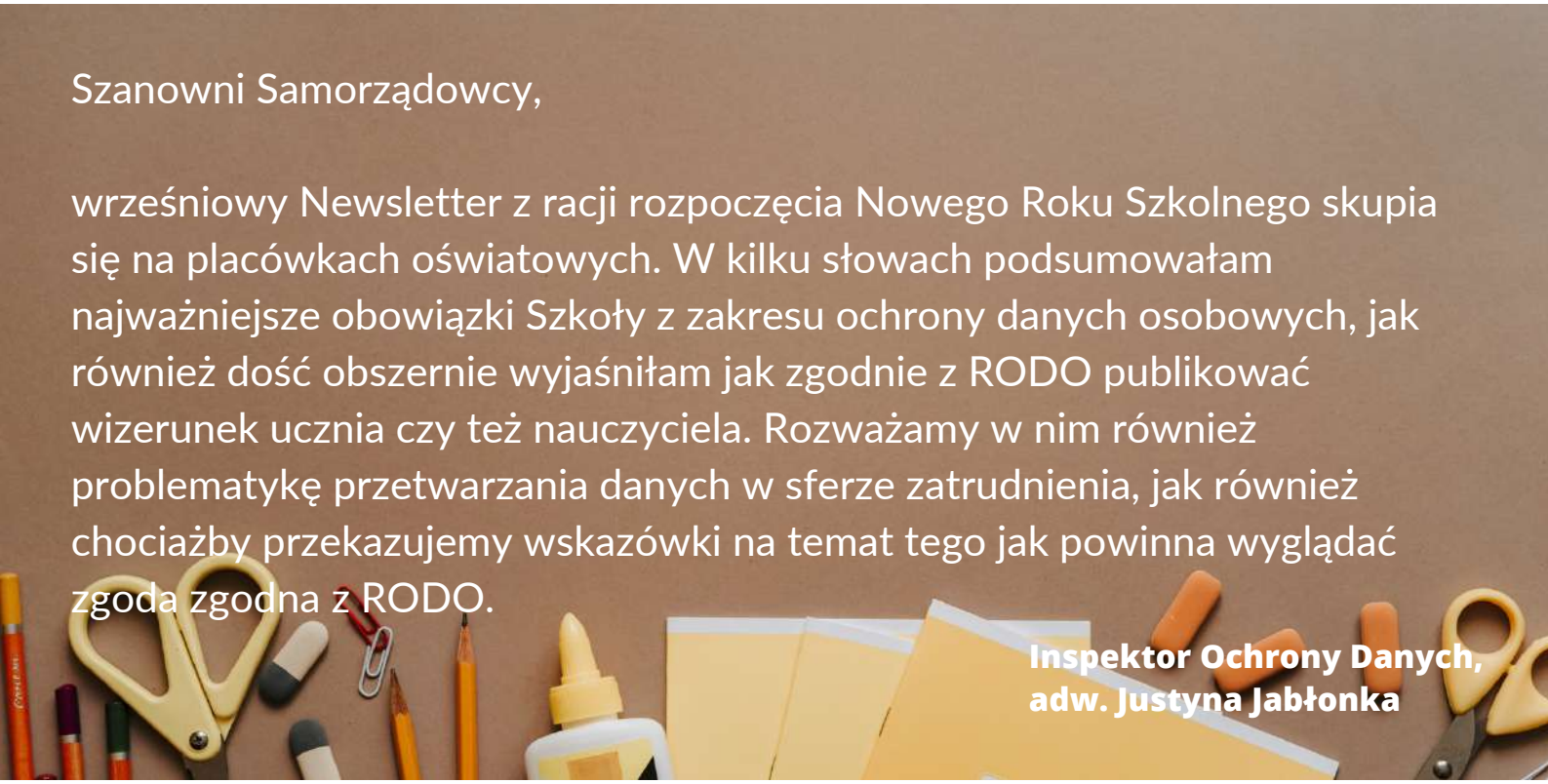
JUSTYNA JABŁONKA

Sierpień / Wrzesień 2023
Nr 6-7/2023

KANCELARIA WYRZYKOWSCY

Newsletter
INSPEKTORA OCHRONY DANYCH
ADW. JUSTYNY JABŁONKI



Szanowni Samorządowcy,

wrześniowy Newsletter z racji rozpoczęcia Nowego Roku Szkolnego skupia się na placówkach oświatowych. W kilku słowach podsumowałam najważniejsze obowiązki Szkoły z zakresu ochrony danych osobowych, jak również dość obszernie wyjaśniłam jak zgodnie z RODO publikować wizerunek ucznia czy też nauczyciela. Rozważamy w nim również problematykę przetwarzania danych w sferze zatrudnienia, jak również chociażby przekazujemy wskazówki na temat tego jak powinna wyglądać zgoda zgodna z RODO.

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

Na Nowy Rok Szkolny proponuję:

I. Ochrona Danych Osobowych w Szkole. Obowiązki Administratora Danych – Szkoły, w Nowym Roku Szkolnym.

Wraz z nadchodzącym rokiem szkolnym, nieodzowne jest przypomnienie o kluczowych obowiązkach związanych z ochroną danych osobowych w placówkach edukacyjnych. Rozpoczęcie nowego roku to czas, w którym Szkoła musi skupić się na zapewnieniu pełnej zgodności z przepisami Rozporządzenia Ogólnego o Ochronie Danych Osobowych, dalej: RODO. W niniejszym artykule omówię te istotne aspekty, aby zapewnić płynny start edukacyjny we wrześniu.

- **PAMIĘTAJ O OBOWIĄZKU INFORMACYJNYM:** Zapewnienie osobom, których dane dotyczą, kompleksowej informacji, zgodnie z przepisami zawartymi w art. 13 i 14 RODO jest obowiązkiem każdej Szkoły, która musi poinformować o celach, sposobach, źródłach oraz zakresie przetwarzania danych osobowych. Sposób spełnienia obowiązku informacyjnego jest dowolny, ale należy pamiętać, że trzeba go spełnić w sposób jasny, przejrzysty i łatwo dostępny.
- **PAMIĘTAJ O PODSTAWIE PRAWNEJ DO PRZETWARZANIA DANYCH:** Szkoła, przetwarza dane na podstawie przepisów odnoszących się ściśle do funkcjonowania oświaty. Przede wszystkim są to: Prawo oświatowe, Karta Nauczyciela; ustawa o systemie oświaty, ustawa o systemie informacji oświatowej, ustawa o finansowaniu zadań oświatowych, rozporządzenia do ww. ustaw.
- **PAMIĘTAJ O ZEBRANIU ZGÓD NA PRZETWARZANIE DANYCH OSOBOWYCH – WIZERUNKU DZIECI:** Na szkole ciąży obowiązek uzyskania zgody od uprawnionej osoby na publikację jej wizerunku. Należy pamiętać, że wykorzystywanie danych osobowych uczniów, np. na stronach internetowych, mediach społecznościowych szkoły i rozpowszechnianie wizerunku wymaga zezwolenia osoby, której wizerunek jest rozpowszechniany bądź jej opiekuna prawnego. Więcej na temat przetwarzanie cudzego wizerunku zgodnie z RODO w kolejnym artykule.
- **PAMIĘTAJ O UPOWAŻNIENIACH DO PRZETWARZANIA DANYCH OSOBOWYCH UDZIELONYCH NOWYM NAUCZYCIELOM, PRACOWNIKOM ADMINISTRACYJNYM W SZKOLE:** Każdy pracownik, który rozpoczynał będzie pracę na danych osobowych dostępnych w szkole powinien być do tego upoważniony przez Administratora – Szkołę. Aby żadna ze stron, tj. upoważniony pracownik i upoważniający – Szkoła, nie miała wątpliwości co do zakresu przekazanego upoważnienia, rekomenduję, aby było ono pisemne.

- **PAMIĘTAJ O ZAWARCIU UMÓW POWIERZENIA PRZETWARZANIA DANYCH:** Umowy te powinny być zawarte przykładowo: z usługodawcami IT, z dostawcą dziennika elektronicznego, z biurem podróży, któremu przekazujemy dane podopiecznych w związku z organizacją wycieczki szkolnej, czy z osobą wykonującą usługi z zakresu BHP. Pamiętaj, że pielęgniarka szkolna, czy lekarz medycyny pracy to oddzielny administrator danych, zatem Szkoła nie zawiera z tymi podmiotami w/w umowy.
- **PAMIĘTAJ O ZABEZPIECZENIACH:** Szkoła powinna wdrożyć odpowiednie dla swojego funkcjonowania i skuteczne środki techniczne i organizacyjne, mające na celu zabezpieczenie danych osobowych przed dostępem nieupoważnionych osób oraz zagwarantowanie ich integralności i poufności. Z praktyki dostrzegam jak ważne jest spisanie i dostosowanie się do wprowadzonej polityki kluczy, wprowadzenie reguł postępowania odnośnie pracy na dyskach zewnętrznych, pendrive'ów – ich zahasłowanie, odpowiednia i ciągła współpraca z osobą odpowiedzialną za zabezpieczenia IT, aż wreszcie odpowiednia pod względem organizacji danej szkoły, tj.„ szyta na miarę" polityka ochrony danych osobowych, z którą faktycznie i rzetelnie zapoznają się nowi pracownicy przed przystąpieniem do pracy.
- **PAMIĘTAJ O WYZNACZENIU IOD:** Szkoła jest zobowiązana do wyznaczenia inspektora ochrony danych, jak również opublikowanie jego imienia i nazwiska na stronie internetowej szkoły oraz powiadomienie o jego powołaniu Prezesa UODO. Inspektor ochrony danych musi posiadać fachową wiedzę w zakresie prawa i praktyk dotyczących ochrony danych, a jego funkcja cechuje się samodzielnością i niezależnością.
- **PAMIĘTAJ O OBOWIĄZKACH Z ZAKRESU OCHRONY DANYCH OSOBOWYCH DOTYCZĄCYCH MONITORINGU WIZYJNEGO:** Szkoły są zobowiązane do przestrzegania przepisów dotyczących przetwarzania danych osobowych w kontekście monitoringu wizyjnego. Te zasady wywodzą się zarówno z RODO, jak i z przepisów bezpośrednio odnoszących się do działań edukacyjnych, zwłaszcza w odniesieniu do uregulowań zawartych w Prawie Oświatowym.
- **PAMIĘTAJ O WŁAŚCIWEJ WERYFIKACJI OSOBY, KTÓREJ CHCESZ UDZIELIĆ INFORMACJI PRZEZ TELEFON:** Najważniejsze jest zidentyfikowanie dzwoniącego oraz ustalenie, czy jest on uprawniony do pozyskania informacji o dziecku. Należy bowiem pamiętać, że Szkoła jest zobowiązana zapewnić, aby dane nie były udostępniane osobom nieupoważnionym. Dlatego w takich sytuacjach

ważne jest dążenie do potwierdzenie, że osoba dzwoniąca jest tą, za którą się podaje. Informacjami służącymi do weryfikacji dzwoniącego może być np. imię i nazwisko dziecka w połączeniu z wiekiem dziecka, imionami rodziców, informacją w co dziecko jest ubrane, w której jest klasie, nazwisko wychowawcy, ostatnie 3 liczby nr PESEL dziecka tj. informacjami, które posiada Szkoła, a które powinien posiadać rodzic, nikt inny. W przypadku wątpliwości co do tożsamości osoby usiłującej pozyskać informacje dotyczące dziecka, powinno się odmówić ich udzielenia.

- **PAMIĘTAJ, IŻ PRZETWARZANIE DANYCH SZCZEGÓLNYCH KATEGORII JEST CO DO ZASADY ZABRONIONE:** W art. art. 9 ust. 2 RODO znajduje się zamknięty katalog, kiedy Szkoła może przetwarzać tego rodzaju dane, tj. będą to zazwyczaj sytuacje:
  - udzielenie przez osobę, której dane dotyczą, lub przez jej opiekuna prawnego (w przypadku niepełnoletnich), wyraźnej zgody na przetwarzanie danych w konkretnym celu lub celach;
  - niezbędność przetwarzania danych do wypełnienia obowiązków i wykonywania poszczególnych praw przez administratora lub osobę, której dane dotyczą w dziedzinie prawa pracy, zabezpieczenia socjalnego i społecznego;
  - niezbędność przetwarzania danych do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, o ile osoba, której dane dotyczą jest niezdolna do wyrażenia zgody;
  - niezbędność przetwarzania danych do celów oceny zdolności pracownika do pracy.

Wreszcie również:

- **PAMIĘTAJ O SZKOLENIACH:** Każda nowo zatrudniona osoba, której praca związana będzie z dostępem do danych osobowych musi poznać zasady dotyczące ich przetwarzania w jednostce, zapoznać się z obowiązującą polityką ochrony danych i innymi wprowadzonymi dokumentami z tego zakresu. Nowy pracownik powinien przejść szkolenie z zakresy ochrony danych osobowych, najlepiej zorganizowane przez wyznaczonego Inspektora Ochrony Danych w tej placówce.

Prawidłowe przetwarzanie danych osobowych uczniów w szkole powinno być jej priorytetem. Zatem życzę, abyście weszli w Nowy Rok Szkolny bezpiecznie!

Autor:
Justyna Jabłonka
Inspektor Ochrony Danych
adwokat

II. Wizerunek ucznia, nauczyciela i zasady jego prawidłowego przetwarzania zgodne z RODO.

Wizerunek osoby jest jej daną osobową chronioną prawem. Wskazuję na to niejednokrotnie podczas spotkań w placówkach oświatowych. Pozwala on zidentyfikować osobę fizyczną. Już samo wykonywanie fotografii, bez ich udostępniania, jest przetwarzaniem, na które niejednokrotnie Szkoła musi posiadać zgodę. Oczywiście mowa tutaj o fotografowaniu związanym z celami zawodowymi, zarobkowymi, gdyż nie będzie to dotyczyło fotografowania na własny użytek przez osobę fizyczną w ramach działalności czysto osobistej lub domowej. Wstawianie zdjęć na media społecznościowe w ramach kąt osobistych nie będzie z tym związane.

1. **Zdjęcie nauczyciela na stronie internetowej szkoły – w ramach przedstawienia osób zatrudnionych w danej placówce.**

Wielokrotnie w mojej praktyce spotkałam się z pytaniem Pani Dyrektor/Pana Dyrektora, czy mogą oni umieścić zdjęcia swoich nauczycieli na stronie www. wraz z imieniem i nazwiskiem w ramach przedstawienia tych osób jako kadry zatrudnionej w tej szkole.
Otóż …

… odnosząc się do art. 22(1) Kodeksu Pracy, dalej: k.p.: Pracodawca może domagać się od podwładnego: imienia (imion) i nazwiska, imion rodziców, daty urodzenia, miejsca zamieszkania (adresu do korespondencji), wykształcenia, przebiegu dotychczasowego zatrudnienia, a także imion i nazwiska oraz daty urodzenia dzieci, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy, jak również numeru PESEL pracownika. Co więcej, pracodawca jest uprawniony do uzyskania od pracownika innych danych osobowych niż wyżej określone, jeżeli obowiązek ich podania wynika z odrębnych przepisów (art. 22 (1) § 4 k.p.). Tylko te dane pracodawca samorządowy będzie mógł przetwarzać na podstawie tego przepisu.
Podsumowując: Wśród wymienionych w art. 22 (1) k.p. danych, co do których przetwarzania legitymowany jest pracodawca, nie znajduje się wizerunek pracownika. Zatem, aby Szkoła mogła zamieścić zdjęcie nauczyciela na swojej stronie internetowej musi w tym przypadku wystąpić inna ku temu podstawa, tj. **zgoda nauczyciela**.

2. Zdjęcie dyrektora, nauczyciela, ucznia na stronie internetowej szkoły – w ramach relacji z wydarzenia szkolnego.

Zgodnie z art. 81 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, rozpowszechnienie wizerunku **wymaga zezwolenia osoby na nim przedstawionej**. W braku wyraźnego zastrzeżenia zezwolenie nie jest wymagane, jeżeli osoba ta otrzymała umówioną zapłatę za pozowanie.

Odnosząc się do powyższego artykułu zacząć należy od wyjaśnienia, **czym jest wizerunek**.

Wizerunek to: zespół cech człowieka podlegających percepcji za pomocą zmysłu wzroku1.

Nośnikiem wizerunku może być natomiast fotografia. Zakres terminu „wizerunek" nie jest ograniczony tylko do tego, co dla człowieka często najbardziej charakterystyczne, czyli do twarzy. To określenie rozciąga się na całą postać osoby fizycznej.

Pamiętaj! Osoba, która występuje na zdjęciu może zakazać rozpowszechniania tego zdjęcia z powołaniem się na swoje **prawo do wizerunku.**

Prawo do wizerunku przysługuje nie tylko osobom publicznym, z ochrony prawa do wizerunku może korzystać każdy.

Zakazuje się rozpowszechniania wizerunku, a więc udostępniania go w taki sposób, że może się z nim zapoznać szerszy krąg osób. Jeśli jednak obraz osoby fizycznej jest rozpowszechniany w sposób, który uniemożliwia jej rozpoznanie, to nie mamy do czynienia z udostępnianiem wizerunku, np. jeśli na ekranie telewizora obraz konkretnej postaci jest całkowicie „rozmyty" i telewidz nie jest w stanie jej rozpoznać, wówczas do naruszenia prawa do wizerunku nie dochodzi.

- **Zgoda na przetwarzanie wizerunku.**

Zezwolenie na rozpowszechnienie wizerunku jest niezbędne, gdy chodzi o jego wykorzystanie w celach publicznych.

Kto udziela tego zezwolenia?

1. **Osoba, której wizerunek ma być wykorzystany** pod warunkiem, że posiada zdolność do czynności prawnych.
2. **Za dziecko poniżej 13 roku życia** (brak zdolności do czynności prawnych) zgody udzielają rodzice (jeden z nich) bądź przedstawiciele ustawowi. W przypadku braku ich zgody czynność ta jest bezskuteczna.
3. **Dziecko powyżej 13 roku życia** posiada ograniczoną zdolność do czynności prawnych, zgoda ta jest ważna, jeśli potwierdzi ją rodzic/przedstawiciel ustawowy.

Udostepnienie wizerunku dziecka jest jego istotną sprawą, zatem rodzice podejmują w tym przedmiocie wspólnie decyzje. W braku porozumienia pomiędzy nimi rozstrzyga tą kwestię sąd opiekuńczy.

Jak powinna wyglądać zgoda na rozpowszechnienie wizerunku?

Zgoda powinna być skonkretyzowana, zatem osoba udzielająca tej zgody musi znać zakres upoważnienia przyznanego podmiotowi, który ten wizerunek będzie wykorzystywał, powinna wiedzieć o **miejscu, czasie, częstotliwości** udostępniania podobizny (wyrok SA w Warszawie z 4.07.2018 r.). **Ważne!** w przypadku wątpliwości w zakresie wykorzystania wizerunku to Szkoła, jako podmiot pobierający zgody będzie musiała udowodnić, że taką zgodą o takim zakresie dysponowała.

Forma udzielenia zgody:

1. Pisemna – pobieranie pisemnych zgód od rodziców/przedstawicieli ustawowych dziecka na początku roku szkolnego na przetwarzanie wizerunku dziecka ze wskazaniem wydarzeń, jak również miejsc, w których ten wizerunek będzie publikowany, np. strona internetowa Szkoły, media społecznościowe, wskazanie czasu takiej publikacji.
2. Dorozumiana – w przypadku organizowania publicznych imprez, gdzie graniczy z cudem odebranie pisemnych zgód, rekomenduję, aby wywiesić na drzwiach wejściowych na wydarzenie informację, iż zdjęcia z tego wydarzenia będą publikowane i wskazać miejsca tych publikacji, np. w mediach społecznościowych, kolejnej gazetce szkolnej. W tym przypadku należy uważać jednak, aby wykonywane zdjęcia stanowiły szczegół całości – o czym poniżej.

- **Rozpowszechnianie wizerunku osoby bez jej zgody. Czy jest to możliwe?**

Jak stanowi art. 81 ustawy o prawie autorskim i prawach pokrewnych zezwolenia nie wymaga rozpowszechnianie wizerunku:

1. osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;
2. osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Pierwsze wyłączenie:

Odnosząc się do pierwszego z wyłączeń, nie potrzebujemy zgody na przetwarzanie wizerunku osoby, która jest powszechnie znana **i jednocześnie** zdjęcie wykonano podczas pełnienia przez nią funkcji publicznych.

Przykład:

Dyrektor szkoły wita zgromadzonych gości na rozpoczęciu roku szkolnego. Nauczyciel szkoły prowadzi wydarzenie związane z 10leciem funkcjonowania placówki.

Ważny w tym przypadku jest również **punkt odniesienia i miejsce**, gdzie wizerunek będzie publikowany, tj. Dyrektor szkoły w małym miasteczku pod Krakowem nie będzie osobą powszechnie znaną w Warszawie. Zatem każda taka sytuacja wymagać będzie zastanowienia do jakiej społeczności trafi wizerunek danej osoby. Jeśli wizerunek ma trafić do osób i w miejsce, gdzie osoba ta jest znana powszechnie i został on wykonany w związku z pełnieniem funkcji publicznej, można opublikować ten wizerunek bez względu na to czy stanowi on szczegół całości czy stanowi on centralny punkt na zdjęciu.

Wyrok SA w Krakowie z 22.03.2018 r., I ACa 1215/17 -> Przewidziany w art. 81 ust. 2 pkt 1 u.p.a.p.p. wyjątek pozwalający na wykorzystanie wizerunku osoby bez jej zgody nie musi się odnosić do osób znanych w całej Polsce, czy nawet w mniejszym lub większym regionie kraju, wystarczy bowiem, aby dana osoba z racji pełnionych funkcji była znana osobom ze środowiska, w którym się obraca.

Drugie wyłączenie:

Odnosząc się do drugiego z wyłączeń, nie potrzebujemy zgody na przetwarzanie wizerunku osoby, stanowiącej szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Co oznacza, wobec tego, „bycie szczegółem całości"?

Wizerunek takiej osoby nie jest centralnym, najważniejszym elementem zgromadzenia czy imprezy. Jest on dopełnieniem, nieistotnym składnikiem ustalenia większej całości. Wizerunek jest natomiast nieistotną częścią całości, jeśli jego usunięcie pozostanie bez wpływu na pozostałą zawartość materiału, nie obniża jego wartości, nie czyni mnie atrakcyjną, nie jest znaczący.

Wyrok SA w Krakowie z 19.12.2001 r., I ACa 957/01 -> Dla zastosowania art. 81 ust. 2 pkt 2 prawa autorskiego rozstrzygające znaczenie ma ustalenie w strukturze przedstawienia relacji między wizerunkiem osoby (lub osób) a pozostałymi elementami jego treści; rozpowszechnianie wizerunku nie wymaga zezwolenia, jeśli stanowi on jedynie element akcydentalny lub akcesoryjny przedstawionej całości, tzn. w razie usunięcia wizerunku nie zmieniłby się przedmiot i charakter przedstawienia.

Jednakże, owe zgromadzenia czy imprezy muszą mieć charakter publiczny a nie prywatny, tj. wesela, komunie inne tego typu. Oznacza to, że ma na nie wstęp szeroki krąg osób a warunkiem jest np. zakup biletu. Miejscami takimi są przykładowo: rynek w mieście, park miejski, ulica, koncert, plaża.

Podsumowując, podejmując decyzję czy Szkoła może udostępnić wizerunek nauczyciela czy ucznia z danego wydarzenia trzeba każdorazowo przeanalizować, czy mamy ku temu podstawę, jak zostało wykonane zdjęcie, co jest jego zawartością. Każda sytuacja wymagać może odrębnej analizy. Pamiętać jednak należy o podpisaniu umowy powierzenia danych, jeśli osoba, która wykonuje fotografie dla Szkoły nie jest jej pracownikiem.

Autor:
Justyna Jabłonka
Inspektor Ochrony Danych
adwokat

III. Zasada przejrzystości a RODO – czego tak naprawdę wymagają od nas przepisy?

Art. 5 RODO wylicza zasady dotyczące przetwarzania danych osobowych, w tym między innymi **zasadę przejrzystości**. Według niej, dane osobowe muszą być *„przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”).*

Zasada ta wymaga zatem, aby wszystkie informacje i komunikaty związane z przetwarzaniem danych osobowych, kierowane do osób, których te dane dotyczą, były zrozumiałe, łatwe do zapoznania się, sporządzone prostym i jasnym językiem. Myślę, że takie wymagania są jak najbardziej oczywiste – osoby, których dane dotyczą, mają prawo do tego aby wiedzieć, przez kogo i w jaki sposób ich dane są przetwarzane, a także jaki jest tego cel. Powinny także znać prawa, jakie im przysługują i jakie są związane z przetwarzaniem ich danych osobowych.

<u>Na czym polega zasada przejrzystości danych?</u>

Do elementów przejrzystości, RODO zalicza udzielenie osobie, której dane są przetwarzane niezbędnych, wskazanych w przepisach RODO informacji (tzw. obowiązek informacyjny) oraz prowadzenie przejrzystej i zrozumiałej komunikacji z tymi osobami.

Pochylmy się szczególnie nad brzmieniem art. 12 RODO zatytułowanego: *Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą.* Zgodnie z ust. 1 ww. przepisu, administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji. Informacji udziela się na piśmie, elektronicznie lub ustnie – ale uwaga, tylko w sytuacji, kiedy innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
Zgodnie natomiast z ust. 5 tego przepisu - informacje oraz komunikacja i są wolne od opłat.

Co konkretnie oznaczają poszczególne wymagania wskazane powyżej?

Przekazywanie informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie może oznaczać, że komunikacja z osobą, której dane dotyczą, powinna odbywać się sposób jednoznaczny, niewprowadzający w błąd, łatwy do przyswojenia – z ograniczeniem ilości informacji do tych, które są niezbędne, a same komunikaty dotyczące przetwarzania danych powinny być wyraźnie wyodrębnione od pozostałych kwestii.

Informacje **przedstawione jasnym i prostym językiem** – czyli tak, aby zrozumiał je każdy odbiorca, z uwzględnieniem np. wieku. Zdania powinny być krótkie i konkretne.

Informacje powinny być **przekazane w łatwy sposób** – czyli taki, który jest czytelny. Trzeba mieć wzgląd na czcionkę (wielkość, kolor) czy format tekstu. Osoba, której dane dotyczą, nie może wyszukiwać wśród wielości informacji podanych w tekście tych, które dotyczą przetwarzania jej danych osobowych.

Informacje powinny być udzielane na piśmie, elektronicznie lub ustnie. Dla zasady rozliczalności (innej, bardzo ważnej w kontekście RODO), najbardziej pożądaną formą będzie pisemna oraz elektroniczna, czyli np., poprzez e-mail. To pozwala nam na dysponowaniem dowodem, że osoba, której dane dotyczą, została odpowiednio poinformowana o kwestiach z tym związanych.

Informacje oraz komunikacja i są **wolne od opłat** co oznacza, że RODO wprowadza jednoznaczny zakaz pobierania opłat w zamian za udzielenie informacji dotyczących danych osobowych.

Warto jeszcze spojrzeć na brzmienie dwóch motywów RODO: motyw 58, który brzmi: *„Zasada przejrzystości wymaga, by wszelkie informacje kierowane do ogółu społeczeństwa lub osoby, której dane dotyczą, były zwięzłe, łatwo dostępne i zrozumiałe, by były formułowane jasnym i prostym językiem, a w stosownych przypadkach, dodatkowo wizualizowane. Informacje te mogą być przekazywane w formie elektronicznej, na przykład za pomocą strony internetowej, gdy są kierowane do ogółu społeczeństwa. Dotyczy to w szczególności sytuacji, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że osobie, której dane dotyczą, trudno jest dowiedzieć się i zrozumieć, czy dotyczące jej dane osobowe są zbierane, przez kogo oraz w jakim celu, na przykład w przypadku reklamy w internecie.*

Zważywszy że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty – gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć." oraz motyw 59, który brzmi „ Należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy niniejszego rozporządzenia, w tym mechanizmy żądania – i gdy ma to zastosowanie bezpłatnego uzyskiwania – w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu. Administrator powinien zapewnić możliwość wnoszenia odnośnych żądań także drogą elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną. Administrator powinien być zobowiązany udzielić odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki – najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania – podać tego przyczyny."

W jakim języku mają zostać przedstawione informacje o przetwarzaniu danych osobowych?

Wobec coraz większej ilości mieszkających w Polsce obywateli innych państw, którzy niekoniecznie posługują się językiem polskim w sposób wystarczający do swobodnej komunikacji, niejednokrotnie pojawia się pytanie, w jakim języku przedstawiać informacje? Jak wskazuje Urząd Ochrony Danych Osobowych, RODO nie narzuca wprost formy, w tym języka, w jakim ma być sporządzona informacja czy też dokumentacja przetwarzania danych osobowych. To zatem – na ten moment - zależy od zaangażowania i otwartości administratora danych, jednak doświadczenie uczy, że zawsze trzeba uwzględniać obowiązki ciążące na administratorze na gruncie RODO.

Warstwowe stosowanie obowiązku informacyjnego.

Obowiązek informacyjny może być też stosowany w sposób warstwowy – takie rozwiązanie dopuszcza Urząd Ochrony Danych Osobowych, a pozwala nam ono na ograniczenie ilości informacji (np. tekstu), z którym musi zapoznać się osoba, której dane dotyczą. W takim przypadku administrator podaje najważniejsze informacje dotyczące przetwarzania danych, tj. tożsamość administratora, cele przetwarzania i prawa osób, których dane dotyczą, a następnie odsyła – np. w formie linku, do pełnej treści klauzuli informacyjnej, tj. najczęściej na stronę internetową i zamieszczoną tam politykę prywatności. Takie rozwiązanie często stosowane jest w stopkach e-mail lub na budynkach.

<u>Czy za nieprzestrzeganie zasady przejrzystości grozi jakaś kara?</u>

Podobnie jak przy naruszeniu innych obowiązków określonych w RODO, tak i tutaj, naruszenie wiąże się z odpowiedzialnością administratora w postaci kary pieniężnej.

Reasumując powyższe:
Starajmy się przekazywać informacje dotyczące przetwarzania danych osobowych w sposób jasny, jak najprostszy, bez skomplikowanej budowy zdania, odesłań, wielości informacji. Jak się okazuje, nie zawsze więcej oznacza lepiej.

Autor:
Justyna Cybulska
zespół Inspektora Ochrony Danych
adwokat

IV. Przetwarzanie danych osobowych w sferze zatrudnienia.

W kilku kolejnych artykułach skupię się na przetwarzaniu danych osobowych **w sferze zatrudnienia.** Pomysł ten pojawił się z uwagi na fakt, że w swojej pracy dostaję wiele pytań od rekruterów czy działów HR – jak przetwarzać dane pracowników lub kandydatów do pracy? Które dane można przetwarzać? Jakie dane i dokumenty można przechowywać i jak długo? Mam więc nadzieje, że ten i kolejne artykuły, rozwieją wątpliwości i będą stanowić dla Państwa pewne wskazówki, jak postępować z danymi pracowników i kandydatów do pracy.

Dzisiaj skupmy się na **danych wrażliwych (konkretnie na danych dotyczących zdrowia) w rekrutacji** – czy w ogóle możemy je przetwarzać?

Na początek przypomnijmy sobie, które dane są **danymi wrażliwymi.**

Zwykłe dane osobowe

Te, które nie są danymi wrażliwymi w rozumieniu art. 9 RODO, tj. m. in imię, nazwisko, PESEL, adres zamieszkania/adres zameldowania, numer i seria dowodu tożsamości, numer telefonu, adres Login, Nick, pseudonim, adres e-mail (jeśli składa się na niego imię i nazwisko).

Wrażliwe dane osobowe (szczególnych kategorii)

Te, o których mowa w art. 9 RODO: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne (czyli takie, które przy użyciu specjalnej techniki prowadzą lub mogą prowadzić do identyfikacji osoby, np. stosowanie programu do rozpoznawania twarzy), dane dotyczących zdrowia, seksualności lub orientacji seksualnej.

W trakcie procesu rekrutacji przetwarzamy wiele danych osobowych kandydatów do pracy, którzy aplikują na określone stanowisko. Z uwagi na powyższe, trzeba zadbać, aby proces rekrutacji zapewniał ochronę danych nam przekazywanych i był prowadzony zgodnie z przepisami prawa o ochronie danych, w tym RODO. Pracownicy działów HR, niejednokrotnie nie wiedzą, jak postępować w sytuacji, kiedy kandydat do pracy przekazuje nam w swojej aplikacji na stanowisko znacznie więcej danych i bardziej szczegółowe, niż to potrzebne i wymagane przez pracodawcę.

Jakie dane można przetwarzać w procesie rekrutacji?

O tym, jakie dane można pozyskiwać w procesie rekrutacji stanowi art. 22(1) § 1 Kodeksu pracy. Zakres ten obejmuje: imię (imiona) i nazwisko, datę urodzenia, dane kontaktowe wskazane przez daną osobę, wykształcenie, kwalifikacje zawodowe, przebieg dotychczasowego zatrudnienia. Jeżeli decydujemy o uzyskaniu od kandydata także innych danych, konieczne jest, aby wykazać, że mamy podstawę prawną takiego żądania. Pracodawca może pozyskiwać innego rodzaju dane o przyszłym pracowniku wyłącznie wtedy, kiedy istnieje przepis prawa umożliwiający powyższe.

Wątpliwości pojawiają się także wówczas, kiedy kandydat aplikuje na stanowisko na podstawie umowy cywilnoprawnej (np. umowy o dzieło lub zlecenie), a nie na podstawie umowy o pracę. Jakkolwiek nie ma żadnych przepisów regulujących jakie dane wówczas pracodawca może pobierać, to praktyka pokazała, że to właśnie Kodeks pracy stanowi wskazówki, które można wykorzystać także i w tej sytuacji.

W każdym przypadku należy pamiętać o zasadzie minimalizmu danych wynikającej z art. 5 RODO. Im mniej danych, tym lepiej, czyli zbieramy tylko takie dane, jakie są niezbędne do osiągnięcia konkretnego celu ich przetwarzania.

Podstawa prawna przetwarzania danych wrażliwych (dotyczących zdrowia) kandydata do pracy – zgoda czy przepis prawa?

Zgodnie z art. 9 ust. 1 RODO, powołanym w wyżej przedstawionym wykresie, co do zasady zabrania się przetwarzania danych osobowych wrażliwych. Z katalogu danych, które przedstawia nam ww. przepis, w procesie rekrutacji najczęściej mogą pojawiać się dane dotyczące zdrowia, szczególnie wówczas, kiedy zatrudniona ma zostać osoba w jakimś stopniu niepełnosprawna. W tracie takiej rekrutacji, kandydat do pracy może przedkładać różnego rodzaju zaświadczenia, z których wynika stan jego zdrowia i stopień niepełnosprawności.

Pochylmy się przez chwilę nad art. 2b ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych:

Art. 2b. 1. Pracodawca przetwarza dane osobowe, w tym dane o stanie zdrowia osób (...)

2) niepełnosprawnych wykonujących pracę nakładczą,

2. Przedstawienie pracodawcy dokumentów potwierdzających dane osobowe o stanie zdrowia jest dobrowolne.

Na przykładzie tego przepisu pojawia się pytanie, czy pracodawca powinien uzyskać zgodę na przetwarzanie danych osobowych wrażliwych w postaci danych o zdrowiu, świadczących o niepełnosprawności? Odpowiedź brzmi – nie. Podstawą prawną nie będzie zgoda, a przepis prawa. Jeśli kandydat decyduje się przedstawić dokumenty wskazujące na jego zdrowia, robi to dobrowolnie, ale na podstawie przepisów prawa, które dają pracodawcy prawo do ich przetwarzania. Jednocześnie, jak podkreśla Prezes UODO, przedstawienie orzeczenia jest konieczne do przyznania osobie z niepełnosprawnością ulg i świadczeń z tego tytułu, odpowiedniego dostosowania miejsca pracy bądź przyznania jej pierwszeństwa.

Dalej idąc, art. 22 (1 b) Kodeksu pracy mówi, że:

Art. 221b. *[Warunki przetwarzania przez pracodawcę innych danych osobowych]*

§ 1. Zgoda osoby ubiegającej się o zatrudnienie lub pracownika może stanowić podstawę przetwarzania przez pracodawcę danych osobowych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika. Przepis art. 221a § 2 stosuje się odpowiednio.

Przepis powyższy stanowi zatem jasno, że zgoda na przetwarzanie danych wrażliwych (w naszym przypadku danych o zdrowiu) jest podstawą do ich przetwarzania (czyli pracodawca może się powołać na zgodę – art. 6 ust. 1 lit. a RODO, jednocześnie jednak musi zadbać o uzyskanie takiej zgody najlepiej pisemnie/elektronicznie, aby wypełnić zasadę rozliczalności) jedynie wówczas, kiedy inicjatywa ich przekazania jest po stronie kandydata do pracy a jednocześnie nie ma przepisów, z których – dla uzyskania pewnych korzyści, jak np. ulgi, świadczenia, wynikałaby konieczność przedstawienia takich danych. Trzeba zatem podkreślić, że jeśli w toku prowadzonej rekrutacji zdarzy się, że kandydat z własnej inicjatywy przekaże pracodawcy dane osobowe wrażliwe, np. o swoim stanie zdrowia, powinien on wyrazić odrębną zgodę na przetwarzanie tego rodzaju danych osobowych, chyba że możliwość ich przetwarzania przez pracodawcę wynika z przepisów prawa, jak w przypadku zatrudniania pracowników z niepełnosprawnościami.

Wymóg uzyskania zgody w formie oświadczenia wynika wprost z art. 9 ust. 2 RODO, zgodnie z którym zgoda na przetwarzanie szczególnych kategorii danych powinna być wyraźna, np. w formie odrębnego oświadczenia.
Jeżeli pracodawca nie uzyskał zgody na przetwarzanie danych wrażliwych, a otrzyma je w procesie rekrutacji od kandydata – oczywiście w sytuacji, kiedy nie mamy przepisu prawa, który mówiłby o konieczności przedstawienia takich danych dla osiągnięcia pewnego rodzaju korzyści, pracodawca powinien dane te niezwłocznie usunąć.
Przykład:
Pan Jan składa CV na stanowisko sprzedawcy biletów (praca siedząca, bez szczególnych wymagań). W ogłoszeniu o pracę, brak jest informacji dotyczących poszukiwania pracowników z niepełnosprawnościami. Pan Jan jednak, lubi o sobie opowiadać, dlatego przedstawia w CV informacje o swoim stanie zdrowia (o przebytej operacji kolana, o zdiagnozowanej cieśni nadgarstka, o zasiłkach i świadczeniach pobieranych niegdyś z uwagi na swój stan zdrowia), dołączając (dla wykazania swojej prawdomówności) dokumenty – zaświadczenia lekarskie i decyzje o zasiłkach/świadczeniach). Pan Jan jednocześnie nie składa żadnego oświadczenia o zgodzie na przetwarzanie danych dotyczących zdrowia w procesie rekrutacji.

Co pracodawca powinien zrobić z takimi dokumentami i danymi osobowymi?
Z powodu braku przepisu prawa, z którego wynikałaby konieczność przedstawienia danych dotyczących zdrowia, a także z uwagi na brak odrębnego oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych dotyczących zdrowia przez pracodawcę, pracodawca powinien usunąć dokumenty i zanonimizować te konkretne dane w CV, tak, aby ich dalsze przetwarzanie nie było możliwe. Nie ma bowiem podstawy prawnej do przetwarzania tego rodzaju danych.

Upoważnienie do przetwarzania danych wrażliwych.
Jak wiemy, niezwykle ważna kwestia w kontekście przetwarzania i zapewnienia ochrony danych osobowych, to upoważnienia do przetwarzania danych nadawane przez pracodawcę pracownikom. Jeśli chodzi o przetwarzanie danych osobowych wrażliwych, to obowiązek posiadania przez pracownika, który dane te przetwarza (tutaj biorącego udział w procesie rekrutacji) upoważnienia, wynika wprost z Kodeksu pracy (art. 22 1 b ust. 3), a nie tylko z praktyki RODO. Zgodnie z tym przepisem, do przetwarzania danych wrażliwych mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych, wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są oczywiście obowiązane do zachowania ich w tajemnicy.

Reasumując.

W procesie rekrutacji pracodawca może przetwarzać dane wrażliwe – np. dane dotyczące zdrowia, jednak musi legitymować się ważną podstawa prawną co do tego. Taką podstawa **mogą być przepisy prawa**, ale może to być **również zgoda** udzielna przez samego kandydata. Jeśli możliwość przetwarzania danych osobowych wrażliwych wynika z przepisów prawa, zgoda nie jest potrzebna, ale jeśli możliwość przetwarzania nie wynika z przepisów prawa, wówczas taka zgoda jest niezbędna.

W każdej sytuacji należy podchodzić do przetwarzania wrażliwych danych z dużą dozą ostrożności i przeprowadzić analizę, czy legitymujemy się podstawą prawa, aby to robić, tym bardziej, że kandydaci do pracy w swoich CV niekiedy umieszczają różne „ciekawostki", które niestety powodują dodatkowe obowiązki po stronie pracodawcy jako administratora.

Autor:
Justyna Cybulska
zespół Inspektora Ochrony Danych
adwokat

V. Aplikacja mObywatel 2.0 i dokument mObywatel.

14 lipca weszła w życie ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz.U. poz. 1234 z późn. zm.) i od tego dnia możliwe jest pobieranie aplikacji mObywatel w wersji 2.0. Aplikacja jest dostępna w sklepach Google Play i App Store, a więc obsługuje dwa najbardziej popularne systemy operacyjne wykorzystywane w urządzeniach mobilnych. Aplikacja jest przedstawiana jako asystent obywatela, który ma sprawić, że załatwianie spraw urzędowych będzie prostsze i wygodniejsze. Dzięki wprowadzonym rozwiązaniom użytkownik ma mieć dostęp do niektórych swoich dokumentów i móc załatwić wybrane sprawy urzędowe bez wychodzenia z domu.

Najważniejszą nowością w aplikacji jest możliwość korzystania z dokument mObywatel, nazywanego też mDowodem. Zgodnie z definicją ustawową dokument mObywatel jest mobilnym dokumentem stwierdzającym tożsamość i obywatelstwo polskie użytkownika aplikacji, którym można się posługiwać na terytorium Rzeczypospolitej Polskiej w relacjach wzajemnej fizycznej obecności stron. Dokument mObywatel pod wieloma względami przypomina dowód osobisty. W szczególności zawiera on podobny zakres danych użytkownika, w tym: nazwisko i imię (imiona), numer PESEL, datę urodzenia, obywatelstwo, imię ojca, imię matki, a także fotografię użytkownika, która jest pobierana z Rejestru Dowodów Osobistych oraz numer, serię, datę wydania i termin ważności. Dokument mObywatel nie jest jednak cyfrową wersją dowodu osobistego i nie może być z nim utożsamiany. Jego seria, numer, data wydania i data ważności nie pokrywają się z danymi dowodu osobistego. Jest to samodzielny dokument tożsamości, którym można posługiwać się niezależnie od posiadanego dowodu osobistego i większości przypadków zamiast niego.

Korzystanie z dokumentu mObywatel jest dobrowolne i nieodpłatne. Nie istnieje prawny obowiązek posiadania i posługiwania się dokumentem mObywatel. Przepisy nakładają natomiast obowiązek akceptowania dokumentu mObywatel jako pełnoprawnego sposobu stwierdzenia tożsamości i obywatelstwa polskiego jego posiadacza. Ustawa przewiduje bowiem, że jeżeli z przepisu prawa wynika obowiązek stwierdzenia tożsamości lub obywatelstwa polskiego na podstawie dokumentu tożsamości, w szczególności na podstawie dowodu osobistego, obowiązek ten uznaje się za spełniony w przypadku stwierdzenia tożsamości lub obywatelstwa polskiego na podstawie dokumentu mObywatel. Posiadacz dokumentu mObywatel sam

decyduje czy w danej sytuacji będzie posługiwał się tym dokumentem czy też innym dokumentem potwierdzającym tożsamość.

Dokumentem mObywatel można posługiwać się zarówno w relacjach pomiędzy osobami prywatnymi (obrocie nieprofesjonalnym i profesjonalnym), jak i w sprawach urzędowych przed organami administracji publicznej i sądami. Nie może on być natomiast wykorzystywany w przypadku wnioskowania o nowy dowód osobisty oraz przy przekraczaniu granicy Rzeczypospolitej i poza jej granicami. Obecnie mDowód nie może być wykorzystywany także do stwierdzenia tożsamości przez instytucje obowiązane w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124), a więc m.in. przez banki. Instytucje te będą zobowiązane stosować przepisy regulujące wykorzystywanie mDowód do identyfikacji i weryfikacji tożsamości klienta od dnia 1 września 2023 r. i wówczas będzie można posługiwać się nim w kontaktach z tymi instytucjami.

Potwierdzenie tożsamości za pomocą dokumentu mObywatel następuje poprzez okazanie dokumentu, a więc podobnie jak w przypadku tradycyjnych dokumentów. Jedyną różnicą jest to, że dokument wyświetla się w aplikacji mObywatel uruchomionej na urządzeniu mobilnym posiadacza.

datę urodzenia, obywatelstwo, imię ojca, imię matki, a także fotografię użytkownika, która jest pobierana z Rejestru Dowodów Osobistych oraz numer, serię, datę wydania i termin ważności. Dokument mObywatel nie jest jednak cyfrową wersją dowodu osobistego i nie może być z nim utożsamiany. Jego seria, numer, data wydania i data ważności nie pokrywają się z danymi dowodu osobistego. Jest to samodzielny dokument tożsamości, którym można posługiwać się niezależnie od posiadanego dowodu osobistego i większości przypadków zamiast niego.

Osoba, której okazywany jest dokument może sprawdzić jego autentyczność jedną z trzech metod: wizualną, funkcjonalną lub kryptograficzną. Podstawowym sposobem sprawdzania autentyczności dokumentu jest zastosowanie metody wizualnej. Polega ona na sprawdzeniu poszczególnych elementów dokumentu, w tym m.in. fotografii; hologramu, który zmienia barwę przy poruszaniu smartfonem; daty ostatniej aktualizacji danych; zegara pokazującego aktualną datę i godzinę; elementu dynamicznego, czyli ruchomego elementu graficznego prezentującego białoczerwoną flagę; grafiki tła umieszczonego za danymi osobowymi. Wykorzystanie tej metody przypomina bardzo weryfikację tradycyjnego dokumentu. Metoda funkcjonalna polega na okazaniu przez posiadacza osobie sprawdzającej wybranych funkcjonalności aplikacji

mObywatel, np. przez wyświetlenie certyfikatu, uruchomienie określonej funkcji, lub określonej zakładki. O sposobie przeprowadzenia weryfikacji tą metodą, w szczególności o zakresie funkcji, które zostaną sprawdzone i kolejności ich sprawdzenia (tzw. scenariusz weryfikacji) decyduje osoba, która dokonuje sprawdzenia.

Metoda ta ma pozwolić przede wszystkim na potwierdzenie, że okazane sprawdzającemu dane są wyświetlane w aplikacji mObywatel, a nie np. jako zrzut ekranu albo zdjęcie. Metoda kryptograficzna polega na sprawdzeniu integralności danych okazanego dokumentu za pomocą odpowiedniej funkcji w aplikacji mObywatel. Proces sprawdzania polega w tym przypadku na wygenerowaniu przez osobę sprawdzającą przy pomocy aplikacji mObywatel kodu QR, który przy wykorzystaniu analogicznej funkcji jest skanowany przez osobę, której dokument podlega sprawdzeniu. Po zeskanowaniu kodu w aplikacji osoby sprawdzającej wyświetla się informacja o potwierdzeniu dokumentu i dane osoby sprawdzanej.

Nie ma obowiązku każdorazowego używania wszystkich trzech metod. Do sprawdzenia tożsamości i weryfikacji dokumentu mObywatel może być wystarczające zastosowanie nawet tylko jednej z nich. Wyboru metody dokonuje osoba dokonująca sprawdzenia.

W praktyce w pierwszej kolejności powinna być zawsze stosowana metoda wizualna. W zdecydowanej większości przypadków będzie ona całkowicie wystarczająca to potwierdzenia tożsamości posiadacza mDokumentu i weryfikacji autentyczności tego dokumentu. W przypadku, gdyby zastosowanie tej metody było niewystarczające należy skorzystać z metody funkcjonalnej, która w istocie jest rozwinięciem pierwszej metody i sprowadza się od wzrokowego sprawdzenia działania innych funkcji aplikacji mObywatel. Najdalej idącą ostrożność należy zachować przy korzystaniu z metody kryptograficznej. Z uwagi na zasadę minimalizacji przy przetwarzaniu danych osobowych i bardziej złożony proces przetwarzania danych, w tym w szczególności na występujący przy tej metodzie element wyświetlania danych osoby sprawdzanej na urządzeniu osoby sprawdzającej po metodę tę należy sięgać dopiero wtedy, gdy pozostałe sposoby okażą się niewystarczające.

W przypadku stosowania metody kryptograficznej do celów służbowych (m.in. przez pracowników urzędów administracji publicznej) może pojawić się problem używania do weryfikacji aplikacji mObywatel zainstalowanej w prywatnym urządzeniu osoby sprawdzającej. Z informacji przekazywanych przez Ministerstwo Cyfryzacji wynika, że

aby zweryfikować tożsamość obywatela, który chce posłużyć się mDowodem, urzędnik musi mieć zainstalowaną na swoim smartfonie aplikację mObywatel. Wypowiedź ta sugeruje, że pracownicy urzędów administracji publicznej mogą, a nawet powinni wykorzystywać do weryfikacji aplikacji zainstalowanych na prywatnych urządzeniach. Należy w tym zakresie zachować jednak daleko idącą ostrożność, wynikającą z potrzeby ochrony prywatności tak osoby, której tożsamość jest weryfikowana, jak i urzędnika, który takiej weryfikacji dokonuje. Wydaje się, że mogą tu pojawić się takie same zastrzeżenia jak w przypadku stosowania do celów służbowych profilu zaufanego. Zastrzeżenia takie zgłasza od pewnego czasu Rzecznik Praw Obywatelskich, który kwestionuje dopuszczalność zobowiązania pracownika do założenia profilu zaufanego i wykorzystywania go do celów służbowych. Wątpliwości te zdaje się podzielać także Prezes Urzędu Ochrony Danych Osobowych, który po interwencji Rzecznika Praw Obywatelskich wszczął z urzędu postępowanie administracyjne w sprawie naruszenia przez Głównego Inspektora Sanitarnego art. 5 ust. 1 lit. a, lit. c RODO, polegającego na braku podstaw prawnych do żądania, aby pracownik uwierzytelniał się w systemie wykorzystywanym przez pracodawcę do realizacji jego zadań, przy użyciu profilu zaufanego.

Postępowanie to nie zostało jeszcze zakończone, ale nie można wykluczać, że Prezes Urzędu Ochrony Danych Osobowych zakwestionuje praktykę wykorzystywania w działalności administracji publicznej profilu zaufanego, a co za tym idzie również innych opartych na podobnych zasadach rozwiązań.

W kontekście tych wątpliwości warto zwrócić uwagę na przewidzianą w ustawie aplikację mWeryfikator, która w założeniu ustawodawcy ma służyć do sprawdzania integralności danych okazanego dokumentu metodą kryptograficzną. Aplikacja ta jest dostępna, jednak w chwili obecnej nie pozwala ona na weryfikację dokumentu mObywatel, gdyż nie umożliwia generowania kodów QR, niezbędnych takiej weryfikacji, a jedynie na ich skanowanie. Jej funkcjonalność jest zatem odwrócona w stosunku do aplikacji mObywatel. W tej chwili nie da się określić kiedy i czy w ogóle ten stan rzeczy ulegnie zmianie.

Wprowadzenie mDowodu to z pewnością krok w dobrym kierunku, jednak jak widać jest to jeszcze narzędzie niedopracowane i nie w pełni funkcjonalne. Posługując się mDowodem, a zwłaszcza wykorzystując go do weryfikacji tożsamości innych osób warto zachować ostrożność i pamiętać o zasadach i ograniczeniach, które wynikają z przepisów o ochronie danych osobowych.

Autor:
Grzegorz Lubeńczuk
zespół Inspektora Ochrony Danych
doktor, radca prawny

VI. Jak powinna wyglądać zgoda na przetwarzanie danych osobowych?

Zgoda jest tylko jedną z możliwych podstaw przetwarzania danych osobowych. Administrator nie musi (a nawet nie powinien) uzyskiwać zgody jeśli dysponuje inną podstawą do przetwarzania danych osobowych, np. zobowiązują go do tego przepisy prawa, gdy jest to niezbędne do wykonania umowy lub, gdy przemawia za tym prawnie uzasadniony interes realizowany przez administratora lub przez stronę trzecią. Zgoda wydaje się jednak najbardziej powszechną, a z całą pewnością najbardziej charakterystyczną podstawą przetwarzania danych osobowych. Przepisy o ochronie danych osobowych, w tym w szczególności przepisy RODO są przez wiele osób kojarzone właśnie z koniecznością uzyskania lub wyrażenia zgody. Jednocześnie pojawia się wiele pytań o formę tej zgody. W praktyce stosowane są bardzo różne, niekoniecznie prawidłowe rozwiązania. Jak więc powinna wyglądać prawidłowo wyrażona zgoda na przetwarzanie danych osobowych?

<u>Zgoda musi być wyraźna</u>

Zgodnie z art. 4 ust. 1 RODO zgoda 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. W kontekście formy zgody, przepis ten przesądza, że zgoda musi być wyrażona w sposób wyraźny i jednoznaczny. Nie może ona zatem być tylko dorozumiana i nie może polegać wyłącznie na braku sprzeciwu. Zgodnie z motywem 32 preambuły RODO milczenie lub niepodjęcie działania nie powinno oznaczać zgody. Treść wskazanego motywu znajduje swoje odzwierciedlenie w stanowisku Europejskiej Rady Ochrony Danych, zgodnie z którym samo kontynuowanie zwykłego korzystania ze strony internetowej nie jest zachowaniem, na podstawie którego można wywnioskować okazanie woli, polegające na wyrażeniu zgody na proponowaną operację przetwarzania (EROD, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, Wersja 1.1). Do wyrażenia zgody konieczne jest zatem podjęcie przez osobę, której dane dotyczą wyraźnego działania.

Zgoda nie musi być wyrażona na piśmie

Żaden przepis RODO nie wymaga uzyskania zgody osoby, której dane dotyczą na piśmie. Motyw 32 preambuły RODO wprost wskazuje, że oprócz formy pisemnej zgoda może mieć formę ustnego oświadczenia, może polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Administrator ma zatem dużą swobodę jeśli chodzi o wybór formy uzyskiwania zgody od osoby, której dane zamierza przetwarzać. Warto jednak pamiętać o obowiązującej na gruncie RODO zasadzie rozliczalności, zgodnie z którą to na administratorze spoczywa obowiązek wykazania, że prawidłowo przetwarza dane osobowe. Zasada ta znajduje swój wyraz m.in. w treści art. 7 ust. 1 RODO, zgodnie z którym, 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.

Teoretycznie administrator będzie mógł dowieść, że uzyskał zgodę na przetwarzanie danych osobowych za pomocą każdego środka dowodowego dopuszczonego prawem, np. powołując na tę okoliczność świadków, jednak mając na względzie treść art. 7 ust. 1 RODO należy rozważyć pozyskiwanie zgody właśnie w formie pisemnej, tak oby administrator dysponował dokumentem potwierdzającym uzyskanie zgody. W przypadku zbierania zgód w innej formie należy zalecić, aby administrator zadbał o odpowiednie udokumentowanie faktu ich wyrażenia (np. poprzez nagranie rozmowy, w czasie której zgoda została wyrażona w formie ustnej lub poprzez dysponowanie odpowiednimi zapisami w systemie informatycznym, gdy zgoda jest wyrażana poprzez zaznaczenie odpowiednich opcji na stronie internetowej).

Zgoda musi być odrębnym oświadczeniem

Art. 7 ust. 2 RODO stanowi, że jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Europejska Rada Ochrony

Danych wskazuje, że zapytanie o zgodę „powinno się wyraźnie odróżniać od pozostałych kwestii:. Jeżeli umowa na papierze obejmuje wiele aspektów niezwiązanych ze zgodą na wykorzystanie danych osobowych, kwestia zgody powinna zostać przedstawiona w wyraźnie odróżniający się sposób lub w odrębnym dokumencie. Podobnie, jeżeli o zgodę prosi się drogą elektroniczną, zapytanie o zgodę musi być odrębne i możliwe do odróżnienia – nie może to być po prostu jeden akapit (EROD, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, Wersja 1.1). Warto zwrócić też uwagę na stanowisko Naczelnego Sadu Administracyjnego, który stwierdza, że przekazanie danych nie jest drobną sprawą życia codziennego i nie ma do niej zastosowania art. 384 § 2 k.c., zgodnie z którym w razie gdy posługiwanie się wzorcem jest w stosunkach danego rodzaju zwyczajowo przyjęte, wiąże on także wtedy, gdy druga strona mogła się z łatwością dowiedzieć o jego treści, a czynności takiej nie konwaliduje późniejsze poinformowanie o treści regulaminu, ani możliwość zgłoszenia zastrzeżeń wobec pewnych form przetwarzania danych (wyrok NSA z dnia 04 kwietnia 2003 r., II SA 2135/02). Zgody na przetwarzanie danych osobowych nie można zatem uzyskać w drodze tej samej czynności co zawarcie umowy czy zaakceptowanie ogólnych warunków usługi.

Nie może ona stanowić elementu treści umowy lub regulaminu. Co do zasady nie należy też łączyć treści zgody z klauzulą informacyjną służącą realizacji obowiązku wynikającego z treści art. 13 i 14 RODO. W tym przypadku należy zadbać o przynajmniej wizualne rozdzielenie ich treści.

Treść zgody

Motyw 42 preambuły RODO wskazuje, że aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone. cele przetwarzania danych osobowych. Kierując się treścią motywu, tożsamość administratora oraz cel przetwarzania danych osobowych należy uznać za minimalną i niezbędną treść zgody na przetwarzanie danych osobowych.

Formułując treść zgody na przetwarzanie danych należy mieć na względzie także art. 7 ust. 3 RODO, który stanowi, że osoba, której dane dotyczą, zanim wyrazi zgodę powinna być poinformowana, że ma prawo w dowolnym momencie wycofać zgodę oraz, że wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Przepis ten nie przesądza o konieczności zamieszczenia w treści zgody informacji o możliwości jej

cofnięcia i jego skutkach, jednak mając na względzie zasadę rozliczalności, która w tym przypadku będzie obligowała administratora do wykazania w razie potrzeby, że przekazał taką informację osobie, której dane dotyczą przed wyrażeniem zgody, można rozważyć zawarcie takiej informacji w treści samej zgody.

Warto też zwrócić uwagę na stanowisko Naczelnego Sądu Administracyjnego, który zauważa, że zgoda nie może mieć charakteru abstrakcyjnego, lecz winna odnosić się do skonkretyzowanego stanu faktycznego, obejmując tylko określone dane oraz sprecyzowany sposób i cel ich przetwarzania (wyrok NSA z dnia 11 kwietnia 2003 r., sygn. akt II SA 3942/2004). Stanowisko to sugeruje, że w treści zgody należy wskazać dane osobowe, których zgoda ta ma dotyczyć lub przynajmniej podjąć próbę ich dookreślenia.

Obowiązek uzyskania wyraźnej zgody

W kilku przypadkach przepisy RODO nakładają na administratora obowiązek uzyskania wyraźnej zgody na przetwarzanie danych osobowych. Wyraźna zgoda jest wymagana, gdy pojawia się poważne ryzyko związane z ochroną danych, a zatem w sytuacjach, w których za właściwy uznaje się wysoki poziom indywidualnej kontroli nad danymi osobowymi. Wymóg uzyskania wyraźnej zgody dotyczy: przetwarzania danych wrażliwych (art. 9 RODO), zautomatyzowanego podejmowania decyzji, w tym profilowania (oraz w art. 22 RODO) oraz przekazywania danych do państw trzecich i organizacji międzynarodowych w przypadku braku odpowiednich zabezpieczeń (art. 45 w zw. z art. 44 RODO).

Konieczność uzyskania w tych trzech sytuacjach wyraźnej zgody oznacza konieczność zawarcia w treści zgody informacji, że dotyczy ona określonej kategorii lub określonego sposobu przetwarzania danych osobowych. Nie rodzi ona natomiast obowiązku uzyskania zgody w jakiejś szczególnej formie, w tym zwłaszcza nie skutkuje koniecznością uzyskania zgody w formie pisemnej. Jak wskazuje Europejska Rada Ochrony Danych wyraźną zgodę można uzyskać np. podczas rozmowy telefonicznej, pod warunkiem że informacje dotyczące wyboru są uczciwe, zrozumiałe i jasne i że organizacja zwraca się do osoby, której dane dotyczą, o konkretne potwierdzenie, np. naciśnięcie przycisku lub ustne potwierdzenie (EROD, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, Wersja 1.1)

„Wyrażam zgodę…"

Jako ciekawostkę, ale jednocześnie praktyczną wskazówkę przy formułowaniu treści zgody na przetwarzanie danych osobowych warto przywołać stanowisko Rzecznika Generalnego Trybunału Sprawiedliwości Unii Europejskiej, zgodnie z którym sformułowanie „przyjmuję do wiadomości, że informacje będą publikowane", nie jest tożsame z wyrażeniem jednoznacznej zgody na konkretny rodzaj szczegółowej publikacji i nie można go określić jako dobrowolne, konkretne wskazanie woli wnioskodawców zgodnie z definicją zgody osoby, której dane dotyczą (Opinia Rzecznika Generalnego przedstawiona w dniu 17 czerwca 2010 r., w sprawach połączonych C-92/09 i C-93/09 Volker und Markus Schecke GbR przeciwko Hesji). Jednocześnie Europejska Rada Ochrony Danych Osobowych wskazuje, że w treści zgody na przetwarzanie danych osobowych należy używać sformułowania: „Niniejszym wyrażam zgodę na przetwarzanie moich danych", a nie na przykład" „Rozumiem, że moje dane będą przetwarzane" (EROD, Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679, Wersja 1.1).

Podstawą RODO a nie ustawa o ochronie danych osobowych

Często spotykaną praktyką jest wskazywanie w treści zgody na przetwarzanie danych osobowych podstawy prawnej jej wyrażenia. Praktyka ta nie ma oparcia w obowiązujących przepisach prawa. Żaden przepis nie wprowadza wymogu, aby podstawę taką wskazywać. Jeżeli jednak administrator decyduje się na wskazanie podstawy prawnej wyrażenia zgody to trzeba pamiętać, że stanowią ją przepisy

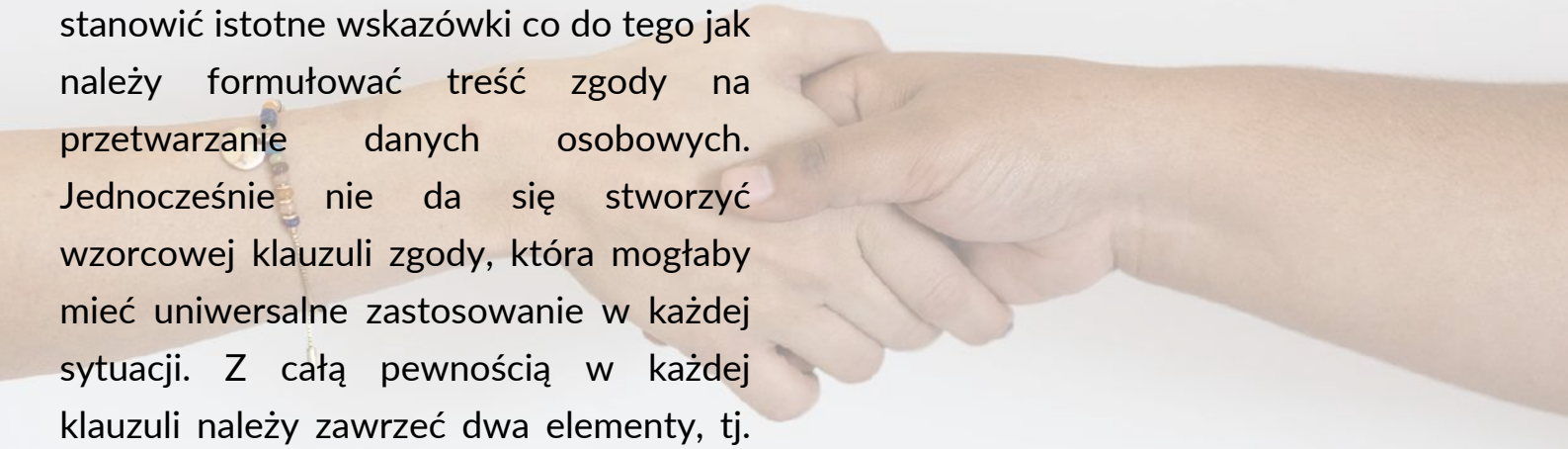
RODO a nie przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. Praktyka polegająca na wskazywaniu jako podstawy wyrażenia zgody i przetwarzania danych osobowych tej ustawy jest nieprawidłowa, gdyż jej przepisy nie odnoszą się do kwestii zgody, koncentrując się co do zasady na ustrojowych i proceduralnych podstawach działania Prezesa Urzędu Ochrony Danych Osobowych.

Uniwersalna treść zgody?

Powyższe informacje stanowią mogą stanowić istotne wskazówki co do tego jak należy formułować treść zgody na przetwarzanie danych osobowych. Jednocześnie nie da się stworzyć wzorcowej klauzuli zgody, która mogłaby mieć uniwersalne zastosowanie w każdej sytuacji. Z całą pewnością w każdej klauzuli należy zawrzeć dwa elementy, tj. określić administratora danych (a więc wskazać komu zgoda jest udzielana) i sprecyzować cel przetwarzania danych osobowych. Jeśli przepisy prawa wymagają uzyskania wyraźnej zgody, konieczne jest zawarcie w jej treści informacji o szczególnej kategorii przetwarzanych danych lub szczególnym sposobie ich przetwarzania.

Warto też rozważyć umieszczenie w treści klauzuli informacji o prawie cofnięcia zgody oraz w miarę możliwości określić zakres przetwarzanych danych. Jednocześnie cały czas trzeba pamiętać, że wymogiem, który wynika wprost z przepisów RODO jest sformułowanie zapytania o zgodę w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

Autor:
Grzegorz Lubeńczuk
zespół Inspektora Ochrony Danych
doktor, radca prawny



JUSTYNA JABŁONKA

KANCELARIA WYRZYKOWSCY

Inspektor Ochrony Danych,
adw. Justyna Jabłonka

www.justynajablonka.pl
www. kancelariawyrzykowscy.pl

BLOG dla JST:
https://kancelariawyrzykowscy.pl/pl/blog-jst/
FB:
https://www.facebook.com/kancelariawyrzykowscy