Zarządzenie nr 5/2018

Dyrektora Kujawsko-Pomorskiego Ośrodka Doradztwa Rolniczego w Minikowie z dnia 25 maja 2018 r.

w sprawie wdrożenia zasad dotyczących przetwarzania danych osobowych w Kujawsko-Pomorskim Ośrodku Doradztwa Rolniczego w Minikowie

Na podstawie § 9 ust. 2 pkt 6 Regulaminu Organizacyjnego Kujawsko-Pomorskiego oraz rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz.UE.L Nr 119, str. 1) i ustawy z dnia 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000) zarządzam, co następuje:

§ 1

Wdrażam do stosowania i przestrzegania:

1. „Politykę Bezpieczeństwa w Zakresie Przetwarzania Danych Osobowych w Kujawsko-Pomorskim Ośrodku Doradztwa Rolniczego w Minikowie" – stanowiący załącznik nr 1 do zarządzenia,
2. „Regulamin Ochrony Danych Osobowych w Kujawsko-Pomorskim Ośrodku Doradztwa Rolniczego w Minikowie" – stanowiący załącznik nr 2 do zarządzenia,
3. „Politykę Kluczy" – stanowiący załącznik nr 3 do zarządzenia,
4. „Regulamin Użytkowania Komputerów Przenośnych"- stanowiący załącznik nr 4 do zarządzenia.

§ 2

W celu zapewnienia właściwego toku przetwarzania danych osobowych wyznaczam:

1) Inspektora Ochrony Danych (IOD) – Romana Gibaszka
2) Administrator Systemu Informatycznego (ASI) – Krzysztofa Lacha

§ 3

Zobowiązuję kierowników komórek organizacyjnych Ośrodka do zapoznania pracowników z treścią niniejszego zarządzenia i jego stosowania

§ 4

Traci moc zarządzenie nr 4/2008 w sprawie wdrożenia dokumentacji przetwarzania danych osobowych w Kujawsko-Pomorskim Ośrodku Doradztwa Rolniczego z dnia 11.02.2008 r.

DYREKTOR

Ryszard Kamiński

Załącznik nr 1
do Zarządzenia nr 5/2018
Dyrektora KPODR w Minikowie
z dnia 25.05.2018 r.

POLITYKA BEZPIECZEŃSTWA
W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH
W KUJAWSKO-POMORSKIM OŚRODKU DORADZTWA ROLNICZEGO
W MINIKOWIE

SŁOWNIK SKRÓTÓW

Ogólne rozporzadzenie o ochronie danych - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE.L Nr 119, str. 1)

Polityka - oznacza niniejszą Politykę Bezpieczeństwa w Zakresie Przetwarzania Danych Osobowych, o ile co innego nie wynika wyraźnie z kontekstu

Dane - oznaczają dane osobowe, o ile co innego nie wynika wyraźnie z kontekstu

Dane wrażliwe - oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej

Osoba - oznacza osobę, której dane dotyczą, o ile co innego nie wynika wyraźnie z kontekstu.

Podmiot przetwarzający - oznacza podmiot lub osobę, której KPODR powierzył przetwarzanie danych osobowych (np. usługodawca - informatyk, podmiot wykonujący usługi zdrowotne)

KPODR – Kujawsko-Pomorski Ośrodek Doradztwa Rolniczego w Minikowie

IOD lub Inspektor - oznacza Inspektora Ochrony Danych Osobowych

RCPD lub Rejestr - oznacza Rejestr Czynności Przetwarzania Danych Osobowych

1. Polityka Bezpieczeństwa w Zakresie Przetwarzania Danych Osobowych w Kujawsko-Pomorskim Ośrodku Doradztwa Rolniczego w Minikowie zwana dalej „Polityką" jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez KPODR w celu spełnienia wymagań ogólnego rozporządzenia o ochronie danych.
2. Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z ogólnym rozporządzeniem o ochronie danych.
3. KPODR zapewnia zgodność przetwarzania danych osobowych z regulacjami ogólnego rozporządzenia o ochronie danych oraz krajowymi przepisami dotyczącymi ochrony danych osobowych, szczególnie w odniesieniu do:
   - pracowników
   - rolników i kotrahentów,
   - danych osobowych powierzonych do przetwarzania podmiotom trzecim.

4. FILARY OCHRONY DANYCH OSOBOWYCH W KPODR

- **Legalność** – KPODR dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
- **Bezpieczeństwo** – KPODR zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
- **Prawa pracownika** – KPODR umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
- **Rozliczalność** – KPODR dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność.

5. ZASADY OCHRONY DANYCH

KPODR działa w oparciu o podstawę prawną – ustawa z dnia 22 października 2004 r. o jednostkach doradztwa Rolniczego (tekst jednolity Dz.U. 2018 poz. 711) i zgodnie z prawem (legalizm);

- rzetelnie i uczciwie (rzetelność);
- w sposób przejrzysty dla osoby, której dane dotyczą (transparentność);
- w konkretnych celach i nie "na zapas" (minimalizacja);
- nie więcej niż potrzeba (adekwatność);
- z dbałością o prawidłowość danych (prawidłowość);
- nie dłużej niż potrzeba (czasowość);
- zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

6. SYSTEM OCHRONY DANYCH

System ochrony danych osobowych w KPODR składa się z następujących elementów:

1) **Inwentaryzacja danych. Ocena skutków dla ochrony danych.**

KPODR w terminie, co najmniej do końca stycznia danego roku kalendarzowego (lub każdorazowo w trakcie roku kalendarzowego - jak dodawane (odejmowane) są kolejne kategorie przetwarzanych danych) dokonuje identyfikacji zasobów przetwarzanych danych osobowych, kategorii danych, zależności między zasobami danych, identyfikacji sposobów wykorzystania danych (inwentaryzacja), w tym:

a) przypadków przetwarzania danych wrażliwych,
b) przypadków przetwarzania danych osób, których KPODR nie identyfikuje (dane niezidentyfikowane),
c) współadministrowania danymi.

2) **Rejestr.** KPODR opracowuje, prowadzi i utrzymuje Rejestr Czynności Przetwarzania Danych Osobowych, który jest narzędziem rozliczania zgodności z ochroną danych.
3) **Umowy powierzenia przetwarzania danych.** KPODR zawiera z podmiotami lub osobami, którym powierza przetwarzanie danych osobowych (np. usługodawca - informatyk, podmiot wykonujący usługi medyczne) odpowiednie umowy, stosownie do art. 28 ogólnego rozporządzenia o ochronie danych.
4) **Podstawy prawne.** KPODR zapewnia, identyfikuje, weryfikuje podstawy prawne przetwarzania danych i rejestruje je w Rejestrze, w tym:
   a) utrzymuje system zarządzania zgodami na przetwarzanie danych i komunikację na odległość *(sprawy dotyczące m.in. pracowników KPODR),*
   b) inwentaryzuje i uszczegóławia uzasadnienie przypadków, gdy przetwarza dane na podstawie prawnie uzasadnionego interesu.
5) **Obsługa praw jednostki.** KPODR spełnia obowiązki informacyjne względem osób, których dane przetwarza, oraz zapewnia obsługę ich praw, realizując otrzymane w tym zakresie żądania, w tym:
   a) **obowiązki informacyjne** - przekazuje osobom prawem wymagane informacje przy zbieraniu danych i w innych sytuacjach oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków,
   b) **możliwość wykonania żądań** - weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających,
   c) **obsługa żądań** - zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminach i w sposób wymagany RODO oraz dokumentowane,
   d) **zawiadamianie o naruszeniach** - stosuje procedury pozwalające na ustalenie konieczności zawiadomienia osób dotkniętych zidentyfikowanym naruszeniem ochrony danych.
6) **Minimalizacja.** KPODR posiada zasady i metody zarządzania minimalizacją (*privacy by default*), a w tym:
   a) zasady zarządzania **adekwatnością** danych,

b) zasady reglamentacji i zarządzania **dostępem** do danych,
c) zasady zarządzania okresem **przechowywania** danych i weryfikacji dalszej przydatności,

7) **Bezpieczeństwo.** KPODR zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:
   a) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii,
   b) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,
   c) dostosowuje środki ochrony danych do ustalonego ryzyka,
   d) posiada system zarządzania bezpieczeństwem informacji; (w tym systemem informatycznym),
   e) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami.
8) ***Privacy by design.*** KPODR zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów lub zadań uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

7. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH

1) RCPD stanowi formę dokumentowania czynności przetwarzania danych osobowych w KPODR. RCPD pełni rolę mapy przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.
2) KPODR prowadzi RCPD, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.
3) RCPD jest jednym z podstawowych narzędzi umożliwiających rozliczanie większości obowiązków ochrony danych.
4) W RCPD, dla każdej czynności przetwarzania danych, którą KPODR uznał za odrębną dla potrzeb Rejestru, odnotowuje co najmniej:
   a) nazwę czynności,
   b) cel przetwarzania,
   c) opis kategorii osób,
   d) opis kategorii danych,
   e) podstawę prawną przetwarzania, wraz z wyszczególnieniem kategorii uzasadnionego interesu KPODR, jeśli podstawą jest uzasadniony interes,
   f) sposób zbierania danych,

g) opis kategorii odbiorców danych (w tym przetwarzających),

h) informację o przekazaniu poza EU/EOG,

i) ogólny opis technicznych i organizacyjnych środków ochrony danych.

8. PODSTAWY PRZETWARZANIA

1) KPODR dokumentuje w RCPD podstawy prawne przetwarzania danych dla poszczególnych czynności przetwarzania.
2) Wskazując ogólną podstawę prawną (zgoda, umowa, obowiązek prawny, żywotne interesy, zadanie publiczne/władza publiczna, uzasadniony cel KPODR). KPODR dookreśla podstawę w czytelny sposób, gdy jest to potrzebne.
3) KPODR wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie itp.).
4) Kierownik komórki organizacyjnej KPODR ma obowiązek znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych. Jeżeli podstawą jest uzasadniony interes KPODR, kierownik komórki ma obowiązek znać konkretny realizowany przetwarzaniem interes KPODR.

9. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

1) W przypadku naruszenia ochrony danych osobowych, Dyrektor KPODR bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 ogólnego rozporządzenia o ochronie danych (Urząd Ochrony Danych Osobowych), chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2) Zgłoszenie naruszenia w KPODR ochrony danych osobowych musi co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
   b) zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

d) opisywać zastosowane lub proponowane środki w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3) Dyrektor KPODR dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

10. WYZNACZENIE INSPEKTORA OCHRONY DANYCH W KPODR

1) Status prawny i zadania Inspektora regulują przepisy Rozdziału IV Sekcji 4 ogólnego rozporzadzenia o ochronie danych.
2) Inspektor w wykonywaniu swoich zadań podlega bezpośrednio Dyrektorowi KPODR
3) Do zadań Inspektora należy w szczególności:
   a) informowanie Dyrektora oraz pracowników KPODR, którzy przetwarzają dane osobowe o obowiązkach wynikających z ogólnego rozporządzenia o ochronie danych osobowych oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach,
   b) monitorowanie przestrzegania ogólnego rozporządzenia o ochronie danych osobowych, innych przepisów dotyczących ochrony danych osobowych oraz prowadzenie szkoleń wewnętrznych zwiększających świadomość pracowników KPODR w zakresie zasad dotyczących ochrony danych,
   c) pełnienie funkcji punktu kontaktowego dla właściwych organów i podmiotów zewnętrznych w kwestiach związanych z przetwarzaniem przez KPODR danych osobowych.

11. CELEM POLITYKI JEST:

1) Zapewnienie wiedzy pracownikom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania.
2) Po zapoznaniu się z zasadami ochrony danych osobowych, pracownicy zobowiązani są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie stosownego oświadczenia.

Załącznik nr 2 do Zarządzenia 5/2018 r.
Dyrektora KPODR w Minikowie
z dnia 25.05.2018 r.

Regulamin
Ochrony Danych Osobowych
w Kujawsko-Pomorskim Ośrodku Doradztwa Rolniczego w Minikowie

Niniejszy Regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami ogólnego rozporządzenia o ochronie danych 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 ww. osób powinna zapoznać się z poniższym Regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych

SPIS TREŚCI

Słownik skrótów

ogólne rozporządzenie o ochronie danych - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz.UE.L Nr 119, str. 1)
Regulamin – Regulamin Ochrony Danych Osobowych w Kujawsko-Pomorskim Ośrodku Doradztwa Rolniczego w Minikowie,
dział PI – Dział Teleinformatyki,
ADO – Administrator Danych Osobowych (Kujawsko-Pomorski Ośrodek Doradztwa Rolniczego),
ASI – Administrator Systemu Informatycznego,

1 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolne instalowanie otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego **jest zabronione.**
4. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
5. Użytkownicy komputerów przenośnych, na których znajdują się dane osobowe lub z dostępem do danych osobowych przez Internet zobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie użytkowania komputerów przenośnych *(załącznik nr 4 do Zarządzenia 5/2018).*

2 ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Tworzenie kont użytkowników wraz z uprawnieniami odbywa się na polecenie przełożonych i wykonywane jest przez pracowników działu PI.
3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień (np. zostać administratorem Windows na swoim komputerze).
4. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
5. Zabrania się pracy wielu użytkowników na wspólnym koncie.
6. Użytkownik rozpoczyna pracę z użyciem identyfikatora i hasła.
7. Użytkownik jest zobowiązany do powiadomienia pracowników działu PI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
8. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym pracownika działu PI.
9. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. **„Polityka czystego ekranu".**
10. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu bądź z programu.
11. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została ona zweryfikowana jako pracownik działu PI. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
12. Po zakończeniu pracy, użytkownik zobowiązany jest:

a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, magnetyczne i optyczne, na których znajdują się dane osobowe.

3 POLITYKA HASEŁ

1. Hasła powinny składać się z 8 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. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.
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 30 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła
8. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
10. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym jednostki.
11. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
12. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

4 ZABEZPIECZENIE BUDYNKÓW I POMIESZCZEŃ

1. Dostęp do budynków KPODR w Minikowie, Oddziałów w Przysieku i Zarzeczewie odbywa się za zasadzie upoważnienia pracowników do otwierania i zamykania użytkowanych budynków kluczami będącymi w ich dyspozycji.
2. Dostęp do pomieszczeń PZDR odbywa się przy pomocy kluczy wydanych upoważnionym pracownikom przez administratorów budynków.
3. Szczegółowy tryb zabezpieczenia obiektów i pomieszczeń biurowych użytkowanych przez pracowników KPODR opisano w Polityce kluczy *(załącznik nr 3 do Zarządzenia 5/2018).*

5 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. **„Polityki czystego biurka"**. Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach,

biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.

2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych miejskich lub w lesie.

6 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA JEDNOSTKĘ

1. Użytkownicy nie mogą wynosić na zewnątrz jednostki wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy/Zleceniodawcy. Do takich nośników zalicz się: wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.
2. Dane osobowe wynoszone poza jednostkę muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich.
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.
6. Zabrania się wynoszenia poza obszar KPODR wymiennych nośników informacji, a w szczególności twardych dysków z zapisanymi danymi osobowymi i pendrivów bez zgody ADO.
7. Dane osobowe wynoszone poza obszar dokumentacji na nośnikach elektronicznych muszą być zaszyfrowane.
8. W sytuacji przekazywania nośników z danymi osobowymi poza obszar jednostki można stosować następujące zasady bezpieczeństwa:
    a. adresat powinien zostać powiadomiony o przesyłce,
    b. dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą,
    c. stosować bezpieczne koperty depozytowe,
    d. przesyłkę należy przesyłać przez kuriera.

7 ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT (ASI) i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na

większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci.

8 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza jednostkę może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza jednostkę należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS-em.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em.
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. **WAŻNE:** Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) w mailach pochodzących od nieznanych nadawców. Są to zwykle „wirusy", które infekują komputer oraz często pozostałe komputery w sieci. **WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.**
7. **WAŻNE:** Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami". Użytkownik „klikając" na takie hiperłącze infekuje komputer oraz inne komputery w sieci. **WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH.**
8. Należy zgłaszać pracownikowi działu PI przypadki podejrzanych emaili.
9. Użytkownicy nie powinni rozsyłać „niezawodowych" emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
11. Użytkownicy powinni okresowo kasować niepotrzebne maile.
12. Konta pocztowe służbowe są odseparowane od poczty prywatnej.
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.

15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
16. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
17. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.
18. Przy korzystaniu z maila, użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.
19. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
20. Użytkownik bez zgody Pracodawcy/Zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące Pracodawcy/Zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

9 OCHRONA ANTYWIRUSOWA

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie pracownika działu PI lub osobę upoważnioną.

10 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 niszczona 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 KPODR 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, twardych dysków, pendrivów z danymi osobowymi,
   j. maile 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.

11 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę/Zleceniodawcę zadaniach,
   b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę/Zleceniodawcę,
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę/Zleceniodawcę,
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
   e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.
2. Osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. 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.
4. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
5. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania jednostki, w tym informacji na temat

sprzętu i oprogramowania, z jakiego korzysta jednostka, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

12 ODPOWIEDZIALNOŚĆ ZA NARUSZENIE REGULAMINU

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.

Załącznik nr 3 do Zarządzenia nr 5/2018 Dyrektora KPODR w Minikowie z dnia 25.05.2018 r.

POLITYKA KLUCZY

1. Ogólne zasady:
   a. polityka kluczy obejmuje budynki KPODR w Minikowie, budynki Oddziałów w Przysieku i Zarzeczewie oraz pomieszczenia Powiatowych Zespołów Doradztwa Rolniczego,
   b. obowiązuje pięciodniowy tydzień pracy od poniedziałku do piątku w godzinach określonych w regulaminie pracy. W dniach targów, wystaw i innych imprez organizowanych na terenie administrowanym przez KPODR obowiązuje czas pracy zgodny z programem tych imprez,
   c. dostęp do pomieszczeń biurowych możliwy jest wyłącznie poprzez wyznaczone do tego drzwi. Wszystkie pozostałe drzwi umożliwiające dostęp do pomieszczeń biurowych powinny być trwale zamknięte na klucz. Zabrania się otwierania tych drzwi przez pracowników bez zgody bezpośrednich przełożonych,
   d. klucze zapasowe do budynków KPODR przechowywane są w:
      - pomieszczeniu działu DA,
      - w pomieszczeniach kierowników PA i ZA,
      - administratorów budynków, w których znajdują się siedziby Powiatowych Zespołów Doradztwa Rolniczego.
2. Nadawanie upoważnień:
   a. prawo pobierania kluczy do pomieszczeń mają wyłącznie osoby upoważnione przez bezpośrednich przełożonych. Obejmują one także dostęp do biura poza godzinami pracy.
   b. udzielenie/anulowanie upoważnienia wymaga wprowadzenia osoby do Ewidencji pobrania/zdawania kluczy prowadzonej przez dział DA, PA, ZA.
3. Wydawanie i zdawanie kluczy w trybie normalnym:
   a. klucze do budynków w Minikowie, Przysieku i Zarzeczewie wydawane są upoważnionym pracownikom działu DA, PA, ZA i pozostają pod ich osobistym nadzorem,
   b. klucze do pomieszczeń zajmowanych przez PZDR znajdują się w posiadaniu kierowników lub upoważnionych przez nich pracowników i pozostają pod ich osobistym nadzorem.
   c. klucze do pomieszczeń biurowych w Minikowie, Przysieku i Zarzeczewie wydawane są przez pracownika działu DA, PA, ZA za pokwitowaniem w

Ewidencji pobrania/zdawania kluczy i w czasie wykonywania obowiązków pozostają pod osobistym nadzorem użytkowników pomieszczeń.

d. klucze do pomieszczenia serwerowni w Minikowie wydawane są przez pracownika działu DA. Klucze pozostają pod osobistym nadzorem osób upoważnionych. Dostęp do tych pomieszczeń osób trzecich odbywa się pod ścisłym nadzorem Kierownika PI.
e. pracownicy działów DA, PA, ZA upoważnieni do wydawania kluczy zobowiązani są do odnotowania pobrania i zdania kluczy w ewidencji pobrań.

4. Wydawanie i zdawanie kluczy w trybie nadzwyczajnym:
   a. wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą bezpośredniego przełożonego lub Kierownika działu DA, PA, ZA.
   b. klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu za poświadczeniem zwrotu w Ewidencji pobrania/zdawania kluczy.
5. Bieżące postępowanie w trakcie dnia pracy:
   a. w godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie,
   b. zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu,
   c. po zakończeniu pracy, klucze służące do zabezpieczenia szaf muszą być przechowywane w zamkniętym biurku. Klucz od biurka znajduje się w miejscu znanym tylko pracownikowi.
   d. po zakończeniu pracy, pracownicy są zobowiązani do:
      - wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych,
      - wyłączenia oświetlenia,
      - zabezpieczenia i zamknięcia okien i drzwi ewentualnie aktywacji alarmu,
   e. za przestrzeganie ww. zasad odpowiada kierownik podległej jednostki.
6. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie następujących konsekwencji:
   a. poniesienie odpowiedzialności wynikających z Kodeksu pracy,
   b. poniesienie odpowiedzialności wynikających z Kodeksu cywilnego.

Załącznik nr 4 do Zarządzenia nr 5/2018
Dyrektora KPODR w Minikowie
z dnia 25.05.2018 r.

REGULAMIN UŻYTKOWANIA KOMPUTERÓW PRZENOŚNYCH

1. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Pracodawcy, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
2. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę Pracodawcy.
3. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym Inspektora Ochrony Danych zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
4. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
   a) zaleca się przenoszenie go w specjalnym futerale,
   b) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru,
   c) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy.
5. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.
6. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
7. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze plików (dyski NAS) lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.
8. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.