencji upoważnień do przetwarzania danych osobowych za lata 2010-2018.
[90] Poz. 4, 9, 11, 12, 14, 17, 18, 23, 25, 40, 44, 48, 50, 51 (w tym 4, 12, 23 i 25 – upoważnienia nieważne na dzień 5 grudnia 2019 r.).
[91] Poz. 14, 18, 23, 25.
[92] Pismo Zastępującego DG z 23 stycznia 2020 r., znak: RzPP-ODO.091.1.13.2019.
[93] Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które wiążą podmiot przetwarzający i Administratora, określają przedmiot i czas trwania przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa Administratora. Taka umowa stanowi w szczególności, że podmiot przetwarzający: przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, zapewnia by osoby upoważnione zobowiązały się do zachowania tajemnicy, podejmuje stosowne środki zapewniające bezpieczeństwo przetwarzania, przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, w miarę możliwości pomaga Administratorowi wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą i obowiązków określonych w art. 32-36 RODO, po zakończeniu świadczenia usuwa lub zwraca wszelkie dane osobowe, udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia nałożonych na niego obowiązków oraz umożliwia Administratorowi przeprowadzenie audytów, w tym inspekcji i przyczynia się do nich.
[94] § 17 ust. 3 *Polityki BDO* powierzenie odbywa się zgodnie z art. 28 RODO, na podst. umowy z podmiotem, któremu zleca się czynności związane z przetwarzaniem danych.
[95] Umowy nr 55/2017 z 30 sierpnia 2017 r., 39/2018 z 24 września 2018 r., 19/2019 r. z 24 października 2019 r. dopuszczały przetwarzanie danych poza siedzibą BRPP, w tym 1 (55/2017) po uzyskaniu zgody.

Skontrolowano 20[96] umów cywilnoprawnych związanych z przetwarzaniem danych osobowych. W 16 przypadkach przetwarzanie danych wymagało umowy powierzenia. W 4[97] powierzenie nie było konieczne z uwagi na przedmiot umowy[98] (1), przetwarzanie danych w siedzibie Urzędu (2) albo udostępnienie danych (1). W 13 umowach (z 16, tj. 81%) zawarto regulacje dot. powierzenia przetwarzania danych osobowych. Natomiast w 3 przypadkach[99] dot. konsultacji medycznych takich umów nie zawarto, pomimo obowiązku wynikającego z art. 28 ust. 3 RODO i § 17 ust. 3 *Polityki BDO.* Realizacja tych 3 umów prowadzona była w oparciu o upoważnienia do przetwarzania danych, także w przypadku wykonywania umowy poza siedzibą. Wyjaśniono[100], że wynikało to z traktowania konsultantów jako *quasi pracowników*. Uznano, że są to osoby fizyczne w większości przypadków świadczące usługi na rzecz BRPP w jego siedzibie, natomiast wymogi dot. umów powierzenia wskazują na obowiązki charakterystyczne dla współpracy z firmami. DG zaznaczył, że praktyka ta została zmodyfikowana i od stycznia 2020 r. konsultanci ds. medycznych przetwarzają dane jako podmioty przetwarzające. Ponadto 1 umowy[101] nie odnotowano w *rejestrze udostępnień.* Wyjaśniono, że powodem było przeoczenie tego obowiązku[102] przez pracowników Departamentu Organizacyjno-Administracyjnego.

20. [umowy powierzenia] Nieprawidłowym było, że w 11 (z 13, tj. 85%) umowach powierzenia nie ujęto części zagadnień wymaganych zgodnie z art. 28 ust. 3 RODO, a jedna z 2 umów powierzenia dot. umowy realizowanej przed rozpoczęciem stosowania RODO została zawarta z 5-miesięcznym opóźnieniem. Ponadto w rejestrze umów powierzenia przetwarzania danych nie zaewidencjonowano 5 umów (z 13, tj. 38%).

Zbadano 13 umów powierzenia (100%). Jedynie w 2 uwzględniono wszystkie warunki, o których mowa w art. 28 ust. 3 RODO. W pozostałych nie określono:

- warunków udzielania zgody Administratora na korzystanie przez procesora z innych podmiotów przetwarzających (2 przypadki)[103],
- czasu trwania przetwarzania danych (3)[104],
- rodzaju danych oraz kategorii osób, których dane dotyczą (2)[105],
- obowiązku przetwarzania przez procesora danych osobowych wyłącznie na udokumentowane polecenie Administratora (5)[106],
- zobowiązania do przestrzegania warunków korzystania z usług innego podmiotu przetwarzającego (3)[107],
- obowiązku wspomagania Administratora, w tym do zapewnienia odpowiednich środków technicznych i organizacyjnych, aby móc wywiązywać się z obowiązku odpowiadania na żądania oraz do wykonywania praw osób, których dane dotyczą (5)[108],
- zobowiązania do wspomagania Administratora w wywiązywaniu się z obowiązków określonych w art. 35-36 RODO (8)[109].

Ponadto w 11[110] umowach nie zobowiązano wykonawcy do prowadzenia rejestru kategorii czynności przetwarzania danych dokonywanych w imieniu Administratora (art. 30 ust. 2 RODO). Jedna umowa powierzenia[111] dot. umowy realizowanej przed rozpoczęciem stosowania RODO została zawarta 31 października 2018 r., tj. z 5-miesięcznym opóźnieniem. Wyjaśniono[112], że wspomniane obowiązki wynikają z RODO i podmioty przetwarzające powinny się liczyć z koniecznością ich wypełnienia nawet wtedy, gdy nie ujęto ich w umowie. W 5 umowach nie uwzględniono środków organizacyjnych, ponieważ usługi były świadczone w BRPP i dlatego uznano, że wykonawcy będą w stanie zapewnić odpowiedni poziomo ochrony danych. Podano[113] również, że 5 umów nie znalazło się w rejestrze umów powierzenia, ponieważ 3[114] z nich po podpisaniu nie zgłoszono do IOD,

[96] 13 umów powierzenia przetwarzania danych osobowych oraz7 umów z wysokim prawdopodobieństwem przetwarzania danych wybranych z zestawienia umów z osobami prawnymi i z osobami fizycznymi.
[97] 1 – prowadzenia audytu wewnętrznego, 1 – zastępstwa sądowego, 1 – szkolenia pracowników oraz 1 – szczepień ochronnych.
[98] Umowa dotyczyła wynagrodzenia za zastępstwo procesowe wykonywane przez pracownika Urzędu.
[99] 2 zawarte z osobami fizycznymi prowadzącymi działalność gospodarczą i 1 zawarta z osobą fizyczną nieprowadzącą takiej działalności.
[100] Pismo DG z 6 lutego 2020 r., znak: RzPP-ODO.091.1.2019.
[101] Umowa nr 2017/13/BRPP z 12 czerwca 2017 r.
[102] Zgodnie z §16 ust. 7 *Polityki BDO* kierownicy komórek prowadzą rejestr udostępnień danych osobowych innym podmiotom, zgodnie ze wzorem zawartym w załączniku.
[103] Nr 44/2019, 11/2019.
[104] Nr 21/2018, 55/2018, 3/2019.
[105] Nr 23/2018, 4/2019.
[106] Nr 11/2019, 21/2018, 44/2019, 55/2018, 3/2019.
[107] Nr 44/2019, 3/2019, 11/2019.
[108] Nr 23/2018, 21/2018, 4/2019, 55/2018, 3/2019.
[109] Nr 23/2018, 21/2018, 45/2018, 4/2019, 44/2019, 55/2018, 3/2019, 13/2019.
[110] Nr 22/2018, 23/2018, 21/2018, 45/2018, 4/2019, 6/2019, 55/2018, 3/2019, 13/2019, 11/2019, 44/2019.
[111] Nr 22/2018 do umowy nr 95/2017.
[112] Pismo Zastępującego DG z 23 stycznia 2020 r., znak: RzPP-ODO.091.1.13.2019.
[113] Pisma DG z 2 stycznia 2020 r., znak: RzPP-ODO.091.1.5.2019 oraz z 28 stycznia 2020 r., znak: RzPP-ODO.091.1.17.2019.
[114] Nr 3/2019, 11/2019 oraz 13/2019.

1 umowa[115] nie była z nim konsultowana, a 1 umowa[116] została przeoczona. Zadeklarowano, że wszystkie przygotowane umowy będą przekazywane do zaopiniowania przez IOD.

21. [klauzule informacyjne] W przypadku pozyskiwania danych od osób, których one dotyczą (art. 13 RODO), BRPP opracowało klauzule informacyjne, aby zapewnić szczegółowe informacje nt. przetwarzania danych. Klauzule zawierały większość informacji określonych w art. 13 ust. 1 i 2 RODO[117], jednakże wymagają one uzupełnienia. W szczególności dotyczy to informacji nt. zautomatyzowanego podejmowania decyzji (19 z 21 klauzul) oraz konsekwencji niepodania danych (5 z 21 klauzul). Z kolei w przypadku pozyskiwania danych w sposób inny niż od osoby, której dane dotyczą (art. 14 RODO), zakres klauzuli informacyjnej określono w *Polityce BDO*[118]. W ramach *Planu IOD* uwzględniono przegląd i uzupełnienie klauzul informacyjnych.

Przepisy regulują, jakie informacje należy przekazać podmiotom danych w ramach dwóch sposobów pozyskiwania danych: od osoby, której dane dotyczą (art. 13 RODO) albo w inny sposób (art. 14 RODO).

W Biurze funkcjonowała procedura udzielania informacji osobom, których dane dotyczą. Obowiązek informacyjny realizowano w szczególności poprzez zamieszczanie klauzul na stronie internetowej Rzecznika, we wzorach formularzy, w ramach pierwszego pisma skierowanego do adresata. Zidentyfikowano 21 klauzul informacyjnych dot. pozyskiwania danych od osoby, której one dotyczą[119]. W klauzulach tych nie zamieszczono, co było niezgodne z art. 13 ust. 1 i 2 RODO: informacji nt. zautomatyzowanego podejmowania decyzji (19 klauzul)[120], informacji nt. ewentualnych konsekwencji niepodania danych (5)[121], prawa do cofnięcia zgody w każdym momencie (3)[122], informacji o odbiorcach danych (2)[123] oraz w pojedynczych przypadkach: prawa do usunięcia danych[124], okresu przechowywania danych oraz prawa do złożenia skargi do PUODO[125]. Ponadto w klauzuli informacyjnej dot. konferencji[126] przywołano nieprawidłową podstawę prawną, a w komunikacie rozpoczynającym rozmowę na Infolinii Rzecznika wskazano, że dzwoniącym nie przysługują prawa określone w art. 15-22 RODO (prawo dostępu, sprostowania i in.). Wyjaśniono[127], że nie podawano informacji o zautomatyzowanym podejmowaniu decyzji, ponieważ nie występuje ono w BRPP, komunikat na infolinii zawierał błędną informację, a pozostałe braki stanowią przeoczenie. Kontrolowany zadeklarował uzupełnienie klauzul. Ich przegląd został przewidziany w ramach postępowań sprawdzających ujętych w *Planie IOD* na styczeń i luty 2020 r.

Nie opracowano wzoru klauzuli informacyjnej dla osób, których dane pozyskano w inny sposób niż od podmiotu danych (art. 14 RODO). Wyjaśniono[128], że nie wystąpiły przypadki wymagające, by spełnić obowiązek informacyjny w tym zakresie, w szczególności z uwagi na wyłączenie dot. przetwarzania danych na podstawie przepisów prawa[129].

Obowiązkiem Administratora jest zapewnienie podmiotom danych prawidłowych, kompletnych i szczegółowych informacji dot. przetwarzania przez niego danych. Braki poszczególnych informacji z perspektywy odbiorcy mogą wskazywać nie tylko na nierzetelność przygotowania klauzul informacyjnych, ale także na niepełną analizę czynności przetwarzania.

---

[115] Nr 50/2019.
[116] Nr 55/2018.
[117] Podmiotowi danych należy przekazać tożsamość i dane kontaktowe Administratora, dane kontaktowe IOD, cele przetwarzania danych oraz podstawę prawną przetwarzania, prawnie uzasadnione interesy Administratora (dot. art. 6 ust. 1 lit. f RODO), informacje o odbiorcach danych lub o kategoriach odbiorców, informacje o zamiarze przekazania danych do państwa trzeciego lub organizacji międzynarodowej (gdy ma to zastosowanie), okres retencji danych lub kryteria ustalania tego okresu, informacje o prawie do żądania dostępu do danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu, a także o prawie do przenoszenia danych, informacje o prawie do cofnięcia zgody w dowolnym momencie (dot. art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a), informacje o prawie wniesienia skargi do organu nadzorczego, informację, czy podanie danych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, jest zobowiązana do ich podania i jakie są konsekwencje niepodania danych, informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.
[118] Załącznik nr 10 do *Polityki BDO* pn. *Zakres obowiązków informacyjnych.*
[119] Dot.: rozpatrzenia spraw w ramach kompetencji Rzecznika (2), spraw dot. pacjentów szpitala psychiatrycznego, skarg, wniosków i petycji (1); skarg i wniosków (1); petycji (1); dostępu do informacji publicznej, wniosków ws. danych osobowych, infolinii, formularza kontaktowego na stronie internetowej, naboru, praktyk, wolontariatu, zatrudnienia, świadczeń socjalnych, identyfikatorów pracowniczych, zamówień publicznych, umów cywilnoprawnych, konkursu, udziału w konferencji, wejścia na teren BRPP.
[120] Z wyjątkiem zamówień publicznych i naboru do pracy.
[121] Dot. dostępu do informacji publ., realizacji praw pacjentów szpitala psychiatrycznego, wniosków ws. danych osobowych, identyfikatorów pracowniczych i wejść na teren BRPP.
[122] Dot. naboru, konkursu oraz przetwarzania wizerunku w ramach konferencji (w ostatnim przypadku brak informacji był związany z nieprawidłową podst. prawną przetwarzania).
[123] Dot. wejść na teren BRPP i infolinii.
[124] Dot. identyfikatorów pracowniczych.
[125] Dot. konkursu.
[126] Dot. konferencji *Naszym głosem jest pacjent – doświadczenia i wyzwania Rzecznika Praw Pacjenta.*
[127] Pismo DG z 14 stycznia 2020 r., znak: RzPP-ODO.091.1.8.2019 i z 30 stycznia 2020 r., znak: RzPP-ODO.091.1.19.2019.
[128] Pismo DG z 14 stycznia 2020 r., znak: RzPP-ODO.091.1.8.2019.
[129] Zgodnie z art. 14 ust. 5 lit. c RODO przepisy art. 14 RODO dot. obowiązku informacyjnego w przypadku pozyskiwania danych osobowych w sposób inny niż od podmiotu danych nie mają zastosowania w zakresie, w jakim pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego.

22. Zasadnym byłoby wprowadzenie repozytorium klauzul, aby wspierać realizację obowiązku informacyjnego. W BRPP brakowało jednego miejsca, w którym można było znaleźć wszystkie stosowane klauzule. Podczas kontroli zadeklarowano wprowadzenie takiego rozwiązania.

> Podstawowe klauzule stosowane przez pracowników udostępniono im w systemie Elektronicznego Zarządzania Dokumentacją (dalej: EZD) (5) oraz zamieszczono na dysku wspólnym[130]. Pozostałe klauzule wykorzystywane były w ramach zadań, z którymi wiąże się konkretny obowiązek informacyjny, w tym także na stronie internetowej Rzecznika.
>
> W ramach 21 klauzul opisano 19 czynności przetwarzania, natomiast w 2 przypadkach klauzule występowały w 2 wariantach. Pierwszy dotyczył 2 klauzul związanych z wykonywaniem kompetencji ustawowych Rzecznika, w których w różny sposób opisano okres przechowywania danych. Jedna z klauzul w praktyce nie była stosowana[131], ponieważ zamieszczono ją na dysku, ale nie udostępniono w EZD. Drugi przypadek stanowiła wspólna klauzula dla skarg, wniosków i petycji, zamieszczona na stronie internetowej Rzecznika, podczas gdy w Urzędzie stosowano w tym zakresie jednocześnie 2 odrębne klauzule: dla skarg i wniosków (1) oraz petycji (1).

Klauzule obejmujące te same procesy przetwarzania nie powinny występować w różnych wariantach. Nie służy to zapewnieniu przejrzystości w realizacji obowiązku informacyjnego.

23. Klauzule informacyjne były formułowane jasnym i prostym językiem, w zrozumiałej i łatwo dostępnej formie[132].

> RzPPSzP udzielali informacji nt. przetwarzania danych w sposób dostosowany do możliwości pacjentów. We wzorze protokołu prowadzenia sprawy umieszczono skrótową informację dot. spełnienia obowiązku informacyjnego oraz wskazano, gdzie można znaleźć szczegółowe informacje. Ponadto formularz zgłoszenia sprawy przewidywał miejsce na podpisy pacjenta oraz RzPPSzP pod skróconą klauzulą informacyjną. Gdyby pacjent nie mógł się pod nią podpisać, stosowana była adnotacja RzPPSzP o odczytaniu klauzuli. Wyjaśniono, że BRPP dokłada wszelkich starań, aby w pełni realizować obowiązki informacyjne wobec pacjentów, z uwzględnieniem możliwości ich percepcji wynikającej ze stanu zdrowia psychicznego i wieku.

24. **[obowiązek informacyjny przy wykonywaniu kompetencji Rzecznika]** Prawidłowo realizowano obowiązki informacyjne w ramach 20 z 23 spraw (87%), w których przetwarzanie danych odbywało się na podstawie przepisów prawa w ramach kompetencji Rzecznika. Dotyczy to sytuacji, kiedy przetwarzanie było niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 1 lit. c lub e RODO). Natomiast w 2 przypadkach nie dopełniono obowiązku informacyjnego, a w 1 – dokonano tego z opóźnieniem, co było niezgodne z art. 13 RODO[133] i § 13 ust. 1-3 *Polityki BDO*[134].

> Od 1 stycznia 2018 r. do 5 grudnia 2019 r. do Urzędu wpłynęło 151 570 spraw/sygnałów/zapytań (68 965 w 2018 r. i 82 605 w 2019 r.). Zbadano realizację obowiązku informacyjnego w ramach 30 spraw[135], w których dane przetwarzane były na podstawie przepisów prawa zgodnie z art. 6 ust. 1 lit. c i e RODO. W 23 przypadkach obowiązek informacyjny wystąpił, w 7 – nie[136].
>
> W 3 z 23 wspomnianych spraw (13%) nie wykonano obowiązku informacyjnego (2) albo wykonano go z opóźnieniem (1). W jednej ze spraw[137], jak wyjaśniono przez niedopatrzenie, nie dołączono do pisma klauzuli, a w drugiej RzPPSzP nie poinformował pacjenta o zasadach przetwarzania danych[138]. Wyjaśniono[139], że sprawa ta była prowadzona przez nierzetelnego pracownika, z którym rozwiązano umowę o pracę. W kolejnej ze spraw

[130] Razem z 3 dodatkowymi klauzulami.
[131] Pismo DG z 31 stycznia 2020 r., znak: RzPP-ODO.091.1.20.2019.
[132] Zgodnie z art. 12 ust. 1 RODO.
[133] Nakazującym Administratorowi przekazanie informacji podmiotowi danych podczas pozyskiwania od niego danych.
[134] Wskazuje on, że informacje dot. przetwarzanych danych powinny być załączane m.in. do pism kierowanych do podmiotów danych przy pierwszym kontakcie.
[135] W tym 10 z 14.138 (0,1%) spraw w ramach wniosków pacjentów oraz rozpatrywania tych wniosków – JRWA 431 (w 8 przypadkach wystąpił obowiązek informacyjny, a w 2 – nie), 10 z 16.459 (0,1%) w ramach działań RzPPSzP – JRWA 470 (w 8 przypadkach wystąpił obowiązek informacyjny, w 1 przypadku – nie, a w 1 przypadku sprawa wybrana do próby nie istniała) oraz 10 z 796 (1%) w ramach skarg i wniosków – JRWA 051 i 052 (w 7 przypadkach wystąpił obowiązek informacyjny, a w 3 nie).
[136] Z uwagi na termin załatwienia sprawy oraz brak jednej ze spraw (wykreślenie pozycji ze spisu spraw).
[137] Dot. pisma z 26 listopada 2018 r., znak: RzPP-DPW-WPII.431.3000.2018.JW.
[138] Protokół prowadzenia sprawy znak: RzPP-DZP-RzSP-SH.470.99.2019.
[139] Pismo DG z 30 stycznia 2019 r., znak: RzPP-ODO.091.1.19.2019.

klauzulę informacyjną dołączono do drugiego z kolei pisma skierowanego do strony[140], ponieważ pierwsze pismo było adresowane do podmiotu leczniczego, a wnioskodawca otrzymał je jedynie do wiadomości.

25. [obowiązek informacyjny w ramach zgody na przetwarzanie] Prawidłowo realizowano obowiązek informacyjny w 84 % (51 z 61 zbadanych) przypadków przetwarzania danych na podstawie zgody podmiotu danych (art. 6 ust. 1 lit. a RODO). Jednakże obszar ten, ze względu na stwierdzone nieprawidłowości, wymaga wzmocnienia.

W *Rejestrze czynności* zidentyfikowano 5 procesów, w których przetwarzanie danych opiera się na zgodzie, tj. nabory, konkursy, wydawanie identyfikatorów pracownikom, zgoda na przetwarzanie wizerunku w mediach społecznościowych, pliki Cookies. Zbadano realizację obowiązku informacyjnego w ramach 64 zgód na przetwarzanie danych. W 61 przypadkach obowiązek informacyjny wystąpił (39 zgód w 5 naborach[141] i 22 zgody w innych obszarach[142]), a w 3 nie[143].

26. Podczas 1 z organizowanych przez Rzecznika konferencji nie dopełniono obowiązku informacyjnego (dotyczy 5 z 61 zbadanych zgód, tj. 8%), a w ramach kolejnej konferencji (5 z 61 zgód, tj. 8 %) zgody na przetwarzanie wizerunku udzielono na formularzu odrębnym od klauzuli informacyjnej. Naruszono tym art. 13 RODO i § 13 ust. 4 *Polityki BDO*[144].

W przypadku konferencji *Rzecznik Praw Pacjenta – Rzecznikiem Polskiej Psychiatrii* (5 zbadanych zgód) nie spełniono obowiązku informacyjnego. Wyjaśniono[145], że powodem były liczne sprawy, które należało pilnie rozwiązać w zw. z trudnościami kadrowymi dot. organizacji konferencji (nieobecność 1 pracownika i odejście 2 kolejnych z pracy). Odnośnie do konferencji *Naszym głosem jest pacjent – doświadczenia i wyzwania Rzecznika Praw Pacjenta* (5 zbadanych) wyjaśniono, że do zaproszeń załączano klauzulę informacyjną, jednak była ona odrębnym od zgody dokumentem.

27. W większości procesów zgody udzielane były w sposób jednoznaczny, zrozumiały i świadomy (84%, tj. 51 z 61 badanych zgód). Wyjątek stanowi formularz opracowany przez BRPP w ramach konkursu artystycznego dla dzieci. Nieprawidłowo sformułowano w nim treść zgody opiekunów prawnych na przetwarzanie danych, ponieważ nie uwzględniała ona danych osobowych dzieci (dot. 10 poddanych kontroli zgód).

W przypadku wydawania identyfikatorów oraz udziału w konferencji i konkursie, zgody wyrażano w ramach opracowanego przez Urząd wzoru. W przypadku naborów kandydaci wyrażali zgody na przetwarzanie danych w CV albo jako zgodę traktowano złożenie przez nich dokumentów. Wśród badanych przypadków nie była wymagana odrębna zgoda dot. danych szczególnej kategorii.

W konkursie *Psychiatria w moich oczach* (10 badanych przypadków) opiekunowie dzieci na opracowanym przez BRPP formularzu wyrażali zgodę na przetwarzanie tylko swoich danych, nie zaś dzieci – uczestników konkursu. Wyjaśniono[146], że wynikało to z niedopatrzenia przy tworzeniu formularza na podst. innego konkursu dla dorosłych. Wskazano przy tym, że z pozostałej treści oświadczeń wynika, że intencją Rzecznika było uzyskanie zgody na przetwarzanie danych małoletnich uczestników konkursu.

28. Zastrzeżenia budzi, że Regulamin pracy Biura przewidywał obowiązek noszenia identyfikatora ze zdjęciem, a jednocześnie od pracowników pobierano zgody na przetwarzanie wizerunku (art. 6 ust. 1 lit. a RODO). Takie rozwiązanie nie gwarantuje zachowania dobrowolności przy wyrażaniu zgody na przetwarzanie wizerunku pracowników.

Regulamin pracy w BRPP[147] wśród obowiązków pracowników przewidywał konieczność noszenia identyfikatora ze zdjęciem. Jednocześnie od pracowników pobierano zgodę na przetwarzanie danych, w tym wizerunku, umieszczonych na identyfikatorze (2 badane

[140] Zamiast do pisma z 17 czerwca 2019 r., znak: RzPP-DPW-WPI.431.1111.2019.EKA (pismo przekazane do wiadomości wnioskodawcy), klauzulę załączono do odpowiedzi z 24 września 2019 r., znak: RzPP-DPW-WPI.431.1111.2019.EKA.
[141] Badaniu poddano 5 z 92 naborów (tj. 5%), w tym 3 nabory w okresie przechowywania akt (2019 r.) oraz 2 nabory – po zakończeniu takiego okresu (2018 r.).
[142] 10 z 44 (23%) zgód na udział w konkursie „Psychiatria w moich oczach", 10 z 425 (2%) zgód na upublicznienie wizerunku, 2 ze 186 (1%) zgód dot. identyfikatorów pracowniczych – dot. osób wyłonionych w badanych naborach.
[143] W przypadku 3 wyłonionych w naborach pracowników nie wydano do czasu kontroli identyfikatorów, w związku z czym nie pobrano od nich zgód na przetwarzanie wizerunku.
[144] *Jeżeli przesłanką legalności przetwarzania danych osobowych jest zgoda osoby, której dane dotyczą, należy pod klauzulą informacyjną umieścić klauzulę zgody wraz z odrębnym miejscem na podpis* (…).
[145] Pismo DG z 30 stycznia 2019 r., znak: RzPP-ODO.091.1.19.2019.
[146] Pismo DG z 30 stycznia 2019 r., znak: RzPP-ODO.091.1.19.2019.
[147] § 11 ust. 1 pkt 15 zarządzenia nr 32/2017 DG z 12 grudnia 2017 r. ws. wprowadzenia regulaminu pracy w Biurze Rzecznika Praw Pacjenta (ze. zm.).

zgody). Wyjaśniono[148], że pobieranie zgody było nadmiarowe, ponieważ pracodawca jest uprawniony do wprowadzenia obowiązku noszenia przez pracowników identyfikatora ze zdjęciem.

Zgodnie ze stanowiskiem PUODO[149], ze względu na to, że wizerunku pracownika nie ma wśród danych wskazanych w Kodeksie pracy[150], aby pracodawca mógł je pozyskać i umieścić np. na identyfikatorze, musi legitymować się zgodą pracownika[151]. Zgoda taka musi być udzielona dobrowolnie, tj. z uwzględnieniem możliwości odmowy jej udzielenia bez żadnych negatywnych konsekwencji, jak również odwołania w każdym czasie. Jeśli Administrator w ramach RODO zidentyfikowałby inną podstawę przetwarzania, której w trakcie kontroli nie przedstawiono, musi być w stanie – zgodnie z zasadą rozliczalności – ją wykazać. Nie może natomiast stosować różnych podstaw prawnych dla tej samej czynności przetwarzania.

29. Przez ponad rok przechowywano aplikacje kandydatów złożone w ramach jednego z naborów, co było niezgodnie z zasadą ograniczonego przechowywania i wewnętrznie ustalonym okresem retencji[152].

Zasada ograniczonego przechowywania (art. 5 ust. 1 lit. e RODO) wymaga, by dane przechowywać przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

W BRPP przez ponad rok przechowywano aplikacje 7 osób z naboru przeprowadzonego w 2018 r., podczas gdy termin ich wykorzystania upłynął 13 stycznia 2019 r. Wyjaśniono[153], że aplikacje są niszczone na bieżąco po upływie okresów wskazanych w klauzulach informacyjnych, z wyjątkiem przeoczenia w badanym naborze. Poinformowano również o ponownej weryfikacji dokumentacji dot. naborów.

30. W Urzędzie nie funkcjonował system rejestrowania i zarządzania zgodą na przetwarzanie danych z uwagi na nieznaczną liczbę pozyskiwanych zgód. Dokumenty dotyczące zgód przechowywano w aktach spraw, w których zostały pozyskane.

Zgody przechowywane były w aktach pracowniczych oraz w aktach spraw, w ramach których udzielano zgody. Tam też miały być przechowywane wycofania zgód, jednak takie przypadki nie wystąpiły.

31. **[realizacja praw osób, których dane dotyczą]** Odpowiedzi na wnioski osób, których dane dotyczą (7 z 8; 88%) – z jednym wyjątkiem[154] – były udzielane w terminie określonym w 12 ust. 3 RODO, tj. bez zbędnej zwłoki, nie później niż w ciągu miesiąca od ich otrzymania. Zastrzeżenia budzi, że odpowiedzi na te wnioski udzielali IOD i pracownicy BRPP, którzy nie posiadali upoważnień do tego typu czynności, co było niezgodne § 15 ust. 2 pkt 5 *Polityki BDO*.

1 z 8 wspomnianych wniosków załatwiono nieterminowo, tj. 54 dni po jego otrzymaniu[155]. Wyjaśniono[156], że naruszenie terminu wynikało z przekazania IOD pisma przez jeden z departamentów po blisko miesiącu od daty wpływu. Wniosek o kopię danych znajdował się w dalszej części dokumentacji, dlatego konieczna była analiza całej 51-stronicowej korespondencji.

Zgodnie z § 15 ust. 2 pkt. 5 *Polityki BDO* odpowiedzi na wnioski dot. realizacji praw osób podpisuje Administrator albo osoba przez niego upoważniona. Tymczasem na 8 wniosków – 6 załatwił IOD, 1 – DG, 1 – pracownik BRPP. Wyjaśniono, że przyjęto praktykę, że odpowiedzi na wnioski podmiotów danych zazwyczaj podpisuje lub załatwia IOD, a inne osoby w ramach wyjątku od tej zasady.

---

[148] Pismo DG BRPP z 30 stycznia 2019 r., znak: RzPP-ODO.091.1.19.2019.
[149] *Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców* opublikowany 4 października 2018 r. na stronie https://uodo.gov.pl/pl/383/545.
[150] Ustawa z 26 czerwca 1974 r. Kodeks pracy (Dz. U. z 2019 r. poz. 1040, ze zm.).
[151] Z wyjątkiem sytuacji, w których wizerunek jest przetwarzany na podstawie odrębnych przepisów prawa.
[152] Zarządzenie nr 7/2018 DG z 5 marca 2018 r. ws.. wprowadzenia polityki naboru i rekrutacji na stanowiska urzędnicze oraz ogłoszenie o naborze 33191 z 12 września 2018 r.
[153] Pismo DG z 30 stycznia 2019 r., znak: RzPP-ODO.091.1.19.2019.
[154] Sprawa nr RzPP-ODO.0132.128.2018.
[155] Wniosek, który wpłynął do Urzędu 17 października 2018 r. załatwiono 11 grudnia 2018 r.
[156] Pismo Zastępującego DG z 24 stycznia 2020 r., znak: RzPP-ODO.091.1.14.2019.

Realizacja zadań zgodnie z przyjętą praktyką, a nie określonymi w Urzędzie procedurami wskazuje na konieczność wzmocnienia nadzoru nad stosowaniem regulacji wewnętrznych albo potrzebę zmiany procedur.

32. Urząd posiadał rejestr wniosków podmiotów danych w ramach realizacji ich praw wynikających z RODO.

> Rejestr zawierał 7 wpisów (5 dot. udostępnienia danych, 1 – informacji o okresie przechowywania danych, 1 – usunięcia danych). Nie ujęto w nim, że w jednej ze spraw[157] złożono 2 wnioski. Do BRPP wpłynęły 2 wnioski od tego samego wnioskodawcy (28 listopada 2018 r. z prośbą *udostępnienie nagrania* oraz 11 grudnia 2018 r. z prośbą o *przesłanie nagrania*). W rejestrze uwzględniono tylko pierwszy wniosek. Wg Kontrolowanego korespondencja z 11 grudnia 2018 r. została potraktowana jako kontynuacja wniosku z 28 listopada 2018 r. i w istocie jest to 1 wniosek.

W omawianym przypadku drugie pismo należało uznać za ponowny wniosek dot. realizacji praw. Z tego względu powinno być odrębnie odnotowane w rejestrze, mimo że oba wnioski wpłynęły od jednego wnioskodawcy i zostały ujęte w ramach jednej sprawy.

33. [naruszenia ochrony danych] Zgodnie z art. 33 ust. 5 RODO zdarzenia dot. naruszeń ochrony danych były dokumentowane, co pozwalało bez trudu – z jednym wyjątkiem (z 10 badanych spraw) – określić okoliczności ich wystąpienia, skutki oraz podjęte działania. Nie wystąpiły naruszenia ochrony danych, wymagające zawiadomienia PUODO ani osób, których dane dotyczą. Pozytywnie należy ocenić, że w Urzędzie opracowano *Dobre praktyki w zakresie troski o ochronę danych osobowych*.

> W związku z przypadkami naruszeń ochrony danych opracowano i udostępniono wszystkim pracownikom *Dobre praktyki w zakresie troski o ochronę danych osobowych*. Zaewidencjonowano 31 incydentów w zakresie ochrony danych (20 w 2018 r. i 11 w 2019 r.). Badaniu poddano 10 z nich (32%)[158], w tym 3 zakwalifikowane jako naruszenia i 7 jako zdarzenia powodujące ryzyko naruszeń. W żadnym przypadku naruszenie nie powodowało obowiązku poinformowania PUODO lub podmiotu danych. W jednej ze spraw[159] dokumentacja dot. zdarzenia zawierała niejednoznaczne informacje, czy do naruszenia faktycznie doszło, czy też nie. W sprawozdaniu z tej sprawy, jak wyjaśniono[160] przez przeoczenie, nie podano także zakresu danych, którego zgłoszenie dotyczy.

34. Procedura postępowania w sytuacji podejrzenia bądź stwierdzenia naruszenia bezpieczeństwa danych nie była w pełni przestrzegana. Niezgodności dotyczą analiz ryzyka naruszeń (§ 31 ust. 7 *Polityki BDO*) oraz uzasadnień dla niezgłaszania naruszeń PUODO i podmiotom danych (§ 29 ust. 2 *Polityki BDO*).

> Niezgodnie z § 31 ust. 7 *Polityki BDO* w żadnej ze spraw (10) kierownicy komórek nie sporządzili analiz dot. ryzyka naruszeń. Wyjaśniono[161], że uczestniczyli oni w ustalaniu okoliczności zdarzenia oraz w jego kwalifikacji jako naruszenia. Taka praktyka, w opinii Kontrolowanego, okazała się efektywniejsza. BRPP planuje, że w nowej *Polityce BDO* zadanie to nie będzie przypisane kierownikom komórek.
>
> Niezgodnie z § 29 ust. 2 *Polityki BDO* w dokumentacji 7[162] z 10 spraw nie wskazywano jednoznacznie powodów decyzji niezgłoszenia zdarzeń do organu nadzorczego lub niezawiadomienia podmiotu danych. Braki wynikały z niezakwalifikowania zdarzenia jako naruszenia (6) bądź przeoczenia (1)[163].

Zgodnie z § 29 ust. 2 *Polityki BDO* w dokumentacji dot. podejrzenia bądź stwierdzenia naruszenia bezpieczeństwa danych należy w szczególności wskazać powody decyzji niezgłoszenia naruszenia do organu nadzorczego (PUODO) oraz niezawiadomienia podmiotu danych. Należy też podać przyczyny, dla których Administrator uznaje ryzyko naruszenia praw i wolności osób fizycznych za mało prawdopodobne. W celu zapewnienia

---

[157] Sprawa nr RzPP-ODO.0132.144.2018.
[158] Dobór próby celowy, z uwzględnieniem różnic dot. charakteru zdarzeń związanych z naruszeniem ochrony danych osobowych. Badaniu poddano sprawdzenia nr 3/2018, 10/2018, 12/2018, 18/2018, 20/2018, 2/2019, 3/2019, 6/2019, 8/2019, 10/2019.
[159] Dot. sprawozdania ze sprawdzenia doraźnego nr 3/2018.
[160] Pismo DG z 20 stycznia 2020 r., znak: RzPP-ODO.091.1.12.2019.
[161] Pismo DG z 20 stycznia 2020 r., znak: RzPP-ODO.091.1.12.2019.
[162] Sprawozdania ze sprawdzeń doraźnych: nr 10/18 i 3/2019; 12/2018, 20/2018, 8/2019 i 10/2019; 2/2019.
[163] Pismo DG z 20 stycznia 2020 r., znak: RzPP-ODO.091.1.12.2019.

Administratorowi i organowi nadzoru kompletnych i przejrzystych informacji ważne jest, by każdorazowo wyraźnie opisać ten aspekt w prowadzonej dokumentacji.

35. O wysokiej świadomości pracowników w zakresie ochrony danych świadczy, że zgłaszali oni IOD nie tylko naruszenia, ale także zdarzenia potencjalnie świadczące o ryzyku naruszenia. Jednak w 3 z 10 (30%) przypadków nieprawidłowo oceniono charakter incydentu. Przyjęto, że nie doszło do naruszenia ochrony danych, pomimo że nastąpiło przypadkowe ujawnienie albo udostępnienie danych, o którym mowa w art. 4 pkt 12 RODO.

> Zgodnie z art. 4 pkt 12 RODO naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
>
> W 2 sprawach wysłano wiadomość do innego adresata (do urzędu miasta zamiast do szpitala[164] oraz do innego podmiotu leczniczego[165]), a przez to ujawniono dane pacjentów, w tym dot. zdrowia. W Urzędzie przyjęto, że nie doszło do naruszeń z uwagi na kompetencję Rzecznika do kontaktu z adresatami, obowiązek zachowania przez nich danych w tajemnicy oraz brak możliwości identyfikacji osoby, której dane dotyczą. W innej sprawie[166], stwierdzono m.in., że dokumentacja medyczna, w posiadaniu której był jeden z RzPPSzP, została pod jego nieobecność przełożona z zamykanej na klucz szafy do kartonu, który został zaklejony, a następnie przeniesiony do innego pomieszczenia. Uznano, że nie doszło do nieuprawnionego przetwarzania danych, ponieważ karton został zabezpieczony w kancelarii szpitala, a przedstawiciel jednostki zapewnił o podjęciu działań zmierzających do zabezpieczenia dokumentacji.

Niezależnie od oceny małego prawdopodobieństwa, że zdarzenie stanowiło zagrożenie dla praw lub wolności osób fizycznych w ramach wspomnianych sytuacji, przypadkowe udostępnienie danych podmiotom, do których nie były one kierowane, wypełnia znamiona naruszenia określone w art. 4 pkt 12 RODO.

36. Zastrzeżenia budzi, że w BRPP nie określono, kiedy i przez kogo następuje stwierdzenie naruszenia ochrony danych. W praktyce ocena ta ujmowana była w sprawozdaniu IOD dot. naruszeń. Naruszenie nie było jednak akceptowane albo zatwierdzane przez Administratora, pomimo że to do niego należała decyzja dot. zgłoszenia naruszenia do PUODO oraz poinformowania podmiotu danych. Brak precyzyjnego terminu stwierdzenia naruszenia przekładał się także na trudność w ustaleniu początku biegu terminu na zgłoszenie naruszenia do PUODO. Tym samym przyjęte w BRPP rozwiązanie nie odpowiadało zasadzie rozliczalności.

> Administrator zgodnie z zasadą rozliczalności (art. 5 ust. 2 RODO), jest odpowiedzialny za przestrzeganie przepisów RODO i musi być w stanie to wykazać.
>
> W *Polityce BDO* nie uregulowano kto, w jakim momencie i w jakiej formie stwierdza naruszenie ochrony danych. Wskazano natomiast, że do obowiązków Administratora należy m.in. decyzja o konieczności zgłaszania naruszeń PUODO[167]. Analizę w tym zakresie prowadził IOD w ramach sprawozdania ze sprawdzenia doraźnego, jednak nie było ono akceptowane/zatwierdzane przez Administratora. Wyjaśniono[168], że wstępną analizę zasadności zgłoszeń i powiadomień prowadzi IOD we współpracy z pracownikami BRPP, a następnie sprawa przedstawiana jest Rzecznikowi albo jego Zastępcy i DG. Wskazano, że *Administrator nie zatwierdza formalnie sprawozdania, ale nie przyjmuje go też tylko do wiadomości*. Niejednokrotnie od czasu zawiadomienia Administratora o wszczęciu postępowania doraźnego do czasu otrzymania sprawozdania Rzecznik, jego Zastępca albo DG są w kontakcie z IOD. Wobec tego *sprawozdanie stanowi dokument zamykający działania, w tym ocenę ryzyka naruszenia praw i wolności osób fizycznych, podejmowane nie tylko przez IOD*.
>
> Zgodnie z art. 33 ust. 1 RODO, jeżeli naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych, należy je zgłosić organowi nadzorczemu nie później niż w terminie

[164] Sprawdzenie doraźne nr 20/2018.
[165] Sprawdzenie doraźne nr 12/2018.
[166] Sprawdzenie doraźne nr 10/2019:
[167] Zgłoszenie należało do obowiązków Administratora. W jego imieniu mógł działać w tym zakresie także IOD.
[168] Pismo DG z 8 stycznia 2020 r., znak: RzPP-ODO.091.1.6.2019 i z 20 stycznia 2020 r., znak: RzPP-ODO.091.1.12.2019.

72 godzin po stwierdzeniu naruszenia. Zgodnie z § 30 ust. 2 *Polityki BDO* 72-godzinny termin na zgłoszenie naruszenia do PUODO biegnie od momentu przyjęcia do wiadomości przez Administratora, że doszło do naruszenia. W rejestrze naruszeń natomiast przewidziano konieczność odnotowania terminu na zgłoszenie naruszenia dla IOD, a nie dla Administratora. Wyjaśniono z kolei, że termin 72 godzin rozpoczyna bieg z momentem *stwierdzenia naruszenia w BRPP, a nie przez RPP czy IOD*. Wskazano, że w praktyce czas ten liczony jest od chwili, gdy pracownik poweźmie wiadomość o tym, że okoliczności faktyczne sprawy wskazują na naruszenie ochrony danych[169].

Wg *Wytycznych dot. zgłaszania naruszeń danych osobowych*[170] Administrator *stwierdza* naruszenie, kiedy ma on wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych. Z tego powodu moment stwierdzenia naruszenia powinien być precyzyjnie określony. Przyjęte w BRPP rozwiązania rodzą istotne ryzyko w sytuacji wystąpienia naruszenia, o którym należałoby poinformować PUODO.

37. W Urzędzie rejestrowano informacje o incydentach dotyczących okoliczności naruszenia ochrony danych, jego skutków oraz podjętych działań zaradczych[171]. Jednakże, niezgodnie z § 29 ust. 1 pkt 6 *Polityki BDO* oraz *Wytycznymi dot. zgłaszania naruszeń danych osobowych,* w większości przypadków w rejestrach naruszeń nie wskazywano uzasadnień dot. niezgłoszenia naruszenia do PUODO ani podmiotu danych. *Wytyczne* te zalecają, by w przypadku podjęcia decyzji o niezgłoszeniu naruszenia, udokumentować to w ewidencji wraz z podaniem przyczyny, dla której ryzyko naruszenia praw i wolności osób fizycznych uznano za mało prawdopodobne. Część informacji zawartych w rejestrach była także niepełna.

Rejestry naruszeń były prowadzone dla każdego roku oddzielnie i zawierały niezbędne dane dot. m. in. okoliczności naruszenia danych, ich skutków oraz podjętych działań, w tym informacje nt. ewentualnych powiadomień PUODO/podmiotu danych. W większości pozycji brakowało jednak uzasadnień dla braku konieczności powiadomień. Dotyczy to wszystkich 11 wpisów w *Rejestrze naruszeń* za 2019 r. oraz 13 z 20 (65%)[172] pozycji *Rejestru naruszeń* za 2018 r. Kontrolowany wskazał[173], że informacje te ujmowane są w sprawozdaniach ze sprawdzeń doraźnych.

Okoliczność, że w sprawozdaniach dot. naruszeń ujmowano szczegółowe informacje nie wyłącza obowiązku odnotowania wymaganego zakresu danych w rejestrze naruszeń. W *Polityce BDO* nie przewidziano wyjątków od obowiązku rejestrowania uzasadnień we wspomnianym zakresie.

Rejestr naruszeń za 2018 r., założony z początkiem 2018 r., był niezgodny ze wzorem określonym w *Polityce BDO*, która obowiązywała od 25 maja 2018 r. Rejestry w 2 pozycjach zawierały nieprawidłową[174] datę zgłoszenia naruszenia, a w 3 przypadkach[175] nie opisano w ogóle (1) lub części (2) podjętych działań i decyzji. Niezgodności te były, jak wyjaśniono, błędami i przeoczeniami. Ponadto w 2 przypadkach[176] w rejestrze, jako skutek, wskazano *Nieuprawniony dostęp do danych osobowych* zamiast *możliwość nieuprawnionego dostępu*. We wszystkich wierszach *Rejestru naruszeń* za 2019 r. i 7 wierszach za 2018 r.[177] nie podawano godzin zgłoszenia IOD naruszenia bezpieczeństwa danych. Wyjaśniono[178], że godzina ta odnotowywana jest w systemie EZD.

Rejestr naruszeń ochrony danych powinien rzetelnie dokumentować zgłoszenia i prezentować wyniki sprawdzeń doraźnych, w tym precyzyjnie określać, czy i kiedy do naruszeń faktycznie doszło oraz jakie są ich skutki.

---

[169] Pismo DG z 8 stycznia 2020 r., znak: RzPP-ODO.091.1.6.2019 i z 20 stycznia 2020 r., znak: RzPP-ODO.091.1.12.2019.
[170] Wytyczne Grupy Roboczej Art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01).
[171] Stosownie z art. 33 ust. 5 RODO.
[172] Z wyłączeniem poz. 9-11, 14, 18-20, w których odwoływano się wprost do ryzyka lub wysokiego ryzyka i braku potrzeby wysyłania zawiadomień.
[173] Pismo DG z 8 stycznia 2020 r., znak: RzPP-ODO.091.1.6.2019.
[174] Dot. sprawdzeń doraźnych nr 10/2018 i 8/2019.
[175] Dot. sprawdzeń doraźnych nr 12/2018, 18/2018 i 20/2018.
[176] Dot. sprawdzeń doraźnych nr 2/2019 i 3/2019.
[177] Poz. 2-8 *Rejestru naruszeń* za 2018 r.
[178] Pismo DG z 8 stycznia 2020 r., znak: RzPP-ODO.091.1.6.2019.

38. [nazywanie spraw w EZD] W nazwach 7[179] z 30 (23%) spraw prowadzonych w systemie EZD wskazywano dane pacjentów, w tym także dot. zdrowia, co było niezgodne z zasadą minimalizacji danych oraz zasadami nazywania spraw w Urzędzie. Tym samym już na poziomie spisu spraw widoczne były dane osobowe pacjentów, w części także z informacjami nt. zdrowia.

> Zasadę minimalizacji danych określono w art. 5 ust. 1 pkt c RODO, tj. dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
>
> Wyjaśniono[180], że w nazwach spraw wskazywano dane pacjentów, żeby łatwiej je można było wyszukiwać. Nadzór nad prawidłowością nazywania i prowadzenia spraw w EZD sprawowali kierownicy komórek. Adekwatność przetwarzanych danych podlegała także nadzorowi IOD i, jak zadeklarowano, będzie ona weryfikowana w ramach postępowań sprawdzających. Podczas kontroli zapewniono, że kierownikom komórek zostanie przekazana informacja o konieczności pomijania danych osobowych w nazwach spraw.

39. [dokumentacja przetwarzania danych osobowych] W celu zapewnienia prawidłowości procesu przetwarzania danych regulacje BRPP w tym zakresie wymagają doskonalenia, ponieważ występują w nich braki lub nieścisłości. Pomimo że zidentyfikowano słabości procedur w ramach audytów[181] oraz *Planu IOD*, przez 1,5 roku od przyjęcia dokumentacji przetwarzania, nie były wprowadzane do niej istotne zmiany[182]. W trakcie kontroli procedowano projekt nowej *Polityki BDO*, jednak należy zintensyfikować działania w tym zakresie. Obszary wymagające dalszego doskonalenia obejmują w szczególności wprowadzenie albo doprecyzowanie regulacji w zakresie:

- podziału ról i obowiązków w systemie ochrony danych – w celu wyeliminowania sytuacji, w których zadania były wykonywane przez osoby, którym formalnie nie powierzono takich obowiązków, np. w zakresie rozpatrywania i udzielania odpowiedzi na wnioski podmiotów danych (IOD zamiast Administratora) lub dokonywania analiz naruszeń ochrony danych (IOD zamiast kierowników komórek);
- oceny skutków – dot. procedur i metodyki jej przeprowadzania;
- obowiązku informacyjnego – dot. obowiązku przedstawienia klauzuli informacyjnej osobie, której dane pozyskano od innej osoby, m.in. najpóźniej przy pierwszym ujawnieniu danych innemu odbiorcy (art. 14 ust. 3 lit. c RODO), obowiązku ponownego zastosowania klauzuli wobec osób, których dane zebrano w innym celu niż zamierzony (art. 13 RODO), okoliczności odstąpienia od realizacji obowiązku informacyjnego (art. 3-4 uodo i art. 13 ust. 4 RODO);
- konieczności przeprowadzania okresowych przeglądów i aktualizacji dokumentacji przetwarzania oraz osób za nie odpowiedzialnych;
- powierzania danych – dot. obowiązku uwzględniania w umowach kar umownych za naruszenie postanowień umowy i przepisów prawa w zakresie ochrony danych oraz uwzględnienia przesłanki rozwiązania umowy ze skutkiem natychmiastowym w przypadku naruszenia zasad ochrony danych;
- realizacji praw podmiotów danych – dot. uszczegółowienia trybu postępowania z wnioskiem o realizację praw osób[183], zakresu informacji w rejestrze wniosków podmiotów danych, możliwości odstąpienia od potwierdzania przetwarzania danych, gdy służy to realizacji zadania publicznego i niewykonanie tego potwierdzenia jest niezbędne dla realizacji celów publicznych, o których mowa w art. 23 ust. 1 RODO[184];
- naruszenia ochrony danych – dot. terminu na powiadomienie osoby, której dane dotyczą, uwzględnienia w zawiadomieniu zaleceń co do minimalizacji potencjalnych niekorzystnych skutków (motyw 86 RODO), ujęcia kwestii prawnie uzasadnionego

[179] Sprawy nr RzPP-DZP-RzSP-DC.470.111.2019, RzPP-DZP-WRI.431.90.2019, RzPP-DZP-WRII.431.100.2019, RzPP-DPW-WPI.431.1111.2019, RzPP-DPW-WPI.052.10.2019, RzPP-DPW-WSO.431.50.2019, RzPP-DPW-WPII.052.99.2018.
[180] Pismo DG z 6 lutego 2020 r., znak: RzPP-ODO.091.1.21.2019.
[181] ZA-1/2018 *Ocena działań podjętych przez BRPP w celu dostosowania jednostki do przepisów prawa wynikających z RODO i KRI*; Zadanie sprawdzające wykonanie rekomendacji nr ZA-1/2018; ZA-3/2019 *Realizacja zadań Inspektora Ochrony Danych w Biurze Rzecznika Praw Pacjenta, w szczególności w zakresie zgodności z procedurami wewnętrznymi obowiązującymi w Biurze*.
[182] 2 zmiany obejmowały zarządzenie nr 2/2019 Rzecznika Praw Pacjenta z 28 stycznia 2019 r. dot. wprowadzenia *Zespołu ODO* oraz zarządzenie nr 8/2019 Rzecznika Praw Pacjenta z 24 maja 2019 r. dot. wprowadzenia funkcji Zastępcy Administratora Systemów Informatycznych.
[183] W tym procedury rozpatrywania wniosków, np. terminu realizacji wniosków, obowiązku i osób odpowiedzialnych za powiadomienie każdego odbiorcy, któremu ujawniono dane osobowe o fakcie sprostowania, usunięcia albo ograniczenia przetwarzania danych; procedury dla dostarczenia kopii danych.
[184] Ograniczenie praw i obowiązków ma służyć celom zw. z szeroko rozumianym bezpieczeństwem, m.in. bezpieczeństwem narodowym lub publicznym, obronie, zapobieganiu przestępczości, ochronie niezależności sądów i postępowania sądowego, ochronie osoby, której dot. lub praw i wolności innych osób, egzekucji roszczeń cywilnoprawnych.

interesu organów ścigania (motyw 88 RODO), wzoru notatki dot. okoliczności naruszenia oraz analizy ryzyka praw i wolności;
- analizy ryzyka – dot. procedury oceny ryzyka, określenia metodyki jej prowadzania oraz wskazania osób odpowiedzialnych;
- obowiązków Rzecznika w sytuacji, gdyby zyskał status procesora, w tym w zakresie prowadzenia rejestru kategorii czynności.

Wyjaśniono[185], że w *Polityce BDO* nie zostały powtórzone wszystkie zasady, wykazy i szczegóły procedur wynikające z RODO. Nie zakładano również ujęcia w niej wzorów wszystkich pism, zestawień, notatek i innych dokumentów. Zadeklarowano jednak wprowadzenie zmian w regulacjach. W szczególności uwzględnione zostaną kompleksowe procedury postępowania, tak aby były przejrzyste dla osób zobowiązanych do ich stosowania. Wskazano, że trwające prace nad zmianą *Polityki BDO* stanowiły wynik zebranych doświadczeń, a także spostrzeżeń i uwag przedstawionych w trakcie czynności kontrolnych. W Urzędzie w czasie kontroli podejmowano działania mające na celu wzmocnienie i uzupełnienie dokumentacji systemu ochrony danych, np. opracowano wzór umowy powierzenia danych. W Biurze nie określono zasad pseudonimizacji, ponieważ Kontrolowany nie stwierdził potrzeby jej stosowania.

40. [testowanie środków technicznych i organizacyjnych] Administrator wywiązywał się z obowiązku[186] regularnego testowania i doskonalenia stosowanych środków technicznych i organizacyjnych.

Wyjaśniono[187], że prowadzono m.in. bieżącą analizę stanu urządzeń IT, wymianę najstarszych stacji roboczych i urządzeń peryferyjnych, testy weryfikacji nieautoryzowanych prób wykorzystania konta użytkownika, sprawdzano poprawność działania systemu backupowego. Prowadzone były także systematyczne wizyty służb IT u wszystkich pracowników, zbierano zgłoszenia dot. prawidłowości funkcjonowania sprzętu, organizowano regularne spotkania, w trakcie których omawiano bieżące sprawy ze szczególnym uwzględnieniem kwestii ochrony danych. Ponadto prowadzono szkolenia dla pracowników oraz zaplanowano postępowania sprawdzające IOD.

41. [realizacja rekomendacji audytu wewnętrznego] Pozytywnie należy ocenić, że przeprowadzono audyt wewnętrzny dot. ochrony danych osobowych zarówno w 2018 r., jak i 2019 r. Dzięki temu Rzecznik posiadał informację o słabościach systemu. Z 6 rekomendacji wydanych w 2018 r. zostało wdrożonych 5 (tj. 83%), natomiast w 2019 r. wdrożono 4 z 12 (tj. 33%)[188]. Pozostałe, z wyjątkiem 1 uznanej za bezprzedmiotową, były w trakcie realizacji.

W 2018 r., jak i 2019 r., przeprowadzono audyty zapewniające[189], jak i czynności sprawdzające[190] do audytu z poprzedniego roku w zakresie ochrony danych. Wydano 18 rekomendacji (6 w 2018 r. i 12 w 2019 r.). Rekomendacje z 2018 r. zostały przekazane Rzecznikowi 31 grudnia 2018 r. Jedna zalecająca zaktualizowanie dokumentacji w obszarze danych osobowych pozostawała w trakcie wdrażania. Z 12 rekomendacji otrzymanych przez BRPP 3 grudnia 2019 r. zrealizowano 4 dot. m.in. monitoringu prowadzonego w BRPP, natomiast 1 dot. ułatwienia dostępu do danych kontaktowych IOD na stronie internetowej została uznana za bezprzedmiotową, ponieważ uzyskanie informacji nie wymagało nadmiernego wysiłku. Pozostałe 7, które m.in. dot. wykonania przez IOD kontroli w zakresie prawidłowości stosowania klauzul informacyjnych, wdrożenia kryteriów wyboru podmiotu przetwarzającego i oceny umowy powierzenia danych, wprowadzenia instrukcji postępowania w sytuacji naruszenia danych oraz rozpatrywania żądań osób, których dane dotyczą, na 31 stycznia 2020 r. były w trakcie realizacji.

42. [informacja nt. działań podjętych po kontroli] Po zakończeniu czynności kontrolnych Rzecznik poinformował[191] o podjęciu szeregu istotnych działań wzmacniających

---

[185] Pismo DG z 8 stycznia 2020 r., znak: RzPP-ODO.091.1.6.2019, z 14 stycznia 2020 r., znak: RzPP-ODO.091.1.8.1.2019; z 16 stycznia 2020 r., znak: RzPP-ODO.091.1.10.2019, z 20 stycznia 2020 r., znak: RzPP-ODO.091.1.12.1.2019; 29 stycznia 2020 r., znak: RzPP-ODO.091.1.18.2019; z 31 stycznia 2020 r., znak: RzPP-ODO.091.1.20.2019, pismo IOD z 27 stycznia 2020 r., znak: RzPP-ODO.091.1.16.2019.
[186] Zgodnie z art. 47a ust. 4 pkt 3 *ustawy o RPP*.
[187] Pismo DG z 31 stycznia 2020 r., znak: RzPP-DOD.091.1.20.2019.
[188] Stan na dzień 31 stycznia 2020 r.
[189] ZA-1/2018 *Ocena działań podjętych przez BRPP w celu dostosowania jednostki do przepisów prawa wynikających z RODO i KRI* i ZA-3/2019 *Realizacja zadań Inspektora Ochrony Danych w Biurze Rzecznika Praw Pacjenta, w szczególności w zakresie zgodności z procedurami wewnętrznymi obowiązującymi w Biurze.*
[190] ZA-5/2018 *Zadanie sprawdzające wykonanie rekomendacji z zadania audytowego dotyczącego oceny przetwarzania danych osobowych w BRPP z uwzględnieniem rzeczników praw pacjenta szpitala psychiatrycznego* oraz ZA-4/2019 *Zadanie sprawdzające wykonanie rekomendacji ZA-1/18 Ocena działań podjętych przez BRPP w celu dostosowania jednostki do przepisów prawa wynikającego z RODO i KRI.*
[191] Pismo z 3 czerwca 2020 r., znak: RzPP-ODO.091.122.2019.

obszar ochrony danych osobowych w Urzędzie. W szczególności przyjęto nową Politykę Ochrony Danych Osobowych[192], zmieniono zasady zawierania umów z podmiotami zewnętrznymi oraz wydawania dla takich podmiotów upoważnień do przetwarzania danych osobowych, a osobom nieupoważnionym nadano uprawnienia we wspomnianym zakresie. Podjęto prace nad wprowadzeniem nowego *Rejestru czynności* oraz powołano 9-osobowy *Zespół ODO,* w skład którego weszli reprezentanci wszystkich komórek organizacyjnych BRPP. Ponadto, na IV kwartał 2020 r. zaplanowano audyt sprawdzający w zakresie funkcjonowania systemu ochrony danych osobowych.

Biorąc pod uwagę przedstawione ustalenia i oceny, po uwzględnieniu informacji o podjętych działaniach, zalecam Panu Ministrowi:

1. Kontynuowanie działań gwarantujących, że dane osobowe będą przetwarzane wyłącznie przez osoby posiadające prawidłowe upoważnienia, w tym odpowiednia aktualizacja upoważnień wydanych przed rozpoczęciem stosowania RODO.
2. Wdrożenie *Rejestru czynności* zawierającego pełną i prawidłową informację o wszystkich czynnościach przetwarzania danych osobowych w BRPP.
3. Prawidłową realizację obowiązku informacyjnego, w szczególności poprzez aktualizację klauzul informacyjnych.
4. Wzmocnienie nadzoru nad realizacją procedur związanych z naruszeniami ochrony danych oraz obszarem pozyskiwania zgód na przetwarzanie danych, aby w przyszłości nie powielać nieprawidłowości opisanych w pkt. 26-27 *Wystąpienia*.
5. Wdrożenie prawidłowych środków ochrony danych osobowych z uwzględnieniem wyników zaktualizowanej i zatwierdzonej analizy ryzyka naruszenia praw i wolności osób.
6. Rzetelne prowadzenie ewidencji upoważnień do przetwarzania danych osobowych oraz rejestrów: umów powierzenia przetwarzania danych oraz udostępnień danych.
7. Ujednolicenie w regulacjach wewnętrznych podstaw prawnych dla przetwarzania wizerunku pracowników na identyfikatorach oraz prawidłowe ich wdrożenie.
8. Zapewnienie efektywnego wykonywania zadań przez *Zespół ODO* w celu skutecznego wsparcia działań Administratora.

Proszę Pana Ministra o przedstawienie, w terminie 60 dni od daty otrzymania *Wystąpienia*, informacji o sposobie wykonania zaleceń, wykorzystaniu wniosków lub o przyczynach ich niewykorzystania albo o innym sposobie usunięcia stwierdzonych nieprawidłowości. Jednocześnie, po przeprowadzeniu audytu sprawdzającego w zakresie funkcjonowania systemu ochrony danych osobowych, proszę o przesłanie jego wyników oraz informacji nt. realizacji ewentualnych rekomendacji w tym obszarze.

Informuję, że od *Wystąpienia* nie przysługują środki odwoławcze.

Podstawa prawna:
Art. 46 ust. 1 i 3, art. 47, 48 i 49 *ustawy o kontroli.*

Z poważaniem

w zastępstwie
Szefa Kancelarii Prezesa Rady Ministrów
Paweł Szrot

Sekretarz Stanu
Zastępca Szefa Kancelarii Prezesa Rady Ministrów
/-podpisano kwalifikowanym podpisem elektronicznym-/

[192] Zarządzenie nr 13/2020 Rzecznika Praw Pacjenta z 26 maja 2020 r. w sprawie wprowadzenia Polityki Ochrony Danych Osobowych w BRPP oraz Instrukcji Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych w BRPP.