KOLMERS LEGAL

GRUDZIEŃ 2019 R.

PRZEWODNIK PO RODO DLA BRANŻY HOTELARSKIEJ

AUTOR:

RADCA PRAWNY

ILONA ŚWIDERSKA-ĆWIK

REDAKCJA

PIOTR TARNOWSKI

SPIS TREŚCI

1 TYTUŁEM WSTĘPU.

Mimo że od wejścia w życie przepisów RODO (tj. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. 95/46/WE (ogólne rozporządzenie o ochronie danych) upłynął już ponad rok, nadal spora grupa przedsiębiorców na hasło „RODO" ma – przynajmniej – mieszane uczucia. Wokół przepisów dotyczących ochrony danych osobowych narosło bardzo wiele mitów, chociażby takich, że powinno się wyposażać biura w specjalne szafy czy niszczarki zgodne z RODO. Dostosowanie działalności hotelu do przepisów z zakresu ochrony danych osobowych należy przede wszystkim rozpocząć od ustalenia wszystkich procesów (obszarów), w których dochodzi do przetwarzania danych osobowych. Mówiąc najogólniej, należy ustalić jakie dane osobowe hotel pozyskuje, w jakim zakresie je przetwarza. Począwszy od rekrutacji, kadr i płac, zajęć wynagrodzenia, benefitów pracowniczych, poprzez flotę samochodową i GPS, ewidencję kluczy do pomieszczeń, pocztę elektroniczną i tradycyjną, monitoring, bazę obecnych i byłych klientów, rachunki, faktury, umowy z dostawcami, kończąc na stronie internetowej, czy dokumentach rejestrowych danej organizacji itp.). Niektórzy nazywają powyższe czynności audytem, inni inwentaryzacją. Ważne jest również ustalenie, czy przedsiębiorca prowadzący hotel, przetwarza dane osobowe jako administrator, współadministrator, czy może jako podmiot przetwarzający, który przetwarza dane osobowe w imieniu administratora.

Istotne jest jednak podkreślenie, że nie wystarczy samo przygotowanie dokumentacji (tj. wykupienie pakietu RODO w promocyjnej cenie), ale dostosowanie tejże dokumentacji do danej (konkretnej) organizacji oraz do procesów przetwarzania danych, które w niej zachodzą. To także bieżące szkolenie i uświadamianie pracowników, którzy tak naprawdę stanowią z jednej strony filar danej firmy, ale są też ryzykiem danej organizacji, bowiem zazwyczaj to oni najczęściej będą mieli do czynienia z danymi osobowymi przetwarzanymi przez hotel. Trzeba zawsze pamiętać, że hotel jako organizacja „żyje" i się zmienia, zatem również RODO musi być dostosowywane na bieżąco do tych zmian. Aby dostosować hotel do przepisów dotyczących ochrony danych osobowych przede wszystkim należy obserwować procesy przetwarzania danych osobowych, by na bieżąco wprowadzać zmiany, czy to w zabezpieczeniach czy procedurach.

W niniejszej publikacji przedstawiam, jak zgodnie z prawem przetwarzać dane osobowe prowadząc hotel czy pensjonat, jakie przesłanki przetwarzania danych osobowych będą miały zastosowanie w konkretnych przypadkach, jakie obowiązki spoczywają na hotelu jako administratorze danych osobowych.

Poniżej przedstawiam też 10 podstawowych zasad dotyczących ochrony danych osobowych, o których – według mnie – każdy powinien pamiętać:

1. zapewnij podstawy prawne do przetwarzania danych osobowych;
2. realizuj zasadę minimalizacji danych, ograniczenia celu oraz zasadę rozliczalności;
3. spełniaj obowiązek informacyjny wobec osób, których dane osobowe dotyczą;
4. posiadaj wewnętrzną dokumentację RODO;
5. prowadź rejestr czynności przetwarzania danych oraz rejestr kategorii czynności przetwarzania;
6. spełniaj obowiązek zawierania umów powierzenia przetwarzania danych osobowych;
7. umieść na stronie internetowej politykę prywatności;
8. zapewnij bezpieczeństwo danych osobowych, w tym zapewnij, że dane osobowe nie będą dostępne dla osób nieuprawnionych do ich przetwarzania;
9. informuj o naruszeniach bezpieczeństwa danych osobowych organ nadzoru oraz osoby, których dane osobowe dotyczą;
10. powołaj Inspektora Ochrony Danych, jeżeli podlegasz obowiązkowi.

Zanim jednak przejdziemy do omawiania powyższych zasad, zaczniemy od podstaw – czyli od tzw. RODO krok po kroku, tj. od fundamentalnych pojęć z zakresu ochrony danych osobowych. Zapoznanie się z nimi ułatwi poruszanie się po niniejszej publikacji.

Mam szczerą nadzieję, że niniejsza publikacja pomoże – tym, którzy już zadbali o ochronę danych osobowych – usystematyzować i uporządkować wiedzę, a hotelom i pensjonatom, przed którymi dopiero wdrożenie RODO – liczę, że przewodnik pozwoli na pełniejsze przygotowanie się do procesu audytu i lepsze zrozumienie tematu.

Życzę udanej lektury!

radca prawny
Ilona Świderska-Ćwik

2 PODSTAWOWE POJĘCIA Z ZAKRESU OCHRONY DANYCH OSOBOWYCH. CZYM SĄ DANE OSOBOWE?

Podstawowe definicje z zakresu ochrony danych osobowych, które ułatwią poruszanie się po niniejszej publikacji:

a. **ADMINISTRATOR** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych(art. 4 ust. 7 RODO);

b. **PODMIOT PRZETWARZAJĄCY** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 ust. 8 RODO);

c. **INSPEKTOR OCHRONY DANYCH OSOBOWYCH** - osoba wyznaczona do pełnienia tej funkcji na podstawie przepisów RODO (art. 37-39 RODO);

d. **PREZES UODO** – Prezes Urzędu Ochrony Danych Osobowych;

e. **DANE OSOBOWE** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (art. 4 pkt 1 RODO). Wyróżnia się następujące kategorie danych osobowych:

- dane zwykłe (np. imię, nazwisko, adres zamieszkania, data i miejsce urodzenia, numer telefonu, wykonywany zawód, adres e-mail);
- dane szczególnej kategorii, uprzednio nazywane danymi wrażliwymi (np. pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby) oraz dane dotyczące wyroków i naruszeń prawa;

W kontekście powyższego, **DANE BIOMETRYCZNE** oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne, zaś **DANE DOTYCZĄCE ZDROWIA** oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

f. **PRZETWARZANIE** - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

g. **NARUSZENIE OCHRONY DANYCH OSOBOWYCH** - oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

h. **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.

3 JAKIE ZASADY OBOWIĄZUJĄ PRZY PRZETWARZANIU DANYCH OSOBOWYCH?

Przetwarzanie danych osobowych, wg RODO odbywa się z poszanowaniem określonych reguł, które to szczegółowo zostały określone w art. 5 RODO.

Podstawowa zasada RODO to przetwarzanie danych osobowych zgodnie z prawem. Innymi słowy, administrator danych, czyli hotel czy pensjonat, by mógł przetwarzać dane osobowe gości, czy chociażby swoich pracowników, współpracowników, musi posiadać ku temu właściwą podstawę prawną. RODO wprowadza zasadę zgodności z prawem, co oznacza, że przetwarzanie danych osobowych musi być oparte na przesłance z katalogu zawartego w przepisach RODO (art. 6 RODO wobec danych zwykłych, art. 9 RODO w przypadku danych szczególnych oraz art. 10 wobec danych dotyczących wyroków karnych i naruszeń prawa).

Kiedy zatem przetwarzanie danych osobowych jest zgodne z prawem? Wg art. 6 RODO w następujących przypadkach:

a. kiedy osoba, której dane dotyczą, wyraziła na to zgodę;
b. przetwarzanie jest niezbędne w celu wykonania umowy lub w celu podjęcia działań niezbędnych przed zawarciem umowy;
c. przetwarzanie jest niezbędne w celu wypełnienia obowiązku prawnego ciążącego na hotelu czy pensjonacie;
d. przetwarzanie jest niezbędne w celu ochrony żywotnych interesów osoby, której dane dotyczą;
e. kiedy hotel czy pensjonat realizuje zadanie w interesie publicznym;
f. kiedy przetwarzanie wynika z prawnie uzasadnionego interesu.

Rzetelność i przejrzystość
Gdy hotel przetwarza dane osobowe powinien również przestrzegać pozostałych reguł określonych w RODO, tj. zasady rzetelności i przejrzystości. Zasada ta oznacza, że wszelka korespondencja kierowana do klienta, gościa hotelowego, subskrybenta newslettera, w tym przede wszystkim klauzule informacyjne zawierające informacje o przysługujących danej osobie uprawnieniach, powinny być czytelne i napisane prostym, zrozumiałym językiem.

Ograniczenie celu przetwarzania danych i minimalizacja danych osobowych
RODO mówi wprost – hotel może zbierać dane osobowe w konkretnych, wyraźnych i prawnie uzasadnionych celach.

Co to oznacza?
Załóżmy, że hotel pozyskał dane osobowe swoich klientów w celu świadczenia usługi zakwaterowania. Usługa została wykonana. Niemniej jednak, w celach marketingowych, pracownik działu promocji chciałby wykorzystać wizerunek klienta lub chociażby jego imię i nazwisko na swojej stronie internetowej (np. gdy w hotelu przebywał znany gwiazdor lub influencer). Zgodnie z zasadą ograniczonego celu, nie można wykorzystać danych klienta do innego celu niż tego, w którym zostały pozyskane, bez odpowiedniej podstawy. Jako, że w naszym przykładzie dane pozyskane były tylko w celu realizacji konkretnej usługi, nie zaś w celu umieszczenie ich na stronie internetowej – nie można ich tak wykorzystać.

Z kolei zasada minimalizacji danych wg RODO oznacza, że można przetwarzać tylko te dane osobowe klientów, które są niezbędne do osiągnięcia celu przetwarzania. Na przykład: Jeśli hotel zamieścił na swojej stronie internetowej usługę wysyłki newslettera, to w celu wykonania ww. usługi niezbędne jest pozyskanie od odbiorcy adresu e-mail i ewentualnie imienia. Niezgodne z zasadą minimalizacji danych byłoby pozyskiwanie dodatkowo np. stanu cywilnego, daty urodzenia (chyba, że w newsletterze znajdują się informacje tylko dla osób pełnoletnich) czy adresu zamieszkania.

Zasada prawidłowość lub inaczej zasada merytorycznej poprawności
Będąc administratorem danych hotel zobowiązany jest do tego, aby dane osobowe przez niego pozyskiwane były poprawne i w razie potrzeby uaktualniane lub w przypadku, gdy są one nieprawidłowe, winny być niezwłocznie usunięte.

Ograniczenie przechowywania danych osobowych
Administrator danych – hotel, pensjonat czy ośrodek wypoczynkowy, powinien przechowywać dane osobowe w formie umożliwiającej ich identyfikację przez okres nie dłuższy, niż jest do niezbędne to zrealizowania celów, w których te dane są przetwarzane. Innymi słowy, nie można ich przetwarzać w nieskończoność.

Integralność i poufność
Zasada powyższa jednoznacznie wskazuje, że hotel czy pensjonat powinien zastosować takie zabezpieczenia za pomocą odpowiednich środków technicznych lub organizacyjnych, by zapewniały one adekwatne bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem, a także przypadkową ich utratą, zniszczeniem i uszkodzeniem.

Rozliczalność
Należy pamiętać, że prowadząc hotel czy pensjonat to właściciel jest administratorem danych osobowych swoich klientów i odpowiada za przestrzeganie wszystkich powyższych zasad i w przypadku ewentualnej kontroli powinien być w stanie wykazać/udowodnić, że przetwarza dane osobowe zgodnie z prawem, w tym przede wszystkim zgodnie z RODO.

4 PODSTAWY PRZETWARZANIA DANYCH OSOBOWYCH. JAKIE DANE OSOBOWE I W JAKIM CELU SĄ PRZETWARZANE PRZEZ HOTEL?

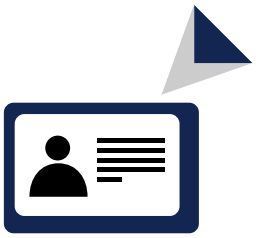
Hotele, ośrodki wypoczynkowe, czy nawet te najmniejsze pensjonaty gromadzą przede wszystkim dane osobowe swoich klientów - gości. Jeśli zatem firma oferuje swoim gościom usługi z zakresu udostępnienia noclegu to jest administratorem ich danych osobowych. Hotel przetwarza te dane osobowe w celu niezbędnym do wykonania umowy, której stroną jest gość hotelowy lub do podjęcia działań na żądanie tejże osoby przed zawarciem umowy (art. 6 ust. 1 lit. b RODO).

Bez wątpienia w celu zawarcia umowy, hotel może zbierać następujące dane osobowe swoich gości:
- imię i nazwisko;
- adres;
- dane kontaktowe.

W przypadku konieczności wystawienia na przedsiębiorcę (tj na osobę fizyczną prowadzącą działalność gospodarczą) faktury (zgodnie z art. 106e ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług) konieczne okaże się również pozyskanie następujących danych:
- nazwy firmy;
- NIP;
- Adres siedziby.

Pozyskiwanie nr PESEL – czy jest konieczne?
Problematyczne - w procesie rejestracji - może okazać się zbieranie numeru PESEL, jednak może to być konieczne do dochodzenia przez hotel ewentualnych roszczeń (np. odszkodowawczych) związanych z usługą noclegu. Może bowiem zdarzyć się sytuacja, że gość hotelowy zniszczy należące do hotelu mienie.

A co z dowodem osobistym?
W celu zawarcia umowy z gościem hotelowym, hotel może zażądać przedstawienia dowodu osobistego lub innego dokumentu tożsamości jedynie „do wglądu", czyli do weryfikacji i spisania koniecznych (tj. nie wszystkich) danych osobowych do zawarcia tejże umowy, ewentualnie również danych niezbędnych do realizacji celów wynikających z prawnie uzasadnionych interesów realizowanych przez hotel (administratora), zgodnie z art. 6 ust. 1 lit. f RODO (w celu np. dochodzenia ewentualnych roszczeń). Zaleca się jednak, by kwestię konieczności okazania pracownikowi recepcji dokumentu potwierdzającego tożsamość gościa uregulować w regulaminie hotelu.



Sprzeciw gości hotelowych może budzić praktyka wynoszenia przez recepcjonistę dokumentu tożsamości gościa poza recepcję lub w miejsce, gdzie gość hotelowy nie będzie widział swojego dokumentu. Kontrowersyjne jest również wykonywanie kserokopii lub skanowanie dokumentu tożsamości, w świetle najnowszych zmian przepisów, jak również w świetle ostatniego stanowiska Prezesa Urzędu Ochrony Danych Osobowych, w kontekście wykonywania przez banki kserokopii dowodu osobistego. Prezes Urzędu Ochrony Danych Osobowych wskazał bowiem, że kopiowanie dokumentów tożsamości niemal przy każdej czynności budzi wątpliwości organu nadzorczego. Dlatego Prezes UODO stanowczo sprzeciwia się takiej praktyce. Zwrócił także uwagę, że sporządzanie kopii dokumentów tożsamości ułatwia ich wykorzystywanie do innych celów przez podmioty nieupoważnione, w tym do kradzieży tożsamości.

Czy w związku z wynajmem pokoju hotel powinien pozyskać jeszcze dodatkowo zgodę na przetwarzanie danych osobowych?

Nie. Podstawą prawną przetwarzania danych osobowych gościa hotelowego jest art. 6 ust. 1 lit. b RODO, czyli zawarcie umowy. Nie jest zatem zalecane pobieranie odrębnej zgody na świadczenie usługi noclegu. Taka zgoda mogłaby być zbierana od gości w przypadku świadczenia na ich rzecz usługi polegającej na wysyłce newslettera bądź udostępnienia danych partnerom biznesowym współpracującym z hotelem.

Ponadto, trzeba pamiętać, że hotel nie przetwarza tylko danych swoich gości hotelowych w celu świadczenia dla nich usług noclegowych, ale:

a. jeśli – poza usługą noclegową - świadczy usługi np. w zakresie umożliwienia klientom organizacji w hotelu przyjęcia okolicznościowego, to w tym przypadku także jest administratorem danych klientów (zazwyczaj podstawa prawna będzie art.6 ust.1 lit. b RODO);

b. jeśli organizuje konferencję, to jest administratorem danych osobowych zaproszonych na nią gości;

c. jeśli rekrutuje i zatrudnia pracowników np. na stanowisko kelnera/-ki, kucharza, czy recepcjonistki, to jest również administratorem ich danych osobowych. W tym zakresie powinien pobierać dane wymienione szczegółowo w Kodeksie pracy. Pracodawca może „żądać" od kandydata do pracy tylko tych danych osobowych, które zostały wyczerpująco wskazane w art. 22(1) § 1 Kodeksu Pracy. Podstawą prawną przetwarzania danych osobowych pracowników jest ww. przepis oraz art. 6 ust. 1 lit. b RODO (w związku z zawarciem umowy o pracę), jak również art. 6 ust. 1 lit. c RODO bowiem ciążą na hotelu obowiązki z zakresu rozliczeń finansowych, czy rozliczeń z Zakładem Ubezpieczeń Społecznych. Zwrócić w tym miejscu należy uwagę, że zgodnie z przywołaną wcześniej zasadą minimalizacji pobierania danych osobowych pracodawca powinien gromadzić tylko te dane, które są konieczne do celu, jakim jest zatrudnienie danej osoby. W kontekście przetwarzania danych w rekrutacji i zatrudnieniu pojawiają się też kwestie związane z testami psychologicznymi wykonywanymi w ramach rekrutacji (które budzą nadal wiele wątpliwości), czy przetwarzaniem danych w związku z koniecznością wykonania szkoleń z zakresu BHP. RODO pojawia się również w kontekście chociażby listy obecności pracowników;

d. jeśli hotel objęty jest monitoringiem wizyjnym, to hotel również jest administratorem danych osobowych osób na nim zarejestrowanych (zazwyczaj podstawą prawną jest art. 6 ust. 1 lit. f RODO), w szczególności wizerunków i cech szczególnych osób (hotel zatem musi dodatkowo ustalić czy dochodzi do przetwarzania danych szczególnych, danych biometrycznych w rozumieniu art. 9 ust. 1 RODO), a także np. numerów identyfikacyjnych, takich jak numery tablic rejestracyjnych pojazdów. Zatem rejestrowanie i przechowywanie nagrań z monitoringu jest również przetwarzaniem danych osobowych, zaś sam monitoring nie może być np. środkiem nadzoru nad pracownikami oraz nie może obejmować nagrywania dźwięku. W klauzuli informacyjnej (o której mowa w dalszej części niniejszego e-booka) dotyczącej monitoringu należy koniecznie wskazać cel przetwarzania danych, podstawę prawną, okres przechowania nagrań.

Do ustalenia jest również sposób wprowadzenia monitoringu w kontekście przepisów kodeksu pracy. Jeśli hotel zdecydował się zlecić prowadzenie monitoringu firmie zewnętrznej, powinien pamiętać o zawarciu z nim umowy powierzenia przetwarzania danych osobowych. Zgodnie z wytycznymi Prezesa UODO, podejmując decyzję o wprowadzeniu monitoringu, administrator musi pamiętać o przeprowadzeniu oceny skutków dla ochrony danych. Jest ona wymagana, gdy operacja przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Zgodnie z art. 35 ust. 3 lit. c RODO, jest ona obowiązkowa dla monitorowania miejsc dostępnych publicznie. Zalecamy zapoznać się ze szczegółowymi wskazówkami Prezesa Urzędu Ochrony Danych Osobowych dotyczącymi monitoringu wizyjnego, dostępnymi pod poniższym linkiem: https://uodo.gov.pl/pl/138/354;

e. jeśli hotel prowadzi działania marketingowe i wysyła np. newsletter, czyli internetowy informator/biuletyn dostarczany drogą elektroniczną regularnie do zainteresowanych klientów/subskrybentów, to w tym przypadku również jest ich administratorem danych osobowych (zazwyczaj imienia i adresu e-mail), o czym szerzej w dalszej części niniejszej publikacji.

Jakie dane osobowe hotel może pozyskać od osoby ubiegającej się o zatrudnienie, a jakie od pracownika?
Kodeks pracy, w art. 22(1) wprost wskazuje jakie dane osobowe pracodawca może pozyskać od osoby ubiegającej się o zatrudnienie, tj. może żądać podania danych osobowych obejmujących:
- imię (imiona) i nazwisko;
- datę urodzenia;
- dane kontaktowe wskazane przez taką osobę;
- wykształcenie;
- kwalifikacje zawodowe;
- przebieg dotychczasowego zatrudnienia.

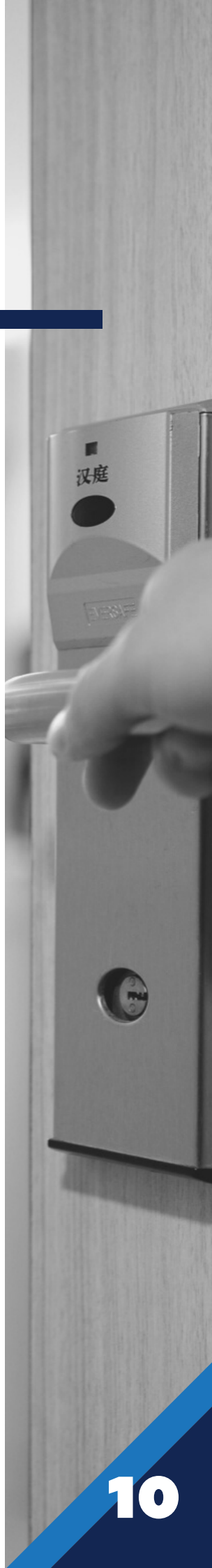
Natomiast, pracodawca żądać może od pracownika podania dodatkowo danych osobowych obejmujących:
- adres zamieszkania;
- numer PESEL, a w przypadku jego braku - rodzaj i numer dokumentu potwierdzającego tożsamość;
- inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy;
- wykształcenie i przebieg dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie;
- numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.

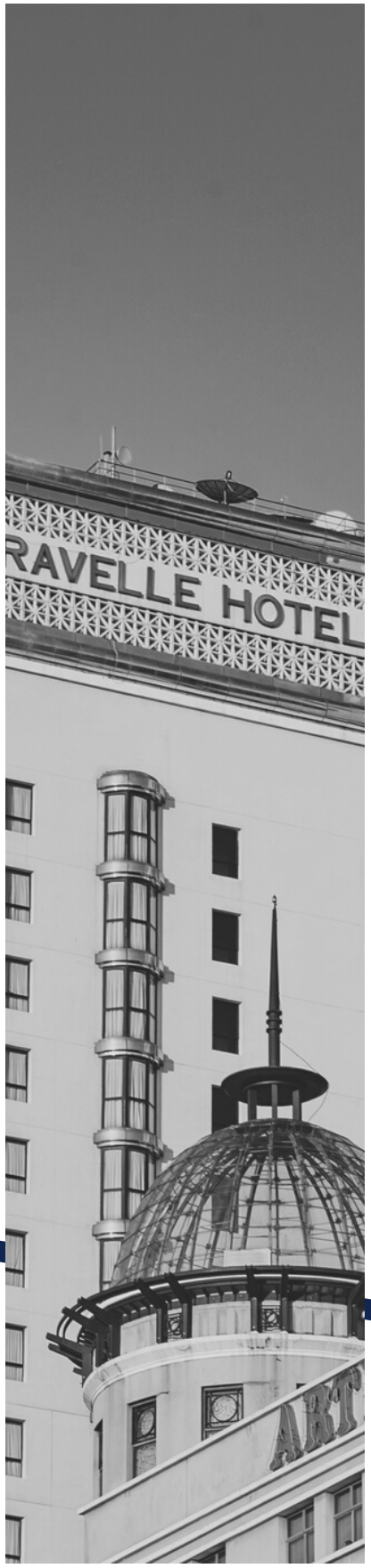
Pracodawca może żądać innych danych, gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.

Czy hotel może pozyskiwać od swoich gości hotelowych dane szczególnej kategorii?

Zgodnie z RODO, co do zasady przetwarzanie danych szczególnych kategorii jest zabronione. Oczywiście, od tego zakazu istnieją wyjątki i np. przetwarzanie danych szczególnej kategorii jest możliwe, jeśli osoba, której dane dotyczą udzieli na przetwarzanie tych danych wyraźnej zgody.

W przypadku, gdy hotel świadczy usługi z zakresu medical SPA, dochodzi w takim przypadku do przetwarzania danych osobowych do celów realizacji świadczeń zdrowotnych (hotel może gromadzić w szczególności informacje o odbytych zabiegach, chorobach i innych dolegliwościach swoich gości, przyjmowanych lekach w celu postawienia diagnozy i świadczenia usług w zakresie opieki medycznej – czyli dochodzi do przetwarzania danych dotyczących zdrowia). W tym zakresie zastosowanie znajdzie ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta oraz Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania. Podstawą prawną przetwarzania danych osobowych w tym celu jest art. 9 ust. 2 lit. h RODO oraz art. 24 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. Istotne jest ustalenie zakresie przetwarzania danych osobowych, okresu przechowywania dokumentacji medycznej (mając na uwadze art. 29 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta), czy możliwości udostępnienia dokumentacji medycznej osobom upoważnionym.
Pamiętać również należy o spełnieniu obowiązku informacyjnego zarówno z art. 13 RODO, jak również z art. 14 RODO w przypadku np. pozyskiwania danych osobowych z Narodowego Funduszu Zdrowia. W kontekście danych szczególnej kategorii pojawia się rozważenie przeprowadzenia oceny skutków dla ochrony danych osobowych. Ocena taka jest przeprowadzana, jeśli przetwarzanie danych osobowych wiąże się z wysokim ryzykiem naruszeń praw i wolności osoby fizycznej (art. 35 RODO). Na marginesie zauważyć należy, że również w przypadku świadczenia usług spa (wyłącznie pielęgnacyjnych zabiegów) może dochodzić do przetwarzania danych osobowych szczególnej kategorii. Właściwą w tym przypadku podstawą prawną przetwarzania danych osobowych jest wyraźna zgoda – art. 9 ust. 2 lit. a RODO. Zaleca się w tym przypadku pozyskanie zgody pisemnej, celem ewentualnego wykazania, iż faktycznie osoba wyraziła taką zgodę (zgodnie z zasadą rozliczalności).





Czy hotel może pozyskać dane osobowe dziecka?

Zgodnie z motywem 38 preambuły RODO dzieci wymagają szczególnej ochrony danych osobowych, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych.

Zgodnie z art. 8 ust. 1 RODO w przypadku usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku zgodne z prawem jest przetwarzanie danych osobowych dziecka, które ukończyło 16 lat. Jeżeli dziecko nie ukończyło 16 lat, takie przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody. Dane dziecka (szczególnie wiek) mogą pojawić się w kontekście zniżek udzielanych przez hotel, czy świadczenia usług medycznych np. w zakresie oceny rozwoju ruchowego dziecka, wykrycia ewentualnych wad rozwojowych.

Rezerwacja miejsca w hotelu przez zewnętrzny system rezerwacyjny.

Większość hoteli, a także spora część domów gościnnych i pensjonatów korzysta z internetowych pośredników, platform oraz narzędzi SaaS, którzy umożliwiają klientowi bezpośrednie dokonanie rezerwacji noclegu w danym hotelu. W takiej sytuacji dochodzi do przekazania (udostępnienia) danych osobowych przyszłego gościa hotelowego przez owego pośrednika do hotelu. Zazwyczaj taki pośrednik staje się administratorem danych osobowych klienta, bowiem ustala sam cele i sposoby przetwarzania. W zakresie zaś udostępnienia danych wskazać należy, że hotel również staje się ich administratorem, bowiem decyduje sam o celach przetwarzania danych. W takim przypadku należy pamiętać o spełnieniu obowiązku informacyjnego wynikającego z art. 14 RODO.

5 POBÓR OPŁATY MIEJSCOWEJ, UZDROWISKOWEJ A PRZETWARZANIE DANYCH OSOBOWYCH PRZEZ HOTEL.

Zgodnie z ustawą z dnia 12 stycznia 1991 r. o podatkach i opłatach lokalnych rada gminy może wprowadzić opłatę miejscową. Opłatę miejscową pobiera się od osób fizycznych przebywających dłużej niż dobę w celach turystycznych, wypoczynkowych lub szkoleniowych:
- w miejscowościach posiadających korzystne właściwości klimatyczne, walory krajobrazowe oraz warunki umożliwiające pobyt osób w tych celach;
- w miejscowościach znajdujących się na obszarach, którym nadano status obszaru ochrony uzdrowiskowej na zasadach określonych w ustawie z dnia 28 lipca 2005 r. o lecznictwie uzdrowiskowym, uzdrowiskach i obszarach ochrony uzdrowiskowej oraz o gminach uzdrowiskowych (Dz.U. z 2017 r. poz. 1056);
- za każdą rozpoczętą dobę pobytu.

Inkasentami ww. opłaty są podmioty prowadzące ośrodki wypoczynkowe, hotele, sanatoria, pensjonaty, kwatery, apartamenty, wynajmujące domy letniskowe oraz podmioty, które świadczą usługi w zakresie pobytu i zakwaterowania osób fizycznych przebywających. Podmioty te zobligowane są do realizacji obowiązków polegających na pobraniu opłaty miejscowej (uzdrowiskowej). Niektóre hotele prowadzą ewidencję określającą jedynie liczbę gości przebywających w hotelu. Niemniej jednak coraz częściej zdarza się, że gmina wprost wskazuje, że hotel lub pensjonat ma obowiązek prowadzenia ewidencji osób zobowiązanych do uiszczania opłaty miejscowej (tj. imię i nazwisko, adres zamieszkania, okres pobytu, liczbę dni za które pobrana jest opłata). Ewidencja powyższa zapewne jest prowadzona celem prawidłowego poboru opłaty i może być przedmiotem kontroli. Na inkasencie (hotelu) ciąży bowiem obowiązek przechowywania dokumentów do czasu przedawnienia zobowiązania podatkowego. W tym zakresie podstawą przetwarzania danych osobowych jest art. 6 ust.1 lit. c RODO w związku z konkretną uchwałą rady gminy. Celem przetwarzania danych jest bowiem konieczność realizacji obowiązku uiszczania opłaty miejscowej.

6 PRZEZ JAKI OKRES HOTEL MOŻE PRZECHOWYWAĆ DANE GOŚCI?

Okres przechowywania danych osobowych uzależniony jest od celu przetwarzania tychże danych osobowych przez hotel, przy uwzględnieniu także wszelkich wymogów przewidzianych w przepisach powszechnie obowiązującego prawa (np. prawa pracy czy przepisach podatkowych). Wskazuje się zatem, że dane będą przechowywane przez okres niezbędny do realizacji umowy, a także przez okres, w którym mogą ujawnić się roszczenia związane z tą umową. Ponadto, dane muszą być gromadzone przez okres wymagany obowiązującym prawem, w związku z koniecznością realizacji przez hotel różnorakich obowiązków, np. podatkowych. Natomiast w przypadku zastosowania monitoringu wizyjnego hotel powinien wskazać okres przechowywania nagrań.

Pamiętać należy, że w sytuacji świadczenia innych usług, okres przechowywania danych osobowych może być inny. Na przykład:

a. w sytuacji przetwarzania danych ostanie zdrowia, okres ten został wskazany w ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta, tj. przez 20 lat, zgodnie z art. 29 ust. 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, z zastrzeżeniem wyjątków przewidzianych w tejże ustawie;

b. w sytuacji przetwarzania danych osobowych na podstawie zgody – do czasy wycofania tejże zgody.

c. w przypadku rekrutacji – do czasu zakończenia procesu rekrutacji (chyba że kandydat wyraził zgodę na udział w przyszłych rekrutacjach).

Zaleca się zatem, by hotel dokonywał okresowych przeglądów przechowywania danych osobowych swoich gości czy np. byłych pracowników, zgodnie z motywem 39 RODO: *aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu.*

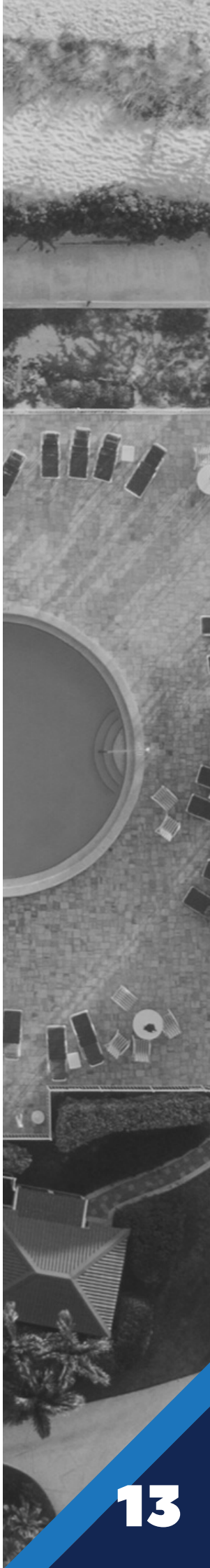
7 JAKIE PRAWA PRZYSŁUGUJĄ OSOBOM, KTÓRYCH DANE OSOBOWE HOTEL PRZETWARZA?

Każda osoba, której dane osobowe dotyczą, posiada następujące prawa:

a. **prawo do cofnięcia zgody** – oznacza, że można cofnąć wyrażoną zgodę w każdym momencie, bez podawania przyczyny;

b. **prawo dostępu do danych osobowych** – osoba, której dane dotyczą, może żądać od hotelu informacji o przetwarzaniu jej danych, przysługuje jej uprawnienie do uzyskania dostępu do tych danych, ich kopii, oraz do uzyskania informacji o celach przetwarzania, kategoriach danych osobowych, odbiorcach lub kategoriach odbiorców, którym dane zostały lub zostaną ujawnione, o okresie przechowywania danych lub o kryteriach ich ustalania, o przysługujących osobie prawach związanych z przetwarzaniem jej danych osobowych, o możliwości wniesienia skargi do organu nadzoru, o źródle pozyskania danych osobowych, jeżeli nie zostały pozyskane bezpośrednio od osoby, której dane dotyczą, oraz o profilowaniu i zautomatyzowanym przetwarzaniu decyzji;

c. **prawo do sprostowania** – osoba, której dane dotyczą może żądać ich sprostowania lub uzupełnienia (art. 16 RODO);



d. **prawo do zapomnienia** – osoba, której dane dotyczą może żądać usunięcia jej danych osobowych, z zastrzeżeniem, że jeżeli osoba wyraziła zgodę na przetwarzanie danych osobowych, żądanie usunięcia odniesie taki sam skutek jak cofnięcie zgody (art. 17 RODO);

e. **prawo do ograniczenia przetwarzania** – osoba, której dane dotyczą może żądać ograniczenia przetwarzania danych osobowych przez hotel (art. 18 RODO), tj. zażądać zaprzestania ich przetwarzania z wyjątkiem ich przechowywania, w sytuacjach, gdy:
- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych na okres, w którym hotel będzie weryfikował ich prawidłowość;
- osoba, której dane dotyczą, kwestionuje zgodność z prawem przetwarzania danych osobowych przez hotel;
- hotel nie potrzebuje już tych danych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony jego roszczeń;
- osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania – do czasu podjęcia decyzji przez hotel co do zasadności sprzeciwu;

f. **prawo do wniesienia sprzeciwu** – osoba, której dane dotyczą może wnieść sprzeciw wobec przetwarzania jej danych osobowych w prawnie uzasadnionych celach hotelu;

g. **prawo do przenoszenia** – osoba, której dane dotyczą może przenieść swoje dane osobowe, tj. otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe, które dostarczyła Podmiotowi, jeżeli ich przetwarzanie odbywa się na podstawie zgody, lub zażądać przesłania tych danych innemu, wskazanemu przez osobę, której dane dotyczą, administratorowi (art. 20 RODO).

8 OBOWIĄZEK INFORMACYJNY, CZYLI PRZEDSTAWIENIE TZW. KLAUZULI INFORMACYJNEJ.

W momencie pobierania danych osobowych np. od gościa hotelowego, każdy administrator zobowiązany jest do zrealizowania obowiązku informacyjnego względem osoby, której dane osobowe przetwarza. Obowiązek powyższy będzie konieczny zarówno, gdy dane osobowe pozyskuje bezpośrednio od konkretnej osoby (art. 13 RODO), jak i niebezpośrednio (art. 14 RODO).

<u>Kiedy hotel będzie zobowiązany do realizacji tego obowiązku?</u>
Obowiązek przedstawienia klauzuli informacyjnej pojawia się w następujących (przykładowych – jest to katalog otwarty) sytuacjach:
1. w trakcie rejestracji gości hotelowych;
2. podczas procesu rekrutacji, jak również podczas zatrudniania pracownika;
3. stosowania monitoringu wizyjnego;
4. każdorazowo w przypadku zmiany celu przetwarzania.

Zazwyczaj gość hotelowy posiada wiedzę, kto jest administratorem jego danych osobowych w związku z realizacją świadczenia usługi noclegowej. Jednakże praktyka pokazuje, że często jednak nie sposób stwierdzić i wykazać (zgodnie z zasadą rozliczalności), jakim zakresem informacji o administratorze i dokonywanym przez niego przetwarzaniu osoba, której dane dotyczą, dysponuje. Często wiedza ta jest niepełna, zaś administratorowi trudno jest ocenić, co właściwie wie podmiot danych i jakiej jakości są to informacje. Jeśli zatem hotel nie ma możliwości wykazania, że osoba, której dane dotyczą, dysponuje już informacjami wynikającymi z art. 13 ust. 1–3 RODO, powinien spełniać wobec niej obowiązek informacyjny za każdym razem, gdy pozyskuje jej dane.

Jakie informacje powinna zawierać klauzula informacyjna?

Poniżej szczegółowa lista z przykładami. Klauzula powinna zawierać następujące informacje:

1. kto jest administratorem danych osobowych;

Na przykład: *Administratorem Państwa danych osobowych jest spółka działająca pod firmą Hotel Kolmers sp. z o.o. z siedzibą w Warszawie pod adresem: ul. Stare Podwale 430, 02-548 Warszawa, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie pod nr KRS: 0000123456, NIP: 1231234565, kapitał zakładowy: 100.000 zł. Dane kontaktowe: biurohotel@kolmers.pl; tel.: 22 111 33 99.*

2. czy został wyznaczony inspektor ochrony danych osobowych; jeśli tak, to należy podać dane kontaktowe do inspektora;

Na przykład: *Administrator wyznaczył Inspektora Ochrony Danych Osobowych w osobie Pana Jana Kowalskiego. Kontakt do Inspektora: inspektor@hotelkolmers.pl*

3. w jakim celu i na jakiej podstawie przetwarzane są dane osobowe;

Na przykład: *W przypadku dokonywania rezerwacji noclegu można wskazać, że dane osobowe gości są przetwarzane przez administratora w celu dokonania rezerwacji noclegu. Podstawą prawną przetwarzania danych osobowych pozyskanych przez hotel jest umowa o świadczenie usług hotelarskich (art. 6 ust. 1 lit. b RODO).*

4. okres przetwarzania danych osobowych;

Na przykład: *W przypadku rekrutacji można wskazać, iż dane osobowe osób uczestniczących w procesie rekrutacji będą przetwarzane do czasu zakończenia procesu rekrutacji, a przypadku gdy została wyrażona odrębna zgoda na udział w przyszłych rekrutacjach - przez okres np. dodatkowo 6 miesięcy.*

Czyli po zakończonym procesie rekrutacji, pracodawca powinien trwale usunąć dane osobowe kandydatów do pracy.

5. kto jest lub może być odbiorcą danych osobowych;

Na przykład: *Państwa dane mogą zostać udostępnione lub przekazane następującym kategoriom odbiorców:*
a) organom władzy publicznej, podmiotom wykonującym zadania publiczne lub działającym na zlecenie organów władzy publicznej, w zakresie i w celach, które wynikają z przepisów prawa,
b) podmiotom współpracujących z administratorem na zasadzie zleconych usług i zgodnie z zawartymi umowami powierzenia, tj. podmiotom świadczącym usługi transportowe i taksówkarskie w przypadku zamówienia dla gościa transportu, firmom świadczącym usługi informatyczne, księgowe, usługi marketingowe.

6. jakie prawa przysługują osobie, której dane przetwarzasz;

Na przykład: *Przysługują Pani/Panu odpowiednie prawa wynikające z RODO, tj.*
a) prawo dostępu do danych osobowych, w tym prawo do uzyskania kopii tych danych;
b) prawo do żądania sprostowania (poprawiania) danych osobowych – w przypadku, gdy dane są nieprawidłowe lub niekompletne;
c) prawo do żądania usunięcia danych osobowych;
d) prawo do żądania ograniczenia przetwarzania danych osobowych;
e) prawo do przenoszenia danych osobowych w przypadku, gdy przetwarzanie odbywa się na podstawie umowy zawartej z osobą, której dane dotyczą lub na podstawie zgody wyrażonej przez taką osobę oraz gdy przetwarzanie odbywa się w sposób zautomatyzowany;
f) prawo do cofnięcia zgody na przetwarzanie danych osobowych w zakresie, w jakim przetwarzanie Pani/Pana danych osobowych odbywa się na podstawie udzielonej zgody, z zastrzeżeniem, że cofnięcie zgody nie ma wpływu na zgodność z prawem przetwarzania danych, którego dokonano na podstawie zgody przed jej wycofaniem;
g) w przypadku uznania, iż przetwarzanie przez Administratora Pani/Pana danych osobowych narusza przepisy RODO, przysługuje Pani/Panu prawo do wniesienia skargi do właściwego organu nadzorczego. Organem nadzorczym wobec Administratora w zakresie danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych.

7. informację, czy dane osobowe będą podlegały profilowaniu, zautomatyzowanym podejmowaniu decyzji oraz o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

Na przykład: *Pani/Pana dane osobowe nie będą wykorzystane do profilowania Pani/Pana lub do zautomatyzowanego podejmowania decyzji względem Pani/Pana.*

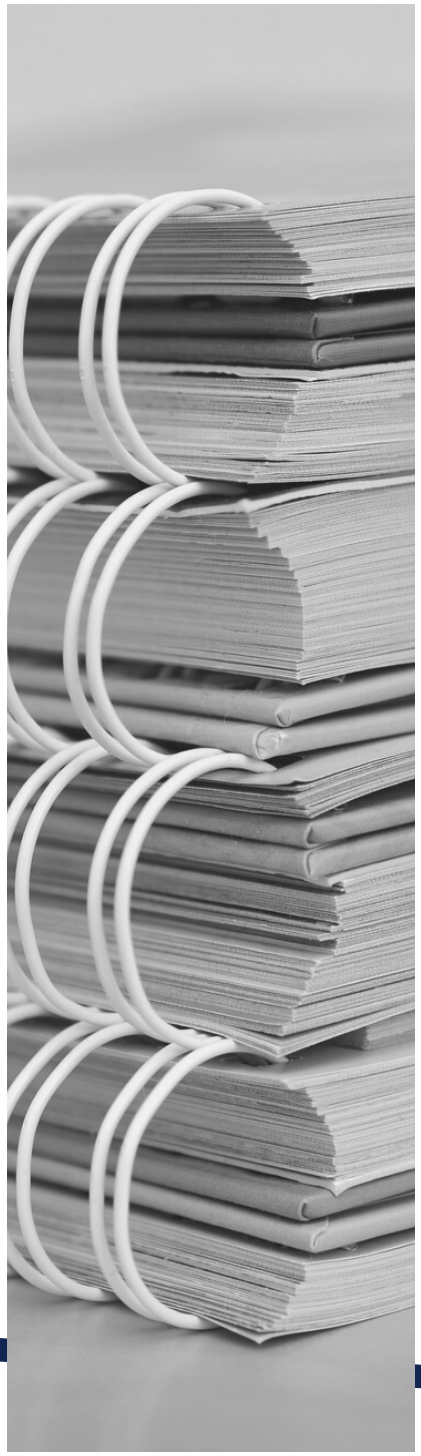
Jak zostało wyżej wspomniane, zdarzają się sytuacje, gdy dane osobowe pozyskiwane są od podmiotu trzeciego. Klauzula informacyjna – poza informacjami wskazanymi powyżej – powinna również zawierać wskazanie źródła pochodzenia tych danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych (art. 14 RODO). Ponadto, hotel pozyskując dane od osoby trzeciej, powinien poinformować osobę, której dane uzyskał o treści ww. klauzuli w rozsądnym terminie, tj. po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca, lub najpóźniej przy pierwszej komunikacji z osobą.

Jak hotel może spełnić obowiązek informacyjny?

Dość często zdarza się, że treść klauzuli informacyjnej umieszczona jest tuż przy recepcji, na stronie internetowej, bądź wręczana w momencie dokonywania rezerwacji w hotelu, tak by każdy z gości hotelowych miał możliwość zapoznania się z jej treścią.

W przypadku umożliwienia swoim gościom rezerwacji noclegu drogą telefoniczną treść klauzuli można dodatkowo odsłuchać wybierając odpowiedni numer. W przypadku zaś dokonywania rezerwacji za pomocą formularza dostępnego na stronie internetowej, klauzula informacyjna może znaleźć się w potwierdzeniu rezerwacji/w regulaminie lub polityce prywatności.

9 JAKĄ DOKUMENTACJĘ Z ZAKRESU OCHRONY DANYCH OSOBOWYCH POWINIEN POSIADAĆ HOTEL?



Przepisy RODO nie zawierają praktycznie żadnych wytycznych odnoszących się do sposobu prowadzenia dokumentacji przetwarzania danych osobowych, jak również jej zawartości. RODO w art. 24 ust. 2, stanowi jedynie, że środki techniczne i organizacyjne, które powinien wdrożyć administrator danych, mogą obejmować wdrożenie odpowiednich polityk ochrony danych osobowych. Obszary, w odniesieniu do których RODO nakreśla pewne formalności to:

- prowadzenie rejestru czynności przetwarzania i rejestru kategorii czynności przetwarzania, o których mowa w art. 30 RODO;
- zgłaszanie naruszenie ochrony danych do organu nadzorczego – art. 33 ust. 3 RODO;
- prowadzenie wewnętrznej dokumentacji stanowiącej rejestr naruszeń ochrony danych, o którym mowa w art. 33 ust. 5 RODO;
- zawartość raportu dokumentującego wyniki przeprowadzonych ocen skutków dla ochrony danych – art. 35 ust. 7 RODO.

Bezwzględnie należy pamiętać, że RODO nie narzuca konkretnej nazwy ani struktury tego dokumentu. Można go nazwać polityką ochrony danych osobowych czy polityką bezpieczeństwa. Ważna jest natomiast jego treść, a w zasadzie ważne jest, by hotel był w stanie wykazać, że wymienione rejestry po prostu posiada i aktualizuje. Taki dokument umożliwi bowiem wykazanie również realizacji przez administratora zasady rozliczalności.

Zaleca się, by taki wewnętrzny dokument został „stworzony” po przeprowadzeniu w hotelu audytu polegającego na ustaleniu przede wszystkim przepływu danych osobowych w organizacji, określeniu celu przetwarzania, wszelkich podstaw prawnych, weryfikacji istniejącej dokumentacji z zakresu ochrony danych osobowych oraz ocenie stopnia zabezpieczeń danych osobowych i stosowanych środków technicznych i organizacyjnych. Innymi słowy, dokument określony jako polityka bezpieczeństwa, powinien zostać utworzony po dokonaniu tzw. mapowania procesów przetwarzania danych osobowych.

Poniższa tabela zawiera przykładowe **informacje**, które - naszym zdaniem - **powinny znaleźć się w polityce bezpieczeństwa danych osobowych hotelu:**

- Wykaz danych osobowych przetwarzanych przez hotel;
- Zakres praw i obowiązków Inspektora Ochrony Danych Osobowych;
- Procedura zgłaszania naruszeń;
- Zakres postępowania w zakresie obsługi wniosków;
- Procedura nadawania oraz realizacji upoważnień;
- Procedura wyboru i kontroli podmiotu przetwarzającego;
- Procedury zabezpieczeń IT;
- Procedura oceny skutków.

POLITYKA BEZPIECZEŃSTWA

Wykaz danych osobowych przetwarzanych przez hotel, podstawy i cele przetwarzania oraz czas przetwarzania danych osobowych i okres przechowywania danych osobowych oraz wzory klauzul informacyjnych	Powyższe informacje mogą zostać zawarte w **rejestrze czynności przetwarzania danych osobowych**, który to rejestr może stanowić załącznik do polityki. Elementy obligatoryjne oraz forma rejestru zostały zawarte w art. 30 RODO. Obowiązek prowadzenia rejestru czynności przetwarzania nie dotyczy przedsiębiorców lub podmiotów zatrudniających mniej niż 250 osób. Zaznaczyć jednak należy, że zwolnienie z obowiązku prowadzenia rejestru nie będzie jednak miało zastosowania co do tych przedsiębiorców lub podmiotów w przypadku gdy: - przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, - nie ma charakteru sporadycznego, lub - obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1 RODO lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO. Warto rozważyć prowadzenie ww. rejestru, w przypadku nawet braku obowiązku, jako że jest to dobre narzędzie do oceny i monitorowania procesów przetwarzania w danym hotelu.
Zakres praw i obowiązków Inspektora Ochrony Danych Osobowych oraz procedura jego powołania	Hotel powinien przeprowadzić analizę, która pomoże stwierdzić, czy należy powołać IOD. Nawet jeśli okaże się, że nie musiał powoływać inspektora, będzie mógł udowodnić, że wziął pod uwagę odpowiednie czynniki. Wyznaczenie inspektora jest bowiem dla jednych podmiotów obligatoryjne, a dla innych dobrowolne. Nawet jeśli hotel wyznaczy inspektora sam z siebie, osoba pełniąca tą funkcję będzie mieć takie same obowiązki i prawa, co inspektor wyznaczany obowiązkowo. W przypadku powołania Inspektora Ochrony Danych, hotel jest zobowiązany powiadomić organ nadzorczy o tym fakcie, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu wyznaczonego IOD.

Zakres praw i obowiązków Inspektora Ochrony Danych Osobowych oraz procedura jego powołania	Urząd Ochrony Danych Osobowych na swojej stronie internetowej udostępnia w tym zakresie odpowiednie formularze: *https://uodo.gov.pl/pl/p/formularze-zwiazane-iod* Do obowiązków IOD należy m.in. informowanie administratora oraz jego pracowników o ciążących na nich obowiązkach związanych z przetwarzaniem danych osobowych, monitorowanie przestrzegania przepisów, współpraca z organem nadzorczym.
Procedura zgłaszania naruszeń ochrony danych do Urzędu Ochrony Danych Osobowych	Procedura powinna zawierać informacje: - na czym polega naruszenie ochrony danych osobowych, - kiedy powinno nastąpić zgłoszenie takiego naruszenia do Prezesa UODO, a kiedy hotel jest z tego zwolniony; - kiedy następuje zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych oraz - wszelkie kwestie związane z prowadzeniem rejestru naruszeń ochrony danych. Na poinformowanie PUODO o naruszeniu hotel ma 72 godziny. Zawiadomienie powinno zawierać: - ogólny opis naruszenia, tj. jego charakter, wskazywać kategorię oraz szacunkową ilość osób, których naruszenie dotyczy; - informację kontaktową do IOD lub innej, wskazanej w tym celu osoby; - opis możliwych konsekwencji naruszenia; - opis zastosowanych lub planowanych do zastosowania środków mających na celu ograniczenie lub usunięcie konsekwencji naruszenia. Jeżeli nie uda się hotelowi zebrać wszystkich niezbędnych informacji w ciągu 72 godzin, powinien wysłać zawiadomienie z zebranymi do upływu 72 godzin informacjami, a następnie sukcesywnie uzupełniać wymagane informacje.
Zakres postępowania w zakresie obsługi wniosków osób, których dane są przetwarzane przez hotel	Procedura powinna zawierać określone zasady prowadzenia komunikacji z osobą, której dane dotyczą, tj. tryb rozpoznawania wniosków, kiedy następuje odmowa realizacji wniosku, tryb weryfikacji tożsamości osób składających wnioski. Procedura może również zawierać przykładowe formularze wniosków.
Procedura nadawania oraz realizacji upoważnień do przetwarzania danych osobowych	Hotel, zgodnie z zasadą rozliczalności, musi być w stanie wykazać, że osoby dopuszczone do przetwarzania danych osobowych działają na jego polecenie. W tym celu zazwyczaj wręcza się np. pracownikom pisemne upoważnienia. Polityka bezpieczeństwa w tym zakresie może zostać dodatkowo uzupełniona o wzór takiego upoważnienia oraz rejestr osób upoważnionych do przetwarzania danych osobowych.

Procedura wyboru i kontroli podmiotu przetwarzającego	Tylko, jeśli hotel zamierza zawierać umowy powierzenia przetwarzania danych. Pojawia się wtedy też konieczność prowadzenia rejestru umów powierzenia przetwarzania danych.
Procedury zabezpieczeń systemów IT i nośników IT	Procedura taka może zawierać informacje dotyczące np. rozpoczęcia, zawieszenia i zakończenia pracy w systemach IT, postępowania w przypadku wystąpienia naruszeń w systemach IT, czy użytkowania komputerów przenośnych oraz tworzenia kopii zapasowych.
Procedura oceny skutków dla ochrony danych osobowych	Czyli wdrożenie środków umożliwiających odpowiednie zarządzanie ryzykiem naruszenia praw i wolności osób, których dane dotyczą. W praktyce oznacza to, że hotel powinien stale monitorować ryzyko powodowane przez czynności przetwarzania w celu określenia, kiedy dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Kilka słów dodatkowo o zawieraniu przez hotel umów powierzenia przetwarzania danych osobowych.

W niektórych sytuacjach hotel może posłużyć się przy przetwarzaniu danych osobowych innym, zewnętrznym podmiotem działającym w jego imieniu, czyli podmiotem przetwarzającym (inaczej zwanym również procesorem). W takiej sytuacji zawiera się właśnie umowy powierzenia przetwarzania danych osobowych.

Skorzystanie ze wsparcia takiego podmiotu jest stosowane zwłaszcza w sytuacji oddelegowania pewnego zakresu obowiązków na zewnętrzny podmiot, tj. w przypadku skorzystania z usług firm świadczących obsługę np. z zakresu:

a. księgowości;
b. rekrutacji;
c. transportowych, taksówkarskich (np. sytuacja gdy hotel powierza zewnętrznej firmie dane gości hotelowych korzystających z usług odbioru i dojazdu z lotniska do hotelu);
d. hostingowych, informatycznych, teleinformatycznych;
e. pośrednictwa w rezerwacji noclegu w hotelu;
f. niszczenia dokumentów;
g. archiwizacji.

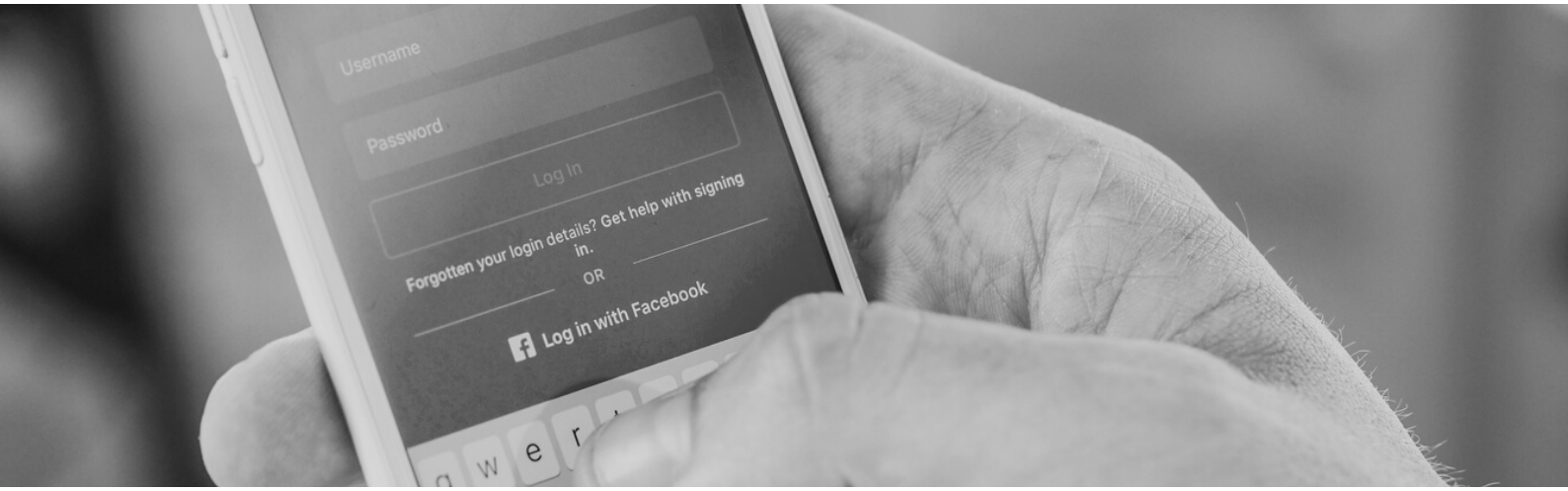
Co powinna zawierać umowa powierzenia przetwarzania danych osobowych:
a. określenie przedmiotu przetwarzania, celu, charakteru przetwarzania danych osobowych;
b. wskazanie czasu trwania przetwarzania oraz rodzaju powierzanych danych osobowych;
c. wskazanie kategorii osób, których dane dotyczą w związku z powierzeniem;
d. zapewnienie procesora, aby osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy;
e. zobowiązania do podjęcia środków bezpieczeństwa przetwarzania;
f. określenie warunków podpowierzenia przetwarzania danych;
g. zobowiązanie do wsparcia administratora w realizacji żądań praw osób, których dane dotyczą oraz innych obowiązków wskazanych w art. 32-36 RODO, odnoszących się do zapewnienia odpowiedniego poziomu bezpieczeństwa danych;
h. zawarcie uprawnienia administratora do podjęcia decyzji usunięciu lub zwróceniu wszelkich danych osobowych w związku z powierzeniem;
i. umożliwienie administratorowi dostępu do informacji do wykazania spełnienia wymogów umowy powierzenia;
j. postanowienia dotyczące umożliwienia administratorowi lub audytorowi, przeprowadzania audytów.

Podkreślić należy, że administrator oraz podmiot przetwarzający ponoszą solidarną odpowiedzialność za naruszenie przepisów RODO (art. 82 RODO). Takie ustalenie zasad odpowiedzialności powoduje, że administrator – przedsiębiorca prowadzący hotel czy pensjonat powinien zwrócić szczególną uwagę nie tylko na zasady przetwarzania danych osobowych w swojej organizacji, ale również dołożyć staranności przy wyborze podmiotu przetwarzającego dane osobowe.

10 DOSTOSOWANIE STRONY INTERNETOWEJ HOTELU DO PRZEPISÓW RODO.

Wdrożenie RODO w hotelu, to nie tylko przygotowanie dokumentacji wewnętrznej, ale również wprowadzenie odpowiednich zabezpieczeń w przypadku podejmowania działań w sieci. Powyższe oznacza, że również strona internetowa powinna być dostosowana do przepisów z zakresu ochrony danych osobowych, bowiem dane osobowe są gromadzone również za pomocą stron www poprzez, np. udostępnione formularze kontaktowe, wtyczki czy ciasteczka cookies.

Zaleca się zatem, by na stronie internetowej hotelu zamieścić politykę prywatności (zawierającą m.in. informacje dotyczące plików cookies, czy szczegółowe informacje o przetwarzaniu danych osobowych) dostępną dla każdego użytkownika odwiedzającego stronę hotelu, czy pensjonatu.



Jeśli zatem na stronie internetowej hotelu jest zamieszczony:

a. formularz kontaktowy umożliwiający przesyłanie zapytania (ze wskazaniem danych, które pozwolą udzielić klientowi odpowiedzi) - koniecznie należy zwrócić uwagę na to, jakie dane osobowe pozyskiwane są za jego pomocą. Zdarzają się bowiem formularze, które wymagają podania zarówno adres e-mail, jak i nr telefonu (o skrajnych przypadkach, w których wymagane jest wpisanie daty urodzenia czy miejscu zamieszkania nie wspominając). Powyższe nie jest oczywiście błędem, z tymże należy pamiętać o zasadzie minimalizacji. Zatem uzależnienie podania wszystkich tych danych od zadania pytania, może okazać się nadużyciem. Aby udzielić odpowiedzi na pytanie np. w zakresie dostępności parkingu hotel nie powinien wymagać podania płci czy wieku, gdyż te informacje są dla udzielenia odpowiedzi bez znaczenia. Również w przypadku formularza kontaktowego należy pamiętać o obowiązku informacyjnym (informacja o przetwarzaniu danych osobowych może być w wersji skróconej, tylko należy w takim przypadku dodatkowo podpiąć link do polityki prywatności);

b. formularz zapisu na newsletter - podobnie jak w przypadku formularza kontaktowego, należy pamiętać o zasadzie minimalizacji danych osobowych oraz o klauzuli informacyjnej; zgoda na zapis na newsletter może przybrać formę wyraźnego działania potwierdzającego, a nie tylko formalnego oświadczenia. Przykładowo, Ministerstwo Cyfryzacji dopuszcza podanie przez odbiorcę adresu e-mail w polu formularza internetowego opisanego słowami: „*podaj swój adres e-mail, jeżeli chcesz otrzymywać od nas informacje o …*”.

c. formularz umożliwiający rezerwację pokoju w hotelu. Podobnie jak w przypadku dwóch ww. formularzy należy zweryfikować jakie dane hotel gromadzi i spełnić obowiązek informacyjny. W sytuacji pozyskiwania danych osobowych klientów dotyczących kart płatniczych i kredytowych należałoby zweryfikować kwestie zapewnienia odpowiedniego bezpieczeństwa tych danych.

W kontekście zamieszczenia na stronie internetowej hotelu wtyczek, pojawia się również kwestia korzystania w tym zakresie z usług podmiotów przetwarzających dane poza UE. Przekazywanie danych do państw trzecich jest możliwe, gdy państwo to spełni określone wymogi, tj. gdy Komisja Europejska stwierdzi, że to państwo zapewnia odpowiedni poziom ochrony danych osobowych. Hotel musi zatem zapewnić legalność transferów tych danych.

11 MARKETING BEZPOŚREDNI HOTELU.

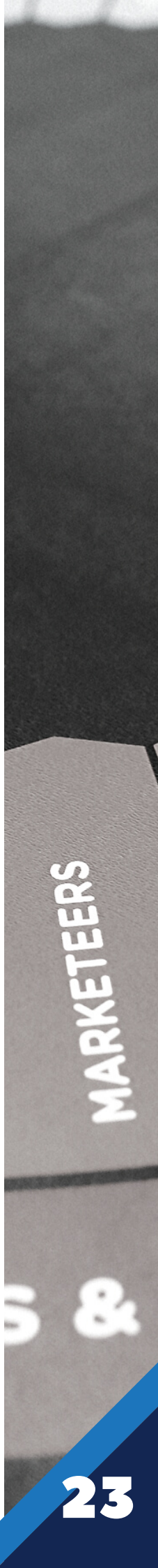
Zgodnie z RODO, a dokładnie z motywem 47 RODO, nie zawsze potrzebna jest zgoda, żeby przetwarzać dane osobowe w celach marketingu bezpośredniego. Wspomniany motyw wskazuje, że swoje marketingowe działania można oprzeć na tzw. uzasadnionym interesie administratora. Niestety jednak, w przypadku marketingu należy dodatkowo pamiętać nie tylko o RODO, ale również o innych obowiązujących przepisach, tj. o ustawie o świadczeniu usług drogą elektroniczną (np. w zakresie wysyłania e-maili marketingowych) oraz ustawie prawo telekomunikacyjne (np. przy wysyłce SMS z treścią zawierającą informacje marketingowe). Wyżej wymienione ustawy wprost wskazują, że jakakolwiek komunikacja z klientem, czy to za pomocą środków komunikacji elektronicznej telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego, bez uzyskania uprzednio zgody jest zakazana.

W jakiej formie powinna być wyrażona zgoda na marketing?

RODO, w art. 4 ust. 11 stwierdza, że 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. RODO wprost wskazuje, że jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Jeżeli zatem hotel pozyskał zgodę subskrybenta tylko i wyłącznie na wysyłkę newslettera, nie powinien wysłać swoim gościom informacji handlowych zaprzyjaźnionej firmy, jeśli nie uzyskał uprzednio od niego zgody na powyższe.

Nie tylko RODO zakazuje tzw. spamu, czyli rozsyłania niezamówionych (bez uzyskania zgody) informacji handlowych.
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, w art. 10 ust. 1 także zakazuje spammingu. Powyższe odnosi się on nie tylko do masowego przesyłania niezamówionych informacji, ale także do przesyłania pojedynczych niezamówionych informacji.



12 JAKIE KARY PRZEWIDUJE RODO?

Prezes Urzędu Ochrony Danych Osobowych jest uprawniony do nakładania na przedsiębiorcę, który naruszył postanowienia RODO, kary pieniężnej. Do okoliczności, które organ będzie brał pod uwagę decydując o ukaraniu danego podmiotu oraz ustalając wysokości kary należą m. in.: charakter, czas i waga naruszenia, umyślność lub nieumyślność podmiotu, wdrożone u administratora środki organizacyjne oraz techniczne, czy też sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, a w szczególności, czy i w jakim zakresie przedsiębiorca zgłosił naruszenie.

Administracyjnej karze pieniężnej w wysokości do 10.000.000 EUR, a w przypadku przedsiębiorstwa –w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego(przy czym zastosowanie ma kwota wyższa)podlegają następujące naruszenia przepisów:

a. naruszenie obowiązków administratora i podmiotu przetwarzającego wymienionych w RODO, jak np.: brak weryfikacji wyrażenia zgody przez opiekuna dziecka, które nie ukończyło jeszcze 16 roku życia, na przetwarzanie jego danych osobowych, brak prowadzenia rejestru operacji przetwarzania, brak powołania IOD w przypadkach obligatoryjnych, bark informowania organu nadzorczego o naruszeniach w zakresie ochrony danych osobowych, nieprzestrzeganie obowiązków związanych z certyfikacja przedsiębiorcy przez stosowny podmiot;
b. naruszenie obowiązków podmiotu certyfikującego wymienionych w RODO;
c. naruszenie obowiązków podmiotu monitorującego związanych z podjęciem stosownych działań w przypadku stwierdzenia naruszenia przez danego przedsiębiorcę zatwierdzonego kodeksu postępowania.

Administracyjnej karze pieniężnej w wysokości do 20.000.000 EUR, a w przypadku przedsiębiorstwa –w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa) podlegają następujące naruszenia przepisów:
a. naruszenie podstawowych zasad przetwarzania, w tym warunków zgód na przetwarzanie określonych w RODO;
b. naruszenie praw osób, których dane są przetwarzane;
c. naruszenie przepisów dotyczących przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej;
d. nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy lub niezapewnienie dostępu organowi nadzorczemu;
e. naruszenie obowiązków wynikających z przepisów krajowych danego państwa członkowskiego, uchwalonych na podstawie RODO;
f. nieprzestrzeganie środków naprawczych nałożonych przez organ nadzorczy.

Nałożenie na przedsiębiorcę prowadzącego hotel ww. administracyjnej kary pieniężnej nie zwalnia go z ewentualnej odpowiedzialności cywilnej wobec osób, których dane dotyczą.

13 POWIADOMIENIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH.

Naruszeniem ochrony danych osobowych jest naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych w ramach prowadzonej przez administratora danych działalności.

Urząd Ochrony Danych Osobowych wydał poradnik (dostępny pod adresem: https://uodo.gov.pl/pl/134/1029), który szczegółowo określono czym jest naruszenie ochrony danych osobowych oraz jak postępować w przypadku wystąpienia takiego naruszenia. Przede wszystkim w przypadku wykrycia przez hotel naruszenia ochrony danych osobowych konieczne jest dokonanie analizy w odniesieniu do wystąpienia ryzyka naruszenia praw i wolności osób fizycznych. Jeżeli w wyniku ww. badania okaże się, że nie ma prawdopodobieństwa wystąpienia takiego ryzyka, hotel jest zwolniony z obowiązku powiadamiania organu nadzorczego o naruszeniu.

Zgodnie z wytycznymi Prezesa Urzędu Ochrony Danych Osobowych:

Z ryzykiem naruszenia praw lub wolności osób fizycznych mamy do czynienia wówczas, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np. dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, nadużycia finansowe, straty finansowe, nieuprawnione cofnięcie pseudonimizacji, utrata poufności danych osobowych chronionych tajemnicą zawodową, naruszenie dobrego imienia lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej. Jeżeli naruszenie dotyczy danych osobowych ujawniających pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych lub danych genetycznych, dotyczących zdrowia lub życia seksualnego, należy uznać, że występuje duże prawdopodobieństwo takiej szkody.

W jaki sposób powiadomić Prezesa UODO o naruszeniu?

Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl na cztery sposoby:

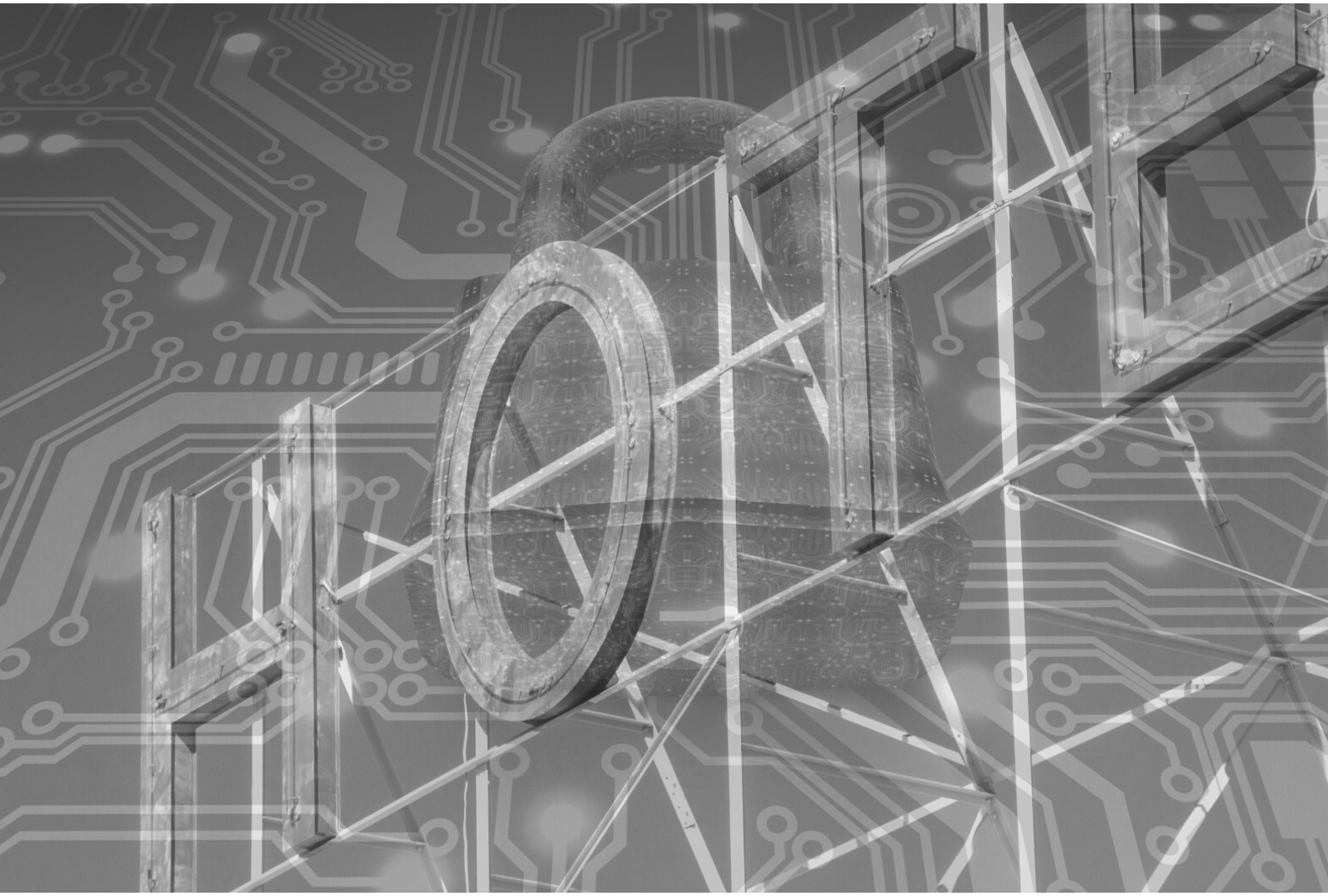
1. elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie biznes.gov.pl;
2. elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP;
3. elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl;
4. tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

Jaki jest termin na zgłoszenie naruszenia ochrony danych osobowych?

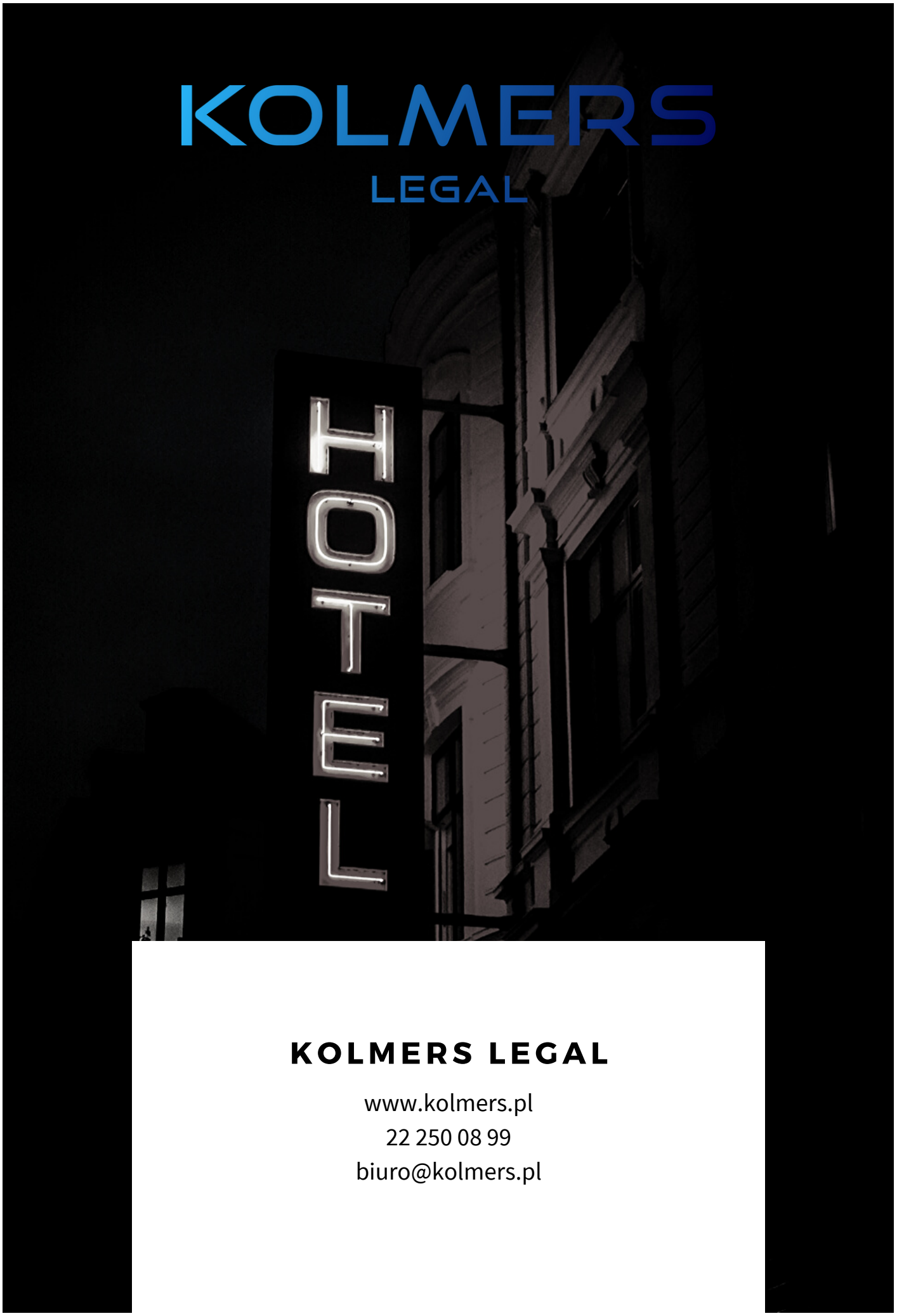
Hotel, w przypadku wystąpienia naruszenia ochrony danych osobowych, powinien dokonać zgłoszenia organowi nadzorczemu bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Kiedy trzeba zawiadamiać o naruszeniu osoby, których dane dotyczą?

W sytuacji, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, hotel bez zbędnej zwłoki zobowiązany jest zawiadamia osobę, której dane dotyczą, o takim naruszeniu (art. 34 RODO).



KOLMERS
LEGAL



KOLMERS LEGAL

www.kolmers.pl
22 250 08 99
biuro@kolmers.pl