**10 najczęstszych błędów, jakie w zakresie ochrony danych osobowych popełniają pracownicy podczas pracy biurowej:**

**1. Brak szyfrowania przesyłanych danych.**

Niestety, częstą praktyką jest przesyłanie dokumentów zawierających poufne informacje, w tym dane osobowe, drogą mailową, bez ich zaszyfrowania. W efekcie dane łatwo mogą trafić w niepowołane ręce, np. przez błąd w adresie odbiorcy lub też odczytanie maila na komputerze odbiorcy przez inną osobę.

Aby tego uniknąć, warto zabezpieczyć pliki hasłem, a hasło przesłać np. SMS-em.

**2. Masowa wysyłka maili z otwartą listą adresową.**

Wysyłając maile do wielu adresatów, nadawcy wpisują wszystkie adresy w polu „DO”, przez co są one widoczne dla każdej osoby, która danego maila otrzyma. To oczywiste naruszenie prawa do prywatności poszczególnych adresatów. Efektem mogą być skargi adresatów, publiczna krytyka takiego postępowania w sieci, np. za pośrednictwem mediów społecznościowych, a nawet sprawa sądowa.

Najprostszym rozwiązaniem jest stosowanie tzw. kopii ukrytej, tj. wpisywanie wszystkich adresatów w rubryce „UDW”. Korespondencję seryjną można również zrealizować poprzez oprogramowanie Microsoft Word w połączeniu z Microsoft Outlook.

**3. Hasła dostępu na karteczkach.**

Współcześnie korzystamy z mnóstwa różnego rodzaju haseł dostępu czy PIN-ów. Często wymogi, jakie muszą spełniać, sprawiają, że są one coraz trudniejsze do zapamiętania. Aby sobie ułatwić, pracownicy firm bardzo często zapisują je sobie na karteczkach i, niemal równie często, umieszczają w widocznych miejscach, np. na biurku przy komputerze. Efektem jest oczywiście możliwość udostępnienia danych nieuprawnionym osobom.

Aby nie być zmuszonym do zapisywania haseł, warto wybrać takie, które łatwo będzie zapamiętać. Co ciekawe, takie hasło wcale nie musi być łatwe do odgadnięcia – wręcz przeciwnie! Dobre hasło dostępu powinno składać się z co najmniej ośmiu znaków, małych i wielkich liter, a także cyfr lub znaków specjalnych. Dobrym hasłem będzie więc np. MojPies-25 lub MojaZuziaMa10Lat! Prawda, że ich zapamiętanie nie będzie trudne?

**4. Nieużywanie niszczarek.**

Jak wynika z badań przeprowadzonych przez UODO, aż 80% dokumentów, które powinny być niszczone w niszczarkach są w polskich firmach i instytucjach po prostu wyrzucane do koszta! Efektem są przypadki znajdowania dokumentacji np. medycznych czy wyciągów z kont bankowych na śmietnikach. Są osoby, które, wiedząc, że takie skarby można tam znaleźć, celowo pod tym kątem przeszukują śmietniki w okolicach biurowców.

Aby uniknąć strat wizerunkowych i odpowiedzialności karnej za bezprawne udostępnienie danych, warto wyposażyć biuro w niszczarkę i, co wydaje się oczywiste, korzystać z niej!

**5. Wynoszenie danych z instytucji bez szyfrowania nośników.**

Coraz częstszą praktyką jest w instytucjach praca zdalna lub też kończenie różnych służbowych zadań w domu. Wiąże się z tym oczywiście zabieraniem z firmy sprzętu elektronicznego i nośników danych. Niestety, bardzo często żadne z tych urządzeń nie są szyfrowane, przez co w przypadku ich zgubienia lub kradzieży, wszystkie zgromadzone na nich dane są bardzo łatwo dostępne dla niepowołanych osób.

Rozwiązaniem jest oczywiście szyfrowanie danych lub też korzystanie ze zdalnego szyfrowanego dostępu do zasobów firmy.

**6. Udostępnianie haseł dostępu niepowołanym osobom.**

Udostępnianie swoich haseł kolegom z pracy jest dość nagminne, szczególnie w sytuacjach związanych z nagłą nieobecnością jakiegoś pracownika, gdy potrzebny jest dostęp do jego danych. Rodzi to takie same zagrożenia, jak w przypadku zostawienia swoich haseł w widocznym miejscu na biurku. Nigdy nie ma pewności, ile osób i w jaki sposób wykorzysta przekazane hasło.

Jeśli istnieje konieczność dostępu do zasobów, do których nikt, poza nieobecnym pracownikiem, nie ma dostępu, istnieje możliwość przydzielenia tymczasowego dostępu do tych zasobów wskazanemu pracownikowi. Otrzymuje on wówczas od administratora IT swój własny login i hasło.

**7. Niewłaściwe ustawienie monitorów komputera.**

Monitory komputerów powinny być ustawione w taki sposób, aby uniemożliwić niepowołanym osobom dostrzeżenie tego, co się na nich aktualnie znajduje. Tymczasem zdarzają się sytuacje, że osoby czekające na przystanku autobusowym mogą łatwo zobaczyć, co na swoim komputerze wyświetla właśnie pracownik banku, którego oddział,
z przeszkloną witryną, znajduje się tuż obok. Aktywni są również różnego rodzaju szpiedzy
gospodarczy, którzy za pomocą teleobiektywów, sprawdzają, co na swoich komputerach wyświetlają pracownicy konkurencyjnych firm, pracujący np. w biurowcu naprzeciwko.

Rozwiązaniem jest takie ustawienie monitorów, by nie były one widoczne ani przez okno, ani przez drzwi, ani nawet przez współpracowników. Dodatkowo, warto zainstalować specjalne filtry, dzięki którym to, co wyświetla się na monitorze jest widoczne jedynie pod bardzo ograniczonym kątem.

**8. Zostawianie na zbyt długo wydruków na ogólnodostępnych drukarkach.**

Częstym rozwiązaniem w wielu firmach są drukarki sieciowe, na których można drukować zdalnie z niemal każdego komputera. Powoduje to oczywiste zagrożenia związane z tym, że nieuprawniona osoba może się przypadkiem zapoznać z danymi na wydrukach.

Aby temu zapobiec należy jak najszybciej odbierać swoje dokumenty z drukarki, bądź też używać funkcji bezpiecznego wydruku – drukowanie rozpocznie się dopiero wówczas, gdy wpiszemy na drukarce swoje hasło.

**9. Telefoniczne udostępnianie danych niezidentyfikowanemu rozmówcy.**

Zdarza się również, że pracownicy przekazują dane przez telefon, bez wcześniejszego upewnienia się, że rozmawiają z osobą upoważnioną do ich uzyskania. Czasem wystarczy, że ktoś przedstawi się jako członek rodziny bądź pracownik banku czy policji, aby w prosty sposób pozyskać interesujące go informacje. Aby upewnić się, że faktycznie rozmawiamy z osobą, za którą rozmówca się podaje, można np. zadzwonić na ogólny numer banku czy komisariatu policji i poprosić o połączenie z daną osobą. Jeśli jest to niemożliwe, lub też w wystarczający sposób nie rozwiewa wątpliwości co do tożsamości czy uprawnień danej osoby do pozyskania danych, zawsze można odmówić przekazania informacji drogą telefoniczną. Możemy poprosić o skierowanie oficjalnego zapytania w formie pisemnej.

**10. Niefrasobliwe rozmowy.**

Niestety, bardzo często można usłyszeć historie z życia różnych firm, wraz z imionami i nazwiskami zaangażowanych w nie osób. Wystarczy wyjąć z uszu słuchawki i na chwilę wsłuchać się w gwar miasta. Czy to jadąc tramwajem, czy czekając na przystanku czy stojąc w kolejce do kasy biletowej w kinie, można się z łatwością dowiedzieć, tego kto ile zarabia, kto dostanie awans, kto zostanie zwolniony, czyje dzieci właśnie wyjeżdżają na zimowisko, itp. Czy na pewno musimy i chcemy rozmawiać o takich sprawach w miejscach publicznych? Jeśli z jakichś powodów odpowiedź będzie twierdząca, postarajmy się przynajmniej nie używać wówczas nazwisk oraz jakichkolwiek innych nazw czy określeń, dzięki którym znacznie ułatwimy identyfikację osób, czy sytuacji, o których rozmawiamy.

Choć czasem nie zdajemy sobie z tego sprawy to jednak tzw. incydenty związane z ochroną danych osobowych zdarzają się w firmach niemal każdego dnia. Efektem, poza oczywistymi stratami finansowymi (utrata klientów, kary sądowe, odszkodowania), są również ogromne straty wizerunkowe.

Opracował:

**IOD UZ**