**10 zasad dotyczących bezpieczeństwa danych w pracy biurowej**

**Według aktualnie obowiązujących przepisów prawa z zakresu przetwarzania i ochrony danych osobowych w biurze należy wprowadzić zestaw zasad dotyczących sposobu zarządzania, ochrony i dystrybucji informacji wrażliwej pozwalający na zapewnienie ochrony danych osobowych.**

Niniejsze zasady zazwyczaj stanowią wyciąg najistotniejszych zapisów zawartych w Polityce bezpieczeństwa informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Powinny obowiązywać pracowników etatowych oraz współpracowników (użytkowników), mających upoważnienia do przetwarzania danych osobowych.

**Zasada 1. Postaw na bezpieczne użytkowanie sprzętu IT**

Podstawowym wymogiem bezpieczeństwa danych jest korzystanie ze sprzętu IT w sposób zgodny z jego przeznaczeniem i jego ochrona przed jakimkolwiek zniszczeniem lub uszkodzeniem. Użytkownik jest zobowiązany do zabezpieczenia sprzętu IT przed dostępem osób nieupoważnionych, a w szczególności zawartości ekranów monitorów.

Pracownik (użytkownik) ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.

Należy zakazać samowolnego otwierania (demontażu) sprzętu IT, instalowania dodatkowych urządzeń (np. twardych dysków, pamięci) oraz podłączania jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego. Warto ustalić, że za zabezpieczanie urządzeń przenośnych typu laptop lub pendrive, szczególnie w trakcie transportu, odpowiada pracownik (o ile otrzymał on zgodę na ich wynoszenie poza obszar przetwarzania danych). Zaś wykorzystywanie prywatnego sprzętu komputerowego do wykonywania zadań służbowych może mieć miejsce za zgodą pracodawcy. Warunki wykorzystywania prywatnych urządzeń oraz zasady bezpieczeństwa danych powinna w takim wypadku określać umowa pomiędzy pracodawcą a pracownikiem regulująca zasady korzystania ze sprzętu i aplikacji.

**Zasada 2. Korzystaj z legalnego oprogramowania**

Użytkownik, którym jest pracownik lub zleceniobiorca powinien korzystać wyłącznie z oprogramowania objętego prawami autorskimi. Użytkownik nie ma prawa kopiować oprogramowania zainstalowanego na sprzęcie IT przez pracodawcę na swoje własne potrzeby ani na potrzeby osób trzecich.

Instalowanie jakiegokolwiek oprogramowania na sprzęcie IT może być dokonane wyłącznie przez osobę upoważnioną.

Użytkownicy nie powinni mieć prawa do instalowania ani używania oprogramowania innego, niż przekazane lub udostępnione im przez pracodawcę. Zakaz dotyczy między innymi instalacji oprogramowania z zakupionych płyt CD, programów ściąganych ze stron internetowych, a także odpowiadania na samoczynnie pojawiające się reklamy internetowe.

W przypadku naruszenia któregokolwiek z powyższych postanowień pracodawca ma prawo niezwłocznie i bez uprzedzenia usunąć nielegalne lub niewłaściwie zainstalowane oprogramowanie.

**Zasada 3. Stosuj ochronę antywirusową**

Należy zobowiązać pracowników ( zleceniobiorców) do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym oraz zakazać wyłączania systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

W przypadku stwierdzenia zainfekowania systemu Użytkownik powinien poinformować niezwłocznie o tym fakcie Informatyka lub osobę upoważnioną.

**Zasada 4. Ogranicz możliwość wykorzystywania Internetu**

Pracownicy powinni korzystać z Internetu w celu wykonywania obowiązków służbowych i przestrzegać przy tym korzystaniu prawa własności przemysłowej i praw autorskich. Wykorzystanie Internetu do celów prywatnych powinno być dopuszczalne wyłącznie okazjonalnie i ograniczone do niezbędnego minimum.

Nie powinni oni korzystać z Internetu w celu przeglądania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec obowiązujących zasad postępowania, a także grać w gry komputerowe w Internecie lub w systemie informatycznym pracodawcy, ściągać z Internetu jakichkolwiek plików muzycznych lub wideo.

W uzasadnionym zakresie pracodawca może zastrzec sobie prawo kontroli czasu spędzanego przez pracownika w Internecie. Pracodawca może również blokować dostęp do niektórych treści dostępnych przez Internet.

**Zasada 5. Korzystaj z poczty elektronicznej tylko do celów służbowych**

System Poczty Elektronicznej powinien być przeznaczony wyłącznie do wykonywania obowiązków służbowych, a pracownicy z niego korzystający powinni być zobowiązani do przestrzegania prawa własności przemysłowej i prawa autorskiego. Korespondencja wpływająca na służbową skrzynkę jest korespondencją służbową. Do celów prywatnych pracownicy powinni użytkować służbową pocztę wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

Korzystanie z Systemu Poczty Elektronicznej do celów prywatnych nie może wpływać na jakość i ilość świadczonej pracy oraz na prawidłowe i rzetelne wykonywanie przez pracownika obowiązków służbowych, a także na wydajność Systemu Poczty Elektronicznej.

Pracownik (użytkownik) powinien być świadomy, że wszelkie wiadomości o charakterze prywatnym utworzone lub odebrane za pośrednictwem Systemu Poczty Elektronicznej pracodawcy przetwarzane są wyłącznie na jego własną odpowiedzialność, a pracodawca ma możliwości prowadzenia kontroli tych wiadomości. Pracodawca nie będzie w tej sytuacji odpowiadać za przypadkowe naruszenie dóbr osobistych pracownika (użytkownika) w postaci naruszenia tajemnicy korespondencji.

Pracownicy nie mają prawa korzystać z Systemu Poczty Elektronicznej w celu przeglądania lub rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

W przypadku przesyłania plików danych osobowych do podmiotów zewnętrznych, warto zobowiązać pracownika do ich spakowania i opatrzenia hasłem (8 znaków: duże i małe litery i cyfry lub znaki specjalne). Hasło należy przesłać odrębnym mailem.

Użytkownik nie ma prawa wysyłać wiadomości zawierających informacje poufne w rozumieniu tajemnicy przedsiębiorstwa, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

Warto uczulić pracowników by nie otwierali wiadomości od nieznanych sobie osób, których tytuł nie sugeruje związku z wypełnianymi przez nich obowiązkami służbowymi. Nie powinni oni też uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną.

Szczególnie należy uważać na wszechobecny **Phishing** – metodę oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań

Należy zakazać również używania systemów teleinformatycznych i zasobów systemowych pracodawcy dla własnych celów komercyjnych.

**Zasada 6. Stawiaj wysokie wymogi używanym hasłom**

Nakładając obowiązek tworzenia hasła do dostępu do zbioru danych pamiętaj, że powinno ono składać się co najmniej z 12 znaków (dużych i małych liter oraz z cyfr lub znaków specjalnych).

**Warto aby zmianę hasła wymuszał system lub użytkownik zobowiązany był do jego manualnej zmiany**.

Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.

Należy również zobowiązać pracownika do zachowania hasła w poufności, nawet po utracie przez nie ważności oraz zakazać jego zapisywania w sposób jawny a także przekazywania jego innym osobom.

**Zasada 7. Ustal procedurę rozpoczęcia, zawieszenia i zakończenia pracy**

Pracownik rozpoczynający pracę z systemem informatycznym przetwarzającym dane osobowe powinien posługiwać się identyfikatorem i hasłem. Trzeba również zadbać o uniemożliwienie osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu. Przed czasowym opuszczeniem stanowiska pracy użytkownik powinien wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.

Po zakończeniu pracy Użytkownik powinien wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy, a także zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

**Zasada 8. Chroń elektroniczne nośniki z danymi osobowymi**

Pracownicy nie powinni wynosić na zewnątrz firmy wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Administratora Danych Osobowych. **Dane osobowe wynoszone poza firmę muszą być zaszyfrowane.**

W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe należy fizycznie zniszczyć nośnik np. przez rozdrobnienie.

Należy zwrócić uwagę aby przekazywanie nośników z danymi osobowymi odbywało się z uwzględnieniem zasad bezpieczeństwa. Adresat powinien zostać powiadomiony o przesyłce, zaś nadawca powinien sporządzić kopię przesyłanych danych. Adresat powinien powiadomić nadawcę o otrzymaniu przesyłki. Jeżeli nadawca nie otrzymał potwierdzenia, zaś adresat twierdzi, że nie otrzymał przesyłki, Użytkownik będący nadawcą powinien poinformować o zaistniałej sytuacji Inspektora Ochrony Danych UR.

**Zasada 9. Chroń dane osobowe w wersji papierowej**

Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne powinny być osoby upoważnione (użytkownicy) oraz kierownicy właściwych jednostek organizacyjnych. Co jednak ważne dokumenty i wydruki zawierające dane osobowe należy przechowywać w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych. Pomieszczenia, w których są przetwarzane dane osobowe, muszą być zamykane na klucz, do którego dostęp posiadają tylko upoważnieni pracownicy.

Użytkownicy zobowiązani są do niszczenia dokumentów i tymczasowych wydruków w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.

W przypadku pomieszczeń, do których dostęp mają również osoby nieupoważnione, mogą one przebywać w tych pomieszczeniach tylko w obecności osób upoważnionych i tylko w czasie wymaganym na wykonanie niezbędnych czynności. Użytkownicy są zobowiązani do stosowania „polityki czystego biurka”. Polega ona na zabezpieczaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.

**Zasada 10. Zapewnij poufności danych osobowych**

Pracownik powinien zachować w tajemnicy dane osobowe, do których ma lub będzie miał dostęp w związku z wykonywaniem zadań służbowych lub obowiązków pracowniczych lub zadań zleconych przez pracodawcę. Danych tych nie powinien wykorzystywać w celach pozasłużbowych bądź niezgodnych ze zleceniem, o ile nie są one jawne. A także nie powinny być przekazywane osobom nieupoważnionym. Pracownik powinien być zobowiązany do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, o ile nie są one jawne.

**Konsekwencje w przypadku naruszenia niniejszych zasad**

Przypadki, nieuzasadnionego zaniechania obowiązków przedstawionych powyżej, które wynikają z Polityki bezpieczeństwa informacji oraz Instrukcji zarządzania systemem informatycznym potraktowane mogą być jako ciężkie naruszenie obowiązków pracowniczych.

Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.

Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

ASI (Administrator systemu informatycznego) może zarezerwować sobie prawo do monitorowania systemów, sieci i zasobów komputerowych, tak by zapewnić poprawne funkcjonowanie tych systemów i śledzić ewentualne nieprawidłowości. Informacja o zakresie i celu kontroli powinna zostać przekazana przed rozpoczęciem działań kontrolnych.

Może on również zarezerwować sobie prawo do ograniczenia/zabrania dostępu do systemów, sieci i zasobów komputerowych w przypadku uzasadnionych podejrzeń naruszenia ww. warunków.

ASI i IOD raportują każde naruszenie ww. zasad, do najbliższego przełożonego, pracodawcy i/lub organów ścigania, co może prowadzić do wdrożenia postępowania dyscyplinarnego i/lub prawnego i w rezultacie do zawieszenia w prawach dostępu do systemów, sieci i zasobów komputerowych, rozwiązania umowy o pracę i/lub postępowania sądowego.

**Podstawa prawna:**

- Ustawa z 10 maja 2018 r. o ochronie danych osobowych (tekst pierwotny: Dz.U. z 2018 r. poz. 1000,).

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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).

- Rozporządzenie ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U nr 100 z 2004 r poz. 1024 zm.).

Opracował:

**IOD UR**