Wskazówki dotyczące bezpiecznego przetwarzania danych osobowych podczas pracy zdalnej

Przepisy dotyczące ochrony danych osobowych (Rozporządzenie RODO, Ustawa o ochronie danych osobowych) nie zabraniają pracy zdalnej, nie zawierają również szczegółowych instrukcji lub obostrzeń z tym związanych. Nie znaczy to jednak, że przy podejmowaniu pracy zdalnej nie powinniśmy brać pod uwagę przepisów o ochronie danych osobowych.

Niezależnie od miejsca, w którym odbywa się praca należy stosować adekwatne środki zabezpieczeń technicznych i organizacyjnych minimalizujących możliwość powstania incydentów związanych z naruszeniem ochrony danych. Należy także mieć na uwadze ogólne zasady dotyczące przetwarzania danych (zawarte w art. 5 ust. 1 lit. f Rozporządzenia RODO m.in integralność i poufność danych), które mówią o tym, że przetwarzanie powinno odbywać się w sposób zapewniający odpowiednie bezpieczeństwo, które zagwarantuje ochronę przed niedozwolonym lub niezgodnym z prawem użyciem, przypadkową utratą, zniszczeniem lub uszkodzeniem.

Poniżej zamieszczono ogólne zasady bezpieczeństwa, których należałoby przestrzegać podczas pracy zdalnej:

1. Pracownik wykonujący pracę zdalną jest zobowiązany zachować poufność przetwarzanych danych oraz sposobów ich zabezpieczenia, a także przetwarzać udostępnione dane osobowe jedynie w celach służbowych. Poza miejscem pracy nie należy prowadzić rozmów dotyczących informacji służbowych podlegających ochronie.
2. Dokumenty w miejscu pracy zdalnej należy zabezpieczyć w ten sposób, aby osoby nieuprawnione (np. domownicy) nie miały możliwości zapoznania się z nimi. Przy opuszczaniu miejsca pracy należy zachować „zasadę czystego biurka” – nośniki zawierające dane osobowe chowane do szaf, szuflad, zamykanie pomieszczenia.
3. Notatki, brudnopisy i inne materiały powstałe w trakcie pracy z dokumentacją należy niszczyć za pomocą niszczarek, bądź w inny sposób uniemożliwiający odczytanie zawartych w nich treści. Nie należy wyrzucać dokumentów (chociaż przedartych częściowo) do kosza na śmieci.
4. Nośników informacji z danymi podlegającymi ochronie nie należy pozostawiać w miejscach ogólnodostępnych i niezabezpieczonych, a także nie należy ich udostępniać osobom nieupoważnionym. Zaleca się, aby dostęp do nośników był chroniony hasłem tak, aby zapewnić odpowiednie bezpieczeństwo danych osobowych na nich zawartych.
5. Sprzęt wykorzystywany do pracy zdalnej powinien być wyposażony w oprogramowanie antywirusowe, aktualizowane na bieżąco. Na bieżąco również należy aktualizować system operacyjny.

6. Dostęp do komputera i/lub programu wykorzystywanego do pracy zdalnej powinien być możliwy wyłącznie z wykorzystaniem indywidualnego identyfikatora oraz hasła. Hasło powinno być odpowiednio złożone – nie powinno być zbudowane za pomocą ciągu znajdujących się obok siebie znaków na klawiaturze lub oparte na prostych skojarzeniach związanych z użytkownikiem (np. nr telefonu, imię i nazwisko, imiona dzieci itp.). Hasło nie powinno być zapisane i przechowywane w miejscach nie gwarantujących ich poufności (np. hasło zapisane na kartce schowanej pod klawiaturą, naklejoną na monitor, itp.).
7. Nie zaleca się domyślnego zapamiętywania haseł dostępu do konta użytkownika w poszczególnych programach wykorzystywanych w pracy zdalnej, w szczególności dziennika elektronicznego, jak i platform wykorzystywanych w kształceniu na odległość.
8. Używanych identyfikatorów i haseł nie należy udostępniać innym osobom, a w przypadku podejrzenia, że osoba postronna weszła w ich posiadanie, należy dokonać ich zmiany. Nie zaleca się używania tych samych haseł w różnych systemach informatycznych.
9. Przed czasowym opuszczeniem stanowiska pracy pracownik zobowiązany jest włączyć wygaszacz ekranu lub wylogować się z systemu/programu. Monitor należy usytuować w taki sposób, aby osoby nieupoważnione nie miały wglądu do danych na nim wyświetlanych.
10. Na komputerze służbowym pracownik nie powinien korzystać z Internetu do celów prywatnych. Powinien unikać wchodzenia na nieznane, czy przypadkowe strony, a także nie podłączać się do nieznanych źródeł Internetu. Zabronione jest zgrywanie na dysk komputera oraz uruchamianie nielegalnych programów oraz plików pobranych z niewiadomego źródła.
11. Po zakończeniu pracy na komputerze należy wylogować się ze wszystkich systemów, programów z których korzystaliśmy, wyłączyć sprzęt komputerowy, upewniając się, że nie zostały w nim żadne nośniki pamięci.
12. Pracując zdalnie koniecznym może okazać się korzystanie z poczty elektronicznej. Taką korespondencję należy prowadzić ze służbowej skrzynki pocztowej. Jeśli pracodawca nie zapewnił służbowych skrzynek poczty elektronicznej, to, jeżeli pracownicy wykorzystują do celów służbowych prywatną skrzynkę, muszą pamiętać, aby korzystać z niej w sposób rozważny i bezpieczny (nie należy otwierać załączników w e-mailach pochodzących od nieznanych nadawców).
13. Szczególną uwagę należy zwrócić na zabezpieczenie danych osobowych udostępnianych w przesyłanych wiadomościach. Zawsze przed wysłaniem wiadomości należy sprawdzić czy w nazwie adresu e-mail nie ma np. przestawionych lub pominiętych znaków tak, aby nie wysłać takiej widomości do osób nieupoważnionych. Podczas wysyłania korespondencji „zbiorczej" należy korzystać z opcji „UDW", dzięki której odbiorcy wiadomości nie będą widzieć wzajemnie swoich adresów e-mail.
14. Zaleca się regularne tworzenie kopii zapasowych.

15. W przypadku utraty lub zgubienia dokumentów/nośników, ich ujawnienia w jakikolwiek inny sposób, a także wystąpienia innych incydentów lub naruszeń ochrony danych należy ten fakt niezwłocznie zgłosić bezpośredniemu przełożonemu.
16. Należy pamiętać o bezpiecznym korzystaniu z komputera i innych urządzeń, zarówno wtedy, gdy zapewnił je pracodawca, jak i wtedy, gdy korzysta się z własnego sprzętu.

Pamiętajmy o tym, że pracując w miejscu pracy zdalnej nadal jesteśmy zobowiązani przestrzegać wszelkich przepisów w zakresie danych osobowych.

Warto także zapoznać się z zaleceniami i wskazówkami dotyczącymi ochrony danych osobowych opublikowanymi na stronie Urzędu Ochrony Danych Osobowych :

- ochrona danych osobowych podczas pracy zdalnej : https://uodo.gov.pl/pl/138/1459
- dane dzieci bezpieczne w sieci : https://uodo.gov.pl/pl/138/1363
- ochrona danych osobowych w szkole : https://uodo.gov.pl/pl/383/479
- tworzenie haseł dostępowych : https://uodo.gov.pl/pl/138/1285

W razie pytań lub wątpliwości służę pomocą
IOD – Katarzyna Synowczyńska
k.synowczynska@oswiata-prudnik.pl