IGHP | IZBA GOSPODARCZA HOTELARSTWA POLSKIEGO

Dane osobowe w hotelarstwie
Czy RODO to rewolucja?

Gdańsk

21 listopada

2017

Dane osobowe

Podstawa prawna regulacji:

1. Chwila obecna – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

2. Od maja 2018 r. - ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – **RODO.**

3. Od maja 2018 r. (?) – ustawa o ochronie danych osobowych (?) i ustawa wprowadzająca ustawę o ochronie danych osobowych.

IGHP

Dane osobowe – czyli co?

RODO - "dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania **osobie fizycznej** ("osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można **bezpośrednio lub pośrednio zidentyfikować**, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

IGHP

Dane osobowe – przykłady

- imiona i nazwiska,
- numery PESEL, NIP, dowodów osobistych, paszportów, praw jazdy,
- adres zamieszkania,
- wizerunek (zdjęcie, zapis monitoringu),
- rejestr wejść i wyjść,
- data urodzenia (wiek),
- adres e-mail,
- adresy IP (w powiązaniu z innymi danymi, np. miejscem zamieszkania),
- **login internetowy lub nazwa użytkownika** (nowość RODO),
- **dane o lokalizacji, położeniu** (nowość RODO),
- informacje finansowe,
- cechy fizyczne tzw. **dane biometryczne** (wzrost, waga) (nowość RODO),
- wykształcenie,
- dane o stanie zdrowia.

Czy potraficie Państwo?

- Zidentyfikować czyje dane osobowe przetwarzacie i na jakiej podstawie prawnej?
- Wskazać cele, dla których przetwarzacie dane osobowe?
- Określić czy wykorzystujecie dane osobowe zgodnie z celami, w jakich zostały zebrane?
- Wskazać jak długo przetwarzcie dane osobowe poszczególnych osób?
- Zidentyfikować zbędne dane osobowe i usunąć je bez szkody dla firmy?
- Określić wszystkie podmioty, którym udostępniacie dane osobowe?
- Określić, czy używane oprogramowanie w firmie jest aktualne?

IGHP

Rozliczalność – zasada klucz

RODO wprowadza zasadę rozliczalności, oznaczającą **obowiązek wykazania zgodnego z prawem przetwarzania danych osobowych.**

Bez możliwości udzielenia odpowiedzi na pytania, nie będziecie w stanie przetwarzać danych w zgodnie z RODO.

IGHP

Rozliczalność - elementy

1. Zasada zgodności z prawem, rzetelności i przejrzystości

2. Zasada ograniczenia celu

3. Zasada minimalizacji danych

4. Zasada prawidłowości

5. Zasada ograniczenia przechowywania

6. Zasada integralności i poufności

Nowe uprawnienia osób, których dane dotyczą

Prawo do przejrzystej komunikacji – art. 12 RODO

Rozszerzony obowiązek informacyjny – art. 13 i 14 RODO

Prawo do bycia zapomnianym – art. 17 RODO

Prawo do ograniczenia przetwarzania – art. 18 RODO

Prawo do przenoszenia danych – art. 20 RODO

Regulacja prawna profilowania, prawo do sprzeciwu – art. 21 i 22 RODO

Nowe obowiązki administratora

1. **Privacy by design/privacy by default** – art. 24 i 25 RODO – Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie RODO i by móc to wykazać (rozliczalność)

2. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były **wyłącznie** te dane osobowe, **które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania**

IGHP

Nowe obowiązki administratora

Ocena ryzyka przetwarzania danych osobowych – art. 32 RODO
Administrator będzie mógł wdrożyć następujące środki ochrony:

- pseudonimizację i szyfrowanie danych osobowych,
- zapewnić zdolność do ciągłej poufności, integralności, dostępności i odporności systemów i usług przetwarzania
- posiadać zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularnie testować i oceniać skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania danych

IGHP

Podstawy prawne przetwarzania

Zgodnie z RODO przetwarzanie jest zgodne z prawem m.in.

- na podstawie zgody osoby, której dane dotyczą,
- w związku z zawartą umową.

Upoważnienie innego podmiotu do przetwarzania danych (outsourcing)

Możliwe są sytuacje, w których przetwarzanie danych osobowych będzie wykonywane w imieniu administratora przez podmiot zewnętrzny.

Przykładowo:

- obsługa kadrowo-płacowa wiąże się z przekazaniem danych osobowych firmie księgowej,
- zarządzanie i support infrastruktury informatycznej może łączyć się z dostępem do danych osobowych.

IGHP

Upoważnienie innego podmiotu do przetwarzania danych (outsourcing)

Nowe wymagania prawne – art. 28 RODO

Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, **określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora**

IGHP

Kary administracyjne - nowość RODO

Kary administracyjne za naruszenie zasad ochrony danych osobowych.

Maksymalna wysokość kar to **20.000.000 euro** lub do **4%** światowego obrotu z poprzedniego roku obrotowego w przypadku przedsiębiorców.

W zależności od stopnia naruszenia, kara może być miarkowana.

IGHP

Pozwy cywilne

RODO rozszerza prawa osób, których dane są przetwarzane w zakresie dochodzenia roszczeń na drodze cywilnoprawnej (pozew o naruszenie zasad przetwarzania danych osobowych).

W tym zakresie mogą również działać **fundacje i stowarzyszenia reprezentujące osoby fizyczne.**

Furtka dla organizacji szantażujących przedsiębiorców (casus klauzul abuzywnych).

IGHP

Propozycje rozwiązań dla branży

1. **Branżowy kodeks postępowania** w zakresie przetwarzania danych osobowych uzgadniany z GIODO (UODO)
2. **Szkolenia** organizowane przez **IGHP**
3. **Audyty** przetwarzania danych osobowych
4. **Standaryzacja procedur** przetwarzania danych osobowych
5. **Certyfikacja** przetwarzania danych osobowych

Działania te zmniejszą ryzyko nakładania kar administracyjnych

IGHP

Dziękujemy za uwagę

Marcin Mączyński
Sekretarz Generalny IGHP

marcin.maczynski@ighp.pl

Bądź z nami w kontakcie!

www.ighp.pl

E-MAIL
ighp@ighp.pl

TELEFON
+48 22 251 79 11
+48 510 006 856

ADRES
ul. Mickiewicza 9 m. 4
01-517 Warszawa