KPMG

Proces zarządzania incydentami na potrzeby GDPR/RODO?

Bezpieczeństwo banków wobec nowych wyzwań
Warszawa, 14.12.2016

Rola administratora danych osobowych wg GDPR

Ile to „dużo” czasu?

Art. 33 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Czas to pieniądz … ?

Artykuł 83 Ogólne warunki nakładania administracyjnych kar pieniężnych

1. Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne, o których mowa w ust. 4, 5 i 6, były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

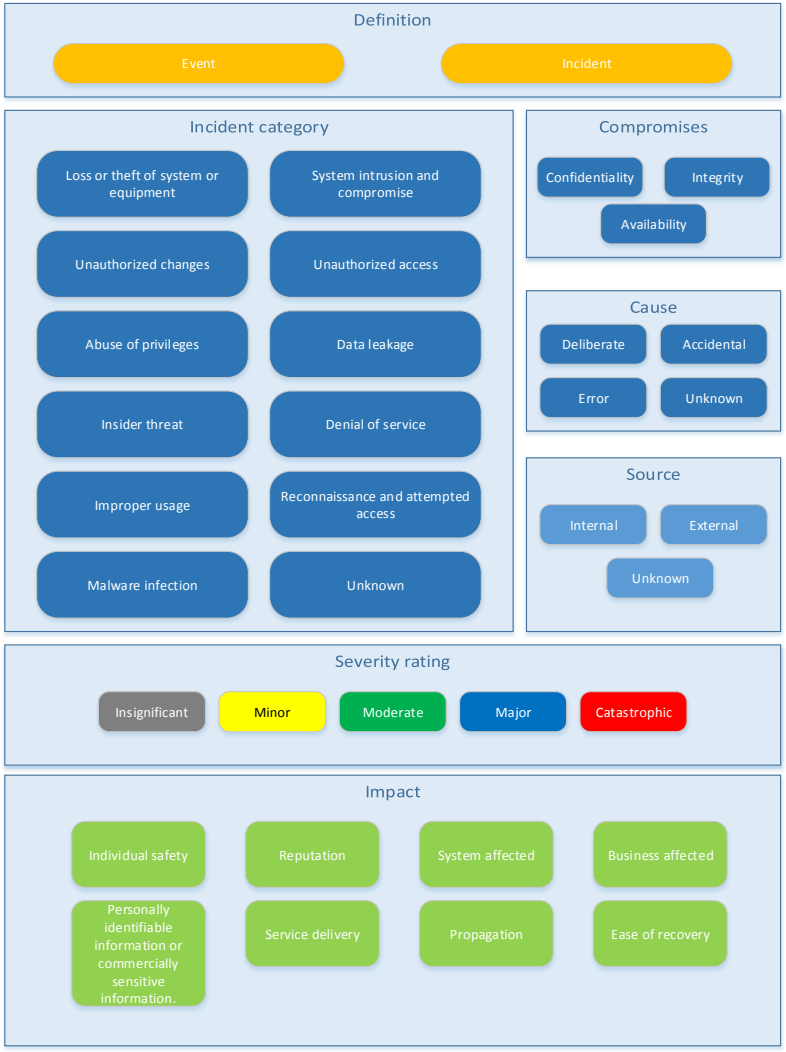
2. Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a)–h) oraz j). Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:

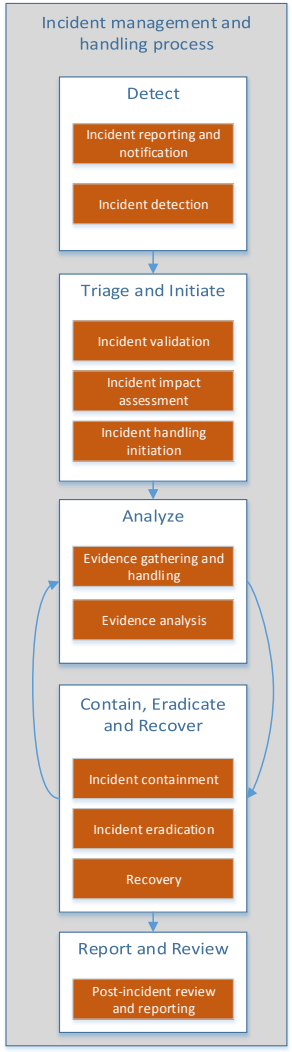
a) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
b) umyślny lub nieumyślny charakter naruszenia;
c) działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
d) stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32;
e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
f) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
g) kategorie danych osobowych, których dotyczyło naruszenie;
h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;
i) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków;
j) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz
k) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

Monitorować, ale co i jak?

1. **Czy wykonano kompletną inwentaryzację danych osobowych?**
   - systemy transakcyjne, CRM,
   - katalogi sieciowe, aplikacje użytkownika końcowego,
   - archiwa, laptopy pracowników, biurka …
2. **Czy przeanalizowaliśmy możliwe rodzaje scenariusze What Could Go Wrong?**
   - Przetwarzanie bez zgody,
   - Przetwarzanie w innym celu,
   - Nieuprawniony dostęp osób trzecich w wyniku…
3. **Czy mamy zidentyfikowane wszystkie potencjalne źródła i miejsca incydentów?**
   - Nieroztropny pracownik,
   - Niezadowolony pracownik,
   - Haker ...

Zarządzanie incydentami i komunikacja kryzysowa





W przypadku kryzysu dla Banku najistotniejsza będzie:

- z operacyjnego punktu widzenia?

  REPUTACJA

- z punktu widzenia GIODO / GDPR?

DOCHOWANIE NALEŻYTEJ STARANNOŚCI

Impact Type	Severity				
	Insignificant	Minor	Moderate	Major	Catastrophic
Individual safety	None/negligible			Any risk to personal safety	Threatens life directly
Reputation	None/negligible	Minor local impact and/or limited short term damage	Moderate embarrassment and/or short term damage	Significant embarrassment, loss of public confidence and/or limited long term damage	Severe embarrassment, loss of public confidence and/or substantial long term damage
Personally identifiable information or commercially sensitive information.	No or negligible disclosure of personal or commercially sensitive information	Minor impact	Measurable impact, breach of regulations or commitment to confidentiality	Significant impact to person or business	Substantial impact to person or business
System affected	None or negligible	Few non-critical systems in a stand-alone or networked environment	Many non-critical systems in a stand-alone or networked environment	Any critical system in a networked environment	Multiple critical systems in a networked environment.
Business affected	No or negligible impact	Small areas within a single business	Most areas within a single business	Multiple business	Whole of business

Podsumowanie

Pozostało 366 dni roboczych

i ciągle ubywa,

w przeciwieństwie do zagrożeń …

Dane kontaktowe:

Paweł Skowroński
Senior Manager

KPMG Advisory Spółka z ograniczoną
odpowiedzialnością sp.k.
ul. Inflancka 4A
00-189 Warszawa

T: +48 (22) 528 1350
K: +48 664 718 627
F: +48 (22) 528 1009
E: pskowronski@kpmg.pl

kpmg.com/socialmedia

kpmg.com/app