DOM POMOCY SPOŁECZNEJ
"ZAMECZEK"
44-144 Kuźnia Nieborowska
ul. Knurowska 13, tel. (32) 235 16 30

KOMUNIKAT DYREKTORA DPS W ZAKRESIE PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH W TRAKCIE PRACY WYKONYWANEJ W TRYBIE ZDALNYM

Wymuszone zaistniałą w Kraju sytuacją epidemiologiczną przejście na wykonywanie obowiązków pracowniczych w trybie zdalnym tzw. („home office") wiązać się może z podwyższonym ryzykiem w zakresie naruszenia ochrony danych osobowych. Mając na uwadze powyższe, Dyrekcja Domu Pomocy Społecznej „Zameczek" w Kuźnik Nieborowskiej pragnie z jednej strony przypomnieć najważniejsze zasady dotyczące przetwarzania i ochrony danych osobowych, z drugiej zaś strony uczulić na konieczność ich rygorystycznego stosowania podczas pracy wykonywanej w warunkach domowych.

W związku ze specyfiką pracy w trybie zdalnym, szczególną uwagę zwrócić należy na:

1. kwestie bezpiecznego i prawidłowego przesyłania dokumentów w formie elektronicznej,
2. zabezpieczenie dokumentów papierowych przed dostępem osób trzecich, w szczególności niepozostawienie ich w miejscu dostępnym dla takich osób,
3. zabezpieczenie dokumentów przed ich zgubieniem bądź przypadkową utratą,
4. odpowiednie zabezpieczenie sprzętu komputerowego, na którym wykonywana jest praca, zwłaszcza jeżeli jest to sprzęt używany również do celów prywatnych,
5. zabezpieczenie dokumentacji papierowej i elektronicznej zawierającej tzw. dane wrażliwe (m.in. w zakresie stanu zdrowia).

We wszelkich sprawach związanych z ochroną danych osobowych, należy zwracać się do Dyrekcji OPS.

I. Zasady ogólne.

1) Każdy Pracownik DPS zobowiązany jest do stałego czuwania nad tym, by nie doszło do wystąpienia sytuacji skutkującej naruszeniem ochrony danych osobowych bądź sytuacji stwarzającej takie ryzyko.
2) W przypadku stwierdzenia lub podejrzenia, iż doszło do naruszenia bezpieczeństwa danych, należy niezwłocznie poinformować o tym fakcie Dyrektora DPS bądź Inspektora Ochrony Danych Osobowych; nieniuchanie spełnienia tego obowiązku może być zakwalifikowane jako rażące naruszenie podstawowych obowiązków pracowniczych.
3) Do typowych sytuacji skutkujących wysokim ryzykiem naruszenia bezpieczeństwa należą:
   a) niewłaściwe zabezpieczenie fizyczne urządzeń i dokumentów;
   Przykład: Pozostawienie niezabezpieczonego komputera z otwartym dokumentem;
   b) niestosowanie zasady czystego biurka;

c) niestosowanie zasady czystego ekranu;

d) prowadzenie rozmowy służbowej, w której przekazywane są Dane Osobowe, w obecności osób nieuprawnionych do zapoznania się z nimi;

e) niestosowanie zasady szczególnej ostrożności przy wynoszeniu dokumentów bądź nośników z terenu DPS.

f) celowe bądź przypadkowe udostępnienie Danych Osobowych osobie nieuprawnionej;

Przykład: wysłanie e-maila zawierającego Dane Osobowe pod niewłaściwy adres;

g) awaria sprzętu bądź oprogramowania służącego do Przetwarzania Danych Osobowych;

h) wystąpienie sygnałów świadczących, że komputer, na którym przetwarzane są Dane Osobowe został zainfekowany wrogim oprogramowaniem;

Przykład: ostrzeżenie ze strony programu antywirusowego, nagłe spowolnienie działania systemu lub automatyczne otwieranie się w przeglądarce podejrzanej strony startowej;

i) niszczenie dokumentacji bez użycia niszczarki bądź wyrzucanie niezniszczonej dokumentacji;

j) pozostawienie niezabezpieczonej dokumentacji zawierającej dane osobowe w miejscu dostępnym dla osób nieupoważnionych do zapoznania się z nimi;

k) wynoszenie Danych Osobowych w wersji papierowej bądź elektronicznej na zewnątrz Obszaru Przetwarzania Danych bez stosownego upoważnienia;

l) pozostawione otwarte drzwi do pomieszczeń lub szaf, gdzie przechowywane są Dane Osobowe pod nieobecność upoważnionych Pracowników;

m) zagubienie bądź kradzież laptopa bądź telefonu zawierającego zapisane Dane Osobowe (w tym np. zdjęcia dokumentów);

n) otrzymywanie podejrzanych e-maili;

o) zapisywanie haseł do systemów w pobliżu komputera.

II. Wybrane środki w celu ochrony bezpieczeństwa Danych Osobowych

1) Każdy Użytkownik zobowiązany jest do ochrony Danych Osobowych przed dostępem, w tym przed ujawnieniem, wobec osób nieupoważnionych.
2) Pracowników obowiązuje tzw. **polityka czystego biurka**. Oznacza to, że dane w formie papierowej mogą znajdować się na biurkach tylko na czas niezbędny na dokonanie czynności służbowych, a następnie muszą być chowane do odpowiednio zabezpieczonych szaf bądź szuflad; w całej rozciągłości obowiązuje to również podczas pracy wykonywanie w domu !
3) Pracowników obowiązuje tzw. **polityka czystego ekranu**. Oznacza to, że monitory komputerów, na których przetwarzane są Dane, są tak ustawione, aby osoby

nieupoważnione nie miały wglądu w Dane; w całej rozciągłości obowiązuje to również podczas pracy wykonywanie w domu !

4) Do dokumentacji medycznej dostęp mają wyłącznie pracownicy posiadający stosowne upoważnienie; podczas korzystania z takiej dokumentacji są oni zobowiązani do zachowania szczególnej ostrożności i zwrócenia szczególnej uwagi, by dane zawarte w niej dane da pozostawały bezpieczne.
5) W wypadku potrzeby wyniesienia komputera przenośnego (np. typu notebook) zawierającego Dane Osobowe lub inne informacje chronione, komputer taki musi być odpowiednio zabezpieczony. Ponadto pracownicy są wówczas zobowiązani do zachowania szczególnej ostrożności w zakresie zapewnienia ochrony i poufności Danych.
6) W przypadku konieczności przeniesienia Danych Osobowych pomiędzy komputerami obowiązuje konieczność zachowania szczególnej ostrożności.
7) Po przeniesieniu Danych użyte w tym celu nośniki należy niezwłocznie wyczyścić, tak aby nie zostały na nich Dane Osobowe.
8) W wypadku niemożliwości skasowania Danych z nośnika (płyta CD-ROM) - należy taką płytę zniszczyć fizycznie.
9) Błędne lub nieaktualne wydruki i wersje papierowe zawierające Dane Osobowe lub inne informacje chronione należy niezwłocznie zniszczyć są za pomocą niszczarki lub w inny mechaniczny sposób uniemożliwiający powtórne ich odtworzenie.
10) Komunikacja ustna (w tym w drodze telefonicznej), mająca charakter służbowy i obejmująca przekazywanie Danych Osobowych w celach służbowych następuję w sposób i w warunkach gwarantujący ochronę tak przekazywanych Danych przed dostępem osób niepowołanych; w szczególności zabronione jest prowadzenie takich rozmów w obecności osób trzecich (chyba, że chodzi o Dane powszechnie jawne).
11) W przypadku konieczności wyniesienia z terenu DPS dokumentów zawierających Dane Osobowe należy zachować szczególną ostrożność. Zabronione jest pozostawianie takich dokumentów w miejscach niegwarantujących odpowiedniego stopnia bezpieczeństwa (samochód, pomieszczenie ogólnodostępne).
12) W odniesieniu do dokumentów zawierających dane wrażliwe wymaga się, aby przewidziane środki ich zabezpieczenia stosowane były ze szczególną skrupulatnością;

III. Wybrane środki bezpieczeństwa w zakresie korzystania ze sprzętu komputerowego

1) Do uwierzytelnienia Użytkowników w systemie używa się haseł lub innych metod zapewniających weryfikację tożsamości Użytkownika.
2) Każdy Użytkownik zobowiązany jest do zachowania w tajemnicy własnych haseł, także po upływie ich ważności.
3) Hasła muszą odpowiadać następującym wymogom:
4) Przed przystąpieniem do pracy z systemem informatycznym Użytkownik zobowiązany

jest dokonać sprawdzenia stanu urządzeń komputerowych oraz dokonać oględzin swojego stanowiska pracy, przy zwróceniu szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie poufności Danych Osobowych.

5) Przed opuszczeniem stanowiska pracy, Użytkownik obowiązany jest:
   a) wylogować się z systemu informatycznego lub
   b) poczekać, aż zaktywizuje się blokowany hasłem wygaszasz ekranu.
6) Kończąc pracę należy:
   a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się Dane Osobowe, przed dostępem osób nieuprawnionych.
7) Korzystając z komputera dostępnego dla większej ilości osób należy zwrócić szczególną uwagę, czy po zakończeniu pracy dokumenty zawierające dane osobowe zostały z niego usunięte/zabezpieczone w sposób uniemożliwiający dostęp bądź usunięcie/nadpisanie przez osobę trzecią; w razie wątpliwości należy zwrócić się do IODO.
8) Na stacjach roboczych używanych zainstalowane być musza programy antywirusowe, podlegające systematycznej, bieżącej aktualizacji, zarówno w zakresie wersji oprogramowania jak i w zakresie bazy wirusów.
9) Użytkownik korzystający z komputera przenośnego jest zobowiązany do zachowania szczególnej ostrożności podczas transportu komputera oraz nie może udostępnić komputera osobom nieupoważnionym.
10) Dane Osobowe przesyłane na nośnikach oraz za pomocą systemów teleinformatycznych powinny być zabezpieczone w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym.
11) Ekrany monitorów powinny być w miarę możliwości wyposażone w wygaszacze zabezpieczone hasłem, które aktywują się automatycznie po upływie określonego czasu od ostatniego użycia komputera.
12) Ekrany monitorów powinny być ustawione w taki sposób, aby uniemożliwić osobom nieupoważnionym odczyt wyświetlanych informacji.
13) W przypadku konieczności przesłania dokumentów cyfrowych zawierających wrażliwe dane osobowe za pośrednictwem systemu teleinformatycznego bezwzględnie wymaga się ich zabezpieczenia za pomocą hasła, które winno być przesłane do adresata inną drogą (np. sms-em).

DYREKTOR
Domu Pomocy Społecznej "Zameczek"
w Kuźni Nieborowskiej
mgr Ewa Zamora

10.04.2020 r.