Zarządzenie nr 6/2019
Kierownika Gminnego Ośrodka Pomocy Społecznej w Kamienicy Polskiej
z dnia 4 listopada 2019 roku

w sprawie: wprowadzenia dokumentu o nazwie „Regulamin Ochrony Danych Osobowych" Gminnego Ośrodka Pomocy Społecznej w Kamienicy Polskiej

§1

Zgodnie z artykułem 24 oraz motywem 78 rozporządzenia parlamentu europejskiego i rady (UE) 2016/679 r, wdrażam Regulamin Ochrony Danych Osobowych Gminnego Ośrodka Pomocy Społecznej , stanowiący załącznik do zarządzenia

§ 2

Każdy pracownik, zgodnie z wykazem, jest obowiązany zapoznać się z treścią Regulaminu Ochrony Danych Osobowych

§ 3

Zobowiązuję wszystkich pracowników do przestrzegania zapisów zawartych w Regulaminie Ochrony Danych Osobowych.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

KIEROWNIK
Gminnego Ośrodka Pomocy Społecznej
w Kamienicy Polskiej
mgr Anna Cierpiał

Regulamin Ochrony Danych Osobowych

Gminnego Ośrodka Pomocy Społecznej w Kamienicy Polskiej

1. PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH

1. Osoby przetwarzające dane osobowe przed dopuszczeniem ich do przetwarzania danych osobowych zapoznają się z niniejszym Regulaminem.
2. Osoby zapoznane z treścią Regulaminu ochrony danych osobowych zobowiązane są podpisać oświadczenie o poufności.
3. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:

    1. przetwarzania danych osobowych wyłącznie w zakresie i celu określonym przez Administratora Danych Osobowych (ADO),
    2. zachowanie w tajemnicy danych osobowych do których ma dostęp w związku wykonywanymi zadaniami właściwymi do zajmowanego stanowiska,
    3. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych w jednostce,
    4. ochrony danych osobowych przed przypadkowym lub nie zgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem, dostępem do danych osobowych oraz ich przetwarzaniem

4. Zabrania się przekazywania lub ujawnienia danych osobom lub instytucją, które nie wykazują się podstawą prawną uprawniającą do dostępu do takich danych.
5. Zabrania się przekazywania bezpośrednio lub telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zidentyfikować.

2. UŻYTKOWANIE SPRZĘTU ELEKTRONICZNEGO

1. Użytkownicy pracują na własnych ,przydzielonych im przez administratora systemów informatycznych kontach. Zabronione jest umożliwienie innym osobom korzystanie z konta innego użytkownika.
2. Każdy użytkownik przetwarzający dane osobowe za pomocą sprzętu elektronicznego (np.na komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) posiada swój własny indywidualny Identyfikator do logowania się.
3. Użytkownicy nie mogą samodzielnie zmieniać przyznanych im uprawnień.
4. Wszystkie osoby przetwarzające dane osobowe, korzystające ze sprzętu elektronicznego (np. z komputerów stacjonarnych, laptopów, monitorów, drukarek, skanerów, urządzeń kserujących, tabletów i telefonów) mają obowiązek jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem.
5. Zabronione jest samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń oraz instalowanie na dysku innego oprogramowania i aplikacji.
6. W przypadku zagubienia ,utraty lub zniszczenia sprzętu, użytkownik ma obowiązek natychmiast zgłosić takie zdarzenie ADO lub Inspektorowi Danych Osobowych (IOD)
7. Dane osobowe zapisane na nośnikach zewnętrznych powinny być szyfrowane.
8. Użytkownicy sprzętu, pracujący z danymi osobowymi muszą dbać o to, by osoby niepowołane nie miały możliwości wglądu do danych wyświetlanych na monitorze komputera.
9. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest wyłączyć blokowany hasłem wygaszacz ekranu lub wylosować się ze systemu.
10. Po zakończeniu pracy, użytkownik zobowiązany jest wylosować się ze systemu informatycznego, następnie wyłączyć sprzęt komputerowy i zabezpieczyć Stanowisko pracy z godnie z Polityką Czystego Biurka

3. POLITYKA HASEŁ

1. Hasła powinny składać się z przynajmniej 8 znaków i zawierać małe+ duże litery + liczby+ znaki specjalne
2. Hasła powinny mieć odpowiedni stopień skomplikowania. Dlatego nie mogą być łatwymi do odgadnięcia słowami.
3. Zabronione jest udostępnianie swoich haseł nieuprawnionym osobom. W przypadku ujawnienia hasła – należy je natychmiast zmienić.
4. Nie wolno ich nigdzie zapisywać, ani naklejać np. na monitorze ,pod klawiaturą komputera oraz w innych miejscach w biurze.
5. Zapasowe hasła przechowywane są u ADO w zaklejonych kopertach zamykanych w szafie metalowej.
6. Hasła należy zmieniać co 60 dni lub w chwili wymuszenia zmiany hasła przez Program lub aplikację.

4. ZASADY POSTĘPOWANIA Z DOKUMENTACJĄ PAPIEROWĄ, ZAWIERAJĄCĄ DANE OSOBOWE

1. Osoby pracujące z danymi osobowymi zobowiązane są do stosowania tzw. Polityki Czystego Biurka. Zgodnie z jej zasadami należy zabezpieczyć dokumenty z danymi osobowymi prze kradzieżą , zniszczeniem lub wglądem osób nieuprawnionych zarówno w czasie godzin pracy, jak i po jej zakończeniu.
2. Osoby przetwarzające dane osobowe zobowiązane są niszczyć niepotrzebną dokumentację oraz wydruki z danymi osobowymi.
3. Zabronione jest pozostawienie Dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami.
4. Zabrania się wyrzucania niezniszczonych Dokumentów na śmietnik lub porzucania ich na zewnątrz, poza jednostką.

5. WYNOSZENIE NOŚNIKÓW Z DANYMI POZA FIRMĘ

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych nośników informacji (np. dysków, pen-diverów, kart pamięci) z zapisem danych osobowych ,bez zgody ADO lub IDO.
2. Jeżeli dokumenty przewozi pracownik, to on jest odpowiedzialny za ich zabezpieczeniem przed utratą i zniszczeniem.
3. Dane osobowe w wersji papierowej muszą być zabezpieczone w odpowiednich torbach i plecach i teczkach. Zaleca się korzystać ze sprawdzonych firm kurierskich.
4. W przypadku wynoszenia poza firmę danych osobowych zapisanych elektronicznie należy je zaszyfrować.

6. REGULACJE DOTYCZĄCE KORZYSTANIA Z INTERNETU

1. Pracownicy zobowiązani są do korzystania z internetu wyłącznie w celach służbowych.
2. Zabronione jest uruchamianie jakichkolwiek innych programów ,których nie ma zainstalowanych przez ADO .Łamanie tej zasady wiąże się z karami służbowymi.(np. instalowanie innych programów, aplikacji i wgrywanie gier)
3. W jednostce wprowadzone są ograniczenia w dostępie do stron internetowych, dlatego zabronione jest wchodzenie na strony o charakterze pornograficznym, przestępczym, hackerskim lub innym zakazanym przez prawo.
4. W opcjach przeglądarki internetowej nie należy włączać opcji uzupełniania formularzy i zapamiętywania haseł.

7. KORZYSTANIE Z POCZTY ELEKTRONICZNEJ

1. E-mali służbowy należy wykorzystywać wyłącznie do wykonywania obowiązków służbowych.
2. Nie wolno wysyłać korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
3. W przypadku wysyłania dokumentacji zawierającej dane osobowe – pliki z danymi należy szyfrować .Innym kanałem dostarczyć hasło otwarcia.
4. Należy zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

5. Przed otwarciem załączników(plików) w mailach zawsze należy przeprowadzić weryfikację nadawcy.
6. Nie należy klikać na hiperlinki w mailach, gdyż mogą one zainstalować programy śledzące lub infekujące Komputer i przejąć dane.
7. W przypadku wysyłania korespondencji seryjnej należy użyć UDW –„ukryte wiadomości"
8. Należy okresowo czyścić zbyteczne maile.
9. Z prywatnej skrzynki pocztowej nie może pracownik przesyłać danych osobowych bez wiedzy ADO

8. ODPOWIEDZIALNOŚĆ DYSCYPLINARNA

Przypadki świadomego naruszenia regulacji Regulaminu Ochrony Danych Osobowych lub nieuzasadnionego zaniechania obowiązków mogą zostać uznane przez ADO za ciężkie naruszenie obowiązków pracowniczych zgodnie z art. 52 kodeksu pracy oraz naruszenie przepisów karnych zawartych w RODO

KIEROWNIK
Miejskiego Ośrodka Pomocy Społecznej
w Kamienicy Polskiej
mgr Anna Cierpiał