

Regulamin Ochrony Danych Osobowych w Przemyskiej Spółdzielni Mieszkaniowej w Przemysłu.

Niniejszy regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

SPIS TREŚCI

1Zasady bezpiecznego użytkowania sprzętu IT, dysków, programów	2
2Zarządzanie uprawnieniami - procedura rozpoczęcia, zawieszenia i zakończenia pracy.....	2
3Polityka haseł.....	2
4Zabezpieczenie dokumentacji papierowej z danymi osobowymi.....	2
5Zasady wynoszenia nośników z danymi poza firmę/organizację.....	3
6Zasady korzystania z internetu.....	3
7Zasady korzystania z poczty elektronicznej.....	3
8Skrócona instrukcja postępowania w przypadku naruszenia ochrony danych osobowych.....	3
9Obowiązek zachowania poufności i ochrony danych osobowych.....	4
10Postępowanie dyscyplinarne.....	4

1 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. Użytkownik odpowiada za zabezpieczenie przed zniszczeniem, uszkodzeniem oraz utratą sprzętu IT (komputerów, urządzeń biurowych, tabletów i smartfonów)
2. Demontaż, instalowanie lub podłączanie dodatkowych urządzeń jest zabronione
3. Użytkownik jest zobowiązany do usuwania tymczasowych plików z nośników/dysków z miejsc, gdzie dostęp do nich miałyby osoby nieupoważnione
4. Użytkownik jest zobowiązany do przekazania informatykowi nośników przeznaczonych do zniszczenia

2 ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik komputerów, programów i systemu operacyjnego zobowiązany jest do pracy na własnym koncie. Zabronione jest udostępnianie konta innemu użytkownikowi
2. Użytkownik nie może zmieniać swoich uprawnień, np. zostać Administratorem na swoim komputerze
3. Użytkownik komputera oraz programów rozpoczyna i kończy pracę logowaniem i wylogowaniem się
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. **zasada czystego ekranu**.
5. Użytkownik przed tymczasowym odejściem od komputera musi włączyć wygaszacz ekranu (**WINDOWS + L**) lub wylogować się z systemu bądź z programu.
6. Zabrania się uruchamiania jakiegokolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik działu informatyki. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
7. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć nośniki elektroniczne, magnetyczne i optyczne na których znajdują się dane osobowe.

3 POLITYKA HASEŁ

1. Hasła powinny składać się z np. **12** znaków
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne)
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
6. Hasła muszą być zmieniane co **60 / 90** dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.

4 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANymi OSOBOWYMI

1. Pracownicy są zobowiązani do stosowania tzw. „**zasady czystego biurka**”. Polega ona na zabezpieczeniu (zamykaniu na klucz) dokumentów oraz nośników np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób postronnych.
2. Pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach.
3. Zabrania się pozostawiania dokumentów w miejscach dostępnych dla osób postronnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik.

5 ZASADY WYNOŚZENIA NOŚNIKÓW Z DANymi POZA FIRME/ORGANIZACJĘ

1. Użytkownicy nie mogą wnosić na zewnątrz niezasyfrowanych nośników z danymi osobowymi (np. przenośnych dysków twardych, pen-drive, płyt CD, DVD, pamięci typu Flash).
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski przenośne, zahastowane pliki, zabezpieczone smartfony).

3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w torbach, plecakach, teczkach w celu zabezpieczenia ich przed zagubieniem i kradzieżą.

6 ZASADY KORZYSTANIA Z INTERNETU

1. Zabrania się instalowania programów z Internetu bez konsultacji z informatykiem.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez takie oprogramowanie.
3. Zabrania się wchodzenia na strony z nielegalnym oprogramowaniem do pobrania oraz na hackerskie.
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupelniania formularzy i zapamiętywania haseł.

7 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Pliki z danymi osobowymi w Wordzie, Excelu, w Pdf lub spakowane (7zip), przed wysłaniem ich do osób trzecich powinny być zahasłowane, a hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.
2. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum (np. 12) znaków: duże i małe litery i cyfry lub znaki specjalne.
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4. **WAŻNE:** Nie otwierać załączników (.zip, .rar, .xslm, .pdf, .exe) w mailach!!!! Są to zwykle „wirusy”, które infekują komputer oraz często pozostałe komputery w sieci. **WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.**
5. **WAŻNE:** Nie wolno „klikać” na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami”. Użytkownik „klikając” na taki hiperlink infekuje komputer oraz inne komputery w sieci. **WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.**
6. Należy zgłaszać informatykowi przypadki podejrzanych emaili.
7. Użytkownicy nie powinni rosyłać „niezawodowych” emaili w formie „łańcuszków szczęścia”.
8. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „**Ukryte do wiadomości – UDW**”. Zabronione jest rosyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości”.
9. Użytkownicy powinni okresowo kasować niepotrzebne emaile.
10. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób współpracujących.
11. Użytkownik bez zgody Pracodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

8 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia Pracodawcy / Zleceniodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
 - a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
 - b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
 - c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do incydentów wymagających powiadomienia, należą:
 - a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
 - b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych);
 - c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. Typowe przykłady incydentów wymagające reakcji:
 - a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
 - b. dokumentacja jest niszczone bez użycia niszczarki;
 - c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
 - d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
 - e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
 - f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy / Zleceniodawcy;
 - g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;
 - h. telefoniczne próby wyłudzenia danych osobowych;
 - i. kradzież, zagubienie komputerów lub CD, twarde dysków, Pen-drive z danymi osobowymi;
 - j. emaile zachęcające do ujawnienia identyfikatora i/lub hasła;
 - k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
 - l. hasła do systemów przyklejone są w pobliżu komputera.

9 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do:
 - a. przetwarzania danych osobowych wyłącznie w celu i zakresie powierzonych jej zadań;
 - b. zachowania w tajemnicy danych osobowych do których ma dostęp;
 - c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych jej zadań;
 - d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;
2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
4. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

10 POSTĘPOWANIE DYSCYPLINARNE

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez Pracodawcę / Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.