Olsztyn, dnia 24.04.2026r.

R A P O R T

z czynności audytowych zrealizowanych przez Inspektora Ochrony Danych w zakresie wypełniania przez Administratora obowiązków oraz zasad przetwarzania danych osobowych określonych w przepisach RODO oraz przepisach prawa krajowego

W dniu 23 kwietnia 2026 roku Maciej Żołnowski realizując zadania Inspektora Ochrony Danych Osobowych określone w art. 39 ust. 1 lit a) i b) Rozporządzenia Parlamentu Europejskiego z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z 24 października 1995 (RODO) - z udziałem osób działających w imieniu Administratora - wykonał w siedzibie Administratora Danych Osobowych tj. Szkoła Podstawowa im. Olimpijczyków Polskich w Kiwitach - niżej wymienione czynności audytowe:

1/ weryfikacja aktualności oraz adekwatności wdrożonego przez Administratora Rejestru czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 RODO;

2/ identyfikacja obszarów przetwarzania danych osobowych dokonywanych w imieniu innego administratora w na podstawie instrumentów, o których mowa w art. 28 ust. 3 RODO, a w przypadku ujawnienia obszarów przetwarzania danych osobowych dokonywanych w imieniu innego administratora aktualizacja Rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, o którym mowa w art. 30 ust. 2 RODO;

3/ weryfikacja wypełniania przez Administratora obowiązków określonych w art. 11 ustawy z dnia 10 maja 2018r. o ochronie danych osobowych w zakresie udostępnienia danych Inspektora Ochrony Danych;

4/ weryfikacja realizacji przez Administratora zasad przetwarzania danych osobowych określonych w art. 5 ust. 1 lit. c) – e) RODO;

5/ weryfikacja w zakresie poprawności realizacji przez Administratora podstaw dopuszczalności przetwarzania danych osobowych określonych w art. 6 ust. 1 lit. a);

6/ weryfikacja w zakresie poprawności realizacji przez Administratora podstaw dopuszczalności przetwarzania danych osobowych określonych w art. 9 ust. 1 i ust. 2 lit. a) – b) RODO;

7/ weryfikacja realizacji przez Administratora sposobu wypełniania obowiązku informacyjnego, o którym mowa w art. 13 ust. 1 i 2 RODO;

8/ przegląd Polityki Ochrony Danych Osobowych w zakresie aktualności stanu faktycznego oraz prawnego;

9/ dodatkowe ustalenia w zakresie przetwarzania przez Administratora danych osobowych m.in.:

- na podstawie przesłanek określonych w art. 6 ust. 1 lit a) – f) RODO lub art. 9 ust. 2 lit a) – j) RODO;
- zgodnie z zasadami dotyczącymi przetwarzania danych osobowych opisanymi w art. 5 ust. 1 lit a) – f) oraz ust. 2 RODO;

- na podstawie uregulowań zawartych w przepisach prawa krajowego w zakresie bezpieczeństwa przetwarzania danych osobowych;

10/ weryfikacja realizacji rekomendacji wskazanych w dokumentacji z czynności zrealizowanych w jednostce przez Inspektora Ochrony Danych Osobowych w dniu 21 stycznia 2025 roku w zakresie wypełniania przez Administratora obowiązków określonych w przepisach dotyczących ochrony danych osobowych w tym środków technicznych i organizacyjnych stosowanych w jednostce w procesie przetwarzania danych osobowych;

W toku czynności służbowych przeprowadzonych w jednostce przez Inspektora Ochrony Danych Osobowych - z udziałem Dyrektor Jednostki - dokonano niżej wskazanych ustaleń:

1/ Ustalono, że na podstawie zarządzenia nr 4 z dnia 01.04.2020r. Administrator dokonał aktualizacji Rejestru czynności przetwarzania danych osobowych, który wdrożony został w jednostce dnia 04.10.2018 roku.

W toku czynności Inspektor Ochrony Danych Osobowych wspólnie z osobą działającą w imieniu Administratora dokonał weryfikacji Rejestru czynności przetwarzania w zakresie zidentyfikowania procesów przetwarzania danych osobowych realizowanych w Jednostce. W toku czynności ustalono, że rejestr wymaga aktualizacji rejestru w niżej wskazanym zakresie:

- Wystawianie oraz odbieranie faktur oraz dostęp do danych osobowych w ramach Krajowego Systemu e-Faktur;
- Import faktur do systemów wewnętrznych w związku z funkcjonowaniem Krajowego Systemu e-Faktur;
- Zarządzanie uprawnieniami w ramach Krajowego Systemu e-Faktur;

W toku czynności przekazano stosowne rekomendacje w przedmiotowym zakresie.

2/ W toku czynności ustalono, że jednostka występuje jako podmiot przetwarzający dane osobowe w imieniu innego administratora na podstawie art. 30 ust. 2 RODO.

W związku z powyższym ustalono, że w Jednostce na podstawie zarządzenia nr 3a/2022 z dnia 11.03.2022r. wdrożono rejestr kategorii czynności przetwarzania danych w imieniu innego administratora, zawierający informacje, o których mowa w art. 30 ust. 2 RODO tj.:

- nazwa każdego administratora, w imieniu którego działa podmiot przetwarzający oraz inspektora ochrony danych;
- kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
- przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej;
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa;

W toku czynności ustalono, że wdrożony w Jednostce rejestr zawiera wszystkie procesy przetwarzania danych osobowych realizowane w imieniu innych administratorów i nie wymaga aktualizacji w przedmiotowym zakresie.

3/ W toku czynności ustalono, że Administrator nie wypełnił - określonego w art. 11 Ustawy o ochronie danych osobowych z dnia 10 maja 2018 roku - obowiązku udostępnienia danych Inspektora Ochrony Danych w postaci imienia, nazwiska oraz adresu poczty elektronicznej. W toku czynności wskazano, że stosownie do treści wyżej wskazanego przepisu "podmiot, który wyznaczył inspektora, udostępnia dane inspektora (...), niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności". Wskazano, że w przypadku podmiotów publicznych właściwym miejscem publikacji tego rodzaju informacji wydaje się strona podmiotowa Biuletynu Informacji Publicznej. W związku z powyższym przekazano stosowne rekomendacje w zakresie wypełnienia przez Administratora

obowiązku określonego w art. 11 Ustawy o ochronie danych osobowych z dnia 10 maja 2018 roku.

4/ W toku czynności wskazano, że w kontekście realizacji przez Administratora zasady określonej w art. 5 ust. 1 lit c) RODO w świetle stanowiska praktyki z zakresu ochrony danych osobowych zgodnie z treścią wskazane przepisu przetwarzane dane powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"). Wskazano, że w świetle stanowiska praktyki z zakresu ochrony danych osobowych adekwatność i stosowność rozumieć można jako konieczność zachowania odpowiednich proporcji zakresu danych do celów przetwarzania i przetwarzanie tylko takich danych, które są potrzebne dla realizacji określonych celów. Dalsza część przepisu zawiera wymóg, aby dane były ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Wymóg niezbędności należy odczytywać łącznie z wymogiem adekwatności i stosowności, co powinno pozwolić na uwzględnienie okoliczności i dopuszczenie przetwarzania danych, które w istotny sposób mogą pomóc osiągnąć cele przetwarzania. Zgodnie ze stanowiskiem doktryny *(m.in. Ogólne rozporządzenie o ochronie danych osobowych, Ustawa o ochronie danych osobowych – Komentarz, Paweł Fajgielski, wydanie 2, Wolters Kluwer, Warszawa 2022)* w praktyce często zdarza się, że cel można osiągnąć łatwiej, szybciej i taniej, wykorzystując dane, bez których osiągnięcie podstawowego celu jest możliwe. Przyjęcie restrykcyjnej wykładni uniemożliwiałoby przetwarzanie jakichkolwiek innych danych niż tylko te, bez których cel nie może zostać osiągnięty. Przykładem może być zakres danych wykorzystywanych do kontaktów z określoną osobą; mając adres pocztowy, można się z tą osobą skontaktować, jednak trwa to zwykle długo, wymaga większego nakładu pracy i dodatkowych kosztów, natomiast mając numer telefonu lub adres e-mail, można się z tą osobą skontaktować znacznie szybciej, łatwiej i taniej. Przyjęcie, że niezbędny jest jedynie adres tradycyjny, uniemożliwiałoby przetwarzanie pozostałych danych, które jednak – zależnie od okoliczności faktycznych – uznać można za adekwatne i stosowne do celu przetwarzania. Wskazano, że zgodnie z poglądami praktyki adekwatność zakłada istnienie pewnego procesu wartościującego i oceniającego, opartego na niezbyt ścisłych kryteriach. Decyzje, jakie w tej mierze podejmuje administrator, podlegać będą w razie sporu kontroli sądowej oraz – w granicach kompetencji przyznanych ustawą – kontroli organu nadzorczego. Niekiedy oceny adekwatności dokonuje prawodawca, wskazując w treści przepisu zakres danych, jakie mogą być przetwarzane dla realizacji określonego przepisami celu przetwarzania, co zasadniczo zwalnia administratora danych z obowiązku samodzielnego dokonywania tego rodzaju oceny i rozstrzygania, czy wskazany przez prawodawcę zakres danych jest adekwatny w stosunku do celów przetwarzania.

W toku czynności wskazano, że zgodnie ze stanowiskiem doktryny *(m.in. Ogólne rozporządzenie o ochronie danych osobowych, Ustawa o ochronie danych osobowych – Komentarz, Paweł Fajgielski, wydanie 2, Wolters Kluwer, Warszawa 2022)* zasada prawidłowości danych określona w ust. 1 lit. d) RODO (określana również mianem prawdziwości danych, merytorycznej poprawności danych bądź zgodności danych z prawdą) wymaga, aby dane osobowe były „prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane". W świetle stanowiska doktryny dbałość o jakość przetwarzanych danych służyć ma ochronie osób, których dane dotyczą. Przetwarzanie danych nieaktualnych, błędnych czy też w inny sposób nieprawidłowych może pociągać za sobą negatywne konsekwencje dla osób, których dane dotyczą, a także dla podmiotów, które te dane przetwarzają, dlatego prawodawca unijny uznaje za kwestię zasadniczą wymóg zapewnienia, aby przetwarzane dane były prawidłowe, tzn. zgodne ze stanem faktycznym, aktualne i nie zawierały błędów. Zasada prawidłowości danych nie powinna być jednak interpretowana jako nałożony na administratora obowiązek systematycznego poszukiwania danych nieprawidłowych. W praktyce takie podejście byłoby niezwykle trudne do realizacji, nie tylko ze względu na ilość przetwarzanych danych, ale także na problemy dotyczące weryfikacji ich poprawności. Dlatego też komentowany przepis rozporządzenia nakłada na administratora obowiązek

uaktualnienia danych „w razie potrzeby". Oznacza to, że administrator powinien reagować na sygnały dotyczące nieprawidłowości, nie ma jednak obowiązku ciągłego przeglądania zasobów swoich baz danych w celu wyszukiwania danych nieprawidłowych. Wskazany przepis nakazuje podjęcie „wszelkich rozsądnych działań", aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. Dokonanie oceny w tym zakresie pozostawiono administratorowi, jednak w razie rozbieżności między administratorem a podmiotem danych (osoby, których dane dotyczą) spory w tym zakresie rozstrzygał będzie organ nadzorczy i sąd administracyjny. Szczegółowe kwestie dotyczące realizacji zasady prawidłowości danych uregulowane są w art. 16 RODO, w którym określono uprawnienie podmiotu danych do żądania od administratora sprostowania lub uzupełnienia danych, oraz w art. 17 RODO, który reguluje kwestie prawa żądania usunięcia danych, natomiast art. 18 RODO przyznaje osobie, której dane dotyczą, prawo do żądania ograniczenia przetwarzania danych.

W toku czynności wskazano, że w kontekście realizacji przez Administratora zasady określonej w art. 5 ust. 1 lit e) RODO w świetle stanowiska doktryny z zakresu ochrony danych osobowych *(m.in. Ogólne rozporządzenie o ochronie danych osobowych, Ustawa o ochronie danych osobowych – Komentarz, Paweł Fajgielski, wydanie 2, Wolters Kluwer, Warszawa 2022)* dane osobowe powinny być „przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane". Oznacza to, że po osiągnięciu celów przetwarzania dane powinny zostać usunięte albo zanonimizowane. W motywie 39 preambuły stwierdzono, że „aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu". Wskazano, że przepisy RODO przewidują obowiązki dotyczące określenia terminów usuwania danych oraz informowania o tym osób, których dane podlegają przetwarzaniu. Dane mogą być przechowywane przez czas nieograniczony po dokonaniu ich anonimizacji, a więc po przekształceniu ich do postaci, która nie pozwala na identyfikację osób, których dane dotyczyły. W ocenie doktryny wymogu tego nie można uznać za spełniony w przypadku ograniczenia identyfikacji poprzez oddzielenie informacji identyfikujących osoby od pozostałych informacji i przechowywania danych identyfikacyjnych oddzielnie (pseudonimizacja). W odniesieniu do niektórych procesów przetwarzania danych przepisy prawa wyraźnie wskazują okresy przechowywania danych. Na przykład przepisy archiwalne przez długi czas przewidywały 50-letni okres przechowywania dokumentacji osobowej pracowników, jednak przepisy te zostały zmienione i okresy te zasadniczo zostały skrócone do lat 10 (zmiany weszły w życie 1.01.2019 r. – zob. ustawę z 10.01.2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją, Dz.U. poz. 357). Jednak w wielu przypadkach brak normatywnego rozstrzygnięcia tej kwestii i administratorowi danych pozostawiono ocenę, czy cele zostały osiągnięte, czy też nie i czy dane są mu nadal potrzebne, jednak jak wskazuje praktyka w rzeczywistości dokonanie tego rodzaju oceny może nie być łatwe. Wskazano, że w art. 5 ust. 1 lit e) RODO przewidziano również odstępstwa od omówionej powyżej zasady ograniczenia przechowywania. Dalsza część art. 5 ust. 1 lit. e) RODO stanowi, że dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych, badań naukowych lub historycznych lub statystycznych, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą. Prawodawca unijny wyszedł z założenia, że realizacja interesu publicznego oraz specyfika przetwarzania danych w przypadku działalności archiwalnej, naukowej, historycznej oraz statystycznej uzasadnia potrzebę wprowadzenia wyjątku od zasady ograniczenia przechowywania danych.

5/ W toku czynności w kontekście określonych w przepisie art. 6 ust. 1 lit a) RODO podstaw legalności przetwarzania danych w kontekście stanowiska doktryny zgoda osoby, której dane dotyczą, na przetwarzanie danych stanowi jedną z przesłanek dopuszczalności przetwarzania danych osobowych.

Zgodnie ze stanowiskiem przedstawionym w komentarzu „Ogólne rozporządzenie o ochronie danych osobowych, Ustawa o ochronie danych osobowych – Komentarz, Paweł Fajgielski, wydanie 2, Wolters Kluwer, Warszawa 2022" wskazany przepis *„precyzuje, że zgoda może być wyrażona w jednym lub większej liczbie określonych celów przetwarzania. Zamieszczenie przez prawodawcę unijnego zgody jako pierwszej wśród podstaw dopuszczalności przetwarzania może być odczytywane jako uznanie istotnego znaczenia tej przesłanki i szczególnej jej roli wśród wszystkich podstaw dopuszczalności przetwarzania. Oparcie przetwarzania danych na podstawie zgody pozwala uwzględnić wolę osoby, której dane dotyczą, i jest jednym z przejawów realizacji prawa do ochrony danych osobowych, na które składa się uprawnienie podmiotu danych do decydowania o sposobie i zakresie przetwarzania danych. Pojęcie zgody osoby, której dane dotyczą, zostało zdefiniowane w art. 4 pkt 11 komentowanego rozporządzenia i oznacza „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". Osoba, która wyraża zgodę, powinna mieć zapewnioną swobodę jej wyrażenia (albo odmowy jej wyrażenia). Oświadczenie dotyczące zgody powinno jasno wskazywać cel i zakres przetwarzania oraz podmiot, którego dotyczy. Osoba składająca oświadczenie powinna być poinformowana, a jej działanie powinno w sposób niebudzący wątpliwości wskazywać na udzielenie zgody, przy czym nie jest tu wymagana określona forma prawna, a oświadczenie może być – co do zasady – złożone per facta concludentia, (...). Zgoda może być wyrażona na przetwarzanie danych w jednym lub wielu celach, przy czym każdy z celów powinien być wyraźnie oznaczony, a oświadczenie powinno być tak skonstruowane, aby pozwalało osobie, której dane dotyczą, wyrazić zgodę na wybrane cele przetwarzania. Łączenie różnych celów przetwarzania w jednym oświadczeniu bez możliwości wskazania celów, na które osoba wyraża zgodę, może prowadzić do swoistego wymuszania zgody, a zgodność z prawem takiego oświadczenia może być kwestionowana".* Wskazano, że jak wynika ze stanowiska doktryny (m.in. „Ogólne rozporządzenie o ochronie danych osobowych, Ustawa o ochronie danych osobowych – Komentarz, Paweł Fajgielski, wydanie 2, Wolters Kluwer, Warszawa 2022") nie ma przeszkód, aby zgoda miała charakter warunkowy co oznaczam że jej skuteczność będzie zależeć od ziszczenia się warunku tzn., że będzie ona legalizowała zbieranie lub inną formę przetwarzania danych dopiero po ziszczeniu się wskazanego warunku. Jak wynika ze stanowiska doktryny zgoda może mieć także charakter terminowy (wyrażać akceptację na przetwarzanie danych przez określony czas). Udzielona zgoda może być także ograniczona terytorialnie (np. do przetwarzania na terenie kraju), podmiotowo (z zastrzeżeniem, że zgoda została udzielona wyłącznie na przetwarzanie dokonywane przez wskazaną osobę zatrudnioną przez administratora) oraz przedmiotowo (w odniesieniu do niektórych tylko danych czy do niektórych celów przetwarzania) *(J. Barta, P. Fajgielski, R. Markiewicz, Ochrona danych osobowych..., s. 403–404).* W kontekście wskazanego na wstępie przepisu zasygnalizowano, że jedną z najważniejszych cech zgody na przetwarzanie danych osobowych jest jej dobrowolność. Jak wynika z treści motywu 43 preambuły RODO *„aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach".* W świetle stanowiska doktryny *„oznacza to, że w przypadku faktycznego braku równowagi między administratorem a podmiotem danych należy zwracać szczególną uwagę na gwarancje dobrowolności, aby nie narazić się na kwestionowanie skuteczności zgody. Nie oznacza to jednak, że zgoda nie może być wykorzystywana jako podstawa dopuszczalności przetwarzania danych przez podmioty publiczne, gdyż także w tym kontekście mogą być spełnione wymogi odnoszące się do zapewnienia swobody i dobrowolności udzielenia zgody. Przykładem dopuszczonego prawem oparcia przetwarzania danych osobowych przez podmioty publiczne (organy administracji publicznej) na omawianej podstawie prawnej jest zgoda na zamieszczenie danych osobowych (numeru telefonu i/lub adresu e-mail) w Rejestrze Danych*

Kontaktowych. W praktyce zgoda na przetwarzanie danych osobowych jest często wykorzystywana przez organy administracji publicznej także przy realizacji różnego rodzaju działań informacyjnych (np. rozsyłania newslettera). Niekiedy przepisy szczególne wskazują na zgodę jako podstawę uprawniającą administratora do udostępniania danych, np. w przypadku publikowania na stronach internetowych danych osób wnoszących petycje". (...) W motywie 43 preambuły wskazano również, że „zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna". Oznacza to, że „oświadczenie" o zgodzie na przetwarzanie danych powinno pozwalać osobie, której dane dotyczą, na odrębne decydowanie o dopuszczalności przetwarzania danych w różnych celach (np. wykorzystywanie przez administratora i udostępnianie innym podmiotom), jeżeli „w danym przypadku byłoby to stosowne", a więc należy w tym zakresie dokonać oceny indywidualnego przypadku i stosownie do okoliczności rozstrzygnąć, czy konieczne jest umożliwienie wyrażenia zgody odrębnie w odniesieniu do różnych operacji przetwarzania. Można jednak przyjąć, że co do zasady wystarczające jest odniesienie zgody do określonego celu przetwarzania, a szczegółowe odnoszenie zgody do poszczególnych operacji przetwarzania będzie wymagane w sytuacjach wyjątkowych uzasadnionych okolicznościami (np. gdy administrator zamierza udostępnić dane innym podmiotom na podstawie zgody osoby). Gdy chodzi o uzależnianie wykonania umowy od zgody, to prawodawca unijny zabrania stosowania tego rodzaju rozwiązania, gdy zgoda nie jest niezbędna do wykonania umowy. Wynika stąd, że prawodawca unijny dopuszcza taką możliwość, gdy zgoda jest niezbędna, m.in. gdy usługa jest oferowana bezpłatnie (np. usługa darmowej poczty elektronicznej), a jest finansowana z przychodów uzyskiwanych z reklam, wówczas zgoda osoby korzystającej z usługi może być uznana za niezbędną dla świadczenia usługi. Należy jednak podkreślić, że zgoda nie powinna dotyczyć danych koniecznych do zawarcia i wykonania umowy, gdyż niezbędność przetwarzania danych dla wykonania umowy stanowi odrębną (samoistną) przesłankę dopuszczalności przetwarzania danych (m.in. „Ogólne rozporządzenie o ochronie danych osobowych, Ustawa o ochronie danych osobowych – Komentarz, Paweł Fajgielski, wydanie 2, Wolters Kluwer, Warszawa 2022"). W kontekście wymienionego przepisu wskazano, że wyrażane w doktrynie wątpliwości co do rzeczywistej swobody wyrażenia zgody odnoszą się np. do sytuacji, gdy podmiotem ubiegającym się o uzyskanie zgody jest pracodawca, a zgody udziela pracownik albo kandydat na pracownika. W ocenie doktryny *„bez wątpienia pomiędzy pracodawcą a pracownikiem (a także kandydatem) istnieje brak równowagi ze względu na stosunek podporządkowania (podległości) lub ubiegania się o zatrudnienie, co może sprawiać, że pracownik (kandydat), obawiając się negatywnych konsekwencji, z zasady nie będzie odmawiał udzielenia zgody. Podstawową przesłanką dopuszczalności przetwarzania danych pracowniczych powinny być przepisy prawa nakładające obowiązek przetwarzania danych i rozstrzygające, w jakim zakresie dane mogą być przez pracodawcę przetwarzane. W art. 22^1 k.p. określone zostały rodzaje danych osobowych, których pracodawca żąda od osoby ubiegającej się o zatrudnienie (§ 1) oraz od pracownika (§ 2), ponadto – zgodnie z § 4 pracodawca żąda podania innych danych osobowych, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa (w tym zakresie podstawą przetwarzania danych są przepisy prawa). Zgoda osoby ubiegającej się o zatrudnienie oraz pracownika jako podstawa przetwarzania danych przez pracodawcę została unormowana w kolejnych dwóch artykułach. W myśl przepisu art. 22^1a § 1 k.p. zgoda może stanowić podstawę przetwarzania przez pracodawcę innych danych osobowych (niż wskazane w art. 22^1 k.p.) z wyjątkiem danych o karalności, natomiast w świetle brzmienia przepisu § 2 tego artykułu brak zgody lub jej wycofanie nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę. W przypadku szczególnych kategorii danych (np. danych dotyczących zdrowia) zgoda może stanowić*

podstawę przetwarzania przez pracodawcę takich danych osobowych wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika (art. 22[1]b § 1 k.p.)". Wskazano, że w ocenie doktryny „*jedną z ważkich kwestii odnoszących się do zgody na przetwarzanie danych jest problem dopuszczalności łączenia zgody na przetwarzanie danych z innymi oświadczeniami o zgodzie (na przesyłanie informacji handlowej bądź na wykorzystywanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących do celów marketingu bezpośredniego) i odbierania w tym zakresie jednego oświadczenia o zgodzie na wskazane powyżej cele. Praktyka tego rodzaju nie zasługuje na aprobatę, w świetle komentowanych przepisów unijnego rozporządzenia wskazanych powyżej oświadczeń o zgodzie nie powinno się utożsamiać i łączyć ze sobą; należy zagwarantować osobie możliwość swobodnego decydowania o przetwarzaniu jej danych w każdym z tych odmiennych celów".* (m.in. „Ogólne rozporządzenie o ochronie danych osobowych, Ustawa o ochronie danych osobowych – Komentarz, Paweł Fajgielski, wydanie 2, Wolters Kluwer, Warszawa 2022"). Wskazano, że w ocenie doktryny „*W praktyce istotny problem stanowi odbieranie zgody na zapas, w sytuacji gdy istnieje inna podstawa dopuszczalności przetwarzania danych (np. przepis prawa nakładający na administratora obowiązek przetwarzania danych bądź przetwarzanie danych jest niezbędne do zawarcia i wykonania umowy). Praktyka tego rodzaju nie zasługuje na uznanie, gdyż może prowadzić do różnego rodzaju wątpliwości i problemów. Jednym z nich jest tworzenie mylnego wyobrażenia u osoby, która wyraża zgodę na przetwarzanie, że osoba ta decyduje o dopuszczalności przetwarzania danych, podczas gdy dopuszczalność przetwarzania może wynikać z innych podstaw (np. przepisu prawa), a osoba, której dane dotyczą, faktycznie pozbawiona jest możliwości decydowania o dopuszczalności przetwarzania danych. Kolejnym problemem w omawianej tu sytuacji może być odwołanie (wycofanie) zgody – osoba, która skorzysta z tego uprawnienia, będzie przekonana, że administrator powinien zaprzestać przetwarzania jej danych, choć faktycznie może być inaczej, jeżeli administrator legitymuje się inną przesłanką dopuszczalności, to dane mogą być nadal przetwarzane, mimo odwołania zgody.* (m.in. „Ogólne rozporządzenie o ochronie danych osobowych, Ustawa o ochronie danych osobowych – Komentarz, Paweł Fajgielski, wydanie 2, Wolters Kluwer, Warszawa 2022").

6/ W odniesieniu do zgody na przetwarzanie szczególnych kategorii danych pozostają aktualne w większości także ustalenia odnoszące się do zgody jako przesłanki dopuszczalności przetwarzania tzw. danych zwykłych, o której mowa w art. 6 ust. 1 lit. a) RODO.

Druga z podstaw dopuszczalności przetwarzania szczególnych kategorii danych została wskazana w art. 6 ust. 2 lit. b) i obejmuje sytuacje, gdy „przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą". Omawiana przesłanka wskazana w unijnym rozporządzeniu uprawnia administratora do przetwarzania danych ze względu na konieczność wypełniania obowiązków i wykonywania uprawnień przez administratora lub podmiot danych, do realizacji których niezbędne jest przetwarzanie danych. Jednak zakres przedmiotowy omawianej przesłanki został ograniczony do trzech dziedzin: 1) prawa pracy, 2) zabezpieczenia społecznego oraz 3) ochrony socjalnej. Jako przykłady przetwarzania danych w oparciu o tę podstawę wskazać można: przetwarzanie przez pracodawcę danych dotyczących chorób zawodowych pracownika; przetwarzanie danych o zdrowiu członków rodziny pracownika na potrzeby przyznania świadczeń socjalnych czy też przetwarzanie danych na potrzeby odprowadzania składek na ubezpieczenie społeczne.

7/ W toku czynności przekazano rekomendacje dotyczące realizacji obowiązku informacyjnego na podstawie art. 6 ust. 1 lit b) RODO gdy, przetwarzanie danych osobowych niezbędne jest do

wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. W związku z powyższym wskazano, że zgodnie ze stanowiskiem doktryny zakres danych, jakie są wymagane, zależy od charakteru umowy, rodzaju świadczenia lub innych okoliczności istotnych z punktu widzenia celu przetwarzania danych. Niekiedy wystarczające są podstawowe informacje identyfikujące osobę, której dane dotyczą, i wskazujące adres jej zamieszkania (konieczne np. do wystawienia faktury), w innych przypadkach zakres danych potrzebnych do wykonania umowy może być szerszy i obejmować różnorodne dane osobowe. Istotne jest jednak, aby zakres danych był adekwatny do celu przetwarzania oraz nie były gromadzone dane zbędne z punktu widzenia realizacji tego celu, zgodnie z zasadą adekwatności i minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c) RODO. *(m.in. Ogólne rozporządzenie o ochronie danych osobowych, Ustawa o ochronie danych osobowych – Komentarz, Paweł Fajgielski, wydanie 2, Wolters Kluwer, Warszawa 2022).* Omawiana przesłanka wyznacza cel przetwarzania danych, który determinuje zakres przetwarzania. Cel przetwarzania, jakim jest wykonanie umowy, obejmuje działania zmierzające do zawarcia umowy, realizację wzajemnych zobowiązań stron umowy oraz dochodzenie roszczeń z tytułu niewykonania bądź nienależytego wykonania umowy. Od tego celu należy odróżnić inne cele, które nie mieszczą się w zakresie wskazanym w omawianej tu podstawie. Jak wynika ze stanowiska doktryny zgodnie z dalszą częścią przepisu art. 6 ust. 1 lit b) RODO przetwarzanie danych jest zgodne z prawem w przypadku podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Oznacza, to że prawodawca unijny dopuszcza przetwarzanie danych osobowych, mające na celu przygotowanie do zawarcia umowy, jednak warunkiem dopuszczalności tego rodzaju działań jest inicjatywa ze strony osoby, której dane dotyczą. Jeżeli podmiot danych wyrazi wobec administratora chęć zawarcia umowy, to przetwarzane danych może opierać się na omawianej tu podstawie, natomiast przesłanka ta nie ma zastosowania w sytuacji, gdy inicjatorem działań zmierzających do zawarcia umowy jest administrator danych (przed rozpoczęciem przetwarzania danych powinien on uzyskać zgodę osoby, której dane dotyczą, na tego rodzaju działania bądź oprzeć je na innej podstawie – tzw. klauzuli prawnie uzasadnionych interesów, uregulowanej w art. 6 ust. 1 lit. f RODO). Przetwarzanie danych osobowych może być również niezbędne na wczesnym etapie zawierania umowy – w ramach różnego rodzaju procedur zmierzających do zawarcia umowy (np. procedury przetargowej), w fazie zawierania umowy przedwstępnej lub umowy ramowej. W tych przypadkach wykorzystywanie omawianej podstawy dopuszczalności przetwarzania należy uznać za zasadne. Zakres danych koniecznych do zawarcia i wykonania umowy może być różny, w zależności od tego, co jest przedmiotem umowy, i innych okoliczności jej zawarcia i wykonania. W tym zakresie można przytoczyć pogląd zaprezentowany przez NSA w jednym z orzeczeń, który zachowuje swoją aktualność mimo zmiany stanu prawnego. W wyroku z 19.12.2001 r. (II SA 2869/00, ONSA 2003/1). Sąd stwierdził, że zakres danych osobowych przetwarzanych w związku z koniecznością wywiązania się z umowy powinien być zróżnicowany w zależności od charakteru i znaczenia umowy; w wypadku umów o istotnym znaczeniu gospodarczym lub społecznym bezpieczeństwo obrotu prawnego wymaga dokładnej identyfikacji stron zawierających umowę i może uzasadniać gromadzenie przez nie danych osobowych w zakresie gwarantującym należyte wywiązanie się ze zobowiązania. W obecnym stanie prawnym zasadne jest m.in. pozyskiwanie przy zawieraniu umowy numeru PESEL kontrahenta ze względu na możliwość ewentualnego dochodzenia roszczeń w postępowaniu uproszczonym – elektronicznym postępowaniu upominawczym, z wykorzystaniem tzw. elektronicznego sądu (przez Internet), gdyż przepisy Kodeksu postępowania cywilnego uniemożliwiają wniesienie powództwa w tym postępowaniu bez wskazania przez wierzyciela numeru PESEL dłużnika.

8/ W toku czynności ustalono, że wdrożona w Jednostce na podstawie zarządzenia nr 13/2025 z dnia 05.09.2025r. Polityka ochrony danych osobowych zawiera ujęte w jej treści rekomendacje oraz wytyczne Urzędu Ochrony Danych Osobowych w zakresie odnoszącym się realizacji określonych w

przepisach RODO zasad przetwarzania danych osobowych oraz obowiązków administratora danych osobowych w kwestii m.in.:

- zasad kwalifikacji incydentów związanych z ochroną danych oraz sposobów postępowania w przypadku naruszenia ochrony danych osobowych;
- sposobu wypełniania przez Inspektora Ochrony Danych w zakresie procesów związanych z obsługą naruszeń danych osobowych.

W toku czynności ustalono, że wdrożona w Jednostce Polityka ochrony danych osobowych wymaga aktualizacji w zakresie ujęcia w treści dokumentacji rekomendacji oraz wytycznych Urzędu Ochrony Danych Osobowych w zakresie odnoszącym się realizacji określonych w przepisach RODO zasad przetwarzania danych osobowych oraz obowiązków administratora danych osobowych w kwestii:

- retencji danych osobowych przetwarzanych za pośrednictwem poczty elektronicznej;

W toku czynności przekazano stosowne rekomendacje w przedmiotowym zakresie.

9/ W toku czynności wskazano, że w zgodnie ze stanowiskiem wyrażonym w decyzji UODO nr DKN.5130.2024.2020 z dnia 11.02.2021r. „W świetle zapisów art. 28 ust. 1 i art. 28 ust. 3 lit. h) rozporządzenia 2016/679, wybór dającego gwarancję odpowiednich zabezpieczeń podmiotu przetwarzającego jest obowiązkiem administratora". Wskazano, że stosownie do informacji zawartych w Biuletynie UODO Nr 4/06/23 „Administrator, zarówno podejmując decyzję, komu powierzyć przetwarzanie danych osobowych, jak i w czasie trwania umowy powierzenia, ma prawo domagać się, aby podmiot przetwarzający udokumentował wdrożenie odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Trudno uznać, aby samo oświadczenie podmiotu przetwarzającego w tej sprawie było wystarczające dla weryfikacji przez administratora kompetencji procesora i spełniania przez niego wymogów z RODO. Ponieważ dane osobowe (stosownie do art. 5 ust. 1 lit. a i lit. f RODO) muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość") oraz w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność"), to bardzo ważne z punktu widzenia administratora jest to, jakiemu podmiotowi powierza przetwarzanie tych danych. Tym bardziej, że art. 5 ust. 2 RODO stanowi, iż to administrator ponosi odpowiedzialność za przetwarzanie danych osobowych zgodnie z tymi zasadami i musi być w stanie wykazać ich przestrzeganie („rozliczalność"). Jednocześnie przepisy RODO stanowią (art. 28), że jeżeli przetwarzanie ma być dokonywane w imieniu administratora, to korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. Wskazują jednak (art. 28 ust. 3 lit. h), że umowa lub inny instrument prawny, na podstawie którego odbywa się przetwarzanie danych przez podmiot przetwarzający, stanowią w szczególności, że podmiot przetwarzający udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. Z wytycznych EROD 7/2020 dotyczących pojęć administratora i podmiotu przetwarzającego zawartych w RODO wynika ponadto, że w czasie oceny procesora „Elementami, które należy wziąć pod uwagę, mogą być: wiedza fachowa podmiotu przetwarzającego (np. wiedza techniczna w zakresie środków bezpieczeństwa i naruszeń ochrony danych); wiarygodność podmiotu przetwarzającego; zasoby podmiotu przetwarzającego oraz stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu

postępowania lub mechanizmu certyfikacji", a także, że „Administrator jest (…) odpowiedzialny za ocenę adekwatności gwarancji udzielonych przez podmiot przetwarzający i powinien być w stanie udowodnić, że poważnie wziął pod uwagę wszystkie elementy przewidziane w RODO. Ocena administratora, czy gwarancje są wystarczające, jest formą oceny ryzyka, która w znacznym stopniu zależy od rodzaju przetwarzania powierzonego podmiotowi przetwarzającemu i musi być dokonywana indywidualnie dla każdego przypadku, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania, a także zagrożeń dla praw i wolności osób fizycznych". W tej kwestii EROD rekomenduje zapoznanie się administratora z odpowiednią dokumentacją (np. polityką prywatności, warunkami świadczenia usług, rejestrem czynności przetwarzania, polityką zarządzania dokumentacją, polityką bezpieczeństwa informacji, sprawozdaniami z zewnętrznych audytów ochrony danych, uznanych międzynarodowych certyfikatów, takich jak normy ISO 27000). Brak weryfikacji podmiotu przetwarzającego oraz jego gwarancji dla przetwarzania zgodnie z przepisami o ochronie danych osobowych może wiązać się z konsekwencjami dla osób fizycznych, których dane osobowe zostały powierzone podmiotowi przetwarzającemu, np. w postaci utraty danych osobowych. Zatem decyzja, komu administrator ma powierzyć przetwarzanie danych osobowych nie może być podejmowana bezpodstawnie. Dopiero po zbadaniu kompetencji i adekwatności wybranego podmiotu przetwarzającego, administrator może przystąpić do zawarcia stosownej umowy powierzenia. Jednocześnie trudno uznać, aby samo oświadczenie podmiotu przetwarzającego o zapewnieniu gwarancji wdrożenia i stosowania odpowiednich środków technicznych i organizacyjnych było dla administratora wystarczające do weryfikacji jego kompetencji i spełniania przez niego wymogów z RODO. Domaganie się przez administratora odpowiedniego udokumentowania określonych oświadczeń jest jednym z jego uprawnień przy dokonywaniu wyboru właściwego podmiotu, któremu zechce powierzyć dane osobowe. Co istotne, nie należy zapominać, że obowiązki administratora w zakresie zapewnienia powierzenia przetwarzania danych osobowych podmiotowi spełniającemu wymogi wskazane w art. 28 ust. 1 RODO, trwają co najmniej tak długo, jak okres powierzenia. Jak wskazano w powołanych wytycznych EROD „Obowiązek korzystania wyłącznie z usług podmiotów przetwarzających zapewniających wystarczające gwarancje zawarty w art. 28 ust. 1 RODO jest obowiązkiem ciągłym. Nie kończy się w momencie zawarcia umowy lub innego aktu prawnego przez administratora i podmiot przetwarzający. Administrator powinien raczej w odpowiednich odstępach czasu weryfikować gwarancje podmiotu przetwarzającego, w tym w stosownych przypadkach przez audyty i inspekcje".

W toku czynności przekazano sugestie w zakresie przetwarzania danych osobowych pracowników w postaci numeru ich prywatnego telefonu komórkowego, które powinno być oparte na przesłankach określonych w art. 6 ust. 1 lit a) RODO tj. zgoda osoby, której dane dotyczą. W związku z powyższym wskazano, że przepisy ustawy - Kodeks pracy nie dają podstaw do żądania od potencjalnego pracownika podania przez niego jego prywatnego numeru telefonu. Wskazano, że w polskim systemie prawnym nie istnieje bowiem żaden przepis, który zobowiązywałby osobę fizyczną do posiadania takiego środka komunikacji. Dysponowanie własnym telefonem jest w pełni dobrowolne. W świetle stanowiska praktyki pracodawca może zatem przetwarzać prywatny numer telefonu potencjalnego pracownika, tylko wówczas, kiedy ten dobrowolnie zamieści go w złożonej przez siebie aplikacji. Wskazane dane osobowe mogą być wtedy przetwarzane wyłącznie na etapie prowadzenia postępowania rekrutacyjnego i do jego celów. Na etapie zatrudniania pracownika, pracodawca, zgodnie z art. 22^1 § 1 - 3 Kodeksu pracy, jest uprawniony do żądania podania określonego spektrum danych osobowych. Powyższe oznacza, że samo zatrudnienie takiej osoby nie daje pracodawcy prawa do zobowiązania pracownika, do podania prywatnego numeru telefonu i korzystania z niego, choćby do celów kontaktu w sprawach zawodowych. W świetle stosownego stanowiska Prezesa UODO (https://uodo.gov.pl/decyzje/DS.523.2704.2022), aby pracodawca mógł przetwarzać, w celach zawodowych, prywatny numer telefonu pracownika, musi uzyskać jego zgodę. W swoim stanowisku organ wskazuje wprost, że zgoda ta powinna mieć formę

pisemną (którą, zgodnie z praktyką należy rozumieć jako pisemną, w tym elektroniczną) i określać zasady kontaktu. Zgodnie z wytycznymi UODO, taka zgoda ma być pisemna i określać zasady kontaktu. UODO wskazuje także, że *„możliwość nawiązywania przez pracodawcę kontaktów z pracownikiem po godzinach pracy powinna być ograniczona jedynie do sytuacji, w której zachodziłyby szczególne warunki uzasadniające takie działanie."* Wskazano, że zgodnie z zasadami RODO pracownik ma prawo w dowolnym momencie wycofać udzieloną zgodę, a pracodawca ma wówczas obowiązek zaprzestać przetwarzania danych wykorzystywanych na podstawie tej przesłanki.

W toku czynności przekazano rekomendacje w zakresie dotyczącym ewentualnej weryfikacji korzystania przez pracowników Jednostki z poczty elektronicznej w związku z realizacją zadań służbowych, w szczególności w zakresie odnoszącym się do poczty elektronicznej działającej w ogólnodostępnych domenach dostawców serwisów internetowych. W związki z powyższym wskazano, że korzystanie z prywatnej skrzynki pocztowej w celach służbowych nie należy do dobrych praktyk bezpieczeństwa z uwagi na liczne ryzyka, jakie niesie tego typu działanie . Wskazano, że w świetle stanowiska praktyki z zakresu bezpieczeństwa informacji komunikacja służbowa powinna odbywać się za pomocą przeznaczonej do tego skrzynki mailowej udostępnionej przez pracodawcę w dedykowanej domenie. W ocenie praktyki podstawowe zagrożenia związane z używaniem prywatnej skrzynki poczty elektronicznej do celów służbowych dotyczą m.in. niżej wskazanych kwestii:

- skrzynka prywatna (w zależności od dostawcy oraz poziomu świadczonej usługi poczty elektronicznej) może być gorzej chroniona od poczty służbowej, np. proces odzyskiwania hasła dla prywatnego konta e-mail może być wadliwie zaprojektowany i atakujący będzie mógł uzyskać do niego dostęp lub filtry antyspamowe mogą być gorszej jakości, co zwiększa ryzyko przeprowadzenia skutecznego ataku phisingowego;
- korespondencja znajdująca się na skrzynce prywatnej może nie podlegać procesom wykonywania kopii zapasowych (co stanowi ryzyko utraty danych);
- ciągłość działania organizacji może zostać przerwana co spowodowane może zostać faktem, że po odejściu pracownika z pracy, organizacja utraci dostęp do informacji, które są jej potrzebne, a które przetwarzane były za pośrednictwem poczty elektronicznej, której ten pracownik był jedynym dysponentem (m.in. brak kopii zapasowych);
- utrata poufności treści korespondencji e-mail co spowodowane jest faktem, że największe podmioty świadczące usługi hostingowe (np. gmail firmy Google) mogą uzyskiwać dostęp do korespondencji e-mail oraz załączników poprzez skanowanie ich treści, a jeżeli serwery dostawcy usługi poczty elektronicznej znajdują się w USA, zgodnie z prawem tam obowiązującym, dostęp do treści wiadomości e-mail może uzyskać również NSA (Amerykańska Agencja Bezpieczeństwa).

W związku z korzystaniem przez Administratora z poczty elektronicznej działającej w ogólnodostępnej domenie dostawcy serwisu internetowego (onet.pl) wskazano, że w świetle stanowiska praktyki z zakresu bezpieczeństwa informacji komunikacja służbowa powinna odbywać się za pomocą przeznaczonej do tego skrzynki mailowej udostępnionej przez pracodawcę w dedykowanej domenie. W ocenie praktyki podstawowe zagrożenia związane z używaniem do celów służbowych skrzynki poczty elektronicznej działającej w ogólnodostępnej domenie dotyczą m.in. niżej wskazanych kwestii:

- skrzynka w ogólnodostępnej domenie (w zależności od dostawcy oraz poziomu świadczonej usługi poczty elektronicznej) może być gorzej chroniona od poczty służbowej, np. proces odzyskiwania hasła dla prywatnego konta e-mail może być wadliwie zaprojektowany i atakujący będzie mógł uzyskać do niego dostęp lub filtry antyspamowe mogą być gorszej jakości, co zwiększa ryzyko przeprowadzenia skutecznego ataku phisingowego;
- korespondencja znajdująca się na skrzynce w ogólnodostępnej domenie może nie podlegać procesom wykonywania kopii zapasowych (co stanowi ryzyko utraty danych);
- ciągłość działania organizacji może zostać przerwana co spowodowane może zostać faktem, że po odejściu z organizacji osoby, która posiada dostęp do skrzynki sama organizacja utraci dostęp do informacji, które są jej potrzebne, a które przetwarzane były za pośrednictwem poczty elektronicznej, której ta osoba była jedynym dysponentem (m.in. brak kopii zapasowych);
- utrata poufności treści korespondencji e-mail co spowodowane jest faktem, że największe podmioty świadczące usługi hostingowe (np. gmail firmy Google) mogą uzyskiwać dostęp do korespondencji e-mail oraz załączników poprzez skanowanie ich treści, a jeżeli serwery dostawcy usługi poczty elektronicznej znajdują się w USA, zgodnie z prawem tam obowiązującym, dostęp do treści wiadomości e-mail może uzyskać również NSA (Amerykańska Agencja Bezpieczeństwa).

W powyższym kontekście wskazano, że w ocenie doktryny (poglądy przedstawicieli nauki prawa, praktyków i komentatorów, wyrażone w publikacjach naukowych, literaturze fachowej i komentarzach do przepisów prawa, orzecznictwo sądów administracyjnych) korzystanie z prywatnych skrzynek e-mail przy wykonywaniu przez pracowników zadań służbowych stanowi naruszenie podstawowych obowiązków pracowniczych. Wskazano, że w kwestii korzystania z prywatnych skrzynek poczty elektronicznej kilkakrotnie wypowiadał się Sąd Najwyższy w Polsce, który m.in. w wyroku z 2019 r. orzekł: "Transferowanie dokumentów pracodawcy z jego serwera na prywatną pocztę elektroniczną należy kwalifikować w kontekście naruszenia podstawowych obowiązków pracowniczych" (II PK 334/17)". W orzeczeniu SN zwrócił również uwagę, że może w takiej sytuacji dojść do naruszenia tajemnicy przedsiębiorstwa i tym samym narazić je na straty. Poważne naruszenie obowiązków pracowniczych może stać się powodem rozwiązania umowy o pracę z winy pracownika.

W toku czynności przekazano sugestie dotyczące dokonanej przez orzecznictwo wykładni stanowisk związanych z obecnością podmiotów publicznych w mediach społecznościowych, w szczególności w kontekście publikowania materiałów zawierających dane osobowe na portalu społecznościowym Facebook. W związku z powyższym wskazano, że Naczelny Sąd Administracyjny w wyroku z dnia 16.10.2024 r. sygn.. III OSK 4984/21 wskazał iż należy uznać, że co do zasady treści publikowane na portalach społecznościowych przez osoby fizyczne nie są objęte działaniem rozporządzenia RODO, o ile działalność ta nie ma zawodowego lub handlowego charakteru i dostęp do nich mają tylko podmioty wyselekcjonowane przez osobę udostępniającą. Innymi słowy w przypadku, gdy przetwarzanie rozciąga się choćby częściowo na przestrzeń publiczną i tym samym jest skierowane poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych, nie powinno ono być rozumiane, jako czynność o czysto "osobistym lub domowym charakterze". Takie stanowisko zaprezentowane zostało również w wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 11 grudnia 2014 r., C-212/13, na który powołał się m.in. Sąd pierwszej instancji. Wskazano, że w kolejnym wyroku o sygn. III OSK 1101/24 z 20.05.2025 r. również NSA stwierdziło iż. Ze względu na dość znaczną liczbę uczestników grupy, na to że skarżący nie był administratorem tej grupy i nie dobierał sobie osobiście jej uczestników, a jedynie do niej przystąpił, a zatem nie pozostawał w

żadnych innych relacjach z tymi osobami poza przynależnością do grupy na (...) nie sposób uznać, aby miało miejsce przetwarzanie danych o charakterze osobistym lub domowym, o którym mowa w art. 2 ust. 2. Kwestia braku osiągania dochodu w kontekście całości okoliczności tej sprawy jest całkowicie irrelewantna, tym bardziej że w praktyce osiąganie dochodu pozwala również na kwalifikację przetwarzania jako dokonywanego w ramach czynności osobistych. Publikacja danych osobowych na zamkniętych portalach społecznościowych (...) nie jest przetwarzaniem danych osobowych przez osobę fizyczną o czysto osobistym lub domowym charakterze w rozumieniu art. 2 ust. 2 lit. c RODO, jeśli osoba fizyczna publikująca dane osobowe nie jest administratorem danej społeczności, nie dobiera sobie osobiści jej uczestników, a tylko do niej przystępuje, a pozostali członkowie grupy nie dysponują uprawnieniem do złożenia wiążącego sprzeciwu w stosunku do jej wniosku o przystąpienie do danej wspólnoty. Wskazano, że przytoczone powyżej wyroki NSA wskazują iż publikując materiały lub posty, w których treści znajdować się będą dane osobowe osób trzecich należy pamiętać o zachowaniu zasad dot. przetwarzania danych osobowych czyli m.in. posiadać podstawę prawną do ich przetwarzania.
W toku czynności na podstawie przytoczonych stanowisk wskazano, że Administrator , podejmując decyzję o publikacji określonych informacji na fanpage jednostki lub prowadzonych przez przedstawicieli organów pochodzących z wyboru w serwisie społecznościowym Facebook powinien uwzględniać niżej wskazane przesłanki:

- czy dla udostępnianej informacji istnieją określone przepisami prawa miejsca publikacji;
- czy udostępniana informacja nie będzie naruszała praw i wolności osób fizycznych;
- czy po stronie podmiotu prowadzącego profil istnieje podstawę prawną, aby udostępnić określony katalog danych osobowych.

W toku czynności wskazano, że we wspomnianym sprawozdaniu z działalności PUODO zamieszczone zostało streszczenie decyzji nakładającej karę na przedszkole za wykorzystanie aplikacji – komunikatora społecznościowego- do przekazania informacji o liście kandydatów przyjętych do konkretnego oddziału przedszkolnego. Wskazano, że przedmiotem postępowania przed Prezesem UODO były nieprawidłowości w przetwarzaniu danych osobowych małoletniego na grupie internetowej w mediach społecznościowych przedszkola z oddziałami integracyjnymi, polegające na udostępnieniu listy dzieci przyjętych do grupy przedszkolnej z imieniem i nazwiskiem małoletniego z dopiskiem litery „o". W ocenie Prezesa UODO przedszkole uznawało grupę internetową jako jeden z kanałów komunikacji z rodzicami. Nie było możliwe przyjęcie, że nauczyciel, który ujawnił na grupie internetowej listę dzieci zawierającą dane małoletniego, działał jako samodzielny i niezależny administrator. Nauczyciel ujawnił listę stworzoną przez przedszkole wobec rodziców dzieci do niego przyjętych. Nie wykonywał on więc czynności o czysto prywatnym charakterze, lecz podejmował działania bezpośrednio związane ze swoją pracą na rzecz przedszkola – administratora znajdujących się na ujawnionej liście. Wobec tego to przedszkole ponosiło odpowiedzialność za ujawnienie osobom nieuprawnionym danych osobowych małoletniego znajdujących się na liście. Pomimo wskazania przez przedszkole sposobu, w jaki dokonywano weryfikacji osób mających dostęp do zamkniętej grupy internetowej, przedszkole nie wykazało żadnej podstawy prawnej ujawnienia w takiej formie danych osobowych dzieci przyjętych do przedszkola. Art. 158 ustawy prawo oświatowe, która w dniu udostępnienia listy, tj. 5 lipca 2022 r. obowiązywała w wersji od 4 czerwca do 12 sierpnia 2022 r. 76 przewidywał, że wyniki postępowania rekrutacyjnego podaje się do publicznej wiadomości w formie listy kandydatów poprzez umieszczenie jej w widocznym miejscu w siedzibie danego podmiotu. Listy te zawierają imiona i nazwiska kandydatów uszeregowane w kolejności alfabetycznej oraz najniższą liczbę punktów, która uprawnia do przyjęcia. Przedszkole zaś nie powołało się w swoich wyjaśnieniach na żadne konkretne przepisy pozwalające na odstępstwo od rozwiązań przyjętych w art. 158 ustawy prawo oświatowe i publikację danych w innej formie – w tym przypadku publikację danych na zamkniętej grupie internetowej. Prezes UODO stwierdził, że doszło do ujawnienia danych osobowych małoletniego jedynie w postaci jego imienia i nazwiska

poprzez umieszczenie listy dzieci przyjętych do przedszkola na zamkniętej grupie internetowej, mimo że prawo oświatowe nie przewiduje takiej formy i nie zostały wykazane żadne podstawy dla odstępstwa od właściwych przepisów prawa oświatowego.

Biorąc pod uwagę sugestie wskazane w przytoczonej decyzji UODO wskazano, że w przypadku komunikacji z rodzicami należy mieć na względzie określoną w przepisach i dobrych praktykach hierarchię sposobów oraz form zapewniających prowadzenie przez placówki oświatowe komunikacji z rodzicami lub opiekunowi prawnemu małoletniego tj.:

1. dziennik elektroniczny,
2. poczta mailowa,
3. kontakt telefoniczny,
4. rozmowa bezpośrednia,
5. komunikatory społecznościowe z zachowaniem zasad dotyczących ochrony danych osobowych, czyli na podstawie zgody wyrażonej przez rodzica / opiekuna prawnego dziecka, w sposób nie wymuszający konieczności posiadania przez rodzica / opiekuna prawnego konta w danej aplikacji.

W związku z przetwarzaniem w Jednostce danych osobowych w postaci wizerunków osób małoletnich na potrzeby Administratora przekazano - opublikowane pod linkiem *https://uodo.gov.pl/pl/file/7251* - stanowisko UODO wyrażone w Biuletynie Nr 3/2026 odnoszące się do publikowania zdjęć dzieci, celem rozważenia stosowania w bieżącej praktyce Jednostki sugestii organu nadzorczego w zakresie minimalizacji ryzyka dla przetwarzania danych osobowych. Wskazano, że w ocenie organu nadzorczego *„Nadmierne rozpowszechnianie wizerunku małoletnich w sieci nie tylko narusza ich prywatność, ale też może powodować realne zagrożenie dla ich bezpieczeństwa. Powinni pamiętać o tym zarówno rodzice i dziadkowie, którzy bezrefleksyjnie wrzucają do sieci zdjęcia swoich pociech, jak i instytucje zajmujące się edukacją i wychowaniem nieletnich, jak szkoły czy przedszkola. Media coraz częściej informują o placówkach edukacyjnych publikujących filmy z udziałem swoich podopiecznych, w których dzieci zachęcają do zapisania się do danej szkoły albo przedszkola. Zdjęcia z rozmaitych ciekawych aktywności, które również mają przyciągnąć nowych chętnych, są na porządku dziennym. Do sprawy odniosła się też Magdalena Bigaj w wywiadzie dla lutowego Biuletynu UODO, wskazując, że w związku z pogłębiającym się niżem demograficznym szkoły i przedszkola stają przed realnym problemem zabiegania o to, by dzieci zostały zapisane właśnie do nich – działania promocyjne będą się więc tylko nasilać. Prowadząc je, nie można jednak zapominać o przepisach o chroniących dane osobowe oraz wizerunek. Zgodnie z wypracowaną w orzecznictwie i doktrynie definicją to ostatnie pojęcie oznacza obraz danej osoby (nie tylko twarz, ale też np. charakterystyczną sylwetkę), utrwalony w jakiś sposób (najczęściej na zdjęciu lub filmie). Jest on dobrem osobistym w świetle Kodeksu cywilnego, a także podlega ochronie na podstawie prawa autorskiego. Wizerunek stanowi również daną osobową, gdyż pozwala na zidentyfikowanie konkretnego człowieka. Rozpowszechnianie wizerunku wymaga zgody danej osoby. Choć prawo autorskie dopuszcza możliwość publikacji bez takiej zgody, jeśli wizerunek konkretnej osoby stanowi tylko szczegółów większej całości, tej podstawy nie można stosować bezrefleksyjnie. Kluczową kwestią jest zawsze ustalenie, czy w danym przypadku faktycznie niezbędne jest, by relacjonować wydarzenie, imprezę czy sprawozdawać przebieg wycieczki z wykorzystaniem wizerunku dzieci. To, że w przepisach mamy do czynienia z potencjalnym zwolnieniem z konieczności pozyskania zezwolenia na rozpowszechnienie, nie oznacza, że w każdych okolicznościach jest to niezbędnie konieczne. Oddzielną sprawą są regulacje dotyczące danych osobowych. Znajdują one zastosowanie zawsze, gdy na podstawie zdjęcia można rozpoznać konkretną osobę. Nawet więc, jeśli stanowi ona szczegół całości (co pozwala na publikację bez zezwolenia w świetle prawa autorskiego), ale można ją zidentyfikować, w grę wchodzą przepisy RODO. Warto też podkreślić, że w motywie 38 tego Rozporządzenia wskazano, iż dane osobowe dzieci wymagają szczególnej ochrony, zaś motyw*

58 zawiera wytyczną nakazującą stosowanie jasnych i prostych komunikatów w przypadku przetwarzania danych dziecka – tak, by mogło ono zrozumieć swoje prawa. Przede wszystkim więc przetwarzanie wizerunku (a więc zarówno jego publikacja w internecie, jak i samo utrwalenie poprzez np. zrobienie zdjęcia) wymaga wskazania jednej z podstaw wymienionych w art. 6 ust. 1 RODO. W grę nie wejdzie lit. b tego przepisu, gdyż publikacja zdjęć nie wydaje się konieczna dla celów wykonania umowy. Ta przesłanka jest nieadekwatna w przypadku publikacji wizerunku w celach marketingowych placówki oświatowej także wówczas, gdy zdjęcia na zamówienie szkoły zostaną odpłatnie przygotowane przez profesjonalnego fotografa. Okoliczność ta nie ma żadnego znaczenia dla rozpowszechniania wizerunku dzieci. Nawet jeśli świadczenie placówki oświatowej chcielibyśmy potraktować jako usługę edukacyjną, placówka ta jest w stanie w pełni realizować program nauczania i zapewniać opiekę nad uczniem bez upubliczniania jego wizerunku w internecie. Publikacja zdjęć jest jedynie działaniem akcesoryjnym, niemającym wpływu na istotę świadczonej usługi (edukacji) – mówi dr hab. Marlena Sakowska-Baryła, prof. Uniwersytetu Łódzkiego, radczyni prawna i partnerka w Sakowska-Baryła, Czaplińska Kancelarii Radców Prawnych, należąca do Społecznego Zespołu Ekspertów przy Prezesie UODO. Tym bardziej trudno się powołać na przesłankę konieczności przetwarzania dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (lit. d). W tym miejscu znów warto odwołać się do wywiadu z Magdaleną Bigaj, która zwróciła uwagę, że w przypadku placówek publicznych żaden przepis nie nakłada na nie obowiązku promocji. Także dr hab. Sakowska-Baryła wskazuje, że w świetle obecnie obowiązującego prawa publikacji wizerunku dziecka przez placówkę oświatową nie można postrzegać w kategoriach obowiązku prawnego. A co za tym idzie, tego rodzaju przetwarzanie danych osobowych nie ma i nie może mieć podstaw w przesłance określonej w art. 6 ust. 1 lit. c RODO. Zwykle publikowanie wizerunków dzieci przez różnego rodzaju placówki odbywa się w celach informacyjno-promocyjnych, a realizowanie takich potrzeb w żadnym razie nie stanowi wypełnienia obowiązku prawnego ciążącego na administratorze, ponieważ taki obowiązek po prostu nie istnieje – tłumaczy ekspertka. Przypomina też, że przetwarzanie danych osobowych na podstawie wspomnianej przesłanki wymaga istnienia konkretnego przepisu prawa krajowego lub unijnego. Co prawda Prawo oświatowe nakłada na szkoły obowiązki w zakresie dokumentowania przebiegu procesu nauczania, ale żaden przepis nie obliguje placówki do prowadzenia publicznej galerii zdjęć czy profilu w mediach społecznościowych. Działania takie wykraczają poza sferę imperium (władczych działań państwa) i przechodzą w sferę promocji, która nie ma nic wspólnego z obowiązkiem prawnym, choć trzeba zauważyć, że szkoły faktycznie prowadzą swoistą politykę informacyjną, z jednej strony promując swoje działania edukacyjne, z drugiej zabiegając o zainteresowanie potencjalnych kandydatów – mówi prof. Sakowska-Baryła. Ekspertka wskazuje też, iż rozpowszechnianie przez placówkę oświatową wizerunków dzieci na podstawie art. 6 ust. 1 lit. f RODO także jest wysoce ryzykowne i – wbrew utartej praktyce – zazwyczaj prawnie bezpodstawne. Przepis ten stanowi bowiem, że przetwarzanie danych osobowych – w tym ich pozyskiwanie i rozpowszechnianie – jest zgodne z prawem, o ile jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, w szczególności gdy jest ona dzieckiem. Choć przez lata obserwowaliśmy rozwój działalności placówek oświatowych prowadzonej w mediach społecznościowych obejmującej głównie szeroką dystrybucję zdjęć i filmów, co bardzo często odbywa się równolegle z umieszczaniem ich także na stronach internetowych placówek, uzasadniona jest analiza tego, czy praktyka ta rzeczywiście znajduje podstawę w prawie, a także, czy faktycznie niezbędne jest realizowanie celów informacyjnych i promocyjnych głównie na bazie rozpowszechniania wizerunków dzieci. Teoretycznie szkoły mogą się powołać na „interes promocyjny" jako uzasadniony prawnie cel przetwarzania, ale przecież musi on przejść tzw. test równowagi i w kolizji między interesem promocyjnym szkoły a prawem do prywatności i ochrony wizerunku dziecka ten ostatni niemal zawsze należy uznać za nadrzędny. Dzieci korzystają ze szczególnej ochrony danych (motyw 38 RODO), co sprawia, że ich interesy przeważają

nad chęcią autopromocji placówki – tłumaczy prof. Sakowska-Baryła. Oczywiście należy tu zachować zdrowy rozsądek i nie chodzi o to, aby przestać informować o działalności szkoły, osiągnięciach uczniów, relacjonować wydarzenia czy promować godne pochwały zachowania. Każdorazowo trzeba jednak rozważyć, czy w tym przypadku niezbędne jest okraszanie przekazywanej informacji zdjęciem lub filmem z udziałem uczniów. Dzieci w szkole zwykle pozostają w sytuacji, w której ograniczona jest ich swoboda i autonomia, a ich pozycja, sposób percepcji rzeczywistości i postrzegania świata zwykle nie sprzyja świadomemu decydowaniu o tym, czy chcą, czy nie chcą być bohaterem filmu, zdjęcia, fotorelacji czy rolki w socialmediach. W przypadku osób niepełnoletnich zgody na przetwarzanie danych udzielają w ich imieniu rodzice lub opiekunowie prawni. Jest to element wykonywania władzy rodzicielskiej, a więc – zgodnie z Kodeksem rodzinnym i opiekuńczym – musi on uwzględniać najlepszy interes dziecka, a także szanować jego godność i prawa. KRO, podobnie jak Konwencja ONZ o prawach dziecka, przewiduje też, że przed podjęciem ważnych decyzji dotyczącej podopiecznego rodzice powinni wysłuchać ich zdania. Oczywiście należy tu uwzględnić wiek i stopień dojrzałości dziecka – nie zawsze bowiem zdaje sobie ono sprawę z konsekwencji wyrażenia takiej zgody. W przypadku starszych dzieci jednak powinno się skonsultować z nimi przed wyrażeniem takiej zgody. Należałoby przyjąć, że człowiek w ogóle – nawet ten jeszcze niepełnoletni – powinien mieć wpływ na to czy, jego wizerunek będzie pozyskany i czy będzie rozpowszechniony. Nie chodzi oczywiście o to, by zabieganie o zgodę na utrwalanie i rozpowszechnianie wizerunku doprowadzić do absurdu poprzez pytanie o nią dzieci w każdym wieku, nawet tych, które nie są w stanie jej wyrazić. Ale przymuszanie do pozowania do zdjęć, szykany z powodu braku zgody na rozpowszechnianie wizerunku, szydzenie z niechęci do pozowania należy uznać za praktyki w wysokim stopniu naganne – wyjaśnia prof. Sakowska-Baryła. Ekspertka wskazuje, że właśnie zgoda w tym przypadku wydaje się najlepszą podstawą prawną. Musi być ona jednak całkowicie dobrowolna (podobnie jest w przypadku pełnoletnich uczniów). Jeśli zatem dziecko nie może wziąć udziału w teatrzyku szkolnym tylko dlatego, że rodzic nie chce, by zdjęcie z tego wydarzenia trafiło na Facebooka, mamy do czynienia z wymuszeniem zgody. Podobnie nie można uzależniać wzięcia przez ucznia udziału w zawodach sportowych czy zajęciach dodatkowych od przymusowego wyrażenia zgody na pozyskanie i rozpowszechnianie wizerunku. Właściwym rozwiązaniem jest zapewnienie dziecku udziału w aktywności przy jednoczesnym zadbaniu, by nie znalazło się ono w kadrze publikowanych zdjęć – zaznacza badaczka. Zgoda musi też mieć charakter uprzedni, być precyzyjna i przejrzysta (m.in. na rzecz jakiego podmiotu jest udzielana i na jaki czas), wyraźnie wskazywać cel i sposób wykorzystania wizerunku oraz jego warunki (np. w jakich serwisach zdjęcie będzie publikowane, z jakim podpisem, czy zostanie poddane jakiejś edycji). Wszystkie powyższe informacje muszą być przekazane zrozumiałym językiem. Kluczowym argumentem przeciwko dzieleniu się zdjęciami dziecka jest jego godność i autonomia. Udostępniając zdjęcia dziecka, odbieramy mu prawo do samodzielnego kształtowania swojej obecności w internecie i podejmowania decyzji o swoim wizerunku. Decyzje podjęte dziś przez rodziców będą z dzieckiem przez całe jego życie – mówi Wojciech Klicki, wiceprezes Fundacji Panoptykon i członek Społecznego Zespołu Ekspertów przy Prezesie UODO. Jak wskazano w broszurze „Wizerunek dziecka w internecie" (opracowanej z udziałem UODO), udostępnianie wizerunku w sieci rodzi poważne zagrożenia. Są one szczególnie poważne w przypadku osób niepełnoletnich. Przede wszystkim publikując wizerunek, tracimy nad nim kontrole – nie wiemy, kto skopiuje to zdjęcie ani do czego go użyje. A użyte może być zarówno w celu dokonania oszustwa (np. fałszywa zbiórka na rzekomo chore dziecko, z wykorzystaniem skradzionego zdjęcia), jak i do cyberprzemocy (np. przerabianie zdjęć, by pognębić ofiarę, lub rozpowszechnianie jej kompromitującego zdjęcia z przeszłości). Bardzo istotne jest to, jak komponowane są zdjęcia lub filmy, co faktycznie prezentują, jak są kadrowane. To, co dla niektórych może być urocze, śmieszne i warte pokazania, dla innych – zwłaszcza dla dzieci – bywa przyczyną znacznego dyskomfortu nie tylko w chwili publikacji, ale także długo po niej. Jak wiemy – w internecie nic nie ginie i właściwie nie jesteśmy w stanie przewidzieć, jak z pozoru niewinne ujęcie, nawet w pewnych okolicznościach uzasadnione interesem edukacyjnym (promocyjnym, informacyjnym),

zostanie wykorzystane w przyszłości – zaznacza prof. SakowskaBaryła. Zdjęcia dzieci mogą być bowiem używane także przez osoby o skłonnościach pedofilskich – w celu wymieniania się na różnych forach dla takich osób, a nawet – zlokalizowania dziecka i nawiązania z nim kontaktu. Szczególnie zdjęcia na profilach czy stronach szkół i przedszkoli mogą pozwolić przestępcy ustalić, gdzie dziecko znajduje się w danych godzinach itp. Ze względu na to ostatnie zagrożenie należy w szczególności unikać publikacji zdjęć małoletnich nie w pełni ubranych (np. na basenie). Niestety technologia deepfake pozwala dziś przerobić w kontekście seksualnym praktycznie każde zdjęcie. Pod koniec roku 2025 wielkie poruszenie wywołała nowa funkcja Groga (modelu sztucznej inteligencji na portalu X), która pozwalała na błyskawiczne „rozbieranie" osób na zdjęciach – tj. generowanie nagich fotografii z ich twarzami. Potencjalnie mogło to dotyczyć także zdjęć dzieci. Co prawda X zablokował już tę funkcję, ale wciąż istnieje wiele podobnych aplikacji. Tylko w styczniu 2026 r. Apple zablokował ich w swoim sklepie 28, lecz wciąż pojawiają się nowe. Dobrze, że sprawa ta odbiła się szerokim echem, bo trudno o bardziej wyrazisty przykład negatywnych konsekwencji publicznego udostępniania wizerunku dzieci. Mam nadzieję, że przemówi on do wyobraźni rodziców – podkreśla Wojciech Klicki. Art. 17 RODO przyznaje nam tzw. prawo do bycia zapomnianym, czyli do usunięcia naszych danych. Dotyczy to również zdjęć zawierających nasz wizerunek. Usunięcia danych możemy domagać się, gdy są już one nieaktualne (np. dziecko dorosło i zmieniło wygląd), nadmiarowe, przetwarzane niezgodnie z prawem lub gdy zgoda na ich przetwarzanie została cofnięta. Po osiągnięciu pełnoletniości dziecko może cofnąć zgodę na publikację, wyrażoną wcześniej przez rodziców. Jak zwróciła uwagę Magdalena Bigaj, w przytaczanym wywiadzie, pojawiły się już pierwsze przypadki młodych ludzi domagających się od szkół usunięcia swoich zdjęć sprzed lat. Prócz skargi na podstawie RODO można domagać się usunięcia zdjęcia z naszym wizerunkiem na podstawie przepisów o ochronie dóbr osobistych. Najpierw należy wezwać podmiot, który te zdjęcia opublikował, do ich bezzwłocznego usunięcia. Jeśli tego nie zrobi, można rozważyć dalsze kroki, np. pozew cywilny, a w pewnych okolicznościach nawet postępowanie karne. Art. 202 par. 4b KK penalizuje bowiem produkcję, rozpowszechnianie, prezentowanie, przechowywanie lub posiadanie pornografii z wykorzystaniem wytworzonego (np. rysunek) lub przetworzonego (np. fotomontaż, deepfake) wizerunku małoletniego uczestniczącego w czynności seksualnej. Dotyczy to więc także zdjęć przerobionych przez wspomniane wyżej aplikacje „rozbierające". Jeśli zdjęcia publikowane są na wielkich platformach społecznościowych, można też domagać się ich usunięcia bezpośrednio od administratorów tych platform – na podstawie Aktu o usługach cyfrowych (DSA). Wojciech Klicki wskazuje, że im dłużej materiał jest dostępny w sieci, tym większe ryzyko jego szerokiego rozpowszechnienia i szkodliwych konsekwencji. Dlatego najpierw zawsze warto zgłosić taką nielegalną treść platformie z żądaniem jej usunięcia. Art. 16 umożliwia bowiem każdej osobie domaganie się usunięcia bezprawnej treści, którą inny użytkownik opublikował na platformie. W tym zakresie DSA obowiązuje bezpośrednio, nie wymaga wdrożenia). Platformy mają co do zasady obowiązek niezwłocznie reagować na takie zgłoszenia. Jeśli tego nie zrobią, same narażają się na to, że mogą za taką treść ponieść odpowiedzialność – tłumaczy ekspert. Art. 6 wspomnianego Aktu o usługach cyfrowych przewiduje bowiem, że hostingodawca (w tym np. portal społecznościowy) nie odpowiada za bezprawne materiały tak długo, jak nie ma wiedzy o ich nielegalnym charakterze. Kiedy jednak zostanie o nim poinformowany, aby uniknąć odpowiedzialności, musi niezwłocznie taką treść usunąć. Ten mechanizm ma skłaniać m.in. platformy do szybkiego reagowania na nielegalne treści. DSA nakłada też na platformy pewne obowiązki proceduralne ws. zgłoszeń na postawie art. 16. Platforma ma obowiązek stworzyć do tego odpowiednią ścieżkę, potwierdzić otrzymanie zgłoszenia (jeśli ma dane kontaktowe użytkownika/użytkowniczki), a następnie rozpatrzyć je „w sposób terminowy, niearbitralny i obiektywny oraz z zachowaniem należytej staranności" (nie może go więc po prostu zignorować, co czasem zdarzało się w przeszłości). Jeśli odmówi usunięcia, musi stworzyć odpowiedni wewnętrzny mechanizm odwoławczy, który umożliwi osobie zgłaszającej zakwestionowanie pierwotnej decyzji – zauważa Wojciech Klicki. Jeśli ta procedura odwoławcza zawiedzie, można także złożyć skargę do sądu lub organu pozasądowego rozwiązywania sporów.

Niestety przez brak ustawy implementującej DSA w Polsce wciąż nie wyznaczono wprost Koordynatora Usług Cyfrowych, do którego można by odwoływać się w kwestiach naruszeń proceduralnych przy rozpatrywaniu odwołania przez platformę".

W toku czynności dokonano weryfikacji realizacji w Jednostce zasad dotyczących ochrony danych osobowych w kontekście stosowania środków technicznych i organizacyjnych w niżej wskazanym zakresie:

- stosowania „polityki czystego biurka";
- stosowania „polityki czystego ekranu";
- stosowania mechanizmów zapewniających uniemożliwianie dostępu do komputera stacjonarnego lub laptopa przez osoby nieuprawnione (tj. blokada ekranu, wylogowanie, przechowywania haseł dostępu do logowania do systemów informatycznych wykorzystywanych do przetwarzania danych osobowych);
- zabezpieczenia dokumentów zawierających dane osobowe w sposób uniemożlwiający dostęp osób nieuprawnionych;
- stosowania procedur związanych z niszczeniem dokumentów zawierających dane osobowe w sposób uniemożlwiający zapoznanie się z treścią tych dokumentów przez osoby nieuprawnione;
- stosowania procedur związanych z przetwarzaniem dokumentów zawierających dane osobowe w przypadku kopiowania tych dokumentów w sposób uniemożlwiający zapoznanie się zawartymi w nich danymi osobowymi przez osoby nieuprawnione;
- stosowania procedur związanych z zabezpieczeniem kluczy do pomieszczeń, w których przetwarzane są dane osobowe w sposób uniemożlwiający dostęp do tych pomieszczeń przez osoby nieuprawnione;

W toku czynności nie stwierdzono uchybień, które mogłyby mieć negatywny wpływ na zapewnienie odpowiedniego poziomu bezpieczeństwa danych osobowych przetwarzanych w zasobach Administratora.

Rekomendacje Inspektora Ochrony Danych Osobowych w zakresie wypełniania przez Administratora obowiązków oraz zasad przetwarzania danych osobowych określonych w przepisach RODO oraz przepisach prawa krajowego:

- w przypadku konieczności powierzenia danych osobowych z zasobów Administratora na rzecz podmiotów trzecich, o którym mowa w art. 28 RODO w związku z przetwarzaniem danych w jego imieniu, przed udostępnieniem danych na rzecz podmiotu trzeciego podjęcie przez Administratora działań zmierzających do uzyskania „gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą";
- w związku ze świadczeniem na rzecz Administratora przez podmiot nie będący podmiotem publicznym usług w zakresie hostingu poczty elektronicznej zapewnienie poufności, dostępności oraz integralności danych osobowych przetwarzanych w imieniu Administratora za pośrednictwem wymienionego źródła poprzez powierzenie danych osobowych do przetwarzania na zasadach określonych w art. 28 ust. 3 RODO na podstawie stosownej umowy powierzenia danych do przetwarzania;
- bieżące prowadzenie w formie stosownego rejestru procesu weryfikacji zakresu oraz okresu obowiązywania umów powierzenia przetwarzania danych osobowych zawieranych przez Administratora z podmiotami przetwarzającymi dane w jego imieniu;
- niezwłoczna realizacja określonego w art. 11 Ustawy o ochronie danych osobowych z dnia 10 maja 2018 roku - obowiązku udostępnienia na stronie internetowej Jednostki oraz podmiotowej stronie

Biuletynu Informacji Publicznej albo „w sposób ogólnie dostępny w miejscu prowadzenia działalności" danych Inspektora Ochrony Danych w postaci imienia, nazwiska oraz adresu poczty elektronicznej;

- niezwłoczna realizacja obowiązku informacyjnego, o którym mowa w art. 13 ust. 1 i 2 RODO w związku z przetwarzaniem danych osobowych na podstawie art. 6 ust. 1 lit c) RODO związanych z wypełnianiem przez Administratora nałożonych na niego obowiązków prawnych poprzez zamieszczenie stosownej klauzuli informacyjnej w dedykowanej zakładce zamieszczonej na stronie internetowej Jednostki oraz w miejscu ogólnodostępnym dla osób, których dane dotyczą;

_____

/pieczęć i podpis Inspektora Ochrony Danych/