Sprawozdanie z działalności PUODO w 2020 r. – cz. I

W dniu 26.08 br. zostało opublikowane sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych („PUODO") w roku 2020 r. („Sprawozdanie"). Prawie 300 - stronicowy dokument obejmuje w szczególności informacje dotyczące wydanych decyzji i rozpatrywanych skarg, kontroli prowadzonych przez PUODO, aktów prawnych, co do których PUODO wydał opinie, odpowiedzi na pytania zadawane przez administratorów i IOD, czy podsumowanie dotyczące zgłaszanych naruszeń ochrony danych osobowych, które wpływały do UODO w 2020 r. Przygotowałam dla Państwa zestawienie najważniejszych i najciekawszych, moim zdaniem, kwestii poruszonych w Sprawozdaniu. Poniżej część I obejmująca informacje statystyczne i kwestie dotyczące naruszeń ochrony danych osobowych zgłaszanych do organu nadzorczego.

Statystyka

Na początek krótkie zestawienie liczbowe:

1. W roku 2020 Prezes Urzędu Ochrony Danych Osobowych **wydał 1866 decyzji administracyjnych**.
2. W roku 2020 do Urzędu Ochrony Danych Osobowych **wpłynęły w sumie 6442 skargi** – w podziale na sektory wygląda to następująco:
   - 1303 skargi na podmioty sektora publicznego;
   - 2519 skarg na podmioty sektora prywatnego;
   - 926 skarg na podmioty sektora zdrowia, zatrudnienia i szkolnictwa;
   - 1694 skargi na podmioty sektora finansowego, ubezpieczeń i telekomunikacji.
3. W 2020 r. Urząd Ochrony Danych Osobowych dokonał analizy **7507 zgłoszeń naruszeń** m.in. pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Spośród nich:
   - 4661 zostało zgłoszonych przez podmioty sektora prywatnego;
   - 2691 przez podmioty sektora publicznego;
   - około 155 zgłoszonych w międzynarodowym systemie informatycznym (IMI).
4. W przypadku **sektora prywatnego** najwięcej zgłoszeń naruszenia ochrony danych osobowych napłynęło od podmiotów:
   - telekomunikacyjnych – 2104;
   - ubezpieczeniowych – 792'
   - banków i podmiotów finansowych – 472;
   - służby zdrowia – 272.

Większa liczba zgłoszeń naruszeń ochrony danych osobowych

Zarówno liczba skarg, jak i zgłoszeń naruszeń ochrony danych osobowych jest wyższa niż w poprzednich latach. Zdaniem PUODO wynika to nie tylko z coraz większej świadomości podmiotów danych co do ich praw oraz administratorów co do ich obowiązków wynikających z art. 33 oraz 34 RODO, lecz także – w przypadku naruszeń - z obawy przed konsekwencjami, o których mowa w art. 58 oraz 83 ust. 4, 5 i 6 RODO. Trzecią przyczyną jest sytuacja spowodowana pandemią koronawirusa. Nowa rzeczywistość związana z pandemią i konieczność podejmowania przez

administratorów dodatkowych środków w celu ochrony zdrowia osób, których dane dotyczą miały wpływ na wystąpienie incydentów bezpieczeństwa w sferach, które nie były wcześniej poddawane szczegółowej analizie pod kątem wystąpienia możliwych zagrożeń i podatności na zagrożenia[1].

Najczęstsze typy naruszeń i działania administratorów

Jak wskazuje PUODO, najczęstsze rodzaje naruszeń ochrony danych osobowych pozostają co do zasady niezmienne – nie ma tu żadnego zaskoczenia. Organ nadzorczy podsumował również, jakie działania podejmowali administratorzy w związku z wystąpieniem naruszeń ochrony danych osobowych w ich organizacji. PUODO nie wskazał, czy środki stosowane przez administratorów były właściwe. Nie wydaje się to jednak zaskakujące. Każdy przypadek jest analizowany indywidualnie i nie można generalnie stwierdzić, że określone działanie będzie przy danych naruszeniach właściwe, ponieważ szczegóły konkretnego stanu faktycznego mogą się jednak różnić. Z pewnością jednak wskazane w Sprawozdaniu środki podejmowane przez administratorów mogą stanowić inspirację dla innych podmiotów, które będą musiały zmierzyć się z naruszeniem ochrony danych osobowych w ich organizacji.

Katalog naruszeń i środków stosowanych przez administratorów przy poszczególnych rodzajach naruszeń zgodnie ze Sprawozdaniem[2] wygląda następująco:

1. **wysłanie korespondencji zawierającej dane osobowe zarówno w formie tradycyjnej, jak i na elektroniczną skrzynkę pocztową e-mail do niewłaściwego odbiorcy** – najczęściej wskutek błędu ludzkiego; w tych przypadkach administratorzy, aby zmniejszyć prawdopodobieństwo wystąpienia tego typu naruszeń w przyszłości, wdrażali środki bezpieczeństwa w postaci m.in.:
    - szyfrowania przesyłanej korespondencji, uniemożliwiającej dostęp do danych osobom nieuprawnionym,
    - dodatkowej weryfikacji adresu korespondencyjnego w momencie gromadzenia danych, polegającej m.in. na konieczności przeliterowania adresu (w przypadku gromadzenia danych przez telefon) lub poprzez wymuszenie ponownego wpisania adresu e-mail w formularzach;
2. **ujawnienie danych niewłaściwej osobie**; w celu ograniczenia tego typu naruszeń w przyszłości, administratorzy:
    - podejmowali działania mające na celu zdyscyplinowanie pracowników,
    - przeprowadzali dodatkowe szkolenia czy instruktarze,
    - dokonywali przeglądu obowiązujących procedur,
    - dodatkowo zwracali się do osób nieuprawnionych o zwrot dokumentów lub ich trwałe zniszczenie;
3. **nieuprawnione uzyskanie dostępu do informacji** – najczęściej wskutek błędów programistycznych ujawniających się po wprowadzeniu aktualizacji danego

[1] Str. 138 – 139 Sprawozdania.
[2] Str. 142 – 145 Sprawozdania.

oprogramowania, braku wewnętrznych testów bezpieczeństwa, które mogły wykazać podatność systemu, czy nieprawidłowego nadania uprawnień w systemach informatycznych; administratorzy podejmowali działania polegające na:

- przeprowadzeniu dodatkowych testów systemów informatycznych w środowisku developerskim,
- przeprowadzeniu analizy nadanych uprawnień, ograniczając nadane uprawnienia do takich, które są niezbędne dla wykonywania obowiązków służbowych użytkowników;

4. **korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem do nadawcy** – w przypadku tego typu incydentów, najczęściej do naruszeń dochodziło w wyniku działań operatora pocztowego; administratorzy, aby zapobiec tego typu naruszeniom w przyszłości:
   - dokonywali aktualizacji instrukcji kancelaryjnej,
   - składali reklamację do operatora pocztowego,
   - podejmowali działania zmierzające do zmiany postanowień umownych zawartych z operatorem,
   - zwracali się do operatora pocztowego o wyjaśnienia w szczególności, jakie środki zostały przez niego zastosowane w celu zmniejszenia prawdopodobieństwa wystąpienia naruszenia w przyszłości;
5. **dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji** – do tego typu naruszeń najczęściej dochodziło w wyniku niefrasobliwości pracowników; w celu obniżenia prawdopodobieństwa wystąpienia tego typu naruszeń w przyszłości, administratorzy danych:
   - podejmowali działania podnoszące świadomość pracowników w zakresie zapewnienia bezpieczeństwa powierzonych dokumentów,
   - upominali osoby odpowiedzialne za wystąpienie naruszenia,
   - dokonywali przeglądu obowiązujących procedur regulujących sytuacje i warunki dopuszczalnego przetwarzania danych osobowych utrwalonych w dokumentacji papierowej lub na innych, przenośnych nośnikach danych, poza siedzibą lub obszarem pomieszczeń zajmowanych przez administratora danych,
   - zgłaszali kradzież organom ścigania;
6. **niezamierzona publikacja lub nieprawidłowa anonimizacja danych w dokumencie** – najczęściej wskutek nieprawidłowej anonimizacji danych lub przeoczenia tego błędu przez pracowników udostępniających materiały i je w sieci; administratorzy w tych przypadkach:
   - przeglądali i modyfikowali procedury udostępniania informacji publicznej, np. wprowadzali dodatkową weryfikację anonimizacji dokumentów,
   - w przypadku publikacji danych na stronie internetowej - usuwali treści ze swoich witryn internetowych;
7. **zgubienie lub kradzież nośnika danych / urządzenia umożliwiającego dostęp do danych** – do tego typu naruszeń najczęściej dochodziło w wyniku kradzieży komputera przenośnego lub zgubienia niezaszyfrowanego elektronicznego

nośnika danych typu „pendrive"; działania podejmowane przez administratorów:

- szyfrowanie elektronicznych nośników danych, uniemożliwiające dostęp do danych osobom nieuprawnionym,
- dokonywanie weryfikacji przestrzegania przez pracowników zasady ograniczonego (w aspekcie czasowym i zakresowym) przechowywania,
- wprowadzanie rozwiązania umożliwiającego zdalne usuwanie danych osobowych ze stacji roboczych znajdujących się poza siedzibą administratora,
- decydowanie się na przechowanie danych „w chmurze",
- zwiększanie świadomość pracowników w zakresie konieczności zapewnienia bezpieczeństwa powierzonym im elektronicznym nośnikom danych,
- zgłaszanie kradzieży organom ścigania;

8. **złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych oraz nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń**; w celu zaradzenia naruszeniu administratorzy:
   - przywracali dane z kopii zapasowych, a w przypadku braku kopii - podejmowali decyzję o ich tworzeniu,
   - korzystali ze wsparcia wyspecjalizowanych podmiotów dokonujących próby odszyfrowania danych,
   - przeprowadzali dodatkowe testy bezpieczeństwa,
   - decydowali się na zakup najnowszego oprogramowania antywirusowego oraz oprogramowania typu „firewall",
   - dokonywali przeglądu oraz zmiany procedur w zakresie stosowania wymogu regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych, mających zapewnić bezpieczeństwo przetwarzania,
   - zgłaszali naruszenie organom ścigania oraz Zespołowi CERT Polska;
9. **ujawnienie danych związane ze zdalnym nauczaniem i pracą zdalną** – naruszenia polegały na nieuprawnionym upublicznieniu wizerunku, udostępnieniu nagrań zawierających dane osobowe osobom nieuprawnionym; administratorzy danych w tych przypadkach:
   - decydowali się przekazywać narzędzia do logowania tuż przed zajęciami/spotkaniami (w celu utrudnienia przekazywania loginu i haseł osobom postronnym),
   - przeprowadzali audyt stosowanych narzędzi do zdalnej nauki/pracy,
   - zwracali nauczycielom uwagę na niebezpieczeństwo ingerencji osób trzecich w prowadzone zajęcia, czy informowali rodziców o konsekwencjach działań.

W kolejnej części zostaną podsumowane skargi składane na podmioty z sektora publicznego, a następnie – z sektora prywatnego oraz wnioski i zalecenia przekazane w związku z tym przez PUODO.

adw. Agnieszka Rapcewicz

Kancelaria Adwokacka Adwokat Agnieszka Rapcewicz RODOwskaz Legal Consulting
ul. Narutowicza 248, 05-400 Otwock
NIP: 9512181110, REGON: 369581146
+48 668 264 604
kontakt@rodowskaz.pl, agnieszka@rodowskaz.pl