WUOZ
5218511

WOJEWODA DOLNOŚLĄSKI

Wrocław, dnia 27 stycznia 2020 r.

NK-KS.431.2.5.2019.MGS

Pani
Barbara Nowak-Obelinda
Dolnośląski Wojewódzki
Konserwator Zabytków

Wystąpienie pokontrolne

W dniach od 12 do 28 czerwca 2019 r. (z przerwami) na podstawie art. 28 ust. 1 pkt 1 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (t. j. Dz. U. z 2019 r. poz. 1464) oraz imiennych upoważnień Wojewody Dolnośląskiego z dnia 10 czerwca 2019 r. znak NK-KS.0030.51.2019.MGS, NK-KS.0030.52.2019.MGS oraz NK-KS.0030.53.2019.MGS zespół kontrolny w składzie: Monika Grzywalska-Świątek – główny specjalista (przewodnicząca zespołu kontrolnego), Ewa Sidyk – kierownik Oddziału Kontroli i Skarg oraz Magdalena Kremienowska – główny specjalista, z Wydziału Nadzoru i Kontroli Dolnośląskiego Urzędu Wojewódzkiego we Wrocławiu, przeprowadził kontrolę problemową w trybie zwykłym w Wojewódzkim Urzędzie Ochrony Zabytków, z siedzibą przy ul. Władysława Łokietka 11, 50-243 Wrocław (zwany dalej WUOZ), której tematem była *Ochrona danych osobowych.*

Okres objęty kontrolą – od 25 maja 2018 r. do dnia kontroli.

Celem kontroli była ocena funkcjonowania systemu ochrony danych osobowych, w szczególności ocena spełnienia wymogów, wynikających z 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 (ogólnego rozporządzenia o ochronie danych) zwanego dalej RODO, ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz. U. z 2019 r. poz. 1781) zwanej dalej UODO i przepisów szczególnych dotyczących ochrony danych osobowych.

Kontrolą objęto następujące obszary:

A. Organizacja systemu ochrony danych osobowych
B. Prawo do przetwarzania danych osobowych
C. Realizacja praw osoby, której dane dotyczą
D. Inspektor ochrony danych

E. Rejestrowanie czynności przetwarzania danych osobowych
F. Ocena skutków przetwarzania danych osobowych
G. Naruszenie ochrony danych osobowych

Kontrolę przeprowadzono w oparciu o zatwierdzony w dniu 13 grudnia 2018 r. przez Wojewodę Dolnośląskiego plan kontroli na I półrocze 2019 r.

Funkcjonowanie systemu ochrony danych osobowych oraz spełnianie wymogów wynikających z ogólnego rozporządzenia o ochronie danych, ustawy o ochronie danych osobowych oraz przepisów szczególnych dotyczących ochrony danych osobowych, w kontrolowanym okresie, **oceniam negatywnie.** W szczególności wpływ na ocenę miały stwierdzone nieprawidłowości w zakresie:

- niewyznaczenia w okresie od 1 maja 2019 r. do 3 czerwca 2019 r. inspektora ochrony danych oraz niezawiadomienie w terminie Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu inspektora ochrony danych,

- niewykazania realizowania obowiązku informacyjnego wynikającego z art. 13 RODO w procesie zamówień publicznych oraz rejestracji korespondencji,

- niewykazanie współadministratorów mimo zidentyfikowania takiej relacji,

- prowadzenie rejestru wszystkich kategorii czynności przetwarzania mimo niewystępowania relacji, w której DWKZ występuje jako podmiot przetwarzający dane w imieniu innego administratora.

W okresie objętym kontrolą funkcję Dolnośląskiego Wojewódzkiego Konserwatora Zabytków we Wrocławiu (zwany dalej DWKZ) pełniła Pani Barbara Nowak-Obelinda, a funkcję Zastępcy Dolnośląskiego Wojewódzkiego Konserwatora Zabytków we Wrocławiu (zwany dalej Zastępca DWKZ) pełnił Pan Daniel Gibski.

Stan faktyczny i ocenę poszczególnych obszarów sporządzono w oparciu o udostępnione w toku wykonywania czynności kontrolnych dokumenty i wyjaśnienia składane przez Zastępcę DWKZ odpowiednio z dnia 6 czerwca 2019 r., 14 czerwca 2019 r., 27 czerwca 2019 r., 4 lipca 2019 r., 8 sierpnia 2019 r.

Obszar A - Organizacja systemu ochrony danych osobowych

W toku czynności kontrolnych w WUOZ kontrolującym udostępniono *Politykę bezpieczeństwa informacji w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu* wraz z 27 załącznikami. Jak ustalono [wyjaśnienia Zastępcy DWKZ z 4 lipca 2019 r. dowód: akta kontroli str. 45-170] ww. Polityka bezpieczeństwa informacji została przyjęta ustnie i na tej podstawie wdrożona, a pracownicy zostali zapoznani z polityką oraz zobligowani do jej stosowania. Odnosząc się do złożonych wyjaśnień w zakresie *ustnego przyjęcia* opisywanej Polityki bezpieczeństwa informacji zauważyć należy, iż w § 5 ust. 4 Polityki ochrony danych osobowych stanowiącej załącznik nr 4 do Polityki bezpieczeństwa informacji określono, iż

Administrator może doprecyzować postanowienia Polityki ochrony danych osobowych w formie odrębnego aktu wewnętrznego takiego jak rozkaz, zarządzenie, decyzja. Zatem przyjąć należy, iż *Polityka bezpieczeństwa informacji* powinna być również wprowadzona aktem wewnętrznym.

Z uwagi na brak daty na dokumencie Polityki Bezpieczeństwa Informacji (mimo przeznaczonej do tego rubryki na dokumencie) kontrolerzy wystąpili o udzielenie informacji kiedy wprowadzono powyższy dokument. W wyjaśnieniach z 8 sierpnia 2019 r. [dowód: akta kontroli str. 295-305] poinformowano, iż cyt. *„Data obowiązywania wskazana jest na dokumentach dostarczonych Kontrolującemu w trakcie kontroli: 25 maja 2019 r.”*, mimo iż RODO obowiązuje od dnia 25 maja 2018 r. (czyli rok wcześniej). Odnosząc się do ww. wyjaśnień wskazać należy, że jedynie na dwóch załącznikach Polityki Bezpieczeństwa Informacji tj. na załączniku nr 4 (Polityka ochrony danych osobowych) oraz załączniku nr 25 (Procedura postępowania względem żądań osób, których dane dotyczą w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu), widnieje zapis że dokument wchodzi w życie z dniem 25 maja 2018 r., zatem jest to data wejścia w życie tych konkretnych załączników do Polityki Bezpieczeństwa Informacji. Biorąc jednak pod uwagę, iż opisywane wyżej załączniki do Polityki Bezpieczeństwa Informacji obowiązują od dnia 25 maja 2018 r. uznać należy wskazaną w wyjaśnieniach datę tj. 25 maja 2019 r. za oczywistą omyłkę pisarską.

W skład Polityki Bezpieczeństwa Informacji wchodzi 27 załączników m. in. Rejestr czynności przetwarzania danych osobowych w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu (zał. nr 1); Rejestr czynności przetwarzania danych osobowych podmiotu przetwarzającego w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu (zał. nr 2); Polityka ochrony danych osobowych (zał. nr 4); Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu (zał. nr 5); Metodyka szacowania ryzyka (zał. nr 24); Procedura postępowania z żądaniami (zał. nr 25); Instrukcja odstąpienia od obowiązku informacyjnego (zał. nr 27).

Kontrola wykazała, iż udostępniona *Polityka bezpieczeństwa informacji w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu* wraz z 27 załącznikami zawiera zarówno wzory dokumentów np. rejestr czynności przetwarzania danych, jak i wypełnione dokumenty podlegające modyfikacjom tj. klauzula informacyjna, rejestr umów powierzenia, rejestr upoważnień, w których wpisy są zmieniane/uzupełniane.

W wyjaśnieniach z 4 lipca 2019 r. poinformowano, że cyt. *„Wedle przyjętej organizacji, w wersji papierowej utrzymywane są wzory dokumentów, które podlegają wypełnieniu (są używane np. wzory upoważnień) w zależności od zaistniałej potrzeby, natomiast w wersji elektronicznej utrzymywane są wzory sensu stricte. Zatem załącznikami do Polityki są zarówno dokumenty jak i wzory. Wzorami są dokumenty, które stanowią załącznik do polityki i nie są wypełnione - w zależności od potrzeby (zaistniałej sytuacji) są one kserowane i wypełniane ręcznie, a następnie załączane do stosownego rejestru, np. rejestru upoważnień dla pracowników do pracy z danymi.*

Współadministrowanie

W piśmie z dnia 6 czerwca 2019 r. w punkcie 2 wskazano, iż cyt. *„Jednostka kontrolowana występuje jako współadministrator danych w postępowaniach, w których organ kontrolowany otrzymał akta sprawy wraz z danymi strony do dalszego prowadzenia, jako organ właściwy”* [dowód: akta kontroli str. 5-7]. Natomiast w Rejestrze czynności przetwarzania danych osobowych w rubryce 2 pn. Nazwa oraz dane kontaktowe współadministratora danych

osobowych (o ile ma to zastosowanie) przy każdym zidentyfikowanym procesie wskazano informację *nie dotyczy*, w tym w m.in. w procesie postępowanie administracyjne – organ I instancji (poz. 38) czy opiniowanie/wydawanie decyzji/w sprawcach ochrony zabytków (poz. 39). W świetle dokonanych w toku kontroli ustaleń wystąpiono do DWKZ o potwierdzenie zidentyfikowanej relacji współadministrowania, mając na uwadze art. 26 ust. 1 RODO, który stanowi, iż *jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami.* W przypadku potwierdzenia występowania Dolnośląskiego Wojewódzkiego Konserwatora Zabytków w roli współadministratora, wystąpiono o przekazanie wspólnych uzgodnień ze współadministratorami dotyczących celów i sposobów przetwarzania, o których mowa w art. 26 ust. i 2 RODO oraz wyjaśnienie przyczyny niewykazania współadministratora w Rejestrze czynności przetwarzania danych osobowych w ww. procesach.

W odpowiedzi, w wyjaśnieniach z dnia 4 lipca 2019 r. Zastępca DWKZ nie odniósł się do braku ujawnienia ww. relacji w Rejestrze czynności przetwarzania, informując wyłącznie, iż cyt. *„Jednostka kontrolowana wskazuje, że nie posiada wspólnych uzgodnień z innymi współadministratorami"* [dowód: akta kontroli str. 268-273].

W nawiązaniu do powyższej informacji oraz złożonych wcześniej wyjaśnień, potwierdzających fakt zidentyfikowania relacji współadministrowania cyt. „w postępowaniach, w których organ kontrolowany otrzymał akta sprawy wraz z danymi strony do dalszego prowadzenia, jako organ właściwy" ponownie poproszono o wskazanie przyczyny niewskazania w Rejestrze czynności przetwarzania danych osobowych relacji współadministrowania w żadnym z procesów przetwarzania danych osobowych. Jednocześnie wystąpiono o wskazanie procesów – poprzez odniesienie się do poszczególnych pozycji ww. Rejestru – w których ww. relacja współadministrowania została zidentyfikowana. W odpowiedzi z dnia 8 sierpnia 2019 r. Zastępca DWKZ ponownie nie odniósł się do przyczyny braku ujawnienia relacji współadministrowania, nie wskazał również procesów, w których ta relacja występuje, wskazując wyłącznie cyt. *"Jednostka kontrolowana wskazuje, iż w tym zakresie także udzieliła już odpowiedzi. Nie jest możliwe przewidzenie wszystkich współadministratorów w każdej sytuacji, zwłaszcza jeżeli następuje przekazanie sprawy"* [dowód: akta kontroli str. 296-299].

W świetle dokonanych ustaleń oraz złożonych wyjaśnień wskazujących, iż organ kontrolowany nie jest w stanie wykazać administratorów, z którymi wiąże go zidentyfikowana relacja współadministrowania (w Rejestrze przetwarzania danych osobowych również brak ujawnionej relacji) oraz wobec braku wspólnych uzgodnień z innymi współadministratorami dotyczących wspólnego ustalania celu i sposobu przetwarzania stwierdzono, iż DWKZ nie wykazał w toku kontroli istnienia relacji, w której występuje jako współadministrator w rozumieniu art. 26 ust. 1 RODO.

Podkreślenia wymaga, iż zgodnie z definicją art. 4 pkt 7 RODO „administrator" *oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.* W kontekście złożonych wyjaśnień należy również przytoczyć pojęcie *odbiorcy*, zdefiniowanego w art. 4 pkt 9 RODO, który oznacza *osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od*

tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.

Natomiast zgodnie z art. 26 ust. 1 RODO, o współadministratorach można mówić w przypadku, gdy co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania. Zatem aby można było wskazywać na istnienie w konkretnym przypadku tak określonej grupy podmiotowej, konieczne jest kumulatywne spełnienie dwóch warunków: po pierwsze – w relacji pozostawać musi co najmniej dwóch administratorów, pod drugie zaś – administratorzy ci muszą wspólnie ustalać cele i sposoby przetwarzania. W tym miejscu zgodzić należy się również ze stanowiskiem doktryny[1], iż „dla stwierdzenia współadministrowania oraz przyznania poszczególnym administratorom statusu "współadministratora" nie wystarcza zatem, by pozostawali oni w jakiejkolwiek relacji związanej z przetwarzaniem danych osobowych. Ich relacja bowiem nacechowana być musi współdziałaniem przy ustalaniu celów i sposobów przetwarzania. Kolejnym zaś krokiem, wprawdzie niekonstytutywnym dla stwierdzenia, że mamy do czynienia ze współadministratorami, ale nieodzownym dla uznania, że współadministratorzy działają zgodnie z prawem, jest dokonanie przez nich wspólnych uzgodnień określających odpowiednie zakresy ich odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO. Skoro współadministratorami mogą pozostawać administratorzy, konieczne jest, by każdy z podmiotów będących w relacji opisanej w art. 26 RODO mógł być kwalifikowany jako "administrator" w rozumieniu art. 4 pkt 7 RODO".

Z treści art. 26 RODO wywodzić można, że współadministrowanie kwalifikować należy jako stan faktyczny, z którym RODO wiąże określone obowiązki i skutki prawne. Przy czym określonego w ww. przepisie współadministrowania nie uzależnia się od uprzedniego istnienia przepisu prawa, czy umowy, które byłyby źródłem relacji administratorów. Dla uznania, że mamy do czynienia ze współadministrowaniem za wystarczające uznać należy więc wyłącznie to, że w danym przypadku istnieje co najmniej dwóch administratorów ustalających wspólnie cele i sposoby przetwarzania, niezależnie od przyczyny, dla której pozostają oni w tym stosunku. Konsekwencją tak określonej relacji współadministrowania pozostają obowiązki dotyczące dokonania odpowiednich wspólnych uzgodnień, o których mowa w dalszej części art. 26 ust. 1 oraz w ust. 2 zd. 1 RODO, a także – zgodnie z art. 26 ust. 2 zd. 2 – konieczność udostępnienia zasadniczej treści tych uzgodnień podmiotom, których dane dotyczą. Uzgodnienia, o których mowa powyżej, traktować należy zatem jako określony w RODO skutek współdziałania pomiędzy co najmniej dwoma podmiotami, którego cechą charakterystyczną jest to, że podmioty te ustalają wspólnie cele i sposoby przetwarzania danych osobowych[2].

Natomiast jak wykazały wyniki kontroli, organ kontrolowany, mimo zadeklarowania, iż występuje jako współadministrator nie był w stanie wykazać jednoznacznie z jakimi administratorami łączy go ta relacja, wykazać wspólnego ustalania celów i sposobów przetwarzania z jakimkolwiek innym administratorem, bądź wykazać istnienia ww. stosunku w przepisach prawa. W świetle powyższego stwierdzono, iż kontrolowany organ nie dokonał

---

[1] Ogólne rozporządzenie o ochronie danych osobowych. Komentarz red. dr Marlena Sakowska-Baryła, Warszawa 2018 ; komentarz do art. 26.

[2] Tamże.

identyfikacji procesów przetwarzania danych osobowych, które mają więcej niż jednego administratora. Podkreślenia wymaga, iż administrator danych, zgodnie z zasadą rozliczalności wyrażoną w art. 5 ust.2 RODO musi być w stanie wykazać przestrzeganie wypełnienia przepisów RODO, w tym również obowiązków wynikających z art. 26 RODO.

W myśl art. 29 RODO podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Natomiast zgodnie z art. 32 ust. 4 RODO Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

W toku kontroli ustalono, że w WUOZ uregulowano zagadnienia dotyczące udzielania upoważnień do przetwarzania danych osobowych w Polityce Bezpieczeństwa Informacji oraz w Polityce ochrony danych osobowych (zał. nr 4 do ww. Polityki Bezpieczeństwa Informacji). W myśl powyższych regulacji cyt. *DWKZ jako Administrator nadaje upoważnienia pracownikom bądź osobom wykonującym zadania na rzecz WUOZ; nadanie upoważnienia następuje w formie pisemnego wniosku złożonego przez właściwego kierownika do DWKZ; odebranie upoważnienia następuje na mocy zwolnienia ze stosunku pracy poprzez wykreślenie z rejestru osób lub zakończenie okresu praktyki/stażu* (pkt. 6.3 Polityki Bezpieczeństwa Informacji). Wykaz osób upoważnionych do przetwarzania danych prowadzi osoba zatrudniona na stanowisku ds. kadr (pkt. 1.5 Polityki Bezpieczeństwa Informacji), a Wzór upoważnienia do przetwarzania danych osobowych stanowi zał. Nr 9 do ww. Polityki Bezpieczeństwa Informacji.

Rozszerzeniem powyższych regulacji są zapisy zawarte w obowiązującej w WUOZ Polityce Ochrony Danych Osobowych. Zgodnie z § 10 pkt 2 ww. Polityki *DWKZ upoważnia osoby zatrudnione w WUOZ bez względu na charakter zatrudnienia, odbywające staż lub praktykę, realizujące zadania na podstawie umowy cywilnoprawnej, realizujące zadania w ramach prac w komisjach, zespołach, grupach roboczych realizujące zadania podczas szkoleń w zakresie niezbędnym do realizacji zadań podczas wykonywanej pracy lub innych czynności.* Przy tym osoby upoważnione do przetwarzania danych osobowych, wraz z nadaniem im upoważnienia do przetwarzania danych osobowych, składają w kadrach, oświadczenie o zachowaniu w tajemnicy danych osobowych i sposobów ich zabezpieczenia; wzór oświadczenia stanowi załącznik nr 11 do Polityki Bezpieczeństwa Informacji (§ 10 pkt 9 Polityki Ochrony Danych Osobowych).

Natomiast w myśl § 10 pkt 12 i 13 ww. Polityki *Upoważnienie do przetwarzania danych osobowych, jak również upoważnienie do nadawania i podpisywania upoważnień wygasa automatycznie wraz z ustaniem stosunku zatrudnienia, zakończeniem wykonywania prac, określonych umową cywilnoprawną / o staż / praktykę, a także obowiązków związanych z pracą w komisjach, zespołach, grupach roboczych. Upoważnienie (...) Administrator może cofnąć o każdym czasie (...)".* W § 10 pkt 7 ww. Polityki zawarto ponadto zapis, iż *DWKZ może pisemnie upoważnić inną osobę do nadawania i podpisywania upoważnień do przetwarzania danych osobowych.* Jednocześnie zgodnie z zapisami § 10 pkt 10 ww. Polityki osoba zajmująca się kadrami przechowuje zgodnie z przepisami właściwymi w sprawach kancelaryjnych „Upoważnienia do przetwarzania danych osobowych", „Upoważnienia do nadawania i podpisywania upoważnień" oraz oświadczenia, o których mowa w § 10 pkt. 10.

W toku kontroli ustalono w oparciu o złożone pismem z 4 lipca 2019 r. wyjaśnienia [dowód: akta kontroli str. 267-273], iż wszyscy pracownicy, którzy pracują z danymi osobowymi w WUOZ, posiadają stosowne upoważnienia, a ewidencję wydanych upoważnień stanowi *Rejestr upoważnień*. Ponadto w opisywanych wyjaśnieniach poinformowano, że cyt.: *„Poza pracownikami upoważnienie udzielane jest praktykantom odbywającym praktyki w WUOZ. Do ww. kategorii osób stosowane są te same upoważnienia jak dla pracowników, ze względu na możliwość kształtowania celu i zakresu udostępnionych danych. Upoważnienia te również ujmowane są w rejestrze".*

W celu potwierdzenia dokonanych ustaleń, weryfikacji poddano przedłożone przez kontrolowany organ upoważnienia do przetwarzania danych osobowych wydane dla następujących pracowników WUOZ: pracownika ds. kadr i obsługi zatrudnienia (Pani J. W.), pracownika prowadzącego rejestr skarg i wniosków (Pana D. G.), pracownika archiwum (Pani M. D.) oraz 4 pracowników zatrudnionych w Wydziale Rejestru i Dokumentacji Zabytków prowadzących postępowania administracyjne (Pani A. W, Pani K. M., Pani B. L., Pani I. Z.-S.) [dowód: akta kontroli str. 258-264].

Stwierdzono, że ww. pracownicy przetwarzający dane osobowe posiadają upoważnienie do przetwarzania danych osobowych zawierające: datę nadania, dane upoważnianego pracownika, zakres upoważnienia, okres ważności upoważnienia, podpisane przez DWKZ. Wszystkie ww. dokumenty wydane zostały po wejściu w życie przepisów RODO, a jako podstawę prawną wydania przywołują ten akt prawny.

Kontrola wykazała, iż wymienieni pracownicy złożyli również oświadczenie o treści: cyt. *Zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, do których mam lub będę miał(a) dostęp w związku z wykonywaniem prac na rzecz Wojewódzkiego Urzędu Ochrony Zabytków we Wrocławiu. Zobowiązuję się przestrzegać polityk, instrukcji, regulaminów i procedur obowiązujących w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu dotyczących ochrony danych osobowych, w szczególności oświadczam, że bez upoważnienia nie będę wykorzystywał(a) danych osobowych ze zbiorów urzędu.* Ponadto w ww. oświadczeniu pracownicy potwierdzili zapoznanie się z przepisami RODO, właściwymi przepisami z zakresu ochrony danych osobowych, w tym informacjami o grożącej odpowiedzialności karnej, a także z procedurami i instrukcjami obowiązującymi w zakresie ochrony danych osobowych w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu [dowód: akta kontroli str. 251-257].

Stwierdzono że wszystkie skontrolowane upoważnienia, jak i oświadczenia zostały sporządzone według wzoru stanowiącego odpowiednio załącznik nr 9 i załącznik nr 11 Polityki bezpieczeństwa informacji.

Ponadto w toku kontroli zweryfikowano spełnienie wymogów wprowadzonych z dniem 4 maja 2019 r. ustawą 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).

W toku kontroli ustalono, iż pracownik zajmujący w WUOZ samodzielne stanowisko ds. kadr posiadał pisemne upoważnienie oraz został zobowiązany do zachowania danych

w tajemnicy, stosownie do wymogu art. 22^{1b} § 3 Kodeksu pracy[3], który stanowi, iż do przetwarzania danych osobowych, o których mowa w art. 9 ust. 1 RODO, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę; osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy.

Umowa powierzenia

Zgodnie z art. 28 ust. 1 i 3 RODO przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

W toku kontroli zweryfikowano czy DWKZ jako Administrator Danych powierza przetwarzanie danych podmiotom przetwarzającym, a jeśli tak czy to powierzenie nastąpiło przy spełnieniu warunków określonych w art. 28 RODO.

Na podstawie Rejestru umów o powierzenie przetwarzania danych osobowych [dowód: akta kontroli str. 117] oraz złożonych w toku kontroli wyjaśnień ustalono, iż w okresie objętym kontrolą DWKZ zawarł 5 umów powierzenia przetwarzania danych osobowych [dowód: akta kontroli str. 5-7].

Analiza przekazanych umów powierzenia wykazała, iż w niżej wymienionych 3 umowach nie zawarto wszystkich elementów określonych w art. 28 ust. 3 RODO. Umowa ujęta pod nr 2 w Rejestrze umów, nie zawiera określenia rodzaju danych osobowych oraz kategorii osób, których dane dotyczą i charakteru przetwarzania. Charakteru przetwarzania nie zawierają również umowy ujęte w poz. 3 i 4 Rejestru – bowiem w załączniku A w punkcie 1.1 w miejscu charakter wpisano: *przetwarzanie danych osobowych przez Procesora.*

Do dokonanych ustaleń w trakcie kontroli Zastępca DWKZ odniósł się w wyjaśnieniach z dnia 4 lipca 2019 r. [dowód: akta kontroli str. 268-273] kwestionując istnienie wskazanych przez kontrolujących odstępstw od wymogów RODO.

W zakresie stwierdzonej nieprawidłowości polegającej na nie zawarciu w umowie ujętej pod poz. 2 w Rejestrze umów określenia rodzaju danych osobowych oraz kategorii osób, których dane dotyczą i charakteru przetwarzania wyjaśniono, iż cyt. „w zawartej umowie w § 1 pkt 1 strony zastosowały skrót myślowy określający powierzenie danych zwykłych i wrażliwych. W umowie strony posługiwały się definicją danych osobowych ujętą w art. 4 pkt 1 rodo". Złożone wyjaśnienia w powyższym zakresie nie zasługiwały na uwzględnienie, z przyczyn, o których mowa poniżej. Przede wszystkim należy zwrócić uwagę, iż wyliczenie szczególnych kategorii danych osobowych (tzw. danych wrażliwych) zawiera art. 9 ust. 1 RODO. Natomiast jak wynika z analizy przedmiotowej umowy, paragraf 1 pkt 1 zawierał następujące brzmienie *„Administrator danych powierza Podmiotowi przetwarzającemu, w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 r. (zwanego dalszej części „rozporządzeniem", dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej umowie".* Jak wynika ze zderzenia brzmienia ww. paragrafu umowy i złożonych wyjaśnień, skrótem myślowym określającym powierzenie danych zwykłych i wrażliwych - zdaniem organu kontrolowanego - ma być zwrot *dane osobowe do przetwarzania.* Biorąc pod uwagę, iż zapisy umowy w żaden

[3] Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (t. j. Dz.U. z 2019 r. poz. 1040 ze zm.)

sposób nie definiowały pojęć użytych w umowie, w szczególności nie wskazywały, iż przez dane osobowe należy rozumieć dane zwykłe i wrażliwe, brak jest podstaw do uznania, iż umowa zawiera wskazanie rodzaju danych osobowych.

Oceniając kontrolowaną umowę pod kątem spełnienia pozostałych wymogów art. 28 ust. 3 RODO, nie uwzględniono również dalszej części wyjaśnień. Jak to zostało przytoczone powyżej, kotrolujący stwierdzili w przedmiotowej umowie powierzenia ponadto brak zapisów dotyczących *kategorii osób, których dane dotyczą* i *charakteru przetwarzania.* W wyjaśnieniach nie wykazano zapisów umowy powierzenia wskazujących na spełnienie tych wymogów. Wyjaśnienia kontrolowanego organu i powołana argumentacja skupiały się wyłącznie wokół kwestii cyt. *„W umowach należy badać, jaki był zgodny zamiar stron i cel umowy, aniżeli opierać się na jej dosłownym brzmieniu"*. Podkreślenia wymaga, iż kontrolujący nie negują intencji stron zawartej umowy, niemniej jednak nie jest możliwe uwzględnienie złożonych wyjaśnień[4], bowiem mimo wskazania, iż cyt. *Zatem o ile nie zawarto literalnego odniesienia do wymogu, to osiągnięto go poprzez zapis ogólny (...)*, nie wykazano żadnego zapisu umowy odnoszącego się do *kategorii osób, których dane dotyczą* i *charakteru przetwarzania.* Przedmiotowy zakres umowy lub innego instrumentu prawnego regulującego przetwarzanie przez podmiot przetwarzający zasadniczo nakreślony został już w motywie 81 preambuły RODO. Wskazano tam, że określać mają one przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą. Stąd w art. 28 RODO wyróżnia się *essentialia negotii,* czyli niezbędne konstrukcyjne elementy umów lub aktów regulujących powierzenie przetwarzania. Mając na uwadze, iż wśród tych elementów, zgodnie z art. 28 ust. 3 RODO muszą się znaleźć zarówno *charakter przetwarzania*, *rodzaj danych osobowych* jak i *kategorie osób, których dane dotyczą*, złożone wyjaśnienia nie zostały uwzględnione za kontrolowane zagadnienie i uznano, iż przedmiotowa umowa nie zawiera wyżej wskazanych trzech elementów.

Zastępca DWKZ również nie zgodził się ze stwierdzeniem, iż umowy ujęte pod poz. 3 i 4 nie zawierają charakteru przetwarzania argumentując to w następujący sposób cyt. *„jednostka kontrolowana nie zgadza się również z twierdzeniem, iż dla umów z pozycji 3 i 4 nie ujęto charakteru przetwarzania. Załącznik A określa jakie dane są przetwarzane oraz wskazuje, że załącznik A jest załącznikiem do umowy powierzenia danych z dnia 25 maja 2018 r. Natomiast w umowie o przetwarzanie danych jako „procesora" strony określiły Centralny Ośrodek Informatyki. Tym samym jest to zapis umowny - zapis techniczny dla uproszczenia poruszania się po umowie. Jak wskazano wyżej, umowy należy interpretować w oparciu o wskazówki art. 65 kc oraz zgodną intencję stron (tj. to co strony chciały osiągnąć), a nie tłumaczyć ją literalnie. W szczególności należy uwzględniać cel umowy i zastosowanych rozwiązań"*. Złożone wyjaśnienia nie zostały uwzględnione. Kontrolujący, jako odstępstwo

[4] „nadto art. 28 RODO określa, że przetwarzanie przez podmiot -przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora. Zapis ten jest odesłaniem do stosowania przepisów i technik ich zawierania oraz wykonywania wedle prawa krajowego. Zgodnie z art. 65 kc oświadczenia woli (umowy) należy tak tłumaczyć, jak tego wymagają ze względu na okoliczności, w których złożone zostało, zasady współżycia społecznego oraz ustalone zwyczaje. W umowach należy badać, jaki był zgodny zamiar stron i cel umowy, aniżeli opierać się na jej dosłownym brzmieniu. Zatem o ile nie zawarto literalnego odniesienia do wymogu, to osiągnięto go poprzez zapis ogólny, który przez wykładnię celowościową i opartą o intencję stron zgodnie strony rozumieją jako wypełnienie wszelkich obowiązków RODO, w szczególności wynikających z art. 28".

od wymogów RODO wskazali, iż w załączniku A w miejscu charakter przetwarzania wskazano cyt. *przetwarzanie danych osobowych przez Procesora.* Powodem uznania ww. sformułowania jako niewypełnienia dyspozycji art. 28 ust. RODO nie jest wyłącznie niesprecyzowanie nazwy procesora, na czym skupiają się wyjaśnienia podmiotu kontrolowanego, a fakt iż jako charakter przetwarzania wskazano *przetwarzanie danych osobowych,* bez uszczegółowienia charakteru. Podkreślenia wymaga, iż RODO nie zawiera definicji pojęć użytych w art. 28 ust. 3 RODO, niemniej jednak w literaturze[5] wskazuje się, że "charakter przetwarzania" może być interpretowany w kontekście art. 27 ust. 2 lit. a oraz art. 30 ust. 5 RODO. W tym przypadku przez charakter przetwarzania można rozumieć przetwarzanie sporadyczne, nieregularne, niesystematyczne albo też cykliczne, częste itp. Tym samym definicja charakteru przetwarzania sprowadza się do sposobów i metod przetwarzania, które charakteryzować mogą właśnie takie czynniki, jak: częstotliwość, powtarzalność, czasowość, długo- bądź krótkoterminowość, masowość, małą lub wręcz nikłą skalę, zautomatyzowanie lub stopień zautomatyzowania operacji, wykonywanie czynności odnoszących się wyłącznie do dokumentów papierowych itp. Podobnie definiuje to inny autor wskazując, iż charakter (operacji) przetwarzania danych to raczej sposób ich dokonywania (częstotliwość/powtarzalność, czasowość, długoterminowość, masowość) z uwzględnieniem rodzajów zastosowanych technologii[6].

Odnosząc się do złożonych wyjaśnień w zakresie umów ujętych pod poz. 3 i 4 w Rejestrze umów zgodzić należy się, iż ww. załącznik A stanowi załącznik do umowy oraz zawiera informacje jakie dane będą przetwarzane, bowiem wskazuje jednoznacznie rodzaj danych osobowych (pkt 3) oraz kategorie osób, których dane dotyczą (pkt 2) a ponadto również obszar, na którym przetwarza będą dane osobowe (pkt 4). Niemniej jednak, żadne z powołanych w wyjaśnieniach zapisy umowy nie wskazują charakteru przetwarzania, w rozumieniu wyżej przytoczonych definicji, co stanowi naruszenie art. 28 ust. 3 RODO.

Analizując zawarte umowy powierzenia, kontrolujący ustalili, iż w umowie ujętej w Rejestrze pod poz. 5 nie wskazano jednoznacznie zapisu stanowiącego, *iż podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora (...)* (art. 28 ust. 3 pkt a RODO), mimo iż pozostałe umowy ten zapis zawierają. W odniesieniu do powyższego ustalenia Zastępca DWKZ wyjaśnił, iż cyt. *(...) niezastosowanie literalnego brzmienia „podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora" nie stanowi uchybienia. Art. 28 ust 3 pkt. a RODO określa warunek materialny umowy o powierzenie danych, a więc kwestie techniczną, a nie formalną, bez której umowa jest nieważna. Wedle interpretacji ww. artykułu przez jednostkę kontrolowaną istotne jest osiągniecie celu zapisu, a więc przetwarzanie danych jedynie w takim zakresie w jakim administrator poleci je przetwarzać. Jeżeli przetwarzanie danych wykonywane jest w ramach realizacji umowy zasadniczej (cywilnej), która stanowi główne źródło relacji łączącej strony, to umowa o powierzenie danych pełni też funkcję polecenia przetwarzania określonych danych w celu realizacji zawartej umowy głównej (cywilnej). Jest to przejaw podstawowych zasad państwa prawa - zasada legalizmu. Zatem brak zapisu, zdaniem jednostki kontrolowanej nie stanowi uchybienia czy odstępstwa".*

---

[5] Ogólne rozporządzenie o ochronie danych osobowych. Komentarz red. dr Marlena Sakowska-Baryła, Warszawa 2018 ; komentarz do art. 28.

[6] Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz red. dr Paweł Litwiński, Warszawa 2018, komentarz do art. 24.

Odnosząc się do złożonych wyjaśnień należy się zgodzić, iż w umowie powierzenia nie jest konieczne zawarcie literalnego brzmienia *„podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora"*. Zważywszy na art. 28 ust. 3 RODO i wyspecyfikowane tam cechy treści umowy powierzenia, aby uznać, iż umowa zawiera wszystkie wymagane elementy należy wykazać, iż zawiera zapisy odnoszące się do obowiązku podmiotu przetwarzającego, o którym mowa w art. 28 ust. 3 lit. a RODO. Organ kontrolowany nie odniósł się w wyjaśnieniach wprost do żadnych zapisów umowy wykazujących spełnienie ww. wymogu. Niemniej jednak, oceniając przedmiotową umowę powierzenia, kontrolujący wzięli pod uwagę własne ustalenia, z których wynika, iż w § 1 pkt 2 umowy powierzenia znajduje się zapis, iż podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową (...) a w § 2 pkt 3 umowy wskazano, iż powierzone przez Administratora dane osobowe będą przetwarzane przez podmiot przetwarzający w celu realizacji umowy z dnia 3 czerwca 2019 r., której przedmiotem jest świadczenie usług Inspektora Ochrony Danych.

Wobec ustalonego stanu faktycznego, mimo niezastosowania w umowie powierzenia literalnego brzmienia *podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie*, stwierdzono, iż powołane powyżej zapisy umowy wskazują, iż przetwarzanie przez podmiot przetwarzający zostało ograniczone do jedynie udokumentowanych poleceń administratora, co stanowi wypełnienie dyspozycji art. 28 ust. 3 lit. a RODO w zakresie zawarcia w umowie ww. obowiązku podmiotu przetwarzającego.

Analizując przyczyny stwierdzonych odstępstw od wymogów określonych w RODO dokonano porównania treści zawartych umów ze wzorem stanowiącym załącznik Nr 13 do Polityki Bezpieczeństwa Informacji w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu. W trakcie trwania czynności kontrolnych udostępniono kontrolującym dwa wzory umów (pierwszy zawierający 2 paragrafy, drugi zawierający 10 paragrafów). Jak wynika, ze złożonych wyjaśnień, pierwszy wzór obowiązywał od dnia 25 maja 2018 roku do dnia 3 czerwca 2019 r., drugi natomiast od dnia 3 czerwca 2019 r. Analiza dokumentów wykazała, iż wyłącznie umowa powierzenia zawarta pod poz. 5 w rejestrze umów (zawarta w dniu 03.06.2019 r.) jest zgodna z drugim wzorem. Pozostałe 4 umowy powierzenia (zawierane w okresie od 25.05.2018 r. do 01.06.2018 r.), nie zostały sporządzone z wykorzystaniem żadnego z dwóch okazanych wzorów.

Zastępca DWKZ wyjaśnił, *(...) Odnosząc się do innych wzorów umów, należy wskazać, iż zgodnie z RODO, obowiązek posiadania procedur obejmuje wszystkie podmioty gospodarcze. Oznacza to, że każdy z nich posiada własny wzór umowy powierzenia danych. Wzory te nie są jednolite ze względu na fakt, iż każdy podmiot w odmienny sposób techniczny tworzy umowy. Umowy inne niż posiadane wzory zostały zawarte w oparciu o otrzymane wzory od podmiotów, z którymi umowy te zostały zawarte"*. W świetle złożonych wyjaśnień ustalono, iż przyczyną stwierdzonych odstępstw od wymogów RODO (w przypadku umów ujętych pod poz. 2-4 Rejestru) było podpisanie umowy według wzoru przedstawionego przez podmiot przetwarzający, mimo iż te umowy nie spełniały wszystkich wymogów RODO.

Jednocześnie analiza wzorów umów powierzenia sporządzonych przez podmiot kontrolowany wykazała, iż pierwszy wzór umowy nie przewidywał wprost zapisów dotyczących charakteru przetwarzania, niemniej jednak drugi wzór (aktualnie obowiązujący od dnia 03.06.2019 r.) został uzupełniony o ten element. W obu wzorach stwierdzono brak

literalnego brzmienia obowiązku podmiotu przetwarzającego określonego w art. 28 ust. 3 lit.a RODO tj. zapisu stanowiącego, iż podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora, niemniej jednak biorąc pod uwagę, iż powyższy obowiązek został wykazany poprzez inne zapisy umowy (np. § 1 pkt 2 oraz § 2 pkt 3 nowego wzoru umowy), nie stwierdzono uchybienia w tym zakresie.

Stosownie do art. 28 ust. 1 RODO, jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób. Celem wykazania spełnienia ww. wymogu wystąpiono o udzielenie informacji w jaki sposób zweryfikowano czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Zastępca DWKZ wyjaśnił, iż cyt. *„Jednostka kontrolowana w trakcie negocjacji zawarcia umowy z podmiotem zewnętrznym zwraca uwagę na obowiązujące przepisy o ochronie danych osobowych, a także przyjmuje oświadczenie o stosowanych zabezpieczeniach i procedurach. Powtórzenie tych oświadczeń przez podmiot przetwarzający następuje w umowie o powierzenie danych w § 3, co doprowadza do przyjęcia drogą kontraktu odpowiedzialności za powierzone dane (...).* Uwzględniając złożone wyjaśnienia wskazujące na przyjętą praktykę weryfikacji podmiotów przetwarzających stwierdzono, iż organ kontrolowany wypełnił wymóg wynikający z art. 28 ust. 1 RODO.

Celem potwierdzenia czy w WOUZ zidentyfikowano wszystkie podmioty zewnętrzne, z którymi należy podpisać umowę powierzenia przetwarzania danych osobowych, dokonano m.in. weryfikacji czy WUOZ korzysta z wybranych programów komputerowych tj.: do obsługi systemu kadrowo-płacowego, rejestracji korespondencji przychodzącej i wychodzącej oraz dokonano ustaleń w zakresie korzystania przez WUOZ z serwerów www., poczty elektronicznej oraz serwisowania komputerów, a następnie dokonano ustaleń na jakiej podstawie nastąpiło świadczenie usług przez podmioty zewnętrzne.

W odniesieniu do ww. wybranych do kontroli elementów systemu informatycznego, na podstawie złożonych wyjaśnień z dnia 4 lipca 2019 r. oraz 8 sierpnia 2019 r. ustalono, iż WUOZ korzysta z serwerów będących własnością Urzędu, ponadto również w zakresie poczty elektronicznej nie jest wykorzystywany hosting zewnętrzny. Jednocześnie ustalono, iż świadczeniem usług informatycznych obejmujących m.in. utrzymanie poczty elektronicznej, serwisowania komputerów oraz serwera zajmuje się podmiot zewnętrzny, z którym – w związku z zawarciem umowy o świadczenie stałej usługi związanej z utrzymaniem i administracją systemu IT [załącznik do wyjaśnień z 4 lipca 2019 r. dowód: akta kontroli str. 268-288] zawarto stosowną umowę powierzenia.

Odnośnie wytypowanych do kontroli programów komputerowych, ustalono, iż WUOZ – na podstawie licencji udzielonych przez producentów - korzysta z systemu kadrowo-płacowego oraz użytkuje system elektronicznego obiegu dokumentów. Korzystanie z ww. systemów odbywa się na serwerze WUOZ.

Ustalenia kontroli wskazują, iż w przypadku systemu elektronicznego obiegu dokumentów, zawarto umowę powierzenia z licencjodawcą systemu.

Natomiast w zakresie systemu kadrowo-płacowego ustalono, iż w okresie objętym kontrolą nie zachodziła konieczność zawarcia umowy powierzenia z licencjodawcą. Jak wynika ze złożonych wyjaśnień Zastępcy DWKZ (....) *system działa offline, zatem nie wymaga połączenia z siecią internet. System zainstalowany jest na jednym stanowisku, na dysku lokalnym, do którego dostęp ma jedynie osoba uprawniona oraz informatyk świadczący*

usługi serwisowe. Analiza przekazanej kontrolującym licencji wskazuje na brak zapisów dotyczących usługi wdrożenia lub pomocy technicznej.

Niemniej jednak w toku kontroli ujawniono przypadek, który daje podstawę do stwierdzenia, iż w WUOZ nie dokonano identyfikacji relacji łączącej podmiot zewnętrzny z DWKZ jako Administratorem Danych, mimo że w związku z realizacją usługi dochodzi do przetwarzania danych osobowych .

Zastępca DWKZ udzielając odpowiedzi na pytanie kontrolujących dotyczące wybranych do kontroli elementów sieci teleinformatycznej o treści: czy dochodzi do wykorzystywania zewnętrznych macierzy dyskowych (hostingowania u podmiotów zewnętrznych) wskazał, iż cyt. *„Wszystkie elementy infrastruktury należą do WUOZ. Wyjątek stanowi BIP, który jest hostowany przez firmę zewnętrzną"*. Mając na uwadze, iż w toku kontroli nie ujawniono żadnej umowy powierzenia obejmującej usługę hostingu BIP, celem weryfikacji, czy w WOUZ zidentyfikowano wszystkie podmioty zewnętrzne, z którymi należy podpisać umowę powierzenia przetwarzania danych osobowych, wystąpiono o udzielenie informacji czy w zakresie BIP, który jest hostowany przez firmę zewnętrzną dochodzi do powierzenia przetwarzania danych osobowych, a jeśli tak o uzasadnienie braku konieczności zawarcia umowy powierzenia z hostingodawcą. W odpowiedzi z dnia 8 sierpnia 2019 r. Zastępca DWKZ wskazał, iż cyt. *WUOZ umieszcza na swojej stronie tylko te dane, które są jawne lub ich jawność wynika z przepisów prawa lub udzielonej zgody. Natomiast w przypadku postępowań lub przypadków, kiedy konieczna jest zgoda osoby fizycznej, jej dane są zanonimizowane i pisma lub informacje w takiej postaci są umieszczane na BIP*. Powyższe wyjaśnienia wskazują, iż - zdaniem organu kontrolowanego - w związku z realizacją ww. usługi dochodzi do ujawniania wyłącznie informacji, które są jawne, a w przypadku gdy wymagana jest zgoda osoby fizycznej – do ujawniania danych wyłącznie zanonimizowanych. Organ kontrolowany nie potwierdził, iż dochodzi do przetwarzania danych osobowych oraz nie wykazał uzasadnienia braku konieczności zawarcia umowy powierzenia. Kontrolujący, dokonując własnych ustaleń [wydruk z BIP, dowód: akta kontroli str. 319] stwierdzili natomiast, iż na stronie BIP WUOZ zamieszczane są w zakładce *Pracownicy poszukiwani* (https://wosoz.ibip.wroc.pl/public/?id=64355) dane osobowe niezanonimizowane w postaci imienia i nazwiska oraz miejsca zamieszkania osoby wyłonionej w wyniku naboru na wolne stanowiska w służbie cywilnej. Ponadto w zakładce *Moja sprawa* (https://wosoz.ibip.wroc.pl/public/?id=36576) znajduje się formularz umożliwiający wyszukanie sprawy, który w kryteriach wyszukiwania ma identyfikatory takie jak PESEL, Numer Dowodu, NIP, REGON [wydruk z BIP, dowód: akta kontroli str. 320-321], co wskazuje na możliwość dostępu przez usługodawcę do wprowadzonych danych osobowych.

Pojęcie *dane osobowe* zostało zdefiniowane w art. 4 pkt 1 RODO. W powołanym przepisie posłużono się terminem "identyfikator" dla zbiorczego określenia wymienionych w nim przykładowych kategorii informacji, które pozwalają na identyfikację, a więc ustalenie tożsamości osoby fizycznej. Identyfikatorami będą zatem takie informacje, jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Wyliczenie to jednak nie jest wyczerpujące. W doktrynie[7] podkreśla się, iż praktyce uznanie, że mamy do czynienia z tak określonym "identyfikatorem", w znacznej mierze uzależnione będzie od kontekstu, w jakim posłużono się informacją (...) a przez to, czy możliwe jest przypisanie jej konkretnej osobie fizycznej.

---

[7] Ogólne rozporządzenie o ochronie danych osobowych. Komentarz red. dr Marlena Sakowska-Baryła, Warszawa 2018 ; komentarz do art. 4.

Podkreślenia wymaga, iż Prezes Urzędu Ochrony Danych Osobowych również stoi na stanowisku, iż na stronie Biuletynu Informacji Publicznej znajdować mogą się dane osobowe.[8]

W świetle dokonanych ustaleń, z których wynika, iż w związku z realizacją usługi hostingu strony BIP WUOZ może dojść do przetwarzania danych osobowych przez podmiot zewnętrzny oraz w oparciu o złożone wyjaśnienia stwierdzono, iż kontrolowany organ nie dokonał rzetelnej analizy relacji łączącej go z podmiotem zewnętrznym świadczącym usługi hostingu BIP. Powierzenie przetwarzania danych osobowych będzie miało miejsce w sytuacji, gdy podmiot zewnętrzny świadczy pewien rodzaj usług w imieniu administratora, z którymi związane jest przetwarzanie danych osobowych. Podkreślenia wymaga, iż w przypadku udostępniania danych bez podstawy prawnej (np. bez uprzednio zawartej umowy powierzania) następuje naruszenie m.in zasady zgodności z prawem (art. 5 RODO). Biorąc pod uwagę, iż w toku kontroli DWKZ nie wykazał jednoznacznie, iż w związku ze świadczeniem usług hostingu BIP, w okresie objętym kontrolą, nie dochodziło do przetwarzania danych osobowych, tym samym stwierdzono, iż nie wykazał w tym zakresie przestrzegania przepisów RODO, co stanowi naruszenie zasady rozliczalności, o której mowa w art. 5 ust. 2 RODO.

Obszar B - Prawo do przetwarzania danych osobowych.

Z przepisu art. 5 ust. 1 RODO wynikają ogólne zasady dotyczące przetwarzania danych osobowych, za przestrzeganie których odpowiedzialny jest każdy administrator (art. 5 ust. 2 RODO).

Podstawowym (choć nie jedynym) wymogiem warunkującym prawidłowość przestrzegania przepisu art. 5 ust. 2 RODO jest prawidłowe przeprowadzenie identyfikacji zachodzących w podmiocie procesów i podstaw prawnych przetwarzania danych osobowych.

Zgodnie z pkt 5.1. i 3. Polityki Bezpieczeństwa Informacji w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu *Administrator samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych* oraz *zapewnia, aby dane te były: - przetwarzane zgodnie z prawem; - zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami; - merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane; - przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.*

W wyniku kontroli ustalono, iż narzędziem – za pomocą którego organ kontrolowany – rozliczył się z obowiązku dokonanej identyfikacji zachodzących w podmiocie kontrolowanym procesów przetwarzania danych osobowych - jest *Rejestr Czynności Przetwarzania Danych Osobowych* prowadzony przez Dolnośląskiego Wojewódzkiego Konserwatora Zabytków [dowód: akta kontroli str. 8-12].

W wyniku kontroli ustalono, iż dla rozpoznanych procesów przetwarzania danych osobowych zidentyfikowano podstawy prawne, o jakich mowa w art. 6 ust. 1 RODO. Z zapisów *Rejestru Czynności Przetwarzania Danych Osobowych* wynika, iż jako podstawę przetwarzania danych osobowych w zidentyfikowanych czynnościach przetwarzania danych osobowych – wskazano art. 6 ust. 1 pkt b); c); e); f) RODO.

[8] Decyzja ZSPU.4213.2019 z dnia 18 października 2019 r. dostępna https://uodo.gov.pl/pl/p/decyzje

Z zapisów Rejestru Czynności Przetwarzania Danych Osobowych, jak i ze złożonych wyjaśnień wynika, iż jedynie przy procesie przetwarzania danych osobowych nazwanym *„rekrutacja do pracy"* (czynność przetwarzania zarejestrowana pod poz. 8 w Rejestrze) podstawą przetwarzania danych może być również zgoda, o której mowa w art. 6 ust.1 a RODO [dowód: wyjaśnienia z dnia 14 czerwca 2019 r., akta kontroli str. 171-173]. Z ustaleń kontroli wynika, iż zgoda – jako podstawa prawna przetwarzania danych osobowych - została zidentyfikowana dopiero od 6 czerwca 2019 r. W związku dokonanymi ustaleniami do Dolnośląskiego Wojewódzkiego Konserwatora Zabytków skierowano pismo o złożenie wyjaśnień w zakresie ustalonych podstaw prawny przetwarzania danych osobowych w procesie rekrutacji. W odpowiedzi organ kontrolowany nie wskazał od kiedy zidentyfikowano zgodę – jako podstawę prawną przetwarzania danych osobowych – przy procesie rekrutacji, wskazując wyłącznie, że okoliczność ta wynika ze stosowanego wzoru, zamieszczonego przez Kancelarię Prezesa Rady Ministrów w elektronicznym systemie nazwanym: Praca w Służbie Cywilnej, działającego w ramach Biuletynu Informacji Publicznej prowadzonego przez KPRM. Jak bowiem wynika z wyjaśnień organ kontrolowany (...) *w trakcie rekrutacji korzysta z możliwości systemu naboru w takim zakresie, w jakim jest to możliwe, i nie ingeruje w treść gotowych i proponowanych treści, w tym klauzul informacyjnych.* [akta kontroli str. 268-273]

Jednocześnie kontrola wykazała, iż organ kontrolowany zidentyfikował również podstawy prawne przetwarzania danych określone w przepisach prawa powszechnie obowiązującego na terytorium Rzeczypospolitej Polskiej, w przypadku wszystkich czynności przetwarzania zidentyfikowanych w Rejestru Czynności Przetwarzania Danych Osobowych, tj. przede wszystkim w przypadkach, w których jako podstawę prawną przetwarzania wskazano art. 6 ust. 1 pkt c) i e) RODO. Powyższe jest zgodne z art. 6 ust. 3 RODO, w myśl którego: podstawa przetwarzania, o którym w ust. 1 lit c) i e) musi być określona w: a) prawie Unii: lub b) w prawie państwa członkowskiego, któremu podlega administrator [dowód: Rejestr Czynności Przetwarzania Danych Osobowych, wyjaśnienia z dnia 8 sierpnia 2019 r. akta kontroli, klauzula informacyjna, str. 8-12, 296-299, 302-305].

Odnosząc się do kwestii przetwarzania danych na podstawie zgody (art. 6 ust.1 a RODO) należy wskazać, iż w myśl art. 7 ust. 1 RODO *jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.* Przy czym zgodnie z art. 4 pkt 11 RODO przez pojęcie zgody osoby, której dane dotyczą należy rozumieć: *dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych* (motyw 32 RODO określa dodatkowe wytyczne odnośnie uzyskiwania zgody). Rozporządzenie o ochronie danych osobowych (RODO) jasno wskazuje więc, że zgoda wymaga oświadczenia od osoby, której dane dotyczą, lub wyraźnego działania potwierdzającego, co oznacza że musi być zawsze udzielona poprzez aktywne działanie lub deklarację. Musi być więc oczywiste, że osoba, której dane dotyczą, zgodziła się na określone przetwarzanie. Przy czym wskazać należy, iż w przypadku szczególnych kategorii danych osobowych (art. 9 ust. 1 RODO) zgoda wymaga formy wyraźnego oświadczenia. Jednocześnie w myśl art. 7 ust. 3 RODO *osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę.*

Przestrzeganie przez Dolnośląskiego Wojewódzkiego Konserwatora Zabytków ww. przepisów odnoszących się do wyrażania zgody zweryfikowano na przykładzie procesu

przetwarzania danych osobowych kandydatów składających dokumenty aplikacyjne w przypadku jedynie 2 ostatnich naborów (Nabory Nr: 48815, 48814) na wolne stanowisko pracy z 4 poddanych kontroli, ogłoszonych w dniu 6 czerwca 2019 r., stwierdzono bowiem, iż przed dniem 6 czerwca 2019 r. treść klauzuli informacyjnej zawartej w ogłoszeniach o naborze, w zakresie podstawy prawnej przetwarzania danych miała brzmienie: *„art. 22[1] Kodeksu Pracy oraz art. 26 i nast. ustawy z dnia 21 listopada 2008 r. o służbie cywilnej w zw. z art. 6 ust. 1 lit. c RODO"* [dowód: akta kontroli str. 307-312].

Czynności kontrolne wykazały, iż w klauzuli informacyjnej każdego z ww. naboru (Nabory Nr 48815, 48814) wskazano iż: *podanie innych danych w zakresie nieokreślonym przepisami prawa, zostanie potraktowane jako zgoda na przetwarzanie danych osobowych. Wyrażenie zgody w tym przypadku jest dobrowolne, a zgodę tak wyrażoną można odwołać w dowolnym czasie. Jeżeli dane będą obejmowały szczególne kategorie danych, o których mowa w art. 9 ust. 2 RODO, konieczna będzie wyraźna zgoda na ich przetwarzanie, która może zostać odwołana w dowolnym czasie.*

W świetle wyżej wymienionych okoliczności faktycznych stwierdzić należy, iż system dokumentowania wyrażenia zgody na przetwarzanie danych osobowych, przyjęty od dnia 6 czerwca 2019 r. przez Dolnośląskiego Wojewódzkiego Konserwatora Zabytków, umożliwiał jednoznacznie wykazanie, iż osoba, która poda dane osobowe w zakresie niewynikającym z przepisów prawa, była świadoma, że już samo podanie przez nią takich danych – będzie uznane za wyrażenie przez nią zgody na przetwarzanie danych osobowych, w zakresie danych niewynikających z przepisów prawa. Jednocześnie przyjęty system umożliwia stwierdzenie, iż w przypadku szczególnych kategorii danych osobowych (art. 9 ust. 1 RODO) – osoba, której dane dotyczą uzyskała informację, iż zgoda – w takim przypadku - wymaga formy wyraźnego oświadczenia. Ponadto przyjęty system umożliwia weryfikację tego, iż osoba, której dane dotyczą – jest informowana o prawie do wycofania zgody, zanim taką zgodę wyrazi.

Powyższe jest zgodne z obowiązkiem określonym w art. 7 ust. 1 i 3 w zw. z art. 4 pkt 11 RODO.

Kontrola wykazała, iż organ kontrolowany wprowadził *wzór zgody* (Załącznik Nr 15 do Polityki Bezpieczeństwa Informacji w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu) [dowód: akta kontroli str. 120].

Z udzielonych pismem z dnia 4 lipca 2019 r. przez organ kontrolowany wyjaśnień wynika, iż: *w trakcie rekrutacji nie jest konieczne posługiwanie się wzorem ustalonym w polityce. W warunkach rekrutacji poddawana jest treść zgody jaka powinna się znaleźć w treści dokumentacji rekrutacyjnej* [dowód: akta kontroli str. 268-273]. Z uwagi na fakt, iż przepisy RODO nie wymagają wyrażania zgody w postaci wyraźnego oświadczenia (za wyjątkiem szczególnych kategorii danych osobowych) złożone wyjaśnienia zostały uwzględnione. Na uwagę zasługuje fakt, iż w przepisie § 17 ust. 5 Polityki Ochrony Danych Osobowych w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu (Zał. Nr 4 do Polityki Bezpieczeństwa Informacji w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu) wskazano, iż *w sytuacjach szczególnych, określonych przez Administratora, zgoda może być odebrana w formie jednoznacznego, wyraźnego działania.*

Obszar C - Realizacja praw osoby, której dane dotyczą

Kontrola wykazała, iż w WUOZ zasady postępowania z żądaniami osób, których dane dotyczą uregulowano w rozdziale X Polityki ochrony danych osobowych zatytułowanym *Prawa osoby, której dane osobowe dotyczą* oraz w *Procedurze postępowania względem żądań osób, których dane dotycząc w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu* stanowiącej załącznik nr 25 do Polityki Bezpieczeństwa Informacji [Dowód: akta kontroli str. 159-165].

Zgodnie z § 20 ust. 2 Polityki ochrony danych osobowych wnioski w sprawie skorzystania z praw osoby, której dane osobowe dotyczą rozpatruje i realizuje właściwy kierownik komórki organizacyjnej, w przypadku wątpliwości co do zgodności z prawem przyjętego postępowania, a w szczególności w sytuacji wątpliwości co do odpowiedzi odmownej lub udostępniania danych, kierownik komórki organizacyjnej na polecenie administratora może zasięgnąć opinii IOD. Zgodnie z § 20 ust. 4 ww. Polityki w przypadku skontaktowania się osoby, której dane dotyczą bezpośrednio z IOD, Administrator lub wskazany przez niego kierownik komórki organizacyjnej są zobowiązani niezwłocznie udzielić mu wszelkiej możliwej pomocy i informacji w celu rozwiązania problemu oraz do spowodowania, aby osoba, która się do niego zwróciła mogła skorzystać ze swoich praw.

Natomiast w *Procedurze postępowania względem żądań osób, których dane dotyczą w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu* opisano zakres i warunki realizacji poszczególnych żądań oraz sposób postępowania z wpływającymi żądaniami.

Zgodnie z art. 15 - 21 RODO osobie, której dane dotyczą przysługuje: prawo dostępu do jej danych osobowych oraz otrzymania ich kopii (art. 15 RODO); prawo do sprostowania danych (art. 16 RODO); prawo do usunięcia danych (art. 17 RODO); prawo do ograniczenia przetwarzania (art. 18 RODO); prawo do przenoszenia danych (art. 20 RODO); prawo do sprzeciwu (art. 21 RODO).

Ponadto osoba, której dane dotyczą może złożyć wniosek:
- o wskazanie podstawy nieprzekazania informacji, o których mowa w art. 13 ust. 3 RODO (w myśl art. 3 ust. 3 UODO),
- o wskazanie podstawy nieprzekazania informacji, o których mowa w art. 14 ust. 1, 2 i 4 RODO (w myśl art. 4 ust. 3 UODO),
- o wskazanie podstawy niewykonania obowiązków, o których mowa w art. 15 ust. 1-3 RODO (w myśl art. 5 ust. 4 UODO).

W toku kontroli ustalono, iż w okresie objętym kontrolą do WUOZ nie wpłynęły żadne wnioski czy też żądania osób, których dane dotyczą, składane na podstawie wskazanych wyżej przepisów prawa [pismo z 6 czerwca 2019 r. dowód: akta kontroli str. 5-7].

Klauzule informacyjne

Zgodnie z art. 13 ust. 1 RODO jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych podaje jej wszystkie informacje, o których mowa w art. 13 ust. 1 i 2 RODO. Natomiast w myśl art. 14 RODO jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą informacje, o których mowa w art. 14 ust. 1 i 2 RODO.

W toku kontroli stwierdzono, że kwestia realizacji obowiązku informacyjnego w WUOZ została uregulowana w rozdziale IX Polityki ochrony danych osobowych pt. *„Realizacja obowiązków informacyjnych"*. W myśl § 18 pkt 1 ww. Polityki w przypadku zbierania danych osobowych bezpośrednio od osób - na formularzach, kwestionariuszach, drukach i innych służących do zbierania danych osobowych – prowadzonych zarówno w formie papierowej, jak i elektronicznej, należy umieszczać na nich klauzulę informacyjną; wzór klauzuli stanowi załącznik nr 14. Natomiast w przypadku pozyskiwania danych osobowych w inny sposób niż od osoby, której dane osobowe dotyczą, Administrator jest zobowiązany realizować obowiązek informacyjny w stosunku do tych osób w sposób określony w art. 14 RODO (§ 19 pkt. 1 ww. Polityki). Zgodnie z § 18 pkt 2, 3, 4 oraz § 19 pkt 2 ww. Polityki kierownik komórki organizacyjnej opracowuje klauzule informacyjne, które powinny być stosowane przy zbieraniu danych osobowych w podległej mu komórce organizacyjnej, oraz odpowiada za stosowanie klauzul informacyjnych. W przypadku wątpliwości związanych ze stosowaniem i opracowaniem klauzuli Administrator może zażądać opinii IOD.

Jednocześnie ustalono, iż w kontrolowanej jednostce stworzono *Instrukcję odstąpienia od obowiązku informacyjnego w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu* (załącznik nr 27 do Polityki Bezpieczeństwa). W punkcie 1 powyższej Instrukcji określono, iż Dolnośląski Wojewódzki Konserwator Zabytków oraz podlegli mu pracownicy zobowiązani są do przestrzegania postanowień art. 13 i 14 RODO. Natomiast w punktach 2 i 3 Instrukcji wskazano przypadki, w których organ odstępuje od obowiązku informacyjnego wynikającego z art. 13 ust. 3 i art. 14 RODO.

Na dzień rozpoczęcia kontroli tj. 12 czerwca 2019 r. w WUOZ obowiązywał 1 wzór ogólnej klauzuli informacyjnej (załącznik nr 14 do Polityki Bezpieczeństwa Informacji), gdzie jako cel przetwarzania danych osobowych wskazano realizację zadań wynikających z obowiązującego prawa, w szczególności ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami. Powyższy wzór klauzuli informacyjnej w okresie objętym kontrolą był modyfikowany [wyjaśnienia z 4 lipca 2019 r. oraz z 8 sierpnia 2019 r., wzory klauzul informacyjnych dowód: akta kontroli str. 268-273, 295-299, 302-305]. Ustalono, iż do dnia 8 maja 2019 r. klauzula informacyjna nie była zamieszczona na stronie BIP jednostki. Pierwsza wersja klauzuli informacyjnej widniała na stronie BIP od 8 maja 2019 r. do 10 czerwca 2019r., a wersja druga od 10 czerwca 2019 r. https://wosoz.ibip.wroc.pl/public/?id=122923. W toku kontroli ustalono, że osobą odpowiedzialną za utworzenie teksu klauzuli jest IOD [wyjaśnienia z 4 lipa 2019 r. dowód: akta kontroli str. 268-273].

Stwierdzono, iż opracowany w WUOZ wzór klauzuli informacyjnej w wersji obowiązującej do dnia 10 czerwca 2019 r. zawierał wszystkie elementy określone w art. 13 ust. 1 i 2 RODO. Natomiast wzór klauzuli informacyjnej obowiązujący od dnia 10 czerwca 2019 r. w zasadzie zawierał wszystkie elementy określone w art. 13 ust. 1 i 2 RODO, niemniej jednak wymóg zawarcia w klauzuli informacji o prawie do wniesienia skargi do organu nadzorczego (art. 13 ust. 2 lit. d RODO) został zrealizowany nieprawidłowo. W powyższym wzorze klauzuli informacyjnej zamieszczono sprzeczne informacje dotyczące organu nadzorczego, albowiem w punkcie 9 wskazano, iż cyt. *„Każdy, kto uważa, że jego dane są przetwarzane w sposób nieprawidłowy ma prawo złożenia skargi do organu nadzorczego względem Wojewódzkiego Konserwatora Zabytków tj. Wojewody Dolnośląskiego (...)"*, natomiast w punkcie 10 wskazano cyt. *„Każdy, kto uważa, że jego dane są przetwarzane w sposób nieprawidłowy ma prawo złożenia skargi do Prezesa Urzędu Ochrony Danych Osobowych (...)"*. Zgodnie z art. 34 ust. 2 UODO organem nadzorczym w rozumieniu RODO jest Prezes Urzędu Ochrony Danych Osobowych. W wyjaśnieniach

z 8 sierpnia 2019 r. poinformowano, iż cyt.: *„Punkt dotyczący wpisania Wojewody Dolnośląskiego jako organu nadzorczego wynikał z błędnie przyjętej dotychczasowej interpretacji przepisów. Po dokładnej analizie art. 51 RODO, dokonano zmiany treści klauzuli informacyjnej, poprzez usunięcie Wojewody Dolnośląskiego jako organu nadzorczego".* Odnosząc się do złożonych wyjaśnień zauważyć należy, iż we wzorze klauzuli informacyjnej stosowanej w WUOZ do 10 czerwca 2019 r. organ nadzorczy był określony prawidłowo tj. Prezes Urzędu Ochrony Danych Osobowych. Zatem wyjaśnienie dotyczące *błędnie przyjętej dotychczasowej interpretacji przepisów* stanowią przyczynę stwierdzonej nieprawidłowości w zakresie określenia organu nadzoru w klauzuli obowiązującej od dnia 10 czerwca 2019 r. Jednocześnie w oparciu o złożone wyjaśnienia stwierdzono, że organ podjął działania naprawcze po zakończeniu czynności kontrolnych, co odzwierciedla treść klauzuli informacyjnej zamieszczonej na stronie https://wosoz.ibip.wroc.pl/public/?id=122923.

Kontrolą objęto realizację obowiązku informacyjnego dla następujących procesów: rekrutacja pracowników (nabory), postępowania skargowo-wnioskowe, zamówienia publiczne, rejestrowanie korespondencji wpływającej i wychodzącej.

W zakresie rekrutacji pracowników ustalono, iż w okresie objętym kontrolą przeprowadzono: 41 naborów w służbie cywilnej, z czego 11 zakończyło się wyborem kandydata, 23 zakończyły się brakiem wyłonienia kandydata, a 7 naborów było w toku. W kontrolowanej jednostce osobą odpowiedzialną za przygotowanie treści ogłoszenia o naborze jest Pani J. W. z działu kadr, natomiast za zatwierdzenie treści ogłoszenia o naborze odpowiedzialny jest administrator [wyjaśnienia z 4 lipca 2019 r. dowód: akta kontroli str. 268-273]. Kontrolą objęto następujące nabory: 28540, 28019, 48814, 48815.

Kontrola wykazała, że w procesie naboru w służbie cywilnej w WUOZ korzystano z klauzuli informacyjnej dostępnej na stronie KPRM przy tworzeniu ogłoszenia o naborze. W wyjaśnieniach z 14 czerwca 2019 r. wskazano, iż cyt.: *„Obowiązek informacyjny w przypadku naborów jest wykonywany wedle możliwości jakie daje formularz wykorzystywany przez portal służby cywilnej. Jednostka kontrolowana nie ma możliwości ingerowania w treść klauzul zawartych w formularzu, zatem w przypadku naborów obowiązek informacyjny jest wykonywany wedle funkcjonalności systemu rekrutacyjnego służby cywilnej. System rekrutacji został zmieniony o stosowne klauzule po wejściu w życie RODO".* Odnosząc się do złożonych wyjaśnień wskazać należy, iż rzeczywiście korzystając ze wzoru klauzuli informacyjnej dostępnej na stronie www.logowanie.nabory.kprm.gov.pl brak jest możliwości edytowania treści powyższej klauzuli informacyjnej. Niemniej jednak osoba wprowadzająca ogłoszenie nie musi korzystać w powyższego wzoru klauzuli informacyjnej i może wprowadzić do ogłoszenia opracowaną przez siebie treść klauzuli informacyjnej, albowiem system umożliwia wybór sposobu wypełnienia klauzuli informacyjnej jako: *Gotowy tekst z informacjami do uzupełnienia* bądź *swobodny opis redaktora.*

Czynności kontrolne wykazały, iż wszystkie skontrolowane ogłoszenia o naborze w korpusie służby cywilnej opublikowane na stronie BIP KPRM i WUOZ zawierały klauzulę informacyjną zawierającą elementy określone w art. 13 RODO. Ustalono, iż w skontrolowanych ogłoszeniach o naborze zamieszczanych do 6 czerwca 2019 r. (dotyczy ogłoszeń nr 28540, 28019) w klauzuli informacyjnej jako podstawę prawną przetwarzania danych wskazywano: *art. 22[1] kodeksu pracy oraz art. 26 i następne ustawy z dnia 21 listopada 2008 r. o służbie cywilnej w związku z art. 6 ust. 1 lit. c RODO* [dowód: akta kontroli str. 313-318]. Natomiast w ogłoszeniach o naborze zamieszczanych od 6 czerwca 2019 r. (dotyczy ogłoszeń nr 48814, 48815) w klauzuli informacyjnej jako podstawa

przetwarzania danych figuruje: *art. 6 ust. 1 lit. b RODO; art. 22[1] kodeksu pracy, ustawa z dnia 21 listopada 2008 r. o służbie cywilnej oraz ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach w związku z art. 6 ust. 1 lit. c RODO; art. 6 ust. 1 lit. a RODO oraz art. 9 ust. 2 lit. a RODO* [dowód: akta kontroli str. 307-312]. Kontrolowany organ nie wyjaśnił, mimo skierowanego przez kontrolerów zapytania, okoliczności zmiany podstawy prawnej przetwarzania danych w procesie rekrutacji, poinformował natomiast, że cyt. (...) *w trakcie rekrutacji korzysta z możliwości systemu naboru w takim zakresie, w jakim jest to możliwe, i nie ingeruje w treść gotowych i proponowanych treści w tym klauzul informacyjnych. Wynika to z jednolitej i spójnej formuły systemu rekrutacji na poziomie całego kraju w ramach służby cywilnej - stosowane rozwiązania są dzięki temu zgodne z obowiązującymi przepisami. Organ nie widzi potrzeby zmiany lub modyfikacji odgórnych, narzuconych przez organa centralne schematów".* W toku kontroli potwierdzono, że na stronie www.logowanie.nabory.kprm.gov.pl we wzorze klauzuli informacyjnej stosowanej w naborach dokonano zmiany podstawy prawnej przetwarzania danych.

Niemniej jednak odnosząc się do złożonych wyjaśnień podkreślenia wymaga, iż to Administrator, jest zobowiązany do identyfikacji podstaw prawnych przetwarzania danych w każdym procesie przetwarzania danych. Zatem również w procesie rekrutacji Administrator powinien zidentyfikować podstawę prawną przetwarzania i odzwierciedlić ją w klauzuli informacyjnej. W przypadku gdy zidentyfikowana przez Administratora podstawa prawna w procesie rekrutacji jest zgodna z podstawą prawną określoną we wzorze klauzuli zamieszczonej na stronie KPRM, wówczas można skorzystać z gotowego tekstu. Natomiast w przypadku zidentyfikowania innych podstaw prawnych przetwarzania, formularz wykorzystywany przez portal służby cywilnej w procesie rekrutacji umożliwia wprowadzenie zidentyfikowanych podstaw.

Zgodnie z art. 13 ust. 1 RODO obowiązek informacyjny powinien być spełniony podczas pozyskiwania danych osobowych. W przypadku rekrutacji pracowników, od 6 czerwca 2019 r. jedną ze zidentyfikowanych przez WUOZ podstaw prawnych przetwarzania danych osobowych jest *zgoda osoby*, którą zgodnie z art. 7 ust. 3 RODO, osoba ma prawo wycofać w dowolnym momencie. Jednocześnie zgodnie z brzmieniem ww. przepisu. *Osoba, której dane dotyczą jest o tym informowana, zanim wyrazi zgodę.* Kontrola wykazała, iż klauzula informacyjna zawarta w ogłoszeniach o naborze od 6 czerwca 2019 r. zawiera informację o możliwości wycofania zgody (art. 13 ust. 2 lit. c RODO).

Klauzula informacyjna zawarta w ogłoszeniach o naborze, jak wcześniej wskazano, zawiera wszystkie elementy określone w art. 13 RODO. Niemniej jednak kontrola wykazała, że w treści klauzuli obowiązującej do 6 czerwca 2019 r., jak i w klauzuli zamieszczanej po tym terminie, błędnie określono odbiorcę danych - *Wojewódzki Urząd Ochrony Zabytków*. Zauważyć należy, iż odbiorca danych zgodnie z dyspozycją art. 4 pkt 9 RODO *oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.* Przyczyną uchybienia polegającego na uznaniu WUOZ za odbiorcę danych jest błędne rozumienie pojęcia odbiorcy danych.

W zakresie realizacji obowiązku informacyjnego w procesie postępowań skargowo – wnioskowych podczas kontroli nie udostępniono dokumentacji, na której odzwierciedlone byłoby (np. poprzez zamieszczenie stosownej adnotacji na dokumencie) załączanie klauzuli

informacyjnej w korespondencji kierowanej do skarżącego/wnioskodawcy. Na podstawie złożonych wyjaśnień ustalono [pismo z 14 czerwca 2019 r., z 27 czerwca 2019 r., z 4 lipca 2019 r. dowód: akta kontroli: 171-173, 250, 268-273], iż ww. obowiązek był realizowany w ten sposób, że cyt. *„(...) wraz z załatwieniem sprawy jest wysyłana do wnioskodawcy/skarżącego klauzula informacyjna wedle załącznika nr 14 (...) do przygotowanej dokumentacji załatwiającej wniosek lub skargę dołączana jest klauzula informacyjna, uprzednio wydrukowana na odrębnej stronie; podlega ona wysyłce do strony postępowania wraz z zawiadomieniem o sposobie załatwienia skargi lub odpowiedzią na wniosek.* Ponadto w złożonych pismem z dnia 4 lipca 2019 r. wyjaśnieniach wskazano cyt.: *„Zgodnie z przyjętą interpretacją przez WUOZ, art. 5 ust. 2 RODO, rozliczność nie polega jedynie na dosłownym wskazywaniu "wykonania określonej czynności". Rozporządzenie RODO jest skonstruowane elastycznie, bowiem uwzględnia także sytuacje niektórych większych organizacji i firm. WUOZ generuje corocznie ok. 70 000 przesyłek. Dlatego też, wedle przyjętej interpretacji art. 5 ust. 2 RODO rozliczalność może być wykazana także poprzez przedstawienie przyjęcia i stosowania określonych procedur, w szczególności określających konieczność wykonywania obowiązku informacyjnego z art, 13 i 14 RODO. Dlatego też wedle posiadanej procedury, do każdego pisma załączana jest klauzula informacja. Takie rozwiązanie dotyczy także postępowań skargowo- wnioskowych".*

Podkreślić należy, iż do dnia 4 maja 2019 r. przepisy prawa nie określały wprost w jaki sposób ma być realizowany obowiązek informacyjny w postępowaniach skargowo – wnioskowych. Natomiast od dnia 4 maja 2019 r. obowiązuje nowelizacja Kodeksu postępowania administracyjnego i zgodnie z dyspozycją art. 226a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t. j. Dz. U z 2019 r. poz. 2096 ze zm.): *Organy właściwe w sprawach skarg i wniosków przekazują informacje, o których mowa w art. 13 ust. 1 i 2 rozporządzenia 2016/679, skarżącemu lub wnioskodawcy przy pierwszej czynności skierowanej do tych osób.* Niniejszy obowiązek wprowadzono ustawą z dnia 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) .

Wskazać należy, iż przyjęta w WUOZ procedura działania polegająca na realizacji obowiązku informacyjnego poprzez dołączanie do przygotowanej dokumentacji załatwiającej wniosek lub skargę klauzuli informacyjnej umożliwia prawidłową realizację obowiązku ciążącego na organie rozpatrującym skargi i wnioski, oczywiście w przypadku gdy powyższe pismo jest pierwszą czynnością kierowaną do tej osoby. Niemniej jednak wskazać należy, iż w oparciu o przedłożoną dokumentację i złożone wyjaśnienia brak jest możliwości zweryfikowania stosowania przyjętej procedury, nie można również ustalić w jaki sposób wykonywany jest nadzór nad realizacją procedury oraz czy jest ona każdorazowo stosowana przez wszystkich pracowników kontrolowanego organu i czy przekazanie klauzuli następuje przy pierwszej czynności skierowanej do tych osób (do czego obliguje art. 226a k.p.a.). Powyższe stoi w sprzeczności z zasadą rozliczalności określoną w art. 5 ust. 2 RODO.

W zakresie dotyczącym zamówień publicznych w piśmie z 14 czerwca 2019 r. poinformowano, iż cyt.: *„W przypadku zamówień publicznych, jednostka kontrolowana posiada instrukcję stosowania przyjętej klauzuli informacyjnej wedle załącznika nr 14. Do tej pory w okresie objętym kontrolą wykonano jedno zamówienie publiczne, przy czym nie zastosowano klauzuli informacyjnej, z tego względu, iż odbiorcami oferty były firmy zorganizowane w formie spółki kapitałowej lub osobowej".* W toku kontroli ustalono, iż przedmiotem wskazanego w piśmie z 14 czerwca 2019 r. zamówienia publicznego była

dostawa 3 samochodów osobowych, a ogłoszenie ukazało się w dniu 25 marca 2019 r. (ogłoszenie nr 527583-N-2019) i zostało zamieszczone na stronie https://wosoz.ibip.wroc.pl/public/?id=122412. Kontrolujący nie uwzględnili złożonych wyjaśnień w zakresie braku obowiązku stosowania obowiązku informacyjnego z uwagi na fakt, iż cyt. *(...) odbiorcami oferty były firmy zorganizowane w formie spółki kapitałowej lub osobowej.* Przede wszystkim wskazać należy, iż żaden przepis prawa nie nakazuje prowadzenia działalności polegającej na handlu pojazdami samochodowymi w formie spółki kapitałowej lub osobowej, zatem powyższą działalność może prowadzić również osoba fizyczna jako jednoosobową działalność gospodarczą. Ponadto zauważyć należy, iż wraz ze złożeniem oferty wykonawca przekazuje zamawiającemu dane osobowe, tj. dane osoby do kontaktu czy dane członków zarządu firmy, zatem po stronie zamawiającego w ramach badania ofert dojdzie do przetwarzania danych osobowych (J. Jarnicka, Prawo zamówień publicznych. Komentarz 2019, wyd. 8).

Stwierdzono zatem, iż kontrolowany organ nie wykazał zrealizowania obowiązku informacyjnego wynikającego z art. 13 ust. 1 i 2 RODO dla procesu zamówień publicznych.

Na marginesie zauważyć należy, iż ustawą z dnia 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) od 4 maja 2019 r. w ustawie Prawo zamówień publicznych wprowadzono przepis art. 8a ust. 1, w myśl którego *Zamawiający realizuje obowiązki, o których mowa w art. 13 ust. 1-3 rozporządzenia 2016/679, przez zamieszczenie wymaganych informacji w ogłoszeniu o zamówieniu, ogłoszeniu o konkursie, specyfikacji istotnych warunków zamówienia, regulaminie konkursu lub przy pierwszej czynności skierowanej do wykonawcy.*

Natomiast w zakresie rejestracji korespondencji przychodzącej i wychodzącej poinformowano w piśmie z 4 lipca 2019 r., że cyt.: *„Na stronie BIP została umieszczona klauzula informacyjna dot. prowadzenia rejestru korespondencji"*. Powyższa klauzula została zamieszczona na stronie WUOZ *https://wosoz.ibip.wroc.pl/public/?id=123666* w dniu 7 lipca 2019 r., zatem z uwagi na okres objęty kontrolą powyższy wzór nie podlegał ocenie. Stwierdzić jednocześnie należy, iż kontrolowany organ nie wykazał w jaki sposób realizował obowiązek informacyjny wynikający z art. 13 ust. 1 i 2 RODO dla procesu rejestrowania korespondencji wpływającej i wychodzącej w okresie objętym kontrolą. Ustalono natomiast, że kontrolowany organ podjął w powyższym zakresie działania naprawcze.

Zgodnie z art. 14 RODO jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, administrator podaje osobie, której dane dotyczą informacje, o których mowa w art. 14 ust. 1 i 2 RODO. W toku kontroli ustalono [wyjaśnienia z 6 czerwca 2019 r. - dowód: akta kontroli str. 5-7], iż w WUOZ zidentyfikowano 2 procesy, w których może dojść do pozyskania danych osobowych w inny sposób niż bezpośrednio od osoby, której dane dotyczą t. j.:

1) Organ kontrolowany otrzymuje dane od innego organu administracji publicznej, sądu prokuratury, policji jako właściwy do prowadzenia sprawy (...).

2) Organ kontrolowany otrzymuje dane określonych osób jako donos lub donos anonimowy. W zakresie drugiego procesu tj. gdy organ kontrolowany otrzymuje dane określonych osób jako donos lub donos anonimowy w piśmie z 6 czerwca 2019 r. wyjaśniono, że organ odstępuje od obowiązku informacyjnego na podstawie art. 4 ust. 1 UODO.

Natomiast jak wskazano w wyjaśnieniach z 6 czerwca 2019 r. w pierwszym z wymienionych przypadków tj. gdy organ kontrolowany otrzymuje dane od innego organu administracji publicznej, sądu prokuratury, policji cyt. *Kontrolowany zawiadamia podmiot, którego dane otrzymał o fakcie otrzymania sprawy do dalszego prowadzenia, a także zgodnie z przyjętą instrukcją zawiadamiania osób, których dane otrzymano wskutek przekazania sprawy, zawiadamia się także o podstawie przetwarzania danych przesyłając odpis karty informacyjnej – zał. nr 14 do przyjętej polityki bezpieczeństwa informacji".* W toku kontroli nie udostępniono dokumentacji, na której odzwierciedlone byłoby (np. poprzez zamieszczenie stosownej adnotacji na dokumencie) załączanie klauzuli informacyjnej. Jednocześnie zauważyć należy, iż przywołany załącznik nr 14 Polityki Bezpieczeństwa Informacji to klauzula informacyjna opracowana dla sytuacji gdy dane osobowe zbierane są od osoby, której dotyczą (art. 13 ust. 1 i 2 RODO). W odpowiedzi na prośbę kontrolerów dotyczącą wskazania przyczyn powyższych rozbieżności, w złożonych pismem z 8 sierpnia 2019 r. wyjaśnieniach poinformowano, że cyt.: *Dotychczas utworzona dokumentacja nie posiadała osobnego wzoru dot. klauzuli informacyjnej na wypadek zaistnienia okoliczności, o których mowa w art. 14 RODO, przez co, ze względu na zbieżność zakresu informacji jakie posiada klauzula informacyjna oparta na art. 13, stosowano zał. nr 14. W ostatnim czasie zaktualizowano dokumentację, poprzez dołączenie nowej klauzuli informacyjnej opartej na art. 14, uzupełniając § 19 PODO.* Podkreślenia wymaga, iż klauzula informacyjna wynikająca z art. 14 RODO powinna zawierać elementy, których nie zawiera klauzula informacyjna wynikająca z art. 13 RODO, np. wskazanie źródła pochodzenia danych osobowych. Zatem stosowanie klauzuli informacyjnej wynikającej z art. 13 RODO do przypadków gdy dane osobowe nie pozyskano od osoby, której dane dotyczą było działaniem nieprawidłowym.

Jednocześnie stwierdzono, iż organ podjął działania naprawcze w powyższym zakresie.

Obszar D - Inspektor ochrony danych

Zgodnie z art. 37 ust. 1 lit. a RODO administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości. Przy czym przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a RODO rozumie się m. in. jednostki sektora finansów publicznych (art. 9 pkt 1 UODO). Kontrola wykazała, iż w okresie objętym kontrolą w WUOZ było wyznaczonych dwóch inspektorów ochrony danych, pierwszy w okresie od 25 maja 2018 r. do 30 kwietnia 2019 r., a drugi od 3 czerwca 2019 r. (nadal) [dowód – wyjaśnienia z 6 czerwca 2019 r. i z 4 lipca 2019 r., pismo z 25 maja 2018 r. o powierzeniu zadań IOD, umowa zlecenia z 3 czerwca 2019 r. dowód akta kontroli str. 5-7, 268-273, 279, 309-311].

Natomiast w okresie od 1 maja 2019 r. do dnia 3 czerwca 2019 r. w kontrolowanej jednostce nie był wyznaczony IOD (wyjaśnienia z 8 sierpnia 2019 r.), co stoi w sprzeczności z zapisami art. 37 ust. 1 lit. a RODO. Kontrolowana jednostka w piśmie z 8 sierpnia 2019 r. poinformowała iż *„Wskazuję, iż od dnia 1 maja 2019 r. do 3 czerwca 2019 r. nie był wyznaczony IOD. Jednostka kontrolowana nie zgadza się ze stwierdzeniem, iż było to odstępstwo od realizacji wymogu art. 37 ust. 1 lit. a RODO bowiem przez ww. okres poszukiwała odpowiedniej osoby na to stanowisko, która spełnia wymogi rozporządzenia (w zakresie wiedzy i umiejętności)".* Powyższe wyjaśnienia nie zostały uwzględniono, uznano je natomiast za przyczynę stwierdzonej nieprawidłowości. [dowód akta kontroli str. 296-299]. Wskazać należy, iż wyznaczenie inspektora jest powinnością organów władzy publicznej. IOD odgrywa kluczową rolę we wprowadzonym przepisami RODO modelu ochrony danych

osobowych, ponieważ jego funkcja została zaprojektowana jako swoisty gwarant właściwego przestrzegania przepisów o ochronie danych osobowych (RODO red. Sakowska-Baryła 2018, wyd. 1).

W myśl art. 11 lit. a ust. 1 UODO podmiot, który wyznaczył inspektora, może wyznaczyć osobę zastępującą inspektora w czasie jego nieobecności, z uwzględnieniem kryteriów, o których mowa w art. 37 ust. 5 i 6 rozporządzenia 2016/679. W toku kontroli ustalono, że w WUOZ we Wrocławiu cyt.: „(...) *nie wyznaczono osoby zastępującej IOD"* [wyjaśnienia z 14 czerwca 2019 r., dowód: akta kontroli str. 172-173].

W zakresie osoby pełniącej funkcję IOD w okresie od 25 maja 2018 r. do 30 kwietnia 2019 r. w oparciu o składane wyjaśnienia (pisma z: 6 czerwca 2019 r., 14 czerwca 2019 r., 4 lipca 2019 r.) oraz dostarczone dokumenty [ustanowienie IOD z 25 maja 2018 r., zaświadczenie z 16 kwietnia 2014 r. nr 003814W potwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych - dowód: akta kontroli str. 275, 279] dokonano następujących ustaleń. Osoba pełniąca funkcję IOD w okresie od 25 maja 2018 r. do 30 kwietnia 2019 r. została wyznaczona do pełnienia powyższej funkcji pismem z 25 maja 2018 r. podpisanym przez Zastępcę DWKZ. Kontrolowany organ nie zawiadomił Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu inspektora ochrony danych osobowych, mimo że zgodnie z art. 10 ust. 1 UODO musi zrealizować powyższy obowiązek w ciągu 14 dni od dnia wyznaczenia IOD. W piśmie z dnia 14 czerwca 2019 r. złożono następujące wyjaśnienia cyt. *„(...) w WUOZ był wyznaczony pracownik na stanowisko IOD, jednakże była to funkcja ustalona wewnętrznie i niezgłaszana do PUODO"* [dowód: akta kontroli str. 172-173]. Podkreślić należy, iż podmiot, który wyznaczył inspektora ochrony danych osobowych, jest zobligowany do przekazania Prezesowi UODO jego dane osobowe, tj.: imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora. Celem powyższego przepisu jest zapewnienie, aby osoby, których dane dotyczą (zarówno wewnątrz jak i spoza organizacji) i organy nadzorcze mogły mieć łatwy i bezpośredni kontakt z IOD, bez konieczności kontaktowania się z innymi jednostkami podmiotu.

Zgodnie z dyspozycją art. 37 ust. 6 RODO inspektor ochrony danych może być członkiem personelu administratora. Natomiast w myśl art. 38 ust. 6 RODO inspektor ochrony danych może wykonywać inne zadania i obowiązki, a administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów. Ponadto zgodnie z art. 38 ust. 3 RODO IOD bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego. W piśmie z 4 lipca 2019 r. nr WUOZ.1610.22.2019.DG.4 wskazano, że osoba wyznaczona na IOD była pracownikiem WUOZ zatrudnionym na stanowisku specjalisty ds. obrony cywilnej. Zarówno z Regulaminu WUOZ jak i ze schematu organizacyjnego jednostki nie wynika czy wskazane stanowisko podlegał bezpośrednio najwyższemu kierownictwu. W toku kontroli nie udostępniono kontrolującym opisu stanowiska zajmowanego przez ww. pracownika bądź też jego zakresu obowiązków (o powyższe dokumenty kontrolerzy wystąpili pismem z 12 czerwca 2019 r.), niemożliwe było zatem ustalenie czy IOD podlegał bezpośrednio najwyższemu kierownictwu oraz czy administrator zapewnił aby zadania i obowiązki IOD nie powodowały konfliktu interesów.

Inspektor ochrony danych w myśl art. 37 ust. 5 RODO jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39. Powyższy przepis nie wskazuje konkretnych kwalifikacji zawodowych, jakie należy brać pod uwagę, wyznaczając IOD, niemniej jednak w świetle wymagań w nim określonych, wydaje się istotne by posiadał on wykształcenie wyższe, w szczególności prawnicze lub informatyczne, w przypadku organów publicznych kwalifikacje w zakresie prawa

i postępowania administracyjnego (dr Gabriela Bar Inspektor ochrony danych – miejsce w organizacji, rola i zadania, PME 2018, nr 4). Wymagany poziom wiedzy fachowej powinien być określony w zależności od przeprowadzonych operacji przetwarzania danych i ochrony wymaganej do przetwarzania danych osobowych. Odpowiednie umiejętności i wiedza obejmują przede wszystkim wiedzę na temat krajowych i europejskich przepisów i praktyk w zakresie ochrony danych, w tym dogłębnego zrozumienia RODO. RODO nie reguluje co prawda zasad czy trybu weryfikacji spełnienia tego wymogu, niemniej jednak certyfikaty, dyplomy oraz inne dokumenty poświadczające wiedzę i doświadczenie inspektora są ważnym kryterium kwalifikacyjnym i argumentem przemawiającym na korzyść osoby wyznaczanej do pełnienia tej funkcji. Kontrolowany organ w piśmie z 4 lipca 2019 r. poinformował, iż pracownik wyznaczony na IOD cyt. „(...) *posiadał szeroką wiedzę z omawianego obszaru, popartą dokumentami w zakresie pracy z danymi niejawnymi tajnymi, co w ocenie administratora uzasadniało kompetencję z zakresu pracy z danymi, które należy chronić*". Do złożonych wyjaśnień nie załączono żadnych certyfikatów, dyplomów czy też innych dokumentów poświadczających wiedzę i doświadczenie w zakresie ochrony danych osobowych. Jedynym dokumentem załączonym do wyjaśnień było zaświadczenie z 16 kwietnia 2014 r. stwierdzające odbycie szkolenia w zakresie ochrony informacji niejawnych. W ocenie kontrolujących złożone wyjaśnienia jak również załączone zaświadczenie z 16 kwietnia 2014 r. nie poświadczają, iż wyznaczony IOD posiadał kwalifikacje zawodowe, a w szczególności fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań określonych w art. 39 RODO. Zauważyć jednocześnie należy, iż znaczenie fachowej wiedzy w zakresie prawa i praktyki zostało dodatkowo podkreślone przez zobowiązanie administratorów i podmiotów przetwarzających do zapewnienia IOD zasobów niezbędnych do utrzymania wysokiego i aktualnego poziomu wiedzy (art. 38 ust. 2 RODO). Wymóg uaktualniania wiedzy i zapewnienia na to środków finansowych jest uzasadniony wobec zmieniającego się stale stanu wiedzy technicznej, rozwoju technologicznego i postępu wielkoskalowych metod przetwarzania danych.

Natomiast w zakresie osoby pełniącej funkcję IOD od 3 czerwca 2019 r. w oparciu o składane wyjaśnienia (pisma z: 6 czerwca 2019 r., 14 czerwca 2019 r., 4 lipca 2019 r.) oraz dostarczone w toku kontroli dokumenty dokonano następujących ustaleń. Osoba pełniąca funkcję IOD od 3 czerwca 2019 r. jest pracownikiem WUOZ zatrudnionym na stanowisku inspektora ds. administracyjnych kar pieniężnych [dowód – wyjaśnienia z 14 czerwca 2019 r., dowód akta kontroli str. 172-173], natomiast funkcję IOD pełni na podstawie umowy zlecenia [dowód – wyjaśnienia z 14 czerwca 2019 r., umowa zlecenia z 3 czerwca 2019 r. dowód akta kontroli str. 172-173, 309-311]. Zgodnie z dyspozycją art. 37 ust. 6 RODO inspektor ochrony danych może wykonywać zadania na podstawie umowy o świadczenie usług. Kontrola wykazała, że DWKZ we Wrocławiu w dniu 3 czerwca 2019 r. zawarł umowę zlecenia na świadczenie usługi pełnienia obowiązków Inspektora Ochrony Danych, którą wykonawca usługi zobowiązał się realizować z dołożeniem należytej staranności, wedle najlepszej posiadanej wiedzy. Zdaniem Grupy Roboczej art. 29 (aktualnie EROD) dobrą praktyką byłoby wskazanie czasu, który należy poświęcić na obowiązki IOD. W umowie zlecenia na świadczenie usług IOD zawartej dniu 3 czerwca 2019 r. nie określono warunków czasowych pełnienia funkcji IOD.

Za realizację ww. umowy świadczenia usług IOD odpowiada DWKZ co stanowi odpowiednik podlegania bezpośrednio najwyższemu kierownictwu. Ponadto IOD będąc pracownikiem WUOZ zatrudnionym na stanowisku inspektora ds. administracyjnych kar pieniężnych podlega bezpośrednio DWKZ, a w swojej pracy nie bierze udział w określaniu

celów i sposobów przetwarzania danych, co mogłoby powodować konflikt interesów, spełniony zatem został wymóg określony w art. 38 ust. 3 i 6 RODO.

Kontrola wykazała, iż wyznaczony z dniem 3 czerwca 2019 r. inspektor ochrony danych ukończył studia pierwszego stopnia na kierunku administracja oraz posiada wykształcenie wyższe prawnicze [dyplomy ukończenia studiów, dowód: akta kontroli str. 203-204]. Ponadto IOD brał udział w szkoleniu *RODO prawne, techniczne i praktyczne aspekty wprowadzenia nowej regulacji*, co potwierdza uzyskany w dniu 13 marca 2018 r. certyfikat [dowód: akta kontroli str. 202]. Kontrolowany organ udokumentował zatem spełnienie przez IOD wymagań dotyczących kwalifikacji zawodowych określonych w art. 37 ust. 5 RODO.

W myśl art. 37 ust. 7 RODO Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

Podmiot, który wyznaczył inspektora ochrony danych osobowych musi w ciągu 14 dni od dnia wyznaczenia zawiadomić o tym fakcie Prezesa Urzędu Ochrony Danych Osobowych, przy czym zawiadomienie musi być sporządzone w postaci elektronicznej i opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP (art. 10 ust. 1 i 6 UODO). W toku kontroli kontrolującym przekazano wraz z pismem z 5 lipca 2019 r. odpis zawiadomienia z dnia 5 lipca 2019 r. nr WriD.0137.4.2019.DG o ustanowieniu Inspektora Ochrony Danych Osobowych w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu adresowany do Prezesa Urzędu Ochrony Danych Osobowych [dowód akta kontroli str. 274, 276-277]. Powyższe zawiadomienie zostało skierowane do PUODO z przekroczeniem 14-dniowego terminu wynikającego z art. 10 ust. 1 UODO, albowiem IOD został wyznaczony 3 czerwca 2019 r., a zawiadomienie ma datę 5 lipiec 2019 r. Zgodnie z art. 10 ust. 1 i 3 UODO zawiadomienie skierowane do Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu IOD musi wskazywać: imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora ochrony danych; pełną nazwę oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot publiczny; numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu. Kontrola wykazała, iż zawiadomienie o wyznaczeniu IOD skierowane do Prezesa Urzędu Ochrony Danych Osobowych przez Zastępcę DWKZ sporządzone zostało w postaci elektronicznej zgodnie z dyspozycją art. 10 ust. 6 UODO, oraz zawierało w zasadzie wszystkie elementy określone w art. 10 ust. 1 i 3 UODO, za wyjątkiem wskazania numeru identyfikacyjnego REGON.

Zgodnie z art. 11 UODO podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, tj. imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności. Ponadto w § 20 Polityki ochrony danych osobowych wskazano, iż cyt.: *„W celu ułatwienia korzystania z praw przez osobę, której dane dotyczą Administrator umożliwia jej kontakt z IOD poprzez umieszczeniu adresu mailowego do niego na stronie internetowej WUOZ"*. W toku kontroli ustalono, w oparciu o wyjaśnienia złożone pismem z 4 lipca 2019 r., iż w okresie objętym kontrolą *Informacja o IOD nie była umieszczona na stronie BIP WUOZ.* Zatem kontrolowana jednostka nie wywiązywała się z obowiązku publikacji danych IOD określonego we wskazanych wyżej przepisach prawa, jak również w przyjętej Polityce ochrony danych osobowych.

W toku kontroli ustalono, iż w § 6 ust. 2 Polityki ochrony danych osobowych stanowiącej załącznik nr 4 do Polityki Bezpieczeństwa Informacji w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu wskazano, iż administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące danych osobowych związane z realizacją jego zadań wynikających z RODO. Ponadto w § 6 ust. 2 Polityki określono jakie zadania wykonuje IOD, a powyższe zapisy uwzględniają wszystkie zadania IOD wynikające z art. 39 RODO [dowód: akta kontroli str. 71-90].

Obszar E – Rejestrowanie Czynności Przetwarzania Danych Osobowych

Przepis art. 30 RODO wskazuje obowiązki rejestrowania czynności przetwarzania danych osobowych zarówno przez administratora, jak i przez podmiot przetwarzający (umocowany umową lub innym instrumentem prawnym do przetwarzania danych osobowych w imieniu innego administratora). Każdy administrator – zobowiązany został do prowadzenia *Rejestru Czynności Przetwarzania Danych Osobowych* (art. 30 ust. 1 RODO), a każdy podmiot przetwarzający powinien prowadzić *Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora* (art. 30 ust. 2 RODO).

Rejestr Czynności Przetwarzania Danych Osobowych:

Czynności kontrolne wykazały, iż Dolnośląski Wojewódzki Konserwator Zabytków - jako Administrator – prowadzi Rejestr Czynności Przetwarzania Danych Osobowych - w formie zgodnej z art. 30 ust. 3 RODO [dowód: akta kontroli str. 8-12].

Podkreślenia wymaga, iż w toku wykonywania czynności kontrolnych kontrolującym przedstawiono dwie wersje Rejestru Czynności Przetwarzania Danych Osobowych. Kontroli poddano wersję drugą Rejestru Czynności Przetwarzania Danych Osobowych.

[dowód: akta kontroli str. 63-66]

W wyniku kontroli stwierdzono, iż poddany kontroli *Rejestr* zwierał większość elementów, o których mowa w przepisie art. 30 ust. 1 RODO, za wyjątkiem imienia i nazwiska inspektora ochrony danych, mimo takiego obowiązku wynikającego z art. 30 ust. 1a) RODO. Z wyjaśnień z dnia 4 lipca 2019 r. udzielonych przez organ kontrolowany wynika, iż brak zawarcia w rejestrze imienia i nazwiska inspektora ochrony danych został uzupełniony [dowód: akta kontroli str. 268-273].

W świetle powyższego należy stwierdzić, iż podmiot kontrolowany podjął działania naprawcze.

Ponadto analiza Rejestru Czynności Przetwarzania Danych Osobowych wykazała, iż:

1) W rubryce Rejestru zatytułowanej: *Powierzenie danych* wskazano: *Tak – banki* (poz. 1, 2, 3); *Tak – podmioty zewnętrzne realizujące szkolenie* (poz. 5,7). Niemniej jednak z przekazanego Rejestru Umów o powierzenie przetwarzania danych osobowych wynika, iż podpisano jedynie jedną umowę na świadczenie usług szkoleniowych z BHP i PPOŻ (co zostało odzwierciedlone pod poz. *5 Rejestru Czynności Przetwarzania Danych Osobowych* w rubryce zatytułowanej: *Powierzenie danych* poprzez zapis: *TAK – podmioty zewnętrzne realizujące szkolenie*). Jednakże z rejestru umów o powierzenie danych nie wynika fakt powierzenia danych osobowych podmiotom zewnętrznym takim jak *bank/ podmiot zewnętrzny realizujący szkolenie*, inne niż te *z zakresu BHP i PPOŻ*

[dowód: akta kontroli str. 117].

W wyjaśnieniach z dnia 4 lipca 2019 r. organ kontrolowany podkreślił, iż wskazanie banków – jako podmiotów przetwarzających danych w przypadków czynności przetwarzania zarejestrowanych pod poz. 1-3 Rejestru – było błędem. W wyjaśnieniach doprecyzowano, iż błędne zapisy należało skorygować [dowód: akta kontroli str. 268-273]. W świetle powyższego należy stwierdzić, iż podmiot kontrolowany podjął działania naprawcze.

W zakresie podmiotów zewnętrznych realizujących szkolenia – wskazanych jako podmioty przetwarzające dane - w przypadków czynności przetwarzania zarejestrowanej pod poz. 7 Rejestru – organ kontrolowany w przedmiotowych wyjaśnieniach wskazał, iż dotyczy do *sytuacji, jakie mogą się zdarzyć w przyszłości – przyszłych szkoleń, dookreślające przy tym, iż wówczas będą zawierane stosowne umowy powierzenia* [dowód: akta kontroli str. 268-273]. Przedmiotowe wyjaśnienia uwzględniono przy ocenie za kontrolowane zagadnienie. Niemniej jednak należy pamiętać, iż jednym z celów prowadzenia przedmiotowego rejestru jest ułatwienie zarówno administratorowi, jak i organowi nadzorczemu kontroli wszystkich procesów przetwarzania danych w organizacji.[9] W związku z czym zapisy rejestru powinny odzwierciedlać aktualne (a nie przewidywane) procesy przetwarzania danych osobowych.

Z przedstawionej przez organ kontrolowany wersji Rejestru Czynności Przetwarzania Danych Osobowych wynika, iż jedynie przy procesie przetwarzania danych osobowych, jakim jest rekrutacja do pracy (nabory) przetwarzanie danych osobowych odbywa się na podstawie udzielonej zgody (art. 6 ust. 1 lit. a RODO) oraz na podstawie przesłanki, o której mowa w art. 6 ust. 1 c RODO (wypełnienie obowiązku prawnego ciążącego na administratorze). Niemniej jednak analiza ogłoszeń o naborze do korpusu służby cywilnej (Nabór Nr 48815, 48814) wykazała, iż oprócz zgody (art. 6 ust. 1 lit. a RODO) oraz art. 6 ust. 1 c) RODO - jako podstawę prawną przetwarzania powołano dodatkowo - art. 6 ust. 1 lit. b RODO – tj. podstawę prawną, w której przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą. W wyjaśnieniach z dnia 4 lipca 2019 r. organ kontrolowany wskazał, iż: w rejestrze nastąpiła omyłka pisarska, prawidłowa kwalifikacja powinna być – art. 6 ust. 1 lit. b) RODO [dowód: akta kontroli str. 268-273]. Złożone wyjaśnienia nie zostały uwzględnione przy ocenie za kontrolowane zagadnienie, bowiem zupełnie inny stan faktyczny wynika ze stosowanych przez organ kontrolowany klauzul informacyjnych zamieszczonych w treści wyżej wymienionych ogłoszeń – w których wskazano trzy podstawy prawne przetwarzania – tj. art. 6 ust. 1 a),b),c) RODO – a nie tylko art. 6 ust. 1 a) i b) RODO.

Z przedstawionej przez organ kontrolowany wersji *Rejestru Czynności Przetwarzania Danych Osobowych* nie wynikało wprost, iż organ zidentyfikował czynność przetwarzania danych osobowych w zakresie odnoszącym się do zamówień publicznych. Z wyjaśnień z dnia 4 lipca oraz z 8 sierpnia 2019 r. wynika, iż do dnia 4 lipca 2019 r. organ kontrolowany proces odnoszący się do zamówień publicznych uwzględniał w pkt 37 Rejestru Czynności Przetwarzania Danych Osobowych (w którym jako cel przewarzania wskazano: *postępowanie administracyjne – rozwiązania zamienne*), a od 5 lipca 2019 r. wprowadził osobną kategorie czynności przetwarzania – tj. zamówienia publiczne. [dowód: akta kontroli str. 268-273]

Odnosząc się do złożonych wyjaśnień należy wskazać, iż cel przetwarzania, o którym mowa w pkt 37 Rejestru Czynności Przetwarzania Danych Osobowych (wersja przed wprowadzeniem nowej kategorii czynności przetwarzania – tj. czynności odnoszącej się do

[9] Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii przetwarzania określonego w art. 30 ust. 1 i 2 RODO: Poradnik Urzędu Ochrony Danych Osobowych, str. 5

zamówień publicznych) nie wskazuje, aby w pkt 37 Rejestru (*postępowanie administracyjne – rozwiązania zamienne*) - do dnia 4 lipca 2019 r. - zidentyfikowano czynność przetwarzania danych osobowych, która dotyczyłaby zamówień publicznych. Jednakże mając na względzie fakt wyodrębnienia przez organ kontrolowany osobnej kategorii czynności przetwarzania – tj. czynności odnoszącej się do zamówień publicznych – złożone wyjaśnienia uwzględniono przy ocenie za kontrolowane zagadnienie.

Rejestr Wszystkich Kategorii Czynności Przetwarzania dokonywanych w imieniu administratora

Pismem z dnia 4 czerwca 2019 r. w imieniu Wojewody Dolnośląskiego zwrócono się do Pani Barbary Nowak – Obelinda – Dolnośląskiego Wojewódzkiego Konserwatora Zabytków o poinformowanie, czy organ kontrolowany prowadzi *Rejestr wszystkich kategorii czynności przetwarzania.* W piśmie z dnia 6 czerwca 2019 r. wskazano, iż *jednostka kontrolowana prowadzi jedynie rejestr czynności przetwarzania danych osobowych.*

Niemniej jednak, analiza przekazanych w trakcie wykonywania czynności kontrolnych dokumentów wykazała, iż kontrolującym przedstawiono dwa dokumenty: pierwszy nazwany jako - *Rejestr kategorii czynności*, oraz drugi - nazwany *Wzorem Rejestru Kategorii Przetwarzania danych osobowych podmiotu przetwarzającego* [dowód: akta kontroli str. 67-69]. W świetle ustalonych rozbieżności pomiędzy udzielonymi wyjaśnieniami, a ustaleniami dokonanymi na podstawie przedłożonych ww. dwóch dokumentów - zwrócono się do podmiotu kontrolowanego o złożenie wyjaśnień w zakresie prowadzonych przez Dolnośląskiego Wojewódzkiego Konserwatora Zabytków dwóch różnych dokumentów jako - *rejestru kategorii czynności przetwarzania danych osobowych*, w tym o poinformowanie, czy któryś z przedłożonych rejestrów jest *Rejestrem Wszystkich Kategorii Czynności Przetwarzania dokonywanych w imieniu administratora*, o którym mowa w art. 30 ust. 2 RODO [dowód: pismo o wyjaśnienia z dnia 26 czerwca 2019 r. oraz z dnia 26 lipca 2019 r. akta kontroli str. 240-249, 289-294].

Pismem z dnia 8 sierpnia 2019 r. podmiot kontrolowany udzielił odpowiedzi „*wzór kategorii czynności przetwarzania danych, jak i rejestr kategorii czynności stanowi przyjęty w WUOZ rejestr kategorii czynności. Rejestr odnosi się do kategorii przetwarzania w Urzędzie we Wrocławiu, jak i do działań podejmowanych w delegaturach*". W złożonych wyjaśnieniach organ kontrolowany nie wskazał wprost, iż przyjęty w WUOZ rejestr kategorii czynności (de facto dwa dokumenty) jest *Rejestrem Wszystkich Kategorii Czynności Przetwarzania dokonywanych w imieniu administratora*, o którym mowa w art. 30 ust. 2 RODO [dowód: akta kontroli str. 296-299].

Odnosząc się do udzielonych wyjaśnień należy wskazać, iż *Rejestr Wszystkich Kategorii Czynności Przetwarzania dokonywanych w imieniu administratora*, o którym mowa w art. 30 ust. 2 RODO – powinien obejmować wszystkie kategorie czynności przetwarzania dokonywanych przez podmiot przetwarzający w imieniu wszystkich administratorów. Ma zawierać m.in. określenie każdego administratora, w imieniu którego działa podmiot przetwarzający oraz kategorie przetwarzań dokonywanych w imieniu każdego z administratorów. W odniesieniu do każdego z administratorów wskazane jest zatem nazwanie poszczególnych powierzeń (zleceń), a zatem rodzaju usług, jakie podmiot przetwarzający na podstawie zawartych umów wykonuje na rzecz poszczególnych administratorów. Uporządkowanie czynności wykonywanych w ramach powierzenia w

kategorie, czyli ich pogrupowanie pod względem rodzaju usług świadczonych przez podmiot przetwarzający, umożliwi łatwy przegląd „powierzeń" zwłaszcza w przypadku podmiotów przetwarzających, które działają na rzecz wielu podmiotów danych lub świadczą wiele różnych usług w zakresie przetwarzania danych [Urząd Ochrony Danych Osobowych – Wskazówki i wyjaśnienia dotyczące rejestrowania czynności i kategorii przetwarzania określonego w art. 30 ust. 1 i 2 RODO, str. 9-10].

W świetle powyższego – dla stwierdzenia, że Dolnośląski Wojewódzki Konserwator Zabytków zobowiązany jest do prowadzenia Rejestru Wszystkich Kategorii Czynności Przetwarzania dokonywanych w imieniu administratora, o którym mowa w art. 30 ust. 2 RODO niezbędne staje się ustalenie, czy pomiędzy Dolnośląskim Wojewódzkim Konserwatorem Zabytków a innym podmiotem – istnieje relacja wskazująca na to, że Dolnośląski Wojewódzki Konserwator Zabytków jest podmiotem przetwarzającym dane osobowe tego podmiotu – który jest administratorem danych osobowych powierzonych Dolnośląskiemu Wojewódzkiemu Konserwatorowi Zabytków w drodze umowy lub innego instrumentu prawnego do przetwarzania danych osobowych w imieniu innego administratora.

Odnosząc powyższe na zapisy obu dokumentów należy wskazać, iż w pierwszym dokumencie – *Rejestr kategorii czynności* - wskazano Dolnośląskiego Wojewódzkiego Konserwatora Zabytków zarówno jako podmiot przetwarzający, jak i administratora. Natomiast w drugim – nazwanym: *Wzorem Rejestru Kategorii Przetwarzania danych osobowych podmiotu przetwarzającego* – jako administratora wskazano - Dolnośląskiego Wojewódzkiego Konserwatora Zabytków – kierownicy Delegatury Wojewódzkiego Urzędu Ochrony Zabytków w Jeleniej Górze, w Legnicy, natomiast jako podmiot przetwarzający – Delegatury Wojewódzkiego Urzędu Ochrony Zabytków w Jeleniej Górze, w Legnicy w Wałbrzychu. Podkreślić należy, iż w myśl art. 92 ust. 4 ustawy z dnia 23 lipca 2003 r. o ochronie zabytków i opiece nad zabytkami (t. j. Dz.U. z 2018 r. poz. 2067 ze zm.) delegatura wojewódzkiego urzędu ochrony zabytków wchodzi w skład wojewódzkiego urzędu ochrony zabytków, którym kieruje wojewódzki konserwator zabytków (art. 92 ust. 1 ww. o ochronie zabytków i opiece nad zabytkami), który jest administratorem danych (Zagadnienia węzłowe grupy roboczej ds. administracji, Ministerstwo Cyfryzacji – styczeń 2019 r.).

Analiza zapisów ww. dokumentów nie wykazała jakiejkolwiek relacji, w której Dolnośląski Wojewódzki Konserwator Zabytków – w imieniu innego administratora danych – występowałby jako podmiot przetwarzający – tj. podmiot zobligowany do prowadzenia Rejestru Wszystkich Kategorii Czynności Przetwarzania dokonywanych w imieniu administratora, o którym mowa w art. 30 ust. 2 RODO, mając na względzie fakt:

- wskazania w pierwszym dokumencie (Rejestr kategorii czynności) Dolnośląskiego Wojewódzkiego Konserwatora Zabytków zarówno jako podmiot przetwarzających, jak i administratora;

- a w drugim dokumencie (Wzór Rejestru Kategorii Przetwarzania Danych Osobowych Podmiotu Przetwarzającego) wskazania: Dolnośląskiego Wojewódzkiego Konserwatora Zabytków (kierownicy Delegatury Wojewódzkiego Urzędu Ochrony Zabytków w Jeleniej Górze, w Legnicy) – jako administratora, natomiast jako podmiot przetwarzający – Delegatury Wojewódzkiego Urzędu Ochrony Zabytków w Jeleniej Górze, w Legnicy w Wałbrzychu, mimo że każda z delegatur wchodzi w skład wojewódzkiego urzędu ochrony zabytków, i nie jest odrębnym administratorem danych, biorąc jednocześnie pod uwagę fakt, iż relacji: administrator (kierownik delegatura Wojewódzkiego Urzędu Ochrony Zabytków) – podmiot przetwarzający (Wojewódzki Urzędu Ochrony Zabytków we Wrocławiu), którego

administratorem danych jest Dolnośląski Wojewódzki Konserwator Zabytków – nie wykazała także analiza umów powierzenia udostępnionych przez Dolnośląskiego Wojewódzkiego Konserwatora Zabytków. [dowód: akta kontroli str. 117]

W świetle powyższego - wobec braku wykazania przez organ kontrolowany jakiekolwiek relacji, w której Dolnośląski Wojewódzki Konserwator Zabytków – w imieniu innego administratora danych – występowałby jako podmiot przetwarzający – tj. podmiot zobligowany do prowadzenia Rejestru Wszystkich Kategorii Czynności Przetwarzania, prowadzenie przez organ kontrolowany przedmiotowych rejestrów stanowi naruszenie art. 30 ust. 2 RODO.

Obszar F- Ocena skutków przetwarzania danych osobowych

Zasada podejścia opartego na ryzyku (risk based approach) jest koncepcją stanowiącą trzon ogólnego rozporządzenia o ochronie danych. Zasada ta uzależnia sposób realizacji obowiązków nałożonych na administratora od charakteru, zakresu, kontekstu i celów przetwarzania danych oraz od ryzyka naruszenia praw i wolności osób, których dane dotyczą, a także ryzyka naruszenia interesów administratora. Została ona wyrażona m.in. w art. 24 oraz 32 RODO.

Wśród obowiązków wynikających z przepisów RODO powiązanych z ww. zasadą należy wskazać na: opracowanie analizy ryzyka, sporządzenie oceny skutków przetwarzania danych – o ile zaistnieją obligatoryjne przesłanki oraz wdrożenie odpowiednich środków technicznych i organizacyjnych oraz zasad ochrony danych w fazie projektowania oraz domyślnej ochrony danych.

Wskazać należy, iż przepisy RODO nakładają na Administratora obowiązki wdrożenia odpowiednich środków technicznych i organizacyjnych:
- *aby przetwarzanie danych osobowych odbywało się zgodnie z rozporządzeniem RODO, i aby móc to wykazać* [art. 24 ust.1 RODO];
- *zarówno przy określaniu sposobów przetwarzania* (privacy by design), *jak i w czasie samego przetwarzania* (privacy by default) [art. 25 ust. 1 RODO].

Podkreślić należy, iż w myśl przepisów RODO – *stosowanie przez administratora zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42* (art. 24 ust 3, art. 25 ust. 3 RODO) – może zostać uznane jako element dla stwierdzenia przestrzegania przez administratora ww. obowiązków.

Jednocześnie z art. 24 ust. 2 RODO wynika dla Administratora obowiązek wdrożenia – jako środki techniczne i organizacyjne (art. 24 ust.1 RODO) – odpowiednich polityk ochrony danych osobowych, które – jak to wynika z motywu 78 Preambuły do RODO – powinny być zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania (*privacy by design*) oraz z zasadą domyślnej ochrony danych (*privacy by default*).

Ponadto z przepisu art. 32 ust. 2 RODO wynika obowiązek, aby Administrator przy ocenie stopnia bezpieczeństwa przetwarzania danych uwzględnił w szczególności ryzyko wiążące się z przetwarzaniem. Jednocześnie z motywu 83 Preambuły do RODO wynika,

iż w celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania.

Administrator wskazał, iż obowiązki wynikające z art. 24 ust. 2 RODO zostały wypełnione poprzez wdrożenie Polityki Bezpieczeństwa Informacji w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu (w tym: Instrukcji Zarządzania System Informatycznym służącym do przetwarzania danych osobowych – zał. Nr 5 do ww. Polityki; Polityki Ochrony Danych Osobowych w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu – zał. Nr 4 do ww. Polityki; Instrukcji postępowania w sytuacji naruszeń ochrony danych osobowych – Zał. Nr 16 do ww. Polityki; Zasady organizacji edukacji z zakresu ochrony danych osobowych – Zał. Nr 19 do ww. Polityki; Procedury postępowania względem żądań osób, których dane dotyczą w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu – Zał. Nr 25 do ww. Polityki; Metodyki szacowania ryzyka naruszenia praw lub wolności osób fizycznych w WOUZ – Zał. Nr 24 do ww. Polityki) [dowód: akta kontroli str. 91-100, 71-90, 121,123, 129- 131, 159-165, 136-158].

Jednocześnie w zakresie wypełnienia przez Administratora obowiązków wynikających z art. 25 RODO i motywu 78 Preambuły do RODO ustalono, iż sporządzona przez organ kontrolowany polityka ochrony danych osobowych (Polityka Bezpieczeństwa Informacji w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu) oraz stosowana praktyka uwzględnia zasadę ochrony danych w fazie projektowania (*privacy by design*) oraz zasadę domyślnej ochrony danych (*privacy by default*).

Na powyższe ustalenia wpływa to, iż zgodnie z zapisem pkt 1.2.2 ww. Polityki Bezpieczeństwa Informacji, akt ten, w zakresie bezpieczeństwa informacji w WUOZ, *jest aktem nadrzędnym w stosunku do wszystkich obowiązujących w urzędzie regulacji.* Ponadto w pkt 1 2.4 ww. Polityki – wskazano iż *ochrona informacji wynikająca z Polityki Bezpieczeństwa Informacji jest realizowana na każdym etapie przetwarzania informacji.* Jednocześnie przepisy procedury kładą nacisk przy przetwarzaniu danych osobowych przez Administratora Danych - na takie kwestie jak: przestrzeganie zasad przewarzania danych osobowych; system zabezpieczenia (bezpieczeństwo fizyczne, techniczne, organizacyjno-proceduralne); właściwe przetwarzanie w aplikacjach; zarządzanie podatnościami technicznymi i ciągłością działania: reagowanie na incydenty związane z bezpieczeństwem informacji oraz minimalizacja ich skutków oraz zarządzanie ryzykiem utraty bezpieczeństwa aktywów informacyjnych WUOZ.

Ponadto w wyjaśnieniach z dnia 4 lipca 2019 r. organ kontrolowany wskazał, iż w toku wykonywania działalności uwzględnia się politykę ochrony danych osobowych w fazie projektowania (*privacy by design*) *przez pryzmat możliwości finansowych, technicznych i organizacyjnych WUOZ. Stosowane są szafki zamykane na klucz, pomieszczenia, w których pracują pracownicy i przechowywane są dokumenty. Zarówno do budynku, jak i na poszczególne piętra dostęp mają tylko pracownicy posiadający kartę dostępu. Do serwerowni oraz szaf pancernych mają dostęp tylko wyznaczeni pracownicy. Pracownicy są szkoleni lub informowani o każdej zmianie organizacyjnej lub zmianach prawnych. Powyższe ma na celu przewidywanie zagrożeń oraz ich unikanie lub minimalizowane na wielu płaszczyznach, a także analizowanie czy obecnie posiadane zabezpieczenia oraz przyjęte procedury organizacyjne będą wystarczające w przyszłości lub przy uwzględnieniu zmian prawnych i technicznych. Na tej podstawie budowana jest dalsza strategia ochrony techniczno-organizacyjnej.* Ponadto w zakresie domyślnej ochrony danych osobowych (*privacy by*

default) podmiot kontrolowany wskazał, iż *stosuje szeroko rozumianą pomoc wobec klientów w zakresie załatwiania spraw poprzez udzielania informacji jakie dane oraz dokumenty są potrzebne do załatwienia spraw urzędowych, aby ograniczyć otrzymane dane osobowe do niezbędnego minimum. Pracownicy są szkoleni z zakresu pracy z danymi osobowymi. Z racji niskiej świadomości prawnej społeczeństwa w znacznej ilości zdarzają się sytuacje, gdzie klienci przekładają zbyt małą ilość danych niezbędnych do wykonywania zadań przez pracownika* [dowód: akta kontroli str. 268-273]. Złożone wyjaśnienia zostały uwzględnione przy ocenie kontrolowanego zagadnienia.

W zakresie obowiązku wynikającego z art. 32 ust. 2 RODO należy stwierdzić iż organ kontrolowany nie rozliczył się z obowiązku wykazania, iż oszacował ryzyko naruszenia praw i wolności osoby, której dane dotyczą, dla każdej zidentyfikowanej operacji przetwarzania danych osobowych zachodzącej w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu, mimo takiego obowiązku wynikającego z art. 5 ust. 2 RODO. Podkreślenia wymaga, iż organ kontrolowany posiada procedurę szacowania ryzyka naruszenia praw lub wolności osób fizycznych – nazwaną Metodyką szacowania ryzyka naruszenia praw i wolności osób fizycznych w WUOZ, stanowiącą załącznik nr 24 do Polityki Bezpieczeństwa Informacji w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu. Niemniej analizy ryzyka naruszenia praw i wolności osób fizycznych nie dokonał [dowód: akta kontroli str. 136-148].

Na wskazaną ocenę wpływ ma przede wszystkim to, iż jednostka kontrolowana - jako analizę ryzyka przekazała jedynie następujące dokumenty nazwane jako: *Akceptuję ryzyka wystąpienia zagrożenia*: *Zabezpieczenia* (sztuk 3); *Słowniki* (sztuk 2); *Ryzyka* (sztuk 2) oraz fakt, że organ kontrolowany w składanych wyjaśnieniach utrzymywał, iż sporządził analizę ryzyka naruszenia praw i wolności osoby, której dane dotyczą, dla każdej zidentyfikowanej operacji przetwarzania danych osobowych zachodzącej w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu, jednakże powyższego faktu w żaden sposób nie zdołał udokumentować. Podkreślenia wymaga, iż samo wskazanie w wyjaśnieniach, iż taka analiza została sporządzona nie może zostać uznane za rozliczenie się z obowiązku oszacowania ryzyka naruszenia praw i wolności osoby, której dane dotyczą, dla każdej zidentyfikowanej operacji przetwarzania danych osobowych zachodzącej w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu, bez jakiegokolwiek dokumentu odzwierciedlającego dokonanie procesu.

Należy wskazać, iż wprawdzie organ kontrolowany przekazał kontrolującym ww. dokumenty – jako analizę ryzyka szacowania ryzyka naruszenia praw i wolności osób fizycznych w WUOZ – niemniej jednak z przekazanych dokumentów nie wynika, na jakim poziomie oszacowano ryzyko dla każdego zachodzącego w jednostce procesu przetwarzania danych osobowych. Przekazane dokumenty obrazują jedynie oszacowany poziom ryzyka zaistnienia danego zagrożenia, a nie poziom ryzyka naruszenia prawa i wolności osób fizycznych dla każdego zachodzącego w jednostce procesu przetwarzania danych osobowych. Za spełnienie takiego obowiązku nie może zostać uznane przedstawienie jedynie i wyłącznie dokumentacji odnoszącej się do analizy prawdopodobieństwa wystąpienia zagrożenia, bowiem ostatnim etapem szacowania przez Administratora Danych Osobowych ryzyka powinno być stworzenie listy operacji przetwarzania danych osobowych z przyporządkowanymi każdej operacji poziomami ryzyka [podobnie w: Poradnik UODO: Jak stosować podejście oparte na ryzyku; Część II (maj 2018), strona 24]. Podkreślić należy, iż sam podmiot kontrolowany w pkt 6.4.2 *Metodyki szacowania ryzyka naruszenia praw i*

wolności osób fizycznych – wskazał, iż szacowanie ryzyka powinno być sporządzone dla każdego zachodzącego jednostce procesu, w którym przetwarzane są dane osobowe, które zostały zidentyfikowane w *Rejestrze Czynności Przewarzania danych osobowych* (pkt 1 Metodyki szacowania ryzyka naruszenia praw i wolności osób fizycznych), a nie tylko w zakresie oszacowania ryzyka wystąpienia zagrożenia.

Podkreślić należy, iż o przekazanie takiej analizy ryzyka (tj. analizy ryzyka naruszenia praw i wolności osoby, której dane dotyczą w każdej zidentyfikowanej operacji przetwarzania danych osobowych) kilkakrotnie wystąpili kontrolerzy zarówno w toku wykonywania czynności kontrolnych, jak i po dokonanych czynnościach kontrolnych.

Zdaniem kontrolujących, przedłożone dokumenty nie stanowią oceny ryzyka naruszenia praw i wolności osoby, której dane dotyczą w każdym zidentyfikowanym rodzaju operacji przetwarzania danych osobowych, a zatem nie zostały sporządzone zgodnie *z Metodyką szacowania ryzyka naruszenia praw i wolności osób fizycznych* ustaloną przez podmiot kontrolowany oraz z uwzględnieniem wytycznych Urzędu Ochrony Danych Osobowych. W żadnym z przekazanych dokumentów nie wskazano bowiem rodzaju operacji przetwarzania danych osobowych z przyporządkowanym im ryzkiem, nie wskazano także klucza (macierzy) przeniesienia oszacowanego ryzyka prawdopodobieństwa wystąpienia zagrożenia na zidentyfikowane rodzaje operacji przetwarzania. Proces szacowania poziomu ryzyka nie został zakończony utworzeniem listy operacji przetwarzania z przyporządkowanymi im poziomami ryzyka.[10]

Wskazać należy, iż organ kontrolowany w wyjaśnieniach z dnia 8 sierpnia 2019 r. odniósł się jedynie do metody szacowania ryzyka zaistnienia zagrożenia oraz do braku obowiązku pisemnego sporządzenia analizy ryzyka, przywołując przy tym przepis pkt 6.4.2 Metodyki szacowania ryzyka naruszenia praw i wolności osób fizycznych. Ponadto w wyjaśnieniach z dnia 4 lipca 2019 r. organ kontrolowany podkreślił, iż wyniki analizy zostały ustnie zatwierdzone przez Dolnośląskiego Wojewódzkiego Konserwatora Zabytków.

[dowód: akta kontroli str. 268-273]

Odnosząc się do udzielonych wyjaśnień należy wskazać, iż metoda szacowania ryzyka zaistnienia konkretnego zagrożenia jest jednym z wielu etapów szacowania ryzyka naruszenia praw lub wolności osoby, której dane dotyczą. Końcowym etapem jest stworzenie listy operacji przetwarzania danych osobowych (m.in. zidentyfikowanych w Rejestrze Czynności Przewarzania danych osobowych) i oszacowanie ryzyka naruszenia praw i wolności osoby, której dane dotyczą w każdej zidentyfikowanej operacji przetwarzania, a nie jedynie i wyłącznie oszacowanie ryzyka zaistnienia danego zidentyfikowanego zagrożenia.

Odnosząc się do braku obowiązku pisemnego sporządzenia analizy ryzyka naruszenia praw i wolności osoby (w tym również do faktu ustnego zatwierdzenia wyników przez organ kontrolowany) należy wskazać, iż przepis 1.4. *Metodyki szacowania ryzyka naruszenia praw i wolności osób fizycznych* faktycznie wskazuje jedynie, iż wynik analizy ma zatwierdzić kierownik jednostki organizacyjnej, po uprzednim zaparafowaniu wyniku przez administratora technicznego, administratora merytorycznego i administratora bezpieczeństwa informacji (inspektora ochrony danych osobowych). Powyższy przepis rzeczywiście nie

[10] Stworzenie listy operacji przetwarzania danych osobowych z przyporządkowanymi każdej operacji poziomami ryzyka rekomenduje także Urząd Ochrony Danych Osobowych w : Poradnik UODO Jak stosować podejście oparte na ryzyku Część II , maj 2018 , strona 24.

wskazuje, iż jedyną formę dokonania takiej analizy jest forma pisemna. Niemniej jednak taka konstrukcja przepisu nie zwalnia organu kontrolowanego z obowiązku wykazania, iż Dolnośląski Wojewódzki Konserwator Zabytków sporządził taką analizę - jak również zastosował w praktyce ustalone przez siebie procedury– tj. nie zwalnia Dolnośląskiego Wojewódzkiego Konserwatora Zabytków z obowiązku wykazania, iż wskazane w przepisie 1.4. Metodyki szacowania ryzyka naruszenia praw i wolności osób fizycznych - podmioty zaparafowały wyniki dokonanej analizy, a kierownik jednostki kontrolowanej zatwierdził wyniki sporządzonej analizy. W ocenie kontrolujących Dolnośląski Wojewódzki Konserwator Zabytków nie wywiązał się z powyżej wskazanych obowiązków, bowiem nie przedłożył kontrolującym jakiegokolwiek dokumentu (w formie pisemnej bądź elektronicznej) potwierdzającego, iż Dolnośląski Wojewódzki Konserwator Zabytków oszacował jakiekolwiek ryzyko naruszenia praw lub wolności osoby, której dane dotyczą dla każdej zidentyfikowanej operacji przetwarzania zachodzącej w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu. Podkreślenia wymaga, iż w myśl pkt 2.6. Polityki Bezpieczeństwa Informacji w Wojewódzkim Urzędzie Ochrony Zabytków we Wrocławiu inicjatorem i koordynatorem procesu szacowania ryzyka jest Inspektor Ochrony Danych.

Ponadto przepis art. 35 ust. 1 RODO nakłada na administratora obowiązek dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, przed rozpoczęciem przetwarzania, jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Analizując przepisy RODO należy stwierdzić, iż przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe, w sytuacji gdy w odniesieniu do operacji przetwarzania danych: 1) zachodzą przesłanki wskazane w art. 35 ust. 1 RODO lub 2) zachodzą przesłanki wskazane w art. 35 ust. 3 RODO, lub 3) organ nadzorczy uzna, że tego rodzaju operacje wiążą się z obowiązkiem przeprowadzenia oceny, tj. zachodzą przesłanki z art. 35 ust. 1 RODO.

Podkreślić należy, iż organ kontrolowany dwukrotnie w składanych wyjaśnieniach wskazał, iż sporządził *ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych.* Niemniej jednak nie przedstawił kontrolującym jakiegokolwiek dokumentu (w formie pisemnej bądź elektronicznej) potwierdzającego, iż taka ocena została przez organ kontrolowany sporządzona [dowód: wyjaśnienia z dnia 6 czerwca oraz 8 sierpnia 2019 r.; akta kontroli str. 5-7, 296-299].

W zakresie odnoszącym się do kwestii oceny skutków planowanych operacji przetwarzania należy wskazać, iż w wyjaśnieniach z dnia 6 czerwca 2019 r. oraz z 8 sierpnia 2019 r. organ kontrolowany wskazał jedynie, iż prowadzi taką ocenę wspólnie z szacowaniem ryzyka. Jednakże na żadnym etapie wykonywanych czynności kontrolnych organ kontrolowany nie przedstawił dokumentu (w formie pisemnej bądź elektronicznej), który mógłby być uznany za ocenę skutków planowanych operacji przetwarzania, która powinna zawierać co najmniej następujące elementy: *a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora; b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów; c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie*

niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy (art. 35 ust. 7 RODO).

W świetle powyższego należy wskazać, iż organ kontrolowany nie sporządził oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, o której mowa w art. 35 ust. 1 i 3 RODO.

Odnosząc się do dokonanych w toku kontroli ustaleń oraz biorąc pod uwagę fakt niewykazania przez organ kontrolowany poziomu ryzyka naruszenia praw lub wolności osób fizycznych przy każdej operacji przetwarzania zidentyfikowanej w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu, stwierdzono, iż kontrolowany organ nie wykazał, iż przeprowadzenie oceny skutków dla ochrony jest nieobowiązkowe, czym naruszył przepis art. 5 ust. 2 RODO.

Jak już zostało podkreślone na wstępie, w świetle przepisów RODO na administratorze ciąży obowiązek wdrożenia adekwatnych środków technicznych i organizacyjnych, których wybór pozostaje w gestii administratora. Niemniej jednak wybór danych środków powinien być poprzedzony analizą ryzyka naruszenia praw lub wolności osób fizycznych. Jak wskazuje się w piśmiennictwie, „środki te powinny być odpowiednie, przez co rozumieć należy dążenie do tego, aby środki były skuteczne, a więc pozwalały na zapobieganie naruszeniom ochrony danych lub ograniczenie do minimum ryzyka ich wystąpienia, mając na względzie fakt, iż całkowite wyeliminowanie ryzyka może nie być realne" (P. Fajgielski, Komentarz do art. 32 [w:] red. P. Fajgielski, Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz. Wolters Kluwer Polska, 2018)[11].

Podkreślenia wymaga, iż skutkiem tego, iż sporządzona analiza ryzyka nie umożliwia odniesienia jej wyników do procesów przetwarzania danych (m.in. zidentyfikowanych w rejestrze czynności przetwarzania) może być brak możliwości potwierdzenia (np. przez organ nadzorczy), iż Dolnośląski Wojewódzki Konserwator Zabytków wdrożył odpowiednie środki techniczne i organizacyjne, aby przetwarzanie danych osobowych w WUOZ odbywało się zgodnie z rozporządzeniem RODO i niemożliwość wykazania działania zgodnego z RODO (art. 24 ust.1 w zw. z art. 5 ust. 2 RODO)[12].

Obszar G - Naruszenie ochrony danych osobowych (np. przez organ nadzorczy),

Kontrola wykazała, iż w kontrolowanej jednostce obowiązuje *Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych* (Zał. Nr 16 do Polityki Bezpieczeństwa Informacji w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu), w której ujęto: *osoby zobowiązane do ochrony danych osobowych, obowiązki osób zobowiązanych do ochrony danych osobowych w sytuacji naruszenia ochrony danych osobowych* [dowód: akta kontroli str. 121-123]. Czynności kontrolne wykazały, iż organ kontrolowany w drodze załącznika Nr 1 do Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych określił wzór *Rejestru naruszeń ochrony danych osobowych w Wojewódzkim Urzędzie Ochronie Zabytków we Wrocławiu*, a w drodze Zał. Nr 2 do ww. *Instrukcji* został określony *Wzór zgłoszenia naruszenia ochrony danych osobowych do właściwego organu nadzorczego*

[11] Stanowisko Prezesa Urzędu Ochrony Danych Osobowych ZSPU wyrażone w decyzji z dnia 18 października 2019 r. ZSPU.421.3.2019.

[12] Jw.

[dowód: akta kontroli str. 124-125]. Kontrola wykazała, iż określony wzór zgłoszenia zawiera rubryki odnoszące się do elementów zgłoszenia o których mowa w art. 33 ust. 3 RODO.

Z udzielonych przez organ kontrolowany wyjaśnień wynika, iż jednostka kontrolowana od dnia 25 maja 2018 r. nie odnotowała przypadków naruszeń ochrony danych osobowych [dowód: wyjaśnienia z dnia 6 czerwca 2019 r.; akta kontroli str. 5-7].

Wobec powyższego brak było możliwości oceny, czy prowadzony rejestr naruszeń ochrony danych dokumentuje wszystkie przypadki zgłoszeń, w tym te, które nie podlegają obowiązkowi przekazania do Prezesa Urzędu Ochrony Danych Osobowych oraz sposób postępowania z poszczególnymi zgłoszeniami.

Mając na względzie fakt podjęcia przez organ kontrolowany działań naprawczych w zakresie zapisów Rejestru Czynności Przetwarzania Danych Osobowych oraz podjęcie działań eliminujących nieprawidłowości stwierdzone w okresie objętym kontrolą, odstępuję od formułowania wniosków pokontrolnych:

- odnoszących się do zapisów (w tym rejestrowania czynności przetwarzania danych osobowych) prowadzonego *Rejestru Czynności Przetwarzania Danych Osobowych* oraz jego obligatoryjnych elementów, o których mowa w art. 30 ust. 1 RODO;

- w zakresie wyznaczania na inspektora ochrony danych osoby posiadającej kwalifikacje zawodowe, a w szczególności fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych osobowych oraz umiejętności wypełniania zadań określonych w art. 39 RODO;

- w zakresie spełnienia wymogu podlegania inspektora ochrony danych najwyższemu kierownictwu oraz zapewnienia aby w przypadku gdy IOD wykonuje inne zadania i obowiązki, nie powodowały one konfliktu interesów.

W celu dalszego usprawnienia funkcjonowania systemu ochrony danych osobowych należy:

1. Zapewnić aby postanowienia Polityki Ochrony Danych oraz zmiany jej postanowień następowały w formie aktu wewnętrznego, stosownie do przyjętych wewnętrznie zasad, w sposób umożliwiający udokumentowanie daty ich wprowadzenia;
2. Dokonać pogłębionej analizy relacji łączącej DWKZ z innymi podmiotami, celem weryfikacji czy występują procesy przetwarzania danych osobowych, które mają więcej niż jednego administratora, a przypadku zidentyfikowania relacji współadministrowania, wykazania działań zgodnych z RODO;
3. Zapewnić realizację obowiązku informacyjnego określonego w art. 13 ust. 1 i 2 RODO podczas pozyskiwania danych osobowych dla wszystkich procesów/operacji przetwarzania danych osobowych oraz zwiększyć nadzór nad realizacją oraz stosowaniem klauzul informacyjnych;
4. W przypadku pozyskania danych osobowych nie od osoby, której dane dotyczą, realizując obowiązek informacyjny podawać osobie, której dane dotyczą wszystkie informacje wymagane art. 14 ust. 1 i 2 RODO;

5. Zapewnić, aby zawarte przez organ kontrolowany umowy powierzenia przetwarzania danych osobowych zawierały wszystkie elementy wymagane w art. 28 ust. 3 RODO, w tym określenie rodzaju danych osobowych, kategorii osób, których dane dotyczą i charakteru przetwarzania;
6. Zidentyfikować relację łączącą DWKZ z usługodawcą hostingu strony BIP WUOZ, celem potwierdzenia działań zgodnych z wymogami RODO lub konieczności ich weryfikacji;
7. Zapewnić aby w jednostce w sposób ciągły (bez przerw) wyznaczona była osoba realizująca zadania inspektora ochrony danych, celem wypełnienia obowiązku wynikającego z art. 37 ust. 1 lit. a RODO;
8. Zawiadamiając Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu inspektora ochrony danych, zachowywać 14-dniowy termin liczony od dnia wyznaczenia inspektora oraz zapewnić aby zawiadomienie zawierało wszystkie elementy określone w art. 10 ust. 1 i 3 UODO;
9. Zapewnić, aby niezwłocznie po wyznaczeniu inspektora ochrony danych, na stronie internetowej Urzędu udostępniane były dane inspektora dotyczące imienia, nazwiska oraz adresu poczty elektronicznej lub numeru telefonu, zgodnie z obowiązkiem określonym w art. 11 UODO;
10. Zagwarantować, aby zapisy rejestru odzwierciedlały aktualne (a nie przewidywane) procesy przetwarzania danych osobowych;
11. Zapewnić jednolitość w stosowanych podstawach prawnych przetwarzania danych osobowych wynikających z zapisów prowadzonego *Rejestru Czynności Przetwarzania Danych Osobowych* oraz tych wskazywanych w ogłoszeniu o naborze do korpusu służby cywilnej;
12. *Rejestr Wszystkich Kategorii Czynności Przetwarzania*, o którym mowa w art. 30 ust. 2 RODO, prowadzić tylko w przypadku zaistnienia relacji, w której DWKZ – w imieniu innego administratora danych – występuje jako podmiot przetwarzający;
13. Zapewnić, aby analiza ryzyka zawierała listę operacji przetwarzania danych osobowych z przyporządkowanymi każdej operacji poziomami ryzyka, zgodnie z wytycznymi Urzędu Ochrony Danych Osobowych.

Na podstawie art. 49 ustawy o kontroli w administracji rządowej wnoszę o poinformowanie o sposobie wykonania zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań, w terminie do dnia **28 lutego 2020 r.**

WOJEWODA DOLNOŚLĄSKI

Jarosław Obremski