trzy dekady
doświadczenia
i sukcesów

SPCG

1988 - 2018

INCYDENT NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH NA GRUNCIE GDPR

DR JACEK BŁACHUT
SENIOR ASSOCIATE, KANCELARIA SPCG

BANKING TECH & SECURITY
27.03.2019

trzy dekady
doświadczenia
i sukcesów

SPCG

1988 - 2018

Incydent naruszenia danych osobowych

RODO (art. 4 pkt 12) - "naruszenie ochrony danych osobowych" (*personal data breach*) 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;

„Naruszenie ochrony danych osobowych”:

- to nie każde naruszenie RODO, a tylko takie, które dotyczy naruszenia zabezpieczeń;
- możliwe tylko po rozpoczęciu przetwarzania danych osobowych;
- może być wynikiem zarówno zachowania nieumyślnego jak i umyślnego.

Incydent naruszenia danych osobowych

Sprawca „naruszenia ochrony danych osobowych”:

- z jednej strony: administrator lub podmiot przetwarzający;
- z drugiej strony: osoba nieuprawniona podejmująca działanie bezprawne (np. osoba dokonująca włamania do systemów informatycznego).

„Naruszenie ochrony danych osobowych” to sytuacja, w której wystąpi określony w ww. przepisie skutek. (np. zniszczenie, utracenie danych osobowych). Brak takiego skutku = brak naruszenia ochrony danych (np. przygotowanie pakietu informacji do odbioru przez osobę nieuprawnioną, która nie zjawia się po odbiór).

Dwie kategorie skutków „naruszenia ochrony danych”:

1. naruszenie integralności danych (zniszczenie, utracenie, zmodyfikowanie),
2. naruszenie poufności danych.

Incydent naruszenia danych osobowych

Zniszczenie Dane nie istnieją lub przestały istnieć w postaci, w której administrator mógłby je wykorzystać.
Przykład: skasowanie plików w systemie informatycznym wraz ze zniszczeniem kopii zapasowej; zniszczenie części dokumentacji papierowej, która pełniła funkcję identyfikującą pozostałe informacje z określonymi osobami.

Utrata Dane mogą nadal istnieć, ale administrator utracił nad nimi kontrolę, nie posiada już do nich dostępu.
Przykład: kradzież dokumentacji; przejęcie systemu informatycznego.

Zmodyfikowanie Zmiana, zniekształcenie danych osobowych; zdekompletowanie danych osobowych.
Przykład: pomieszanie numerów telefonów; zmiany w znajdujących się w bazie nazwiskach.

Ujawnienie Przesłanie, rozpowszechnianie lub udostępnienie danych.
Przykład: wysłanie maila do niewłaściwej osoby.

Dostęp do danych Dostęp osoby trzeciej w wyniku własnego działania, a nie działania osoby realizującej przetwarzanie.
Przykład: włamanie do systemu informatycznego.

Skutki incydentów naruszenia danych osobowych

1. Skutek w postaci obowiązków zgłoszeniowych i dokumentacyjnych
2. Skutek w postaci ryzyka poniesienia odpowiedzialności administracyjnej
3. Skutek w postaci ryzyka poniesienia odpowiedzialności cywilnoprawnej
4. Skutek w postaci ryzyka poniesienia odpowiedzialności karnoprawnej
5. Skutki organizacyjne

Incydent naruszenia danych osobowych

Obowiązki zgłoszeniowe i dokumentacyjne

1. Obowiązek zgłoszeniowy do Prezesa Urzędu Ochrony Danych Osobowych
2. Obowiązek powiadomienia osoby, której dane dotyczą
3. Obowiązek odnotowania incydentu – rejestr incydentów

Zakres ww. obowiązków uzależniony od ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

Incydent naruszenia danych osobowych

Obowiązki zgłoszeniowe i dokumentacyjne

Kiedy zgłoszenie do Prezesa Urzędu Ochrony Danych Osobowych?

Zawsze, **chyba że** jest **mało prawdopodobne**, że naruszenie skutkować będzie ryzykiem naruszenia praw lub wolności osób fizycznych.

Kiedy powiadomienie osoby, której dane dotyczą?

Jeżeli naruszenie może powodować **wysokie** ryzyko naruszenia praw lub wolności osób fizycznych poza sytuacjami wskazanymi w RODO.

Kiedy obowiązek odnotowania incydentu?

W przypadku każdego naruszenia ochrony danych osobowych, tj. gdy spełnione są warunki wynikające z definicji tego pojęcia.

Incydent naruszenia danych osobowych

Obowiązki zgłoszeniowe i dokumentacyjne

Czynniki istotne dla oceny stopnia ryzyka związanego z incydentem (ocena obiektywna):

- rodzaj naruszenia (np. wgląd do danych przez osobę nieupoważnioną, a utrata danych);
- charakter, wrażliwość i zakres danych dotkniętych naruszeniem (np. dane o stanie zdrowia, dane osobowe dzieci);
- łatwość w zidentyfikowaniu osoby, której dane dotyczą, na podstawie danych dotkniętych naruszeniem (np. imię i nazwisko, a ciąg cyfr stanowiących numer rachunku);
- konsekwencje naruszenia dla osób, których dane dotyczą (np. podatność na oszustwo, kradzież tożsamości);
- ilość danych, których dotknęło naruszenie (np. utrata całej bazy danych);
- rodzaj działalności administratora danych (np. bank vs. kwiaciarnia).

Incydent naruszenia danych osobowych

Obowiązki zgłoszeniowe i dokumentacyjne

Przykłady incydentów skutkujących **wysokim ryzykiem (obowiązek powiadomienia osoby)**, por. Kodeks dobrych praktyk ZBP:

- wyciek (tj. niekontrolowane ujawnienie) informacji z bazy danych z numerami kart kredytowych wraz z informacjami pozwalającymi na wykonanie transakcji przez osobę trzecią;
- wyciek bazy zawierającej tylko pojedynczą daną, ale pozwalającą jednocześnie nawiązać kontakt z osobą fizyczną np. numer telefonu, adres email;
- wysłanie pocztą elektroniczną/tradycyjną dokumentów zawierających dane stanowiące tajemnicę bankową do osoby nieupoważnionej (np. błędne wysłanie karty kredytowej);
- przechwycenie oraz wyciek danych/narzędzi służących do logowania i identyfikacji Klientów w bankowości elektronicznej, zagubienie/kradzież dokumentów z danymi Klientów, zerwanie plomb założonych na pojemnikach służących do archiwizacji dokumentów.

Incydent naruszenia danych osobowych

Obowiązki zgłoszeniowe i dokumentacyjne

Przykłady incydentów z **niewielkim prawdopodobieństwem ryzyka (wyłącznie obowiązek udokumentowania incydentu)**, por. Kodeks dobrych praktyk ZBP:

- wyciek (tj. niekontrolowane ujawnienie) informacji z bazy danych z numerami kart kredytowych lub numerami rachunków lub numerami umów (bądź fragmentów tych numerów) nie pozwalających na identyfikację konkretnej osoby;
- zagubienie nośnika danych z plikiem zaszyfrowanym, przy czym klucz używany do odszyfrowania tych danych nie został złamany w wyniku naruszenia;
- błędne wprowadzenie danych kontaktowych Klienta do systemu banku lub rejestru kredytowego, jeżeli w wyniku tego błędu nie doszło do ujawnienia tajemnicy bankowej ani naruszenia interesów konsumenta;
- ujawnienie informacji prawnie chronionych osobie trzeciej, jeżeli do ich ujawnienia doszło w z winy Klienta (np. udostępnienie treści wiadomości SMS).

Incydent naruszenia danych osobowych

Obowiązki zgłoszeniowe i dokumentacyjne

Zgłoszenie incydentu do Prezesa Urzędu Ochrony Danych Osobowych.

- **Jak szybko?** Bez zbędnej zwłoki, max 72h od **stwierdzenia naruszenia**; jeśli później, to z wyjaśnieniem przyczyny opóźnienia. Co do zasady **administrator stwierdza** naruszenie w tym samym momencie, w którym naruszenie stwierdza procesor (procesor musi zawiadomić administratora bez zbędnej zwłoki).
- Podmiot przetwarzający wykonuje zgłoszenie do administratora. Podmiot przetwarzający powinien zgłosić administratorowi każde naruszenie, niezależnie od oceny ryzyka związanego z incydentem.
- **Co ma zawierać zgłoszenie? Przynajmniej:**
  - ✓ opis charakteru naruszenia, w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych, których dotyczy naruszenie;
  - ✓ imię, nazwisko i dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego;
  - ✓ opis możliwych konsekwencji naruszenia oraz opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu i minimalizacji jego negatywnych skutków.

Incydent naruszenia danych osobowych

Obowiązki zgłoszeniowe i dokumentacyjne

Powiadomienie osoby, której dane dotyczą.

- **Jak szybko?** Bez zbędnej zwłoki.
- **Co ma zawierać zawiadomienie?**
  - ✓ opis charakteru naruszenia napisany prostym, zrozumiałym językiem;
  - ✓ imię, nazwisko i dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego;
  - ✓ opis możliwych konsekwencji naruszenia oraz opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu i minimalizacji jego negatywnych skutków.

Incydent naruszenia danych osobowych

Obowiązki zgłoszeniowe i dokumentacyjne

Dokumentacja incydentów może przybrać postać uzupełniania rejestru incydentów.

Musi zawierać: Okoliczności naruszenia | Skutki naruszenia | Podjęte działania zaradcze

Może zawierać dalsze informacje, np.:

- Opis charakteru naruszenia
- Data i godzina stwierdzenia naruszenia
- Źródło naruszenia
- Stopień ryzyka
- Zawiadomienie organu nadzorczego
- Powiadomienie osoby, której dane dotyczą
- Kategorie osób, których dane zostały naruszone
- Przybliżona liczba osób, których dane zostały naruszone
- Kategorie wpisów danych osobowych, których dotyczy naruszenie
- Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie
- Możliwe konsekwencje naruszenia ochrony
- Zastosowane lub proponowane środki w celu zaradzenia naruszeniu
- Zastosowane środki w celu zminimalizowania negatywnych skutków naruszenia

Skutek w postaci ryzyka poniesienia odpowiedzialności administracyjnej

Podstawa nałożenia administracyjnej kary pieniężnej:

- art. 83 ust. 4 RODO – do 10.000.000 euro lub 2 % całkowitego rocznego światowego obrotu

  Naruszenie przepisów dotyczących obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25 -39 oraz 42 i 43 RODO (art. 32 – bezpieczeństwo danych osobowych).

czy

- art. 83 ust. 5 RODO - do 20.000.000 euro lub 4 % całkowitego rocznego światowego obrotu

  Naruszenie przepisów dotyczących podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9. (art. 5 ust. 1 lit. f) RODO: przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych – wymóg integralności i poufności).

Skutek w postaci ryzyka poniesienia odpowiedzialności administracyjnej

Szczególna rola następujących dyrektyw wymiaru kary:

- Umyślny lub nieumyślny charakter naruszenia.
- Działania podjęte w celu zminimalizowania szkody poniesionej przez osobę, której dane dotyczą.
- Stopień odpowiedzialności z uwzględnieniem środków technicznych o organizacyjnych (*privacy by design, privacy by default*, techniczna i organizacyjna ochrona danych).
- Sposób, w jaki organ nadzorczy dowiedział się o naruszeniu (prawidłowość wykonania obowiązku zgłoszeniowego).

Skutek w postaci ryzyka poniesienia odpowiedzialności cywilnoprawnej

Prawo do ochrony sądowej osoby, której dane osobowe były przetwarzane sprzecznie z RODO, w wyniku czego naruszono jej prawa wynikające z rozporządzenia. **Prawo do odszkodowania**.

Właściwość miejscowa: sąd państwa członkowskiego, w którym administrator lub podmiot przetwarzający ma jednostkę organizacyjną lecz możliwość wytoczenia przed sąd miejsca zwykłego pobytu osoby, której dane dotyczą.

Właściwość rzeczowa: w Polsce – Sąd Okręgowy.

Ryzyko wywołania konsekwencji administracyjnych wskutek powództwa cywilnego – obowiązek zawiadamiania przez sąd Prezesa Urzędu Ochrony Danych Osobowych.

Decyzja Prezesa UODO/prawomocny wyrok sądu administracyjnego wiąże sąd cywilny co do stwierdzenia naruszenia przepisów o ochronie danych.

Skutek w postaci ryzyka poniesienia odpowiedzialności cywilnoprawnej

Administrator – każdy uczestniczący w przetwarzaniu odpowiada za szkody, ale:

- nie odpowiada, jeżeli udowodni, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody;
- jeżeli w przetwarzaniu uczestniczy więcej niż jeden administrator, odpowiadają solidarnie.

Podmiot przetwarzający – odpowiada za szkody, gdy:

- nie dopełnił obowiązków, które RODO nakłada bezpośrednio na podmioty przetwarzające lub
- gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

Nie odpowiada, jeżeli udowodni, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody.

Administrator lub podmiot przetwarzający mają **prawo regresu** do pozostałych administratorów lub podmiotów przetwarzających uczestniczących w przetwarzaniu, w zakresie odszkodowania, co do tej części szkody, za którą owi inni uczestnicy ponoszą odpowiedzialność.

Skutek w postaci ryzyka poniesienia odpowiedzialności karnoprawnej

Uchylenie art. 52 Ustawy o ochronie danych osobowych z 1997 r.
(*„Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.”*)

Skutek w postaci ryzyka poniesienia odpowiedzialności karnoprawnej

Ujawnianie lub wykorzystywanie informacji powziętych w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, wbrew przepisom **ustawy** lub przyjętego na siebie zobowiązania **(art. 266 § 1 Kodeksu karnego)**.

Ujawnianie lub wykorzystywanie informacji stanowiącej tajemnicy bankowej, przez osobę obowiązaną do zachowania tajemnicy bankowej, niezgodnie z upoważnieniem określonym w ustawie **(art. 171 ust. 5 Prawa bankowego)**.

Ewentualnie odpowiedzialność na podstawie **art. 296** kk – wyrządzenie szkody wskutek niedopełnienia obowiązków/nadużycia uprawnień (np. niewłaściwego zabezpieczenia danych).

Skutek w postaci ryzyka poniesienia odpowiedzialności karnoprawnej

Odpowiedzialność karna podmiotów zbiorowych.

W aktualnym stanie prawnym:

- możliwość odpowiedzialności w przypadku przestępstwa z art. 171 Prawa bankowego;
- warunkiem odpowiedzialności, czyn określonej w ustawie osoby, potwierdzony prawomocnym wyrokiem skazującym względnie innym wskazanym w ustawie orzeczeniem.

Na gruncie przepisów projektowanej nowej ustawy o odpowiedzialności podmiotów zbiorowych:

- brak katalogu przestępstw, z którym może łączyć się odpowiedzialność;
- brak „prejudykatu” w postaci orzeczenia wobec sprawcy przestępstwa.

Skutki organizacyjne

1. Konieczność rewizji procedur i stosowanych środków

2. Konieczność rozważenia zasadności cofnięcia upoważnień osobom, które przyczyniły się do naruszenia.

3. Konieczność rozważenia rozwiązania umowy o powierzenie przetwarzania danych, w przypadku gdy naruszenie powstało w wyniku zachowania procesora.
   „Administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.”

4. Konieczność rozważenia rezygnacji ze współpracy z innym administratorem przy przetwarzaniu danych, w przypadku gdy naruszenie powstało w wyniku jego zachowania.

Dziękuję za uwagę

dr JACEK BŁACHUT

adwokat
Senior Associate

j.blachut@spcg.pl

tel: +48 12 427 24 24

www.spcg.pl

SPCG

SPECJALIZACJE:

- Spory sądowe i arbitrażowe
- Prawo konkurencji i pomoc publiczna
- Prawo europejskie
- Prawo administracyjne i postępowania sądowo-administracyjne
- Prawo energetyczne
- Prawo telekomunikacyjne
- Prawo karne gospodarcze

Specjalizuje się w prawie karnym (w szczególności prawie karnym gospodarczym), prawie telekomunikacyjnym, prawie konkurencji oraz problematyce ochrony danych osobowych. Posiada bogate i wieloletnie doświadczenie w reprezentowaniu osób fizycznych i prawnych w postępowaniach karnych, w rozmaitych rolach procesowych. Jako pełnomocnik występował w wielu postępowaniach cywilnych, sądowo-administracyjnych oraz administracyjnych, w tym w licznych postępowaniach z udziałem państwowych organów regulacyjnych.

Autor publikacji naukowych z zakresu prawa karnego.

O kancelarii SPCG

Kancelaria SPCG T. Studnicki, K. Płeszka, Z. Ćwiąkalski, J. Górski jest jedną z największych i najstarszych niezależnych firm prawniczych w Polsce. Od ponad 30 lat świadczy kompleksowe usługi prawne w wielu dziedzinach prawa.

Kancelaria SPCG specjalizuje się w kompleksowej obsłudze firm i przedsięwzięć inwestycyjnych, doradztwie w sektorze finansowym i w obszarze rynków kapitałowych oraz w prawie ochrony danych osobowych. Mamy również bogate doświadczenie w zakresie praktyki prawa pracy oraz w prowadzeniu skomplikowanych sporów sądowych i arbitrażowych.

Od wielu lat współpracujemy z czołowymi firmami prawniczymi z Niemiec, Wielkiej Brytanii, Włoch, Francji oraz USA.

SPCG łączą ścisłe związki ze środowiskiem akademickim w Polsce. Czterech partnerów SPCG jest profesorami na wydziale Prawa i Administracji Uniwersytetu Jagiellońskiego.

Nasze kompetencje i doświadczenie są dostrzegane przez obserwatorów branży usług prawnych. Kancelaria oraz prawnicy SPCG zajmują wysokie pozycje w rankingach oraz są rekomendowani w międzynarodowych zestawieniach branżowych, m.in. w: Chambers Europe, Euromoney – Deal Watch, Forbes, Legal 500, PLC Which Lawyer, IFLR 100 oraz Best Lawyers, które oceniają rynek usług prawniczych w Europie i na świecie. Doceniają nas również lokalni audytorzy rynku usług prawnych – plasujemy się w czołówkach rankingów Rzeczpospolitej, a nasi prawnicy otrzymują wyróżnienia wschodzących gwiazd sceny prawniczej w Polsce - Rising Stars.

Zespół SPCG liczy ponad siedemdziesięciu prawników, z czego osiemnastu posiada status partnera. Kancelaria świadczy swoje usługi na terenie całego kraju, realizując zlecenia za pośrednictwem czterech biur zlokalizowanych w Krakowie, Warszawie, Katowicach i Wrocławiu.

RANKED IN Chambers GLOBAL 2019 · The LEGAL 500 EMEA · IFLR 1000 · Best Lawyers® THE WORLD'S PREMIER GUIDE · RZECZPOSPOLITA

www.spcg.pl

Główne specjalizacje

Bankowość i finanse
Prawo ochrony danych osobowych
Nieruchomości i inwestycje budowlane
Łączenie i nabywanie spółek
Spółki i prawo korporacyjne
Rynki kapitałowe
Spory sądowe i arbitrażowe
Prawo konkurencji i ochrona konsumentów
Własność intelektualna
Zamówienia publiczne
Prawo europejskie i zagadnienia regulacyjne
Prawo podatkowe
Prawo administracyjne
Prawo karne gospodarcze
Prawo pracy

SPCG

STUDNICKI
PŁESZKA
ĆWIĄKALSKI
GÓRSKI

Siedziba Kancelarii:
ul. Jabłonowskich 8
31-114 Kraków
tel.: +48 12 427 24 24
faks: +48 12 427 23 33
e-mail: spcg@spcg.pl
www.spcg.pl

Oddział w Warszawie:
ul. Złota 59
00-120 Warszawa
tel.: +48 22 244 83 00
faks: +48 22 244 83 01
e-mail: warszawa@spcg.pl
www.spcg.pl

Oddział w Katowicach:
ul. Warszawska 10
40-006 Katowice
tel.: +48 32 352 19 60
faks: +48 32 353 84 77
e-mail: katowice@spcg.pl
www.spcg.pl

Oddział we Wrocławiu:
ul. św. Mikołaja 7
50-125 Wrocław
tel.: +48 71 722 42 10
faks: +48 71 722 42 11
e-mail: wroclaw@spcg.pl
www.spcg.pl