

Warszawa, 09.04.2024 r.

Rozliczenie roczne PIT – jak uniknąć naruszenia ochrony danych osobowych?

W Polsce roczne rozliczenia podatkowe, czyli PIT (Podatek dochodowy od osób fizycznych), przygotowuje się zazwyczaj po zakończeniu roku podatkowego, który w Polsce pokrywa się z rokiem kalendarzowym, czyli od 1 stycznia do 31 grudnia. Zgodnie z obowiązującymi przepisami, podatnicy mają obowiązek złożyć deklarację podatkową za poprzedni rok podatkowy do końca kwietnia roku następnego.

Oznacza to, że dla roku podatkowego 2023, deklaracja podatkowa (PIT) powinna zostać złożona najpóźniej do końca kwietnia 2024 roku. Jest to ważna data, ponieważ po jej upływie naliczane są sankcje za nieterminowe złożenie zeznania podatkowego, chyba że osoba rozliczająca się ma umowę z urzędem skarbowym, która przedłuża termin składania zeznania podatkowego.

Deklaracje PIT można składać osobiście w urzędach skarbowych, za pośrednictwem internetu (poprzez platformy podatkowe, takie jak e-Deklaracje - <https://www.podatki.gov.pl/e-deklaracje/>), a także za pomocą tradycyjnej poczty.

Kwiecień to wyzwanie dla pracodawców, działów księgowych, doradców podatkowych oraz samych podatników. Same informacje zawarte w rozliczeniu rocznym zawierają dosyć szeroki zakres danych osobowych, w tym przede wszystkim dane dotyczące naszych finansów + np. nasz numer PESEL. W przypadku naruszenia ochrony danych polegającej na przypadkowej utracie PIT-u lub np. poprzez udostępnienie osobie nieuprawnionej, powstaje wysokie ryzyko dla praw i podmiotów danych, a dla samego administratora będzie zapewne skutkowało koniecznością zgłoszenia naruszenia do PUODO lub nawet zawiadomieniem podmiotu/podmiotów danych. Wysyłanie deklaracji podatkowych (PIT) to ważne zadanie każdego podatnika, ale równie istotne jest zapewnienie bezpieczeństwa danych osobowych podczas tego procesu. W dobie cyfryzacji, wiele osób decyduje się na elektroniczną formę przekazywania deklaracji, co wymaga szczególnej uwagi w zakresie ochrony danych osobowych.

W jaki sposób uniknąć naruszenia ochrony danych osobowych przy rocznym rozliczeniu PIT?
Poniżej nasze wskazówki!

1. Korzystanie z bezpiecznych kanałów komunikacji

Podstawowym krokiem w bezpiecznym przekazywaniu PIT jest wykorzystanie bezpiecznych kanałów komunikacji. W przypadku wysyłania dokumentów elektronicznych, zaleca się korzystanie z oficjalnych portali internetowych urzędów skarbowych lub innych zaufanych platform, które stosują szyfrowanie danych. Unikaj przesyłania danych za pomocą niezabezpieczonych wiadomości e-mail, gdzie istnieje ryzyko przechwycenia informacji przez osoby trzecie.

2. Szyfrowanie danych

Szyfrowanie danych jest kluczowym elementem zapewnienia bezpieczeństwa podczas przekazywania PIT-ów. Przed wystaniem deklaracji upewnij się, że wszystkie dokumenty są zaszyfrowane, co oznacza, że są one przekształcane w taki sposób, aby były nieczytelne dla osób nieupoważnionych. Większość platform internetowych stosuje protokoły szyfrowania SSL/TLS, co zapewnia bezpieczną transmisję danych. Jeżeli zamierzamy przesać PIT za pomocą pliku PDF – plik ten powinien być zabezpieczony hasłem. Hasło należy wysłać odrębnym kanałem komunikacyjnym.

3. Hasła i uwierzytelnianie dwuetapowe

Podczas korzystania z platform internetowych do wysyłania PIT, ważne jest, aby stosować silne hasła i aktywować uwierzytelnianie dwuetapowe, jeśli jest to możliwe. Silne hasła powinny zawierać kombinację wielkich i małych liter, cyfr oraz znaków specjalnych, co znacznie utrudni dostęp nieautoryzowanym osobom. Uwierzytelnianie dwuetapowe dodatkowo zabezpieczy dostęp do konta, wymagając oprócz hasła także jednorazowego kodu potwierdzającego, który jest generowany na dodatkowym urządzeniu użytkownika tj. telefonie komórkowym.

4. Aktualizacja oprogramowania i ochrona antywirusowa

Aby zapewnić ochronę przed cyberatakami, ważne jest regularne aktualizowanie oprogramowania i korzystanie z oprogramowania antywirusowego. Aktualizacje oprogramowania zawierają łatki bezpieczeństwa, które poprawiają odporność systemu na ataki, podczas gdy oprogramowanie antywirusowe pomaga wykryć i zneutralizować potencjalne zagrożenia.

5. Unikanie publicznych sieci Wi-Fi

Podczas przekazywania danych podatkowych zaleca się unikanie korzystania z publicznych sieci Wi-Fi, które mogą być podatne na ataki hakerskie. Zamiast tego, używaj własnego zabezpieczonego połączenia internetowego, aby zminimalizować ryzyko nieautoryzowanego dostępu do przesyłanych danych.

6. Zachowanie kopii zapasowych

Nie zapominaj o zachowaniu kopii zapasowych dokumentów związanych z rozliczeniem podatkowym. W razie jakichkolwiek problemów lub utraty danych, posiadanie kopii zapasowej umożliwi szybkie odtworzenie dokumentów i uniknięcie nieprzyjemnych konsekwencji podatkowych.

Bezpieczne przekazywanie plików z rozliczeniem rocznym to istotny element ochrony danych osobowych. Przestrzeganie powyższych zasad pomoże zminimalizować ryzyko naruszenia prywatności oraz uniknąć niepożądanych konsekwencji związanych z wyciekiem danych. Pamiętaj, że dbanie o bezpieczeństwo danych osobowych jest obowiązkiem każdego podatnika i płatnika.

Maciej Łukaszewicz – radca prawny, specjalista ds. ochrony danych osobowych w iSecure Sp. z o.o.