#3 GRUDZIEŃ 2020

PerIODyk

RODO I OCHRONA DANYCH OSOBOWYCH

Drodzy czytelnicy

Witamy Was przedświątecznie!

Michał Zajdowicz
Właściciel firmy Pharos

Nawet się nie obejrzeliśmy, a rok 2020 szybkimi krokami zbliża się ku końcowi. Rok, który był zupełnie inny od lat poprzednich, zdominowany przez pandemię koronawirusa, która wywróciła nasz dotychczasowy świat i stabilizację do góry nogami.

Każdy z nas odczuł skutki tej nowej rzeczywistości, w której przyszło nam żyć.

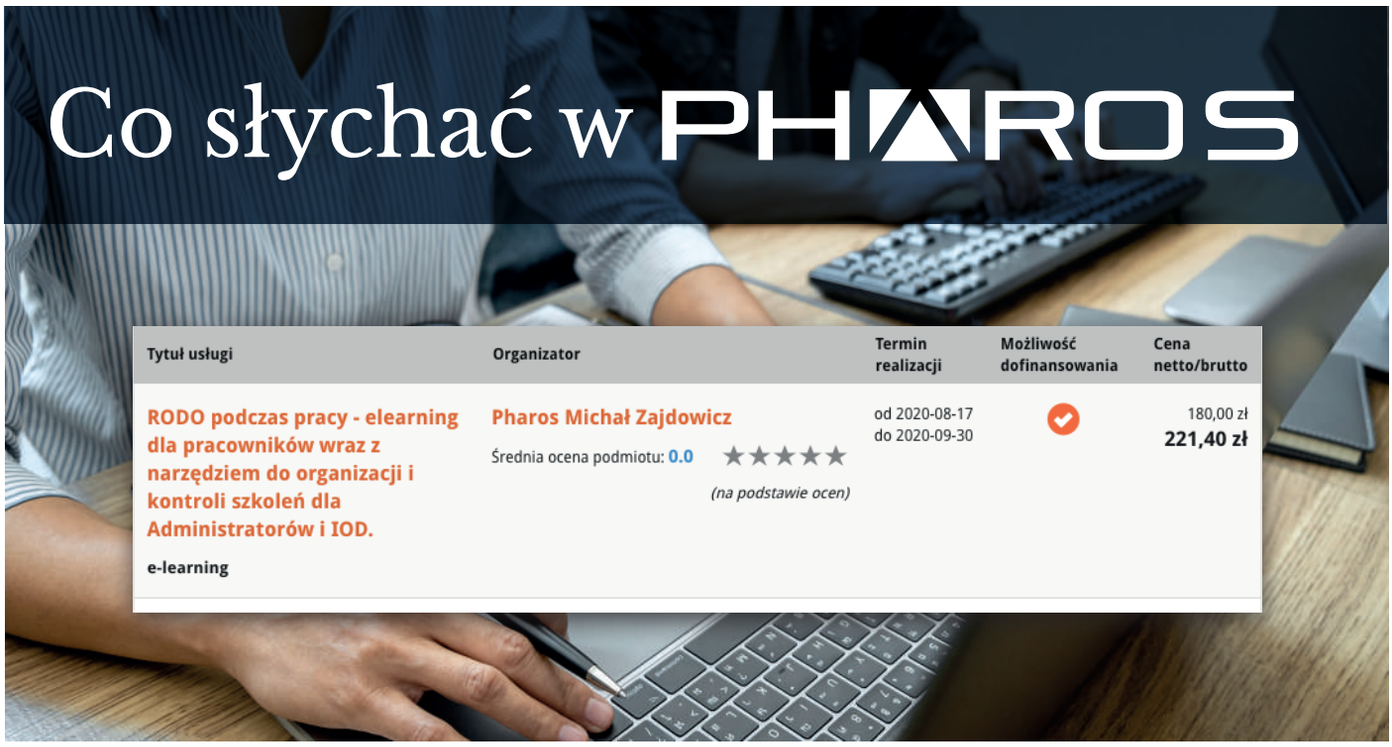
Jednak, mimo tej szczególnej sytuacji, nasze życie i nasza praca toczą się dalej. RODO, obok szalejącej pandemii, ma się dobrze i nie daje o sobie zapomnieć – pojawiają się nowe wytyczne, nowe interpretacje przepisów, a dla podmiotów nieprzestrzegających przepisów z zakresu ochrony danych osobowych nakładane są wciąż nowe kary i upomnienia.

Niestety nagłe rozprzestrzenianie się wirusa SARS-CoV-2 wymusiło pewne zmiany dotyczące stosowania RODO w organizacjach, o których wspominamy w tym numerze. Oprócz tego opisujemy także skutki wyroku TSUE w tzw. Sprawie „Schrems II", który znacznie skomplikował przekazywanie danych osobowych z terenu Europejskiego Obszaru Gospodarczego do USA. Z bieżącego numeru naszego pisma dowiedzą się Państwo dodatkowo, czy wysyłanie kartek pocztowych do naszych kontrahentów jest na pewno zgodne z RODO.

Życzę przyjemniej lektury naszego PerIODyka oraz Wesołych Świąt i wszystkiego dobrego w nadchodzącym 2021 Roku, aby był on zdecydowanie spokojniejszy i stabilniejszy, aniżeli obecny.

I nie zapominajmy o tym, że...

> **CHRONIMY DANE, KTÓRE SĄ WAM**



USŁUGI ROZWOJOWE SZANSĄ NA SUKCES.

✚ Elearning PHAROS już dostępny w BAZIE USŁUG ROZWOJOWYCH (BUR),

✚ Możesz uzyskać **do 80% dofinansowania** dla swoich pracowników na elearning oraz szkolenia stacjonarne z zakresu RODO!

Do Bazy Usług Rozwojowych (BUR) zostaliśmy wpisani dzięki pomyślnemu przejściu audytu jakości naszych usług i otrzymaniu Certyfikatu TGLS. Po co to wszystko? Wpis do BUR daje możliwość uzyskania przez naszych klientów dofinansowania do 80% kosztów szkolenia oraz elearningu. Od sierpnia 2020 r. można skorzystać w BUR z elearningu PHAROS "RODO podczas pracy - elearning dla pracowników wraz z narzędziem do organizacji i kontroli szkoleń przez Administratorów i IOD."
Szczegóły na stronie: pharos.pl/szkolenia-dofinansowane
lub uslugirozwojowe.parp.gov.pl/uslugi/view?id=594958

PO CO SZKOLIĆ PRACOWNIKÓW Z RODO?

Ochrona danych osobowych, tak samo jak ochrona tajemnicy przedsiębiorstwa stanowią wartość ekonomiczną. Baza danych osobowych wraz z rozwojem nowych technologii stanowi o wartości przedsiębiorstwa lub organizacji. Dane i informacje o klientach pozwalają na podnoszenie jakości usług oraz wybór najskuteczniejszych metod reklamowych.

DLA KOGO?

O dofinansownie mogą starać się przedsiębiorcy oraz organizacje, które chcą przeszkolić swoich pracowników.
Z ofert w BUR mogą korzystać zarówno firmy, jak i podmioty publiczne. Ważne, aby usługa była powiązana z celami rozwojowymi i przyczyniła się do realizacji celów biznesowych lub do podnoszenia kompetencji/kwalifikacji zatrudnionych pracowników. Procedury przyznawania środków oraz kryteria, takie jak wielkość dofinansowania oraz maksymalna kwota dofinansowania, różnią się w zależności od wielkości przedsiębiorstwa i województwa, w którym firma jest zarejestrowana.
Więcej informacji o zasadach udzielania wsparcia w danym regionie udzielają Punkty Informacyjne Funduszy Europejskich.
Swój punkt informacyjny znajdziesz na stronie funduszeeuropejskie.gov.pl/strony/o-funduszach/punkty/#/ oczywiście będziemy wpisywać w BUR, kolejne szkolenia. Bądź na bieżąco.
W razie pytań zadzwoń do Magdy pod numer +48 884 797 878! :)

Jak wysyłać życzenia świąteczne zgodnie z RODO?

Autor artykułu: **Magda Judejko**

JAK WYSYŁAĆ KARTKI I E- KARTKI ŚWIĄTECZNE ZGODNIE Z RODO?

+ **RODO nie dotyczy** prywatnych kartek. Życzenia do rodziny i znajomych możesz przesyłać dowoli
+ **RODO dotyczy** firm wysyłających kartki świąteczne

Wysyłanie życzeń świątecznych dość mocno przeniknęło na grunt biznesowy. Szczególnie w 2020 r. w czasie pandemii przedsiębiorcy chcą podtrzymać kontakt z partnerami biznesowymi oraz klientami. Czy wysyłanie kartek świątecznych jest zgodne z RODO? Ze względu na wiele wątpliwości pod koniec 2019 r. UODO wydał stanowisko, w którym podkreśla, że RODO nie ma zastosowania do przesyłania życzeń świątecznych pomiędzy członkami rodziny bądź znajomymi, ponieważ ma to charakter osobisty i domowy. Najwięcej wątpliwości budzi jednak wysyłanie życzeń do klientów i kontrahentów, z którymi prowadzi się współpracę biznesową.

DANE OSOBOWE DOTYCZĄ DANYCH OSÓB FIZYCZNYCH ORAZ PRZEDSIĘBIORCÓW.

Po wejściu w 2018 r. RODO podano w wątpliwość, czy dane przedsiębiorców wpisanych do CEIDG i KRS są chronione, ponieważ definicja danych osobowych mówi o osobach fizycznych. Według decyzji oraz stanowiska UODO definicja danych osobowych odnosi się do osób fizycznych bez względu na rolę, jaką odgrywają (czy są konsumentami, przedsiębiorcami czy pracownikami itd.). Z tego wynika, że podejmując działania B2B, w tym przesyłając kartki świąteczne dla klientów i partnerów, należy posiadać zgodę oraz informować o zasadach ochrony danych osobowych.

UWAGA!

Email biuro@pharos.pl lub Święty Mikołaj sp. z o.o. ul. Szczepankowo 5, 61- 233 Poznań NIE JEST daną osobową i nie trzeba uzyskać zgody na wysłanie e-kartki.
Przy wysłaniu poczty na mzajdowicz@pharos.pl lub PHAROS Michał Zajdowicz, ul. Św. Michała 43, Poznań ze względu na użyte imię i nazwisko w adresie, ktre są danymi osobowymi należy mieć podstawę prawną np. zgodę na kontakt.

JAK PODTRZYMAĆ TRADYCJE WYSYŁAJĄC KARTKI

W SPOSÓB, KTÓRY NIE NARUSZA PRYWATNOŚCI I PRZEPISÓW RODO?

Bez względu na to, czy naszymi klientami są konsumenci, czy też przedsiębiorcy, **warto w pierwszej kolejności ustalić, czy wysłanie kartki nie urazi klienta lub partnera**, a następnie sprawdzić **podstawę prawną do przesłania życzeń świątecznych.**

PODSTAWY PRAWNE DO WYSŁANIA KARTKI/E-KARTKI TZN. MAILINGU ŚWIĄTECZNEGO.

√ **Zgoda** (art. 6 ust. 1 lit. a RODO) powinna zostać wyrażona przez osobę, której dane dotyczą w sposób wyraźny, uprzedni, jednoznaczny i dobrowolny.

W praktyce oznacza to, że treść zgody powinna być napisana jasnym i zrozumiałym językiem, a co najistotniejsze, aby osoba wyrażająca zgodę miała możliwość wyraźnego jej zaznaczenia, np. w pustym "check box" pod Newsletterem.

√ **Uzasadniony interes administratora** - art. 6 ust. 1 lit. f RODO, co ciekawe, stanowisko UODO wskazuje, że przedsiębiorca może mieć uzasadniony interes w utrzymywaniu dobrych relacji biznesowych z klientami.

OBOWIĄZEK INFORMACYJNY

Podstawowym obowiązkiem przedsiębiorcy – administratora danych osobowych jest przekazanie informacji o bezpieczeństwie ochrony danych osobowych, najpóźniej w momencie pozyskania danych.

Klauzula informacyjna powinna zawierać:

- tożsamość i dane kontaktowe administratora,
- dane kontaktowe IOD (jeśli został powołany),
- cel przetwarzania,
- możliwość skorzystania ze swoich praw (dostępu, sprostowania, usunięcia, prawo sprzeciwu itp.)
- okres przechowywania,
- prawo wycofania zgody,
- prawo do sprzeciwu,
- prawo wniesienia skargi do organu nadzorczego.

PODSUMOWUJĄC

Wysyłając życzenia świąteczne warto zadbać o prywatność i ochronę danych swoich klientów. Zwróć uwagę, czy masz podstawę prawną do przesyłania kartki oraz zadbaj o klauzulę informacyjną, ponieważ **bez tego Twoja kartka/e-karta, która miała być wyrazem szacunku i pamięci, może stać się przedmiotem incydentu naruszenia ochrony danych osobowych**.

Dobra rada

Zwróć uwagę na to, aby wysyłając e-kartkę do wielu odbiorców **ukryć adresy email** (UDW - ukryte do wiadomości).

Z praktyki

Jeżeli posiadasz zgodę swojego klienta, partnera lub użytkownika na przesyłanie treści marketingowych i informacji handlowych lub newslettera, **możesz przesłać e-kartę lub kartkę świąteczną** swoim klientom.

Z praktyki

Możesz wysłać e-kartkę lub kartkę do klienta, wobec którego świadczyłeś usługi lub sprzedałeś produkty bez wyraźnej zgody na podstawie uzasadnionego interesu administratora, jednakże musisz wypełnić obowiązek informacyjny, w którym zaznaczysz m.in. prawo klienta do sprzeciwu.

Uwaga

Jeżeli wcześniej informowałeś klientów/partnerów, że ich dane będziesz przetwarzał w celu przesyłania korespondencji poprzez wiadomości e-mail lub tradycyjną pocztą, **nie musisz dołączać klauzuli** do kartki/e-kartki świątecznej.

Koronawirus – czy pracodawca może ujawnić dane osoby zakażonej?

Autor artykułu: **Michał Zajdowicz**

9 MIESIĘCY PANDEMII ZA NAMI

Pandemia koronawirusa, z którą mamy do czynienia od marca b.r. postawiła nasze dotychczasowe życie na głowie. Zamykanie sklepów, miejsc kultury i rozrywki, ograniczenia w przemieszczaniu się, wszechobecne maseczki oraz ciągły strach o zdrowie swoje i najbliższych to nasza rzeczywistość, do której chcąc nie chcąc musieliśmy się przyzwyczaić.

Oczywiście tak nagłe i momentami drastyczne zmiany w codziennym funkcjonowaniu spowodowały także zmiany w przepisach, wymusiły na prawodawcach nowe rozwiązania, które – nie oszukujmy się – często wprowadzają jeszcze więcej chaosu i niepewności niż pomocy. W przypadku pandemii dane osobowe osób chorych, bądź będących na kwarantannie przetwarzane są w całkiem nowych – wcześniej nieznanych sytuacjach, dlatego przyjrzymy się w niniejszym artykule jednemu z bardziej dyskutowanych problemów związanych z danymi osobowymi i zgodności z przepisami RODO.

CZY W MOMENCIE STWIERDZENIA ZARAŻENIA WIRUSEM COVID-19 U PRACOWNIKA PRACODAWCA MOŻE UJAWNIĆ TĘ INFORMACJĘ INNYM PRACOWNIKOM?

W rzeczywistości przed pandemią odpowiedź byłaby jasna i jednoznaczna – w żadnym wypadku nie należy udostępniać takich informacji, gdyż mamy do czynienia z danymi szczególnych kategorii (wrażliwymi) dotyczącymi stanu zdrowia osoby fizycznej (zgodnie z art. 9 RODO).

Obecna sytuacja wymusza na nas jednak podejmowanie szczególnych, budzących wątpliwości metod postępowania. Temat, którym tutaj się zajmujemy, jest jednym z bardziej kontrowersyjnych i pociągnął za sobą – co nie dziwi – wiele dyskusji i niejednoznacznych, a czasem wręcz sprzecznych stanowisk.

STANOWISKO UODO

Wg Urzędu Ochrony Danych Osobowych (UODO), instytucji mającej dbać o bezpieczeństwo danych osobowych obywateli i wskazywać praktyczne rozwiązania na pojawiające się problemy związanych z przetwarzaniem danych, to służby sanitarne powinny wskazywać kierunki podejmowanych działań, nie pracodawcy.

Specustawa przyznaje bowiem Głównemu Inspektorowi Sanitarnemu (GIS) uprawnienie do wydawania decyzji, w których **może zobowiązać inne podmioty do przetwarzania danych i określić zasady takiego przetwarzania**.

Zdaniem UODO pracodawca powinien więc przedstawić kluczowe informacje służbom sanitarnym, które na podstawie dostępnych wiadomości i wiedzy epidemiologicznej mogą podjąć decyzje i wprowadzić odpowiednie rozwiązania. Widzimy tutaj jednoznacznie, że podawanie przez pracodawcę danych zakażonego pracownika stoi w sprzeczności z przepisami RODO.

Niestety w rzeczywistości nie jest to już tak oczywiste, bowiem wszystko miałoby sens, gdyby GIS po otrzymaniu takiej informacji od pracownika działał błyskawicznie, jednak wiemy, że czasem reakcja ze strony służb sanitarnych może trwać od kilku do kilkunastu dni. Po drugie, o ile łatwo odizolować grupę osób pracujących z zakażonym np. na jednym dziale, w dużej firmie, fabryce, to sprawa komplikuje się, gdy mamy do czynienia z niedużą organizacją, zatrudniającą od kilkunastu do kilkudziesięciu pracowników, a osoby takie przemieszczają się z jednego biura do drugiego. Co wtedy zrobić? Skierować na kwarantannę całą firmę? Niosłoby to za sobą wymierne straty dla pracodawcy.

BHP TO OBOWIĄZEK PRACODAWCY

Co jest najważniejsze w zakładzie pracy i związanym z tym zapewnieniem bezpieczeństwa wszystkim pracownikom? Pracodawca musi przede wszystkim dbać o przepisy BHP.
Do podstawowych obowiązków pracodawcy zgodnie z art. 94 Kodeksu Pracy (KP) należy m.in. zapewnienie bezpiecznych i higienicznych warunków pracy.

Pracodawca musi więc nie tylko zorganizować odpowiednie szkolenia dla pracowników, czy kierować ich na okresowe badania lekarskie, ale w obecnej sytuacji **realizacja tego obowiązku wiąże się także z wdrożeniem w zakładzie pracy szczególnych rozwiązań**, które pozwolą zminimalizować ryzyko rozprzestrzeniania się zakażeń. To oznacza nie tylko zapewnienie środków do dezynfekcji, czy przejście na pracę zdalną, o ile to możliwe.

Pracodawca powinien również informować pracowników o możliwości zakażenia w firmie, aby wirus dalej się nie rozprzestrzeniał. I tutaj dochodzimy do sytuacji, że **ujawnienie danych osobowych zakażonego pracownika nie musi być sprzeczne z RODO**.

STANOWISKO EROD

Przepisy RODO nie stoją na przeszkodzie zapewnieniu bezpieczeństwa w miejscu pracy. Przewodnicząca Europejskiej Rady Ochrony Danych (EROD) wydała oświadczenie odnoszące się do pandemii COVID-19. Jak wskazała:
Pracodawcy powinni informować pracowników o przypadkach COVID-19 i podejmować środki ochronne, ale nie powinni przekazywać więcej informacji niż jest to konieczne. W przypadkach, w których konieczne jest ujawnienie nazwiska pracownika, który zarażony jest wirusem (np. w kontekście profilaktyki), a prawo krajowe na to zezwala, pracownicy, których sprawa dotyczy, powinni zostać poinformowani z wyprzedzeniem.

W RODO znajdują się także podstawy prawne dopuszczające przetwarzanie danych osobowych bez uzyskania zgody m.in. w czasie pandemii. Przykładem może być wykorzystywanie tych danych, które są konieczne dla pracodawców ze względu na interes publiczny w dziedzinie zdrowia publicznego. Zgodnie z art. 6 i 9 RODO przetwarzanie danych mogłoby odbywać się także w celu ochrony żywotnych interesów osoby fizycznej, czy w celu spełnienia innego obowiązku prawnego.

STANOWISKO RPO

Zdaniem Rzecznika Praw Obywatelskich (RPO), dochodzimy tutaj do nieco innego, z opisywanym powyżej, stanowiska UODO.
Ujawnienie danych osobowych zakażonego pracownika jest możliwe zgodnie z art. 2092 KP. W przypadku wystąpienia zagrożenia dla zdrowia lub życia pracodawca ma obowiązek między innymi poinformować pracowników o tym zagrożeniu. Ciąży też na nim obowiązek podjęcia działań pozwalających na zapewnienie odpowiedniej ochrony. Takim działaniem może być nie tylko zabezpieczenie miejsca pracy, ale nawet ujawnienie możliwości zakażenia koronawirusem.

Taką informację pracodawca powinien jednak przekazywać jedynie tym pracownikom, którzy rzeczywiście mieli styczność z osobą zarażoną. Takie stanowisko pozostaje w zgodzie ze stanowiskiem EROD cytowanym wyżej. To na pracodawcy spoczywa odpowiedzialność za bezpieczeństwo zdrowia i życia pracownika. Jeśli zaobserwował u pracownika objawy koronawirusa, powinien zgłosić taki przypadek, ale także reagować na potrzeby w zakresie BHP. Obowiązany jest też dostosować środki do zmieniających się warunków pracy.

PODSUMOWANIE

Jak można zauważyć, mimo borykania się z codziennymi problemami związanymi z funkcjonowaniem w czasie pandemii i zapewnienia dalszej działalności firmy, pracodawca jest także skazany na podejmowanie trudnych decyzji – takich, które nie są jednoznacznie opisane i określone prawnie.

My naszym klientom zawsze zalecamy zachowanie zdrowego rozsądku – oczywiście w zgodzie z przepisami RODO, aby podstawowa działalność ich organizacji czy biznesu oraz bezpieczeństwo pracowników, za których są odpowiedzialni, nie zostało utrudnione czy wręcz sparaliżowane przez literalne podchodzenie do przepisów. Dlatego też skłaniamy się do cytowanego powyżej stanowiska RPO w kwestii podawania przez pracodawcę danych zakażonego pracownika.
To wszystko z zachowaniem zasad bezpiecznego przetwarzania danych osobowych i w granicach rozsądku, ale również, by zapewnić bezpieczeństwo pozostałym pracownikom, którzy mogli mieć kontakt z zakażoną osobą z pracy.

Autor artykułu: **Magda Judejko**

PRYWATNOŚĆ VS BIZNES

REWOLUCJA W TRANSFERZE DANYCH OSOBOWYCH UE-USA.

Jak orzekł Europejski Trybunał Sprawiedliwości (dalej TSUE) w lipcu 2020 r. w tzw. Schrems II (C-3111/18), standardowe klauzule umowne z Tarczy Prywatności UE-USA **nie mogą stanowić podstawy dla transferu danych osobowych** do Stanów Zjednoczonych.

Pomimo tego, że korzystamy z wielu rozwiązań technologicznych oferowanych przez dostawców z USA (serwisów, wtyczek, API), TSUE unieważniając Tarcze Prywatności skłania wszystkich do refleksji i działań zmierzających do zachowania równych standardów ochrony danych osobowych i naszej prywatności.

Orzeczenie Schrems II to rewolucja, która stawia prywatność oraz ochronę danych osobowych ponad realia biznesowe i potrzeby związane z przepływem danych osobowych.

Temat jest kluczowy dla ochrony prywatności obywateli UE, ponieważ prawo amerykańskie wymaga, aby spółka Facebook Inc. udostępniała dane osobowe swoich użytkowników amerykańskim organom, takim jak NSA i Federal Bureau of Investigation (FBI) (federalne biuro śledcze USA) w ramach programów nadzoru.

CO SIĘ ZMIENIŁO PO SCHREMS II?

Każdy administrator danych np. przedsiębiorca, burmistrz, czy prezes fundacji, gdy korzysta z usług lub technologii pochodzących z USA lub innych państw spoza UE, musi wykonać weryfikację, czy stopień ochrony danych jest przestrzegany w danym państwie trzecim.

6 KROKÓW DO BEZPIECZNEGO TRANSFERU DANYCH OSOBOWYCH OBYWATELI UE DO USA I PAŃSTW TRZECICH.

Europejska Rada Ochrony Danych osobowych opracowała wytyczne co do tego, jak dostosować się do nowej rzeczywistości i legalnie przekazywać dane.

Krok I Przeanalizuj umowy oraz narzędzia, których używasz. Zastanów się do jakich Państw może następować transfer danych. Wykonaj audyt oraz analizę ryzyka. Wypisz wszystkie narzędzia oraz umowy z firmami/organizacjami spoza UE.

Krok II Jeżeli okaże się, że korzystasz z systemów firm spoza UE, określ podstawę prawną. W relacjach biznesowych z firmami z USA pamiętaj, że tzw. Tarcza Prywatności straciła ważność.

Krok III Dokonaj oceny systemu prawnego państwa, z którym masz umowę lub z którego narzędzi/wtyczek korzystasz. Weź pod uwagę w szczególności, jaki dostęp do danych osobowych firm i organizacji mają organy publiczne.

Krok IV Wprowadź środki techniczne i organizacyjne wspierające ochronę prywatności i utrudniające dostęp do danych przez władze państw trzecich, np. szyfrowanie czy szkolenie dla pracowników.

Krok V Opracuj dodatkowe środki weryfikacji kontrahentów oraz wprowadź procedury bezpieczeństwa.

Krok VI Monitoruj zmiany w przepisach państw trzecich i na bieżąco dokonuj oceny ryzyka przekazania danych.

PODSUMOWANIE

Pomimo tych wytycznych, nadal jest więcej pytań niż odpowiedzi. Należy mieć jednak świadomość, że dane osobowe to podstawa do kierowania do nas odpowiednich komunikatów i to nie tylko reklamowych, a w dobie tak prężnego rozwoju nowych technologii powinniśmy szczególnie dbać o prywatność.

Ocena ryzyka związanego z dokonywaniem transferów danych osobowych jest kluczowa nie tylko w stosunku do Stanów Zjednoczonych, ale i innych państw trzecich. EROD pracuje nad wprowadzeniem kolejnych wytycznych, które mają ułatwić oraz ujednolicić ochronę prywatności obywateli UE podczas transferów.

Autorzy artykułu: **Jarosław Bartkowiak**
Grzegorz Król

Kary i upomnienia dla jednostek administracji publicznej.

Regulacje dotyczące ochrony danych osobowych zrewolucjonizowały postępowanie firm oraz jednostek administracji publicznej w obszarze zabezpieczenia przetwarzanych danych osobowych. Od ponad dwóch lat obowiązuje Rozporządzenie o ochronie danych osobowych (RODO) – **jakie skutki przyniosło wprowadzenie tej regulacji?** Czy dane osobowe są właściwie chronione? Czy nadal mamy problem z interpretacją tego ważnego dla nas przepisu prawnego? Kiedy zgoda jest odpowiednią podstawą prawną do przetwarzania danych osobowych?

Jednostki administracji publicznej mają w tym temacie o wiele łatwiej, do prawie każdej wykonywanej czynności dysponują stosowną podstawą prawną w postaci ustawy lub rozporządzenia. A jednak Urząd Ochrony Danych Osobowych (UODO) **nałożył dwie kary finansowe oraz jedno upomnienie** podmiotom z tego obszaru.

O pierwszej karze dla jednostki administracji publicznej pisaliśmy tutaj szerzej kilka miesięcy temu – dla porządku tylko przypomnimy, iż w wyniku kontroli prowadzonej przez UODO nałożono karę w wysokości 40 tys. zł na Urząd Miasta w Aleksandrowie Kujawskim.

Żyjemy w XXI wieku w dobie bardzo szybkiego postępu technologicznego oraz co za tym idzie wykorzystywania naszych danych osobowych na potrzeby tych technologii. Zarówno danych zwykłych, np.: imienia i nazwiska, numeru telefonu, adresu e-mail, jak i danych szczególnych kategorii, które potocznie nazywamy „danymi wrażliwymi" np.: informacji o naszym stanie zdrowia, poglądach politycznych, danych genetycznych, biometrycznych.

Nowe technologie i postęp pojawiają się także w jednostkach oświatowych. Generalnie ten fakt bardzo cieszy i napawa optymizmem, że nasza młodzież wchodzi w dorosłe życie bez kompleksów z powodu wykluczenia technologicznego.

KARA ZA PRZETWARZANIE DANYCH BIOMETRYCZNYCH W STOŁÓWCE

Niestety właśnie dane biometryczne, a dokładniej nieznajomość lub niedostosowanie do bieżących przepisów prawa, zwłaszcza do ustawy o ochronie danych osobowych oraz RODO były **przyczyną kolejnej wymierzonej kary.**

Prezes Urzędu Ochrony Danych Osobowych 18-02-2020 r. nałożył karę administracyjną w wysokości 20 tys zł na Szkołę Podstawową nr 2 w Gdańsku w związku z naruszeniem polegającym na przetwarzaniu danych biometrycznych dzieci podczas korzystania przez nie ze szkolnej stołówki. **Szkoła przetwarzała dane wrażliwe 680 dzieci bez podstawy prawnej**, mogąc jednocześnie zastosować inne formy identyfikacji uczniów. W tej sprawie trzeba podkreślić, że **przetwarzanie danych biometrycznych nie jest niezbędne dla osiągnięcia celu, jakim jest identyfikacja uprawnienia dziecka do odebrania obiadu**. Szkoła mogła przeprowadzić identyfikację za pomocą innych środków, które nie ingerują tak dalece w prywatność dziecka. Szkoła umożliwiała korzystanie z usług stołówki nie tylko za pomocą odcisku linii papilarnych, ale i karty elektronicznej lub na podstawie nazwiska i numeru umowy.

Zatem, w szkole istniały alternatywne formy identyfikacji uprawnienia dziecka do odebrania obiadu. Ponadto w ukaranej szkole, zgodnie z panującymi tam zasadami wydawania obiadów **uczniowie, którzy nie posiadali identyfikacji biometrycznej musieli przepuszczać wszystkich i oczekiwać na końcu kolejki**. Gdy wszyscy uczniowie z identyfikacją biometryczną weszli do stołówki, rozpoczynało się wpuszczanie pojedynczo uczniów bez identyfikacji biometrycznej. **Tego typu zasady zdaniem Prezesa UODO wprowadziły nierówne traktowanie uczniów i ich bezpodstawne zróżnicowanie**, ponieważ wyraźnie promowały uczniów posiadających identyfikację biometryczną. Ponadto w ocenie UODO wykorzystywanie danych biometrycznych w zestawieniu z celem, w jakim zostały one przetwarzane, było w istotny sposób nieproporcjonalne. System biometryczny identyfikuje te cechy, które są co do zasady niezmienne i niejednokrotnie (jak w przypadku danych daktyloskopijnych), niemożliwe do zmiany.

Z uwagi na unikalność i stałość danych biometrycznych, przekładających się na ich niezmienności w czasie, wykorzystywanie danych biometrycznych powinno odbywać się ze szczególną ostrożnością i rozwagą. **Należy zatem wskazać, że ewentualny wyciek danych biometrycznych skutkował będzie dużym ryzykiem naruszenia praw i wolności osób fizycznych. Odnosi się to w sposób szczególny do danych dzieci, bowiem podjęcie decyzji o udostępnieniu tego rodzaju danych dziecka przez opiekunów prawnych oraz ich ewentualny wyciek nie będzie możliwy do odwrócenia w czasie, nawet po osiągnięciu przez dziecko pełnoletności**.

NA JAKIEJ PODSTAWIE SZKOŁA PRZETWARZAŁA DANE

Ciekawym aspektem tej sprawy jest wyrażenie zgody jako podstawy prawnej przetwarzania danych osobowych. Szkoła w złożonych wyjaśnieniach wskazała, że przetwarzanie danych biometrycznych znajdowało oparcie w dobrowolnej zgodzie rodziców uczniów (opiekunów prawnych).

Zgodnie z art. 4 ust. 11 RODO **"zgoda" osoby, której dane dotyczą 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. Prawodawca unijny w motywie 43 RODO stwierdza jednak, że aby można było mówić o dobrowolności wyrażenia zgody, nie powinna stanowić ona ważnej podstawy prawnej przetwarzania danych osobowych w szczególności w sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem.

Zgodnie z art. 106 ustawy z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2019 r., poz. 1148) w celu zapewnienia prawidłowej realizacji zadań opiekuńczych, w szczególności wspierania prawidłowego rozwoju uczniów, szkoła może zorganizować stołówkę. W związku z tym stwierdzić należy, że podstawą przetwarzania jakichkolwiek danych osobowych dzieci w związku z realizacją tego zadania szkoły nie mogła być zgoda, ponieważ podstawą do przetwarzania danych osobowych dzieci w tym celu przez Szkołę jest art. 6 ust. 1 lit. e) RODO. Oznacza to, że Szkoła przetwarza dane osobowe ucznia na podstawie przepisów prawa, wykonując swoje ustawowe zadania. Nie potrzebuje zatem odrębnej zgody rodziców na przetwarzanie danych osobowych w związku z realizacją tych zadań, tj. świadczeniem usług przez stołówkę szkolną. **W takiej sytuacji zgoda Rodzica nie może być przesłanką legalizującą przetwarzanie danych biometrycznych, ponieważ zgoda stanowi podstawę legalizującą przetwarzanie danych osobowych jedynie wtedy, gdy nie istnieją inne przesłanki przetwarzania.**

KARA UPOMNIENIA DLA SZKOŁY ZA NIEWŁAŚCIWE ZBIERANIE DANYCH

Ankiety w szkołach to temat stary jak świat, ułatwiają pozyskiwanie wiedzy, pomagają w badaniu opinii, generalnie są bardzo pomocnym narzędziem. Jednak **z każdego narzędzia trzeba umiejętnie korzystać**, jedna ze szkół w Dęblinie przeprowadzając kontrowersyjną ankietę przekonała się o tym na własnej skórze. Sprawę naświetliła w październiku 2019 r. gazeta regionalna gdzie opisała zdarzenie, oraz ukazała kulisy sprawy, a także przedstawiła opinię lokalnej społeczności.

Między innymi w następstwie tych działań **Prezes UODO po zakończonym postępowaniu w czerwcu b.r. nałożył karę upomnienia** na Zespół Szkół Ogólnokształcących w Dęblinie (woj. lubelskie) **za przetwarzanie bez podstawy prawnej danych osobowych uczniów** w związku z przeprowadzeniem wśród nich w roku szkolnym 2019/2020 wywiadów pod nazwą „Diagnozowanie sytuacji domowej i szkolnej ucznia. Ankieta dla ucznia".

W ramach przeprowadzonej ankiety doszło do przetwarzania danych osobowych uczniów, w tym także danych osób niepełnoletnich, przede wszystkim ich imion i nazwisk, oznaczenie klasy, określenia opiekunów prawnych (rodziców), informacji o stanie rodziny (pełna, niepełna), a także informacji o śmierci opiekuna prawnego (rodzica), separacji opiekunów prawnych (rodziców), ich wykształceniu i sytuacji zawodowej, liczbie osób w gospodarstwie domowym, **sytuacji finansowej, stanie zdrowia oraz nałogach opiekunów prawnych (rodziców), sytuacji mieszkaniowej oraz o fakcie otrzymania pomocy finansowej.**

Według UODO szkoła przeprowadzając ankietę wśród uczniów, naruszyła zasadę, w myśl której dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Powyższa zasada została rozwinięta w treści art. 6 ust. 1 lit. c) RODO, zgodnie z którym przetwarzanie jest zgodne z prawem wyłącznie w przypadku, gdy – i w takim zakresie w jakim – spełniony jest warunek, iż przetwarzanie to jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Szkoła jako podmiot publiczny **może przetwarzać dane osobowe w zakresie wykonywanych przez niego zadań nałożonych ustawami**. Prawo oświatowe stanowi, że szkoły przetwarzają dane osobowe w zakresie niezbędnym dla realizacji zadań i obowiązków wynikających z tych przepisów. W aktach prawnych regulujących zasady funkcjonowania instytucji oświatowych, nie określa się takich zadań i obowiązków szkół, które uzasadniałyby przetwarzanie danych osobowych uczniów w sposób, w jaki uczyniono to w ukaranym podmiocie, a więc w związku z przeprowadzeniem ankiety. Ankietę przeprowadzono w celu zidentyfikowania uczniów, którzy wymagają udzielenia wsparcia psychologicznego przez szkołę. **Cel sam sobie był jak najbardziej pozytywny**, **natomiast dobór narzędzia i sposób realizacji niedopuszczalny**.

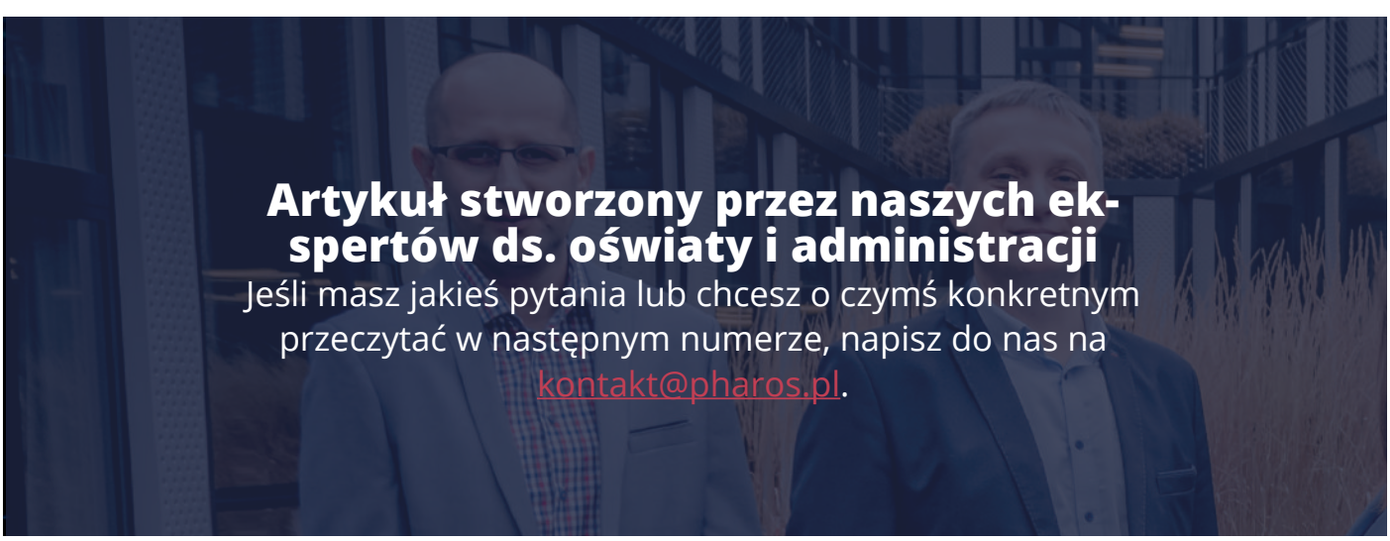
Po wnikliwej analizie i ustalonych okolicznościach tej sprawy Prezes UODO tym razem uznał, że wystarczającą sankcją będzie udzielenie kary upomnienia.

KOMPETENCJE INSPEKTORA OCHRONY DANYCH OSOBOWYCH JAKO ISTOTA

Liczba kar za naruszenia RODO w naszym kraju, jak w całej UE nie jest mała. Dotyczy to zarówno firm, jak i jednostek administracji publicznej, co niestety nie napawa optymizmem. **Czym to może być spowodowane?**

Ciągłym brakiem wiedzy, zrozumienia samego RODO? A może bardzo popularną u nas nadinterpretacją przepisów? **Jest też trzecie prawdopodobieństwo: jednostki administracji publicznej mają ograniczone finanse** i **często korzystają z pomocy „fachowców", firm, których jedynym atutem jest CCC czyli Cena Czyni Cuda**. Podmioty te oferują najniższą cenę za świadczenie usług Inspektora Ochrony Danych lub usług doradczych, niestety na tym dobre wiadomości dla jednostek zlecających wykonanie usług się kończą. Ewentualnie same jednostki zwyczajnie powołują na te funkcje „ochotnika" z własnego personelu. **Osoba, która oprócz dobrych chęci nie posiada niezbędnej wiedzy i doświadczenia nie jest w stanie skutecznie i rzetelnie sprawować funkcji IOD.** Warto przypomnieć zapis z art. 37 ust 5 RODO: „Inspektor ochrony danych jest wyznaczony na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności zadań, o których mowa w art. 39".

Patrząc z optymizmem w przyszłość można mieć nadzieję, że w konsekwencji **sektor publiczny zacznie przykładać jeszcze większą uwagę do bezpiecznego przetwarzania danych osobowych i ochrony prywatności**. Poziom zabezpieczeń i świadomości wzrasta, jest to dobry sygnał dla nas wszystkich, osób fizycznych, które powierzają przetwarzanie danych wielu podmiotom, w tym urzędom, szkołom, itp. **Zjawiskiem najbardziej piętnowanym przez sam Urząd Ochrony Danych Osobowych jest nieprzyznanie się do błędu i brak chęci poprawy** – dlatego warto współpracować z organem nadzoru (UODO), dobrymi inspektorami ochrony danych osobowych, aby poprawić jakość bezpieczeństwa danych oraz uniknąć kar związanych z prowadzeniem nieprawidłowych działań.



ELEARNING

Szkolenia **RODO** na miarę czasów!

NASZ NOWY PRODUKT!

USYSTEMATYZUJ WIEDZĘ SWOJĄ I PRACOWNIKÓW

PLATFORMA ONLINE - **RODO DLA FIRM**

UMÓW SIĘ NA ROZMOWĘ O WDROŻENIU

Dlaczego warto *korzystać z platformy Elearningowej w szkoleniu z RODO?*

- √ **Oszczędza czas pracowników** oraz IOD dzięki automatyzacji procesu szkolenia pracowników z zasad ochrony danych osobowych i RODO
- √ **Daje dostęp do stale aktualizowanej wiedzy** na temat przepisów RODO i **buduje świadomość** bezpieczeństwa danych osobowych
- √ **Umożliwia przeprowadzanie szkoleń zdalnie**, bez konieczności zbierania uczestników w jednym miejscu i czasie, co znacznie ułatwia organizację pracy.
- √ **Pomaga Inspektorom Ochrony Danych** w wykonywaniu ich zadań. Automatyzuje proces szkolenia i nadawania upoważnień do przetwarzania danych

Zobacz platformę w akcji

Poznaj więcej funkcjonalności na **pharos.pl/elearning**
Lub skontaktuj się pod numer +48 884 797 878

Zapraszamy Państwa do rozmowy na temat naszego nowego rozwiązania w postaci platformy Elearningowej. Bardzo chętnie przygotujemy dla Państwa demo lub przeprowadzimy prezentację systemu i możliwości wdrożenia w Państwa Organizacji.

PHAROS

Pharos Michał Zajdowicz
Telefon +48 505 156 508 +48 608 674 589
kontakt@pharos.pl
www.pharos.pl

Zespół tworzący PerIODyk
Redakcja: Magda Judejko
Michał Zajdowicz
Treści artykułów: Magda Judejko
Michał Zajdowicz
Grzegorz Król
Jarosław Bartkwiak
Korekta: Michał Zajdowicz
Marta Szyszka
Skład i grafika: Dawid Skibiński