Uchwała nr 20/2021

Zarządu Krajowej Rady Spółdzielczej

z dnia ..14. maja .....**2021 r.**

w sprawie przyjęcia zmian w treści Polityki Bezpieczeństwa w Krajowej Radzie Spółdzielczej

---

Zarząd Krajowej Rady Spółdzielczej, na podstawie § 9 ust. 1 Statutu Krajowej Rady Spółdzielczej *(Monitor Polski z 1996 r. nr 7, poz. 86)* oraz § I Regulaminu Zarządu Krajowej Rady Spółdzielczej,

postanawia, że

1. Wprowadza Politykę Bezpieczeństwa danych osobowych w Krajowej Radzie Spółdzielczej z dnia 14 maja 2021 r. (Załącznik nr 1 do uchwały)
2. Jednocześnie uchyla się Politykę bezpieczeństwa w Krajowej Radzie Spółdzielczej, przyjętą Uchwałą Zarządu Krajowej Rady Spółdzielczej nr 16/2019 z dnia 23 kwietnia 2019 r., przy czym pozostają w mocy wydane zgodnie z dotychczasową Polityką bezpieczeństwa w Krajowej Radzie Spółdzielczej upoważnienia do przetwarzania danych osobowych
3. Wprowadza Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Krajowej Radzie Spółdzielczej z dnia 14. maja. 2021 r. (Załącznik nr 2 do uchwały)
4. Jednocześnie uchyla się Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Krajowej Radzie Spółdzielczej nr 20/2017 z dnia 16 maja 2017 r.,
5. Z treścią Polityki bezpieczeństwa danych osobowych oraz Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych zobowiązani są zapoznać wszyscy pracownicy Biura Krajowej Rady Spółdzielczej przetwarzający dane osobowe.
6. uchwała wchodzi w życie w terminie 14 dni od podjęcia.

RADCA PRAWNY
Dominik Niszczak

Sekretarz Prezesa Krajowej Rady Spółdzielczej
Ryszard Jaśkowski

PREZES ZARZĄDU
Krajowej Rady Spółdzielczej
dr inż. Mieczysław Grobski

Załącznik nr 1 do uchwały nr 20/2021 Zarządu Krajowej Rady Spółdzielczej z dnia 14 maja 2021 r

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH W KRAJOWEJ RADZIE SPÓŁDZIELCZEJ

Wstęp

W celu zapewnienia w Krajowej Radzie Spółdzielczej zgodności procesu przetwarzania danych osobowych z obowiązującymi przepisami prawa, w szczególności z:

1) Rozporządzeniem 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), dalej: RODO.
2) Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000).

wdraża się do stosowania niniejszą Politykę Bezpieczeństwa Danych Osobowych, zwaną dalej Polityką bezpieczeństwa lub Polityką.

§ 1.

Postanowienia ogólne

1. Celem Polityki bezpieczeństwa danych osobowych w Krajowej Radzie Spółdzielczej jest wskazanie podstaw dla właściwego wykonania obowiązków Administratora danych osobowych w zakresie bezpieczeństwa i prawidłowej ochrony przetwarzanych danych osobowych.
2. Politykę stosuje się do danych osobowych:

1) przetwarzanych w systemach informatycznych,
2) przetwarzanych na nośnikach elektronicznych,
3) przetwarzanych w sposób tradycyjny.

3. Niniejsza Polityka oraz wszystkie dokumenty z nią powiązane są aktualizowane wraz ze zmianami w przepisach prawa dotyczącymi ochrony danych osobowych oraz zmianami wynikającymi z organizacji i funkcjonowania Biura Krajowej Rady Spółdzielczej.

§ 2.

Definicje

1. Określenia użyte w Polityce oznaczają:

1) Administrator danych osobowych (ADO) – Krajowa Rada Spółdzielcza, będącą naczelnym organem samorządu spółdzielczego, działająca na podstawie ustawy z dnia 16 września 1982 r. - Prawo spółdzielcze (Dz. U. Nr 80, poz. 210, z późniejszymi zmianami) oraz Statutu Krajowej Rady Spółdzielczej (uchwała I Kongresu Spółdzielczego z dnia 30

maja 1995 roku), która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

2) Pełnomocnik ds. Ochrony Danych Osobowych (PODO)- osoba wspierająca ADO w realizacji obowiązków dotyczących ochrony danych osobowych,

3) Administrator Systemu Informatycznego (ASI)- osoba upoważniona przez ADO do zarządzania systemem informatycznym, posiadająca odpowiednią wiedzę z zakresu informatyki;

4) Pracownicy - osoby zatrudnione w Biurze Krajowej Rady Spółdzielczej na podstawie stosunku pracy, umów cywilnoprawnych, przedsiębiorcy wykonujący osobiście i jednoosobowo działalność, osoby odbywające staże, praktyki, które na podstawie upoważnienia wykonują prace związane z przetwarzaniem danych osobowych,

5) Użytkownicy- Pracownicy przetwarzający dane w systemie informatycznym,

6) Instrukcja zarządzania systemem informatycznym- instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, która została przyjęta i wdrożona w Biurze Krajowej Rady Spółdzielczej, stanowiąca obok Polityki, podstawowy dokument z zakresu ochrony danych osobowych;

7) Dane osobowe –informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

8) Przetwarzanie danych –operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

9) System– zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

10) Usuwanie danych –zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą;

11) Zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, wyrażone poprzez oświadczenie bądź wyraźne działanie potwierdzające, którym osoba fizyczna, której dane dotyczą, przyzwala na przetwarzanie dotyczących jej danych osobowych.

12) Odbiorca danych –osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

13) Incydent bezpieczeństwa - każde wykryte naruszenie (albo wykryta próba) naruszenia bezpieczeństwa informacji, będące naruszeniem obowiązujących przepisów wewnętrznych lub przepisów prawa, źródłem incydentu bezpieczeństwa może być zarówno przypadkowe, jak i celowe działanie albo zaniechanie;

14) Naruszeniu ochrony danych osobowych – oznacza to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia,

zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

§3.

Podstawy przetwarzania danych osobowych

1. Dane osobowe w Krajowej Radzie Spółdzielczej są:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty;
   2) zbierane w celach konkretnych, wyraźnie określonych i prawnie uzasadnionych i nie mogą być przetwarzane w sposób niezgodny z tymi celami;
   3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
   4) prawidłowe, uaktualniane w razie potrzeby, a także usuwane lub prostowane w razie ustalenia, że są nieprawidłowe w świetle celu ich przetwarzania;
   5) przechowywane w formie ułatwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy niż jest to niezbędne dla celów, w jakich następuje ich przetwarzanie, z zastrzeżeniem wyjątków przewidzianych w RODO;
   6) przetwarzane w sposób zapewniający ich integralność i poufność, a także rozliczalność.
2. Przetwarzanie danych osobowych jest zgodne z prawem, jeśli:
   1) osoba, której dane dotyczą wyraziła na to zgodę;
   2) przetwarzanie jest niezbędne do wykonania umowy łączącej Krajową Radę Spółdzielczą z osobą, której dane dotyczą, w szczególności do wykonania umów z usługodawcami, członkami personelu lub innymi osobami związanymi z Krajową Radą Spółdzielczą stosunkiem prawnym;
   3) przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą;
   4) przetwarzanie jest niezbędne do wypełnienia ciążącego na Krajowej Radzie Spółdzielczej obowiązku prawnego;
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym;
   6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Krajową Radę Spółdzielczą lub przez osobę trzecią, z wyłączeniem sytuacji określonych w RODO;
   7) przetwarzanie jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej.
3. Przesłanki, legalizujące przetwarzanie danych osobowych mogą wystąpić samodzielnie i niezależnie od siebie, albo jednocześnie i łącznie.
4. Krajowa Rada Spółdzielcza informuje osobę, której dane dotyczą o podstawie przetwarzania jej danych osobowych, a w przypadkach określonych w ust. 2 pkt 7 również o podstawie przetwarzania danych osobowych innej osoby fizycznej. Realizacja obowiązku informacyjnego może polegać na umieszczeniu informacji w miejscu ogólnie dostępnym, w siedzibie Krajowej Rady Spółdzielczej albo na jego stronie internetowej lub w stopce wiadomości e-mail.

§4.

Obowiązki Administratora Danych Osobowych (ADO)

1. Administrator Danych Osobowych zobowiązany jest do podjęcia wszelkich działań, których celem jest zapewnienie prawidłowej ochrony danych osobowych przetwarzanych w Krajowej Radzie Spółdzielczej.
2. Do kompetencji Administratora Danych Osobowych należy:
   1) określenie celów oraz strategii działań w zakresie ochrony danych osobowych,
   2) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.
3. Do obowiązków Administratora Danych Osobowych należy:
   1) zapewnienie szkoleń dla pracowników w zakresie ochrony danych osobowych;
   2) opracowanie i wdrożenie dokumentacji dotyczącej ochrony danych osobowych;
   3) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych;
   4) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
   5) zapewnienie ochrony fizycznej pomieszczeń, w których są przetwarzane dane osobowe,
   6) zapewnienie ochrony danych osobowych przetwarzanych w systemach informatycznych oraz nieinformatycznych,
   7) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych;
   8) nadzór nad bezpieczeństwem danych osobowych,
   9) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
   10) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.
   11) przeprowadzenie, jeśli jest wymagana, oceny skutków planowanej operacji przetwarzania dla ochrony danych osobowych – w przypadku, gdy wprowadza się nowy rodzaj przetwarzania danych osobowych;
   12) prowadzenie i aktualizacja rejestru czynności przetwarzania.
4. W Krajowej Radzie Spółdzielczej stosuje się zabezpieczenia, których celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia lub też minimalizację strat związanych ze zrealizowanym zagrożeniem: program antywirusowy, anonimizacja, pseudonominizacja, procedury bezpieczeństwa. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:
   1) poufność danych – rozumianą jako zapewnienie, że dane nie są udostępniane nieupoważnionym osobom;
   2) integralność danych – rozumianą jako zapewnienie, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
   3) rozliczalność danych – rozumianą jako zapewnienie, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
   4) dostępność informacji – rozumianą jako zapewnienie, że osoby upoważnione mają

zapewniony dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne.

§5.

Obowiązki Pracowników

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest szczególne zaangażowanie ze strony Pracowników .
2. Każdy Pracownik zobowiązany jest do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach bezpośrednio do ADO.
3. Pracownicy są zobowiązani do:
   1) postępowania zgodnie z Polityką bezpieczeństwa, Instrukcją zarządzania systemem informatycznym oraz innymi wewnętrznymi regulacjami z zakresu ochrony danych osobowych;
   2) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
   3) ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.
4. Pracownicy zobowiązani są do wykonywania niezbędnych działań w procesie przetwarzania danych celem zapewnienia właściwej ich ochrony, w tym:
   1) przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych;
   2) udzielać informacji zawierających dane osobowe tylko osobom lub podmiotom uprawnionym;
   3) prowadzić rozmowy telefoniczne oraz korespondencję mailową w sposób bezpieczny, tak aby osoba nieuprawniona nie pozyskiwała informacji, jeżeli nie jest ona dla niej przeznaczona;
   4) przechowywać wszystkie dokumenty zawierające dane osobowe w zamkniętych szafach, zawsze wtedy, gdy pracownik opuszcza swoje stanowisko pracy (polityka czystego biurka);
   5) właściwie zabezpieczać wydruki elektroniczne, a także inne, które mogą być tworzone w trakcie kopiowania, skanowania;
   6) w razie wprowadzenia gości na teren Biura, użytkownicy są zobowiązani im towarzyszyć przez cały czas ich pobytu w Biurze i ponoszą za nich pełną odpowiedzialność;
   7) informować ADO o podejrzanych osobach poruszających się w obszarze przetwarzania danych osobowych;
   8) przedkładać ADO projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu bezpieczeństwa ochrony danych osobowych.
5. Przesyłanie danych osobowych drogą elektroniczną w inny sposób niż za pomocą wewnętrznej poczty jest niedozwolone.
6. Wobec Pracownika Biura Krajowej Rady Spółdzielczej, który narusza regulacje z zakresu

ochrony danych osobowych obowiązujące w Krajowej Radzie Spółdzielczej, w tym niniejszą Politykę bezpieczeństwa można wszcząć postępowanie dyscyplinarne.

7. Kara dyscyplinarna orzeczona wobec pracownika winnego naruszeniu regulacji z zakresu ochrony danych osobowych obowiązujące w Krajowej Radzie Spółdzielczej, w tym niniejszej Polityki bezpieczeństwa nie wyklucza odpowiedzialności karnej tej osoby, zgodnie z ustawą oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego o zrekompensowanie poniesionych strat.

§ 6.

Pełnomocnik ds. Ochrony Danych Osobowych (PODO)

1. Administrator danych w celu realizacji zdań wynikających z obowiązków w zakresie stosowania przepisów RODO oraz innych regulacji prawnych ochrony danych osobowych, powołał Pełnomocnika ds. Ochrony Danych Osobowych, do którego zadań należy:
   1) aktualizowanie dokumentów związanych z ochroną danych osobowych;
   2) inicjowanie i wdrażanie usprawnień w zakresie bezpieczeństwa danych osobowych;
   3) bieżące wsparcie, doradztwo i pomoc dla Pracowników w zakresie przetwarzania danych osobowych;
   4) prowadzenie szkoleń w zakresie przetwarzania danych osobowych.;
   5) monitorowanie funkcjonowania zabezpieczeń ochrony danych osobowych;
   6) prowadzenie ewidencji naruszeń ochrony danych osobowych;
   7) przeprowadzanie doraźnych audytów wewnętrznych z zakresu przestrzegania ochrony danych osobowych;
   8) podejmowanie działań zapobiegających przypadkom naruszenia ochrony danych osobowych, usuwających ich skutki lub związane ze skargami dotyczącymi naruszenia ochrony danych osobowych.

§ 7.

Administrator Systemu Informatycznego (ASI)

1. Administrator danych w celu realizacji zdań wynikających z obowiązków w zakresie stosowania przepisów RODO oraz innych regulacji prawnych ochrony danych osobowych, powołał Administratora Systemu Informatycznego (ASI), do którego zadań należy:
   1) bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych,
   2) optymalizacja wydajności systemu informatycznego, instalacje i konfiguracje sprzętu sieciowego i serwerowego, instalacja i konfiguracje oprogramowania systemowego, sieciowego,
   3) nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych,
   4) zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie,
   5) przeciwdziałanie próbom naruszenia bezpieczeństwa informacji,

6) przyznawanie na wniosek ADO prawa dostępu do informacji w systemie informatycznym,
7) wnioskowanie do Administratora lub PODO w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń,
8) zarządzanie licencjami i procedurami ich dotyczącymi,
9) prowadzenie profilaktyki antywirusowej.

§ 8.

Przetwarzanie danych w sposób zautomatyzowany

1. Pracownik przed przystąpieniem do pracy w systemie informatycznym zobowiązany jest sprawdzić czy nie zaszły okoliczności wskazujące na naruszenie danych osobowych. W przypadku podejrzenia zaistnienia takich okoliczności zobowiązany jest poinformować niezwłocznie ADO.
2. Pracownik w celu rozpoczęcia pracy w systemie loguje się wprowadzając swój identyfikator i hasło w sposób uniemożliwiający ich ujawnienie innym osobom. Hasło uprawniające do korzystania z systemu wpisuje osobiście. Użytkownik nie może udostępniać swojego identyfikatora i hasło osobom trzecim.
3. W przypadku awarii, zagubienia hasła lub innych nieprzewidzianych sytuacji zagrażających bezpieczeństwu danych osobowych, każdy pracownik jest zobowiązany do niezwłocznego powiadomienia ADO
4. Pracownicy używający systemu informatycznego są zobowiązani do:
   1) nie przenoszenia danych do/z systemu informatycznego KRS na nośnikach, które nie zostały sprawdzone pod kątem obecności wirusów i innego zagrożenia,
   2) nie korzystania ze stron internetowych nie zapewniających bezpieczeństwa informatycznego
   3) nie otwierania poczty przychodzącej niewiadomego pochodzenia
5. W chwili utraty przez użytkownika praw do korzystania z systemu, Administrator Systemu Informatycznego (ASI) wyrejestrowuje użytkownika z systemu i usuwa jego konto dostępowe.
6. Identyfikator użytkownika, który został wyrejestrowany z systemu nie może zostać przydzielony żadnemu innemu użytkownikowi.
7. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system autoryzacji użytkownika. W celu ochrony przed dostępem do danych komputera z sieci publicznej wykorzystuje się programową zaporę ogniową zarówno w przypadku stacji roboczych jak i serwerów.
8. Każde stanowisko komputerowe posiada funkcję automatycznego włączania wygaszacza ekranu, która zostaje uruchomiona wraz z upływem 5 minut od dokonania ostatniej czynności na urządzeniu komputerowym.
9. Raz na 30 dni Administrator Systemu Informatycznego (ASI) zobowiązany jest zweryfikować listę użytkowników systemu i upewnić się, że wszyscy zarejestrowani użytkownicy mają prawo do korzystania z systemu. W przypadku istnienia w systemie użytkowników, którzy utracili prawo do korzystania z systemu, Administrator Systemu

Informatycznego (ASI) niezwłocznie wyrejestrowuje ich z systemu

§ 9.

Pomieszczenia przeznaczone do przetwarzania danych osobowych, zasady pobierania kluczy

1. Dane osobowe można przetwarzać wyłącznie w miejscach bezpiecznych i będących pod właściwym nadzorem osoby, która przetwarza i nadzoruje przetwarzanie danych osobowych.
2. Pomieszczenia bezpieczne to takie, które nie są pozostawione bez nadzoru odpowiedzialnego Pracownika.
3. Pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz podczas nieobecności upoważnionego Pracownika.
4. Uprawnienia do pobierania kluczy mają wyłącznie osoby upoważnione przez ADO. Klucze do pomieszczeń są wydawane i zdawane za pobraniem z odnotowaniem w ewidencji pobrań.
5. Wydawanie kluczy zapasowych upoważnionym Pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą osób uprawnionych. Klucze zapasowe po ich wykorzystaniu zwracane są niezwłocznie do depozytu.
6. Klucze służące do zabezpieczania biurek i szaf muszą być wyraźnie opisane. Po zakończeniu pracy, klucze służące do zabezpieczania biurek i szaf są przechowywane w zabezpieczonym miejscu.
7. W godzinach pracy klucze pozostają pod nadzorem Pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
8. Obiekt w którym znajduje się Biuro, jak i inne pomieszczenia, są zabezpieczone fizycznie zgodnie z obowiązującymi procedurami i potrzebami, zapewniona jest całodobowa ochrona przez pracowników wyspecjalizowanej zewnętrznej firmy ochroniarskiej, z zastosowaniem w wybranych punktach monitoringu TVCC.
9. W przypadku wykonywania prac naprawczych, remontowych, montażowych przez firmy zewnętrzne, pomieszczenie jest pod stałym nadzorem osoby upoważnionej.
10. Każdy Pracownik w przypadku zauważenia uchybień w zabezpieczeniu pomieszczenia zobowiązany jest niezwłocznie poinformować o tym fakcie ADO.

§ 10.

Procedura postępowania w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

1. Pracownicy są zobowiązani do szczególnej staranności przy przetwarzaniu danych osobowych.
2. Pracownicy każdorazowo przed przystąpieniem do pracy zobowiązani są do dokonania oceny i oględzin miejsca pracy pod kątem, czy nie dokonano jakichkolwiek nieuprawnionych działań związanych z ochroną danych osobowych przez osoby nieuprawnione.
3. Pracownik razie zauważenia naruszenia bezpieczeństwa danych, bądź powzięcia

informacji mogącej mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązany ten fakt niezwłocznie zgłosić Administratorowi Danych Osobowych.

4. Sytuacje, na które Pracownicy powinni zwrócić szczególną uwagę to:
   1) naruszenie lub próba naruszenia integralności, poufności lub rozliczalności danych i systemu,
   2) próba nieuprawnionego dostępu do pomieszczenia lub dostępu do danych osobowych, w tym próba nieuprawnionego logowania lub inny sygnał wskazujący na próbę nielegalnego dostępu do systemu,
   3) niezamierzona zmiana lub utrata danych zapisanych na nośnikach,
   4) losowe zdarzenia, takie jak brak zasilania, pożar itp.,
   5) stwierdzenie braku sprzętu informatycznego, jego części lub nośników zewnętrznych zawierających dane osobowe (wydruki, pamięć zewnętrzna, płyty CD, dysk twardy, itp.).
5. W przypadku uzasadnionego podejrzenia naruszenia ochrony danych osobowych, Administrator przy pomocy PODO przeprowadza wstępne dochodzenie, po czym niezwłocznie, nie później jednak niż w terminie 72 godzin od stwierdzenia naruszenia, przygotowuje zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego w rozumieniu art. 4 pkt 21 RODO oraz ew. zawiadamia osobę, której dane dotyczą o naruszeniu ochrony danych osobowych.
6. Zawiadomienia osoby, której ochrona danych osobowych uległa naruszeniu dokonuje się jedynie w przypadku, gdy naruszenie to może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.
7. Każdy przypadek naruszenia ochrony danych osobowych dokumentuje się w prowadzonej przez PODO ewidencji naruszeń ochrony danych osobowych.
8. Jeśli naruszenie ochrony danych osobowych ma charakter przestępstwa, sprawa kierowana jest do organów ścigania.

§ 11.

Procedura realizacji praw osób

1. Każdy przypadek zgłoszenia przez osobę, której dane dotyczą, woli skorzystania z praw przewidzianych w RODO, jest rozpatrywany indywidualnie.
2. ADO na wniosek osoby, której dane dotyczą umożliwia jej dostęp do danych oraz udziela informacji w zakresie określonym przepisami prawa.
3. ADO na żądanie osoby, której dane dotyczą dokonuje sprostowania danych osobowych lub ich uzupełnienia. Osoba jest zobowiązana do złożenia żądania w formie pisemnej. ADO po złożeniu wniosku przez osobę , której dane dotyczą ma obowiązek usunięcia jej danych osobowych w przypadku gdy:
   1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   2) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
   3) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania;

4) dane osobowe były przetwarzane niezgodnie z prawem;

5) dane osobowe muszą zostać usunięte w celu wywiązania się Administratora danych osobowych z obowiązku prawnego.

4. ADO realizuje żądania osób, których dane osobowe dotyczą w zakresie ograniczenia przetwarzania, w przypadkach wynikających z art. 18 RODO. W przypadkach ograniczenia przetwarzania ADO przechowuje dane osobowe, nie przetwarzając ich, chyba że przetwarzanie danych osobowych następuje w celu ustalenia, dochodzenia lub odmowy roszczeń lub w celu ochrony praw innej osoby fizycznej lub prawnej z uwagi na ważne względu interesu publicznego Unii Europejskiej lub państwa członkowskiego.

§ 12.

Procedura współpracy z podmiotami zewnętrznymi

1. ADO korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają gwarancję wdrożenia odpowiednich środków technicznych i organizacyjnych by przetwarzanie spełniało wymagania RODO oraz chroniło prawa osób, których dane dotyczą
2. Każdorazowe skorzystanie z usług podmiotu przetwarzającego jest poprzedzone zawarciem umowy powierzenia przetwarzania danych osobowych zgodnego ze wzorem umowy zawartym w załączniku nr 5 do niniejszej Polityki bezpieczeństwa.
3. Nie wymaga się zawarcia umowy powierzenia danych, osobowych w przypadku gdy w ramach współpracy przekazywane są dane między podmiotami, co do których pewne jest, że na podstawie zasobów własnych mają już prawo do przetwarzania tych dokładnie danych osobowych
4. Przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić wyłącznie na podstawie przepisów RODO

§ 13.

Upoważnienie do przetwarzania danych osobowych, Ewidencja osób upoważnionych oraz Rejestr czynności przetwarzania

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez Pracownika upoważnienia do przetwarzania danych osobowych podpisanego przez ADO. Upoważnienie nadaje się na okres zatrudnienia na danym stanowisku i wygasa z chwilą ustania zatrudnienia. Wzór upoważnienia stanowi załącznik nr 2 do Polityki.
2. ADO prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, która stanowi załącznik nr 1do Polityki.
3. ADO prowadzi rejestr czynności przetwarzana danych osobowych, zgodnie z art. 30 RODO. Wzór rejestru czynności przetwarzania stanowi załącznik nr 6 do Polityki.
4. Dostęp do rejestru czynności przetwarzania zabezpieczony jest indywidualnym hasłem przyporządkowanym do poszczególnych osób przetwarzających dane osobowe w KRS
5. Osoby uprawnione posiadają dostęp do wszystkich danych zamieszczonych w rejestrze czynności przetwarzania. Wykaz osób uprawnionych zatwierdza ADO.

§14.

Zagadnienia organizacyjne i postanowienia końcowe

1. Wszelkie zasady opisane w niniejszej Polityce bezpieczeństwa są przestrzegane przez osoby upoważnione do przetwarzania danych osobowych ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą. Fakt zapoznania się z Polityką potwierdza się własnoręcznym podpisem na stosownym wykazie.
2. Osoby upoważnione do przetwarzania danych osobowych są szkolone z ochrony danych osobowych. Szkolenie prowadzi Pełnomocnik ds. Ochrony Danych Osobowych bądź inna wyznaczano przez Administratora danych osoba.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz Polityką bezpieczeństwa i innymi związanymi z nią dokumentami obowiązującymi u administratora danych osobowych,
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych. Dokument ten jest przechowywany w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im upoważnień do przetwarzania danych osobowych.
5. Pracownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce bezpieczeństwa i innych związanych z nią dokumentach.
6. Pracownicy za niestosowanie się do zapisów postanowień Polityki, podlegają odpowiedzialności karnej, cywilnoprawnej i administracyjnej wynikającej z aktów prawnych wskazanych we wstępie, a także odpowiedzialności wynikającej z ustawy z dnia 26 czerwca 1974 Kodeks Pracy (Dz.U.2020.1320 t.j. z dnia 2020.07.30 z późn. zm.)
7. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy RODO i ustawy.

Załączniki:

1.1. Ewidencja osób upoważnionych do przetwarzania danych osobowych;
1.2. Wzór upoważnienia do przetwarzania danych osobowych;
1.3. Wzór odwołania upoważnienia;
1.4. Wzór umowy powierzenia przetwarzania danych osobowych;
1.5. Wzór zgody na przetwarzanie danych osobowych;
1.6. Wzór Rejestru przetwarzania danych osobowych;
1.7. Wykaz osób, które zapoznały się z Polityką bezpieczeństwa danych osobowych.

RADCA PRAWNY
Dominik Niszczak

Załącznik nr 1.1

Ewidencja osób upoważnionych do przetwarzania danych osobowych w KRS

Lp.	Imię i Nazwisko	Data upoważnienia	Data zmiany upoważnienia	Data cofnięcia	Uwagi
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					
21.					
22.					
23.					
24.					
25.					
26.					
27.					
28.					
29.					

RADCA PRAWNY
Dominik Niszczak

Załącznik nr 1.2

UPOWAŻNIENIE

do przetwarzania danych osobowych
w Krajowej Radzie Spółdzielczej

Na podstawie: art. 29 i art. 32 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) z 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).

Upoważniam

Panią/Pana .....

do przetwarzania danych osobowych w zbiorach danych osobowych przetwarzanych w **Krajowej Radzie Spółdzielczej,** w zakresie obowiązków wykonywanych na zajmowanym stanowisku pracy. Upoważnienie wygasa wraz z ustaniem stosunku pracy.

.....
pieczęć i podpis działającego w imieniu
Administratora Danych Osobowych

Warszawa, ...
data upoważnienia

RADCA PRAWNY
Dominik Niszczak

OŚWIADCZENIE

oświadczam , że zostałam (em) zapoznana (y) z przepisami:

- 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; RODO; Dziennik Urzędowy Unii Europejskiej L z 2016 r. nr 119, str. 1);
- ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).
- w tym w szczególności:

  - Art. 29 i 32 ust. 4 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 119/1 z 4.5.2016 r.);

Artykuł 29 **Przetwarzanie z upoważnienia administratora lub podmiotu przetwarzającego**

Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Artykuł 32 **Bezpieczeństwo przetwarzania**

4.Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

- Art. 107 i 108 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).

Art. 107. 1. Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.
2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech.
Art. 108. Kto udaremnia lub utrudnia kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Zobowiązuję się do zachowania tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczania, także po zakończeniu pracy w KRS.

Data i podpis osoby upoważnianej: .....

...CA PRAWNY
...minik Niszczak

Załącznik nr 1.3

ODWOŁANIE UPOWAŻNIENIA

do przetwarzania danych osobowych
w Krajowej Radzie Spółdzielczej

Z dniem ..... r., na podstawie art. 29 w związku z art. 28 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 119 z 04.05.2016, str. 1), odwołuję upoważnienie Pana/Pani* ..... do przetwarzania danych osobowych wydane w dniu .....

.....

Czytelny podpis osoby, upoważnionej do wydawania i odwoływania upoważnień

.....

(miejscowość, data)

*niepotrzebne skreślić

RADCA PRAWNY
Dominik Niszczak

Załącznik nr 1.4

Załącznik do Umowy o ..... zawartej w ..... r.

UMOWA POWIERZENIA

PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta dnia____ w_____ pomiędzy:

Krajową Radą Spółdzielczą, powołaną i działającą na podstawie ustawy Prawo Spółdzielcze *(Dz.U.2021.648 t.j. z dnia 2021.04.08)* z siedzibą w Warszawie, ul. Jasna 1 NIP: 526-025-04-98; REGON: 000511344, reprezentowaną przez:

1. ..... - Prezesa Zarządu Krajowej Rady Spółdzielczej
2. ..... – Zastępca Prezesa Zarządu Krajowej Rady Spółdzielczej

zwaną dalej „Administratorem"

a

zwaną dalej „Przetwarzającym"

1. DEFINICJE

Dla potrzeb niniejszej urnowy, Administrator *i* Przetwarzający ustalają następujące znaczenie niżej wymienionych pojęć:

1) **Umowa Powierzenia** - niniejsza umowa;

2) **Umowa Główna** – „.....r.

3) **RODO** - rozporządzenie Parlamentu Europejskiego ı 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. U. UE. L. z 2016 r. Nr i19, str.1).

4) **uodo** – „Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z

RADCA PRAWNY
Dominik Niszczak

2018 r. . poz. 1000)

2. OŚWIADCZENIA STRON

Strony oświadczają, że niniejsza Umowa Powierzenia została zawarta w celu - wykonania obowiązków, o których mowa w art. 28 RODO w związku z zawarciem Umowy Głównej.

3. PRZEDMIOT UMOWY

3.1. W trybie art. 28 ust. 3 RODO, Administrator powierza Przetwarzającemu do przetwarzania dane osobowe, które są niezbędne do realizacji zadań w zakresie obsługi prawnej, stanowiących przedmiot Umowy Głównej. Przetwarzający zobowiązuje się do ich przetwarzania zgodnego z prawem Umową Główną i niniejszą Umową Po wierzenia.

3.2. Przetwarzający może przetwarzać dane osobowe wyłącznie w zakresie, celu oraz na zasadach przewidzianych w Umowie Głównej oraz zgodnie z innymi udokumentowanymi poleceniami Administratora, przy czym za takie udokumentowane polecenia uważa się polecenia przekazywane przez Administratora drogą elektroniczną lub na piśmie.

4. ZASADY POWIERZENIA PRZETWARZANIA

4.1. Przed rozpoczęciem przetwarzania danych osobowych Przetwarzający musi podjąć środki zabezpieczające dane osobowe, o których mowa w art. 32 RODO, a ·w szczególności:

a) uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter zakres, kontekst *i* cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia,

b) obowiązany jest zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku. Przetwarzający powinien odpowiednio udokumentować zastosowanie tych środków, a także uaktualniać te środki w porozumieniu z administratorem,

c) zapewnić, by każda osoba fizyczna działająca z upoważnienia Przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora w celach i zakresie przewidzianym w Umowie Powierzenia,

d) prowadzić w wymaganym zakresie rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Administratora, o którym mowa w art. 30 ust. 2 RODO i udostępniać go Administratorowi na jego żądanie, chyba że Przetwarzający jest zwolniony z tego obowiązku na podstawie art. 30 ust. 5 RODO.

RADCA PRAWNY
Dominik Niszczak

4.2. Przetwarzający zapewnia, aby osoby mające dostęp do przetwarzanych danych osobowych zachowały je oraz sposoby zabezpieczeń w tajemnicy, przy czym obowiązek zachowania tajemnicy istnieje również po realizacji Umowy Powierzenia oraz ustaniu zatrudnienia u Przetwarzającego.

4.3. Przetwarzający zobowiązuje się pomagać Administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO.

4.4. W sytuacji podejrzenia naruszenia ochrony danych osobowych Przetwarzający zobowiązuje się do:

a) przekazania Administratorowi informacji dotyczących naruszenia ochrony danych osobowych w ciągu 24 godzin od jego wykrycia, w tym informacji, o których mowa .w art. 33 ust. 3 RODO,

b) przeprowadzenia wstępnej analizy ryzyka naruszenia praw i wolności osób, których dane dotyczą, i przekazania wyników tej analizy do Administratora w ciągu 36 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych,

c) przekazania Administratorowi - na jego żądanie - wszystkich informacji niezbędnych do zawiadomienia osoby, której dane dotyczą, zgodnie z art. 34 ust. 3 RODO. w ciągu 48 godzin od wykrycia zdarzenia stanowiącego naruszenie ochrony danych osobowych.

4.5. Przetwarzający zobowiązuje się pomagać Administratorowi poprzez odpowiednie środki techniczne i organizacyjne, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w art. 15-22 RODO. W szczególności Przetwarzający zobowiązuje się - na żądanie Administratora - do przygotowania i przekazania Administratorowi informacji potrzebnych do spełnienia żądania osoby, której dane dotyczą, w ciągu 7 dni od dnia otrzymania żądania Administratora.

4.6. Przetwarzający zobowiązuje *się* stosować się do ewentualnych wskazówek lub zaleceń, wydanych przez organ nadzoru lub unijny organ doradczy zajmujący się ochroną danych osobowych, dotyczących przetwarzania danych osobowych, w szczególności w zakresie stosowania RODO.

5. PODPOWIERZENIE PRZETWARZANIA

5.1. Administrator dopuszcza możliwość podpowierzenia przetwarzania powierzonych danych osobowych podwykonawcom Przetwarzającego *(tzw. subprocesorom).* Jeżeli

Przetwarzający zamierza podpowierzyć przetwarzanie danych osobowych swoim podwykonawcom, musi uprzednio poinformować Administratora o zamiarze podpowierzenia oraz o tożsamości (nazwie) podmiotu, któremu ma zamiar podpowierzyć przetwarzanie danych, a także o charakterze podpowierzenia, zakresie danych, celu i czasie trwania podpowierzenia. O ile Administrator nie wyrazi sprzeciwu wobec podpowierzenia w terminie 3 dni od daty zawiadomienia, Przetwarzający uprawniony będzie do dokonania podpowierzenia.

5.2. W przypadku podpowierzenia przetwarzania danych osobowych, podpowierzenie przetwarzania będzie mieć za podstawę umowę, na podstawie której podwykonawca *(subprocesor)* zobowiąże *się* do wykonywania tych samych obowiązków, które na mocy niniejszej Umowy Powierzenia nałożone są na Przetwarzające go. Umowa będzie zawarta w tej same formie co niniejsza Umowa Powierzenia.

5.3. Administratorowi będą przysługiwały uprawnienia wynikające z umowy podpowierzenia bezpośrednio wobec podwykonawcy *(subprocesora).* W przypadku wypowiedzenia lub rozwiązania umowy podpowierzenia, Przetwarzający poinformuje o tym fakcie Administratora w terminie 7 dni od wypowiedzenia lub rozwiązania umowy ·.

5.4. Przetwarzający nie może przekazywać powierzonych mu do przetwarzania danych osobowych do podmiotów znajdujących się w państwach spoza Europejskiego Obszaru. Gospodarczego.

6. AUDYT PRZETWARZAJĄCEGO

6.1. Administrator jest uprawniony do weryfikacji przestrzegania zasad przetwarzania danych osobowych wynikających RODO oraz niniejszej Umowy Powierzenia przez Przetwarzającego, poprzez prawo żądania udzielenia wszelkich informacji dotyczących powierzonych danych osobowych.

6.2. Administrator ma także prawo przeprowadzania audytów lub inspekcji Przetwarzającego w zakresie zgodności operacji przetwarzania z prawem i z Umową Powierzenia. Audyty lub inspekcje, o których mowa w zdaniu poprzedzającym, mogą być przeprowadzane przez podmioty trzecie upoważnione przez Administratora.

6.3. Przetwarzający zobowiązuje się niezwłocznie informować Administratura, jeżeli zdaniem Przetwarzającego wydane mu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych.

7. ZAKOŃCZENIE POWIERZENIA PRZETWARZANIA

7.1. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych osobowych Przetwarzający zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie.

8. POSTANOWIENIA KOŃCOWE

8.1. Wszelkie zmiany i poprawki do niniejszej umowy Strony są zobowiązane dokonywać, pod rygorem nieważności, w formie pisemnych aneksów. Umowa nie zawiera poprawek ręcznych.

8.2. Niniejsza umowa zostaje sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Załącznik nr 1.5

.....

data i miejscowość

Zgoda na przetwarzanie danych osobowych

Ja, niżej podpisana/ny wyrażam zgodę na przetwarzanie moich danych osobowych w zakresie.....

przez Krajową Radę Spółdzielczą z siedzibą w Warszawie, przy ul. Jasnej 1 w celu..... .

Jednocześnie oświadczam, że podane przeze mnie dane osobowe zostały przekazane w sposób dobrowolny i są zgodne z prawdą.

Wdniu została mi przekazana do wiadomości klauzula informacyjną, z której treścią się zapoznałem(-am), mając na uwadze w szczególności informację o celu przetwarzania danych osobowych i prawie dostępu do treści swoich danych, prawie ich poprawiania, wycofania zgody na przetwarzanie danych osobowych oraz prawie wniesienia skargi do organu nadzorczego.

podpis osoby wyrażającej zgodę

RADCA PRAWNY
Dominik Niszczak

Załącznik nr 1.6

LP.	Cel przetwarzania	Kategorie osób	Kategorie danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa podmiotu przetwarzajacego i dane kontakowe *(jeśli dotyczy)*	Kategorie odbiorców *(innych niż podmiot przetwarzajacy)*	Ogólny opis technicznych i organizacyjnych srodków bezpieczeństwa zgodnie z art. 32 ust. 1 ***(jeżeli jest to możliwe)***
	Art.. 30 ust. 1 pkt b	**Art.. 30 ust. 1 pkt c**	**Art.. 30 ust. 1 pkt c**	**Art.. 30 ust. 1 pkt f**	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt d**	**Art.. 30 ust. 1 pkt g**
1.	Rekrutacja pracowników	Kandydaci do pracy	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych, informacja z Krajowego Rejestru Karnego w przypadku nauczycieli	Po zakończeniu procesu rekrutacyjnego	Nie dotyczy	Dane nie są przekazywane innym podmiotom	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla osób upoważnionych.

RADCA PRAWNY
Dominik Niszczak

2.	Prowadzenie ewidencji pracowników zgodnie z Kodeksem Pracy	Pracownicy pomocniczy (recepcjonisci, sprzątaczki, pracownicy gospodarczy), administracyjni oraz nauczyciele	Dane identyfikacyjne, dane adresowe, dane o wykształceniu, przebiegu pracy, absencji (urlopy, zwolnienia lekarskie, rehabilitacyjne,szkoleniowe i inne), dane o zakresie obowiązków, stawce wynagrodzenia, karach i nagrodach oraz inne dane wymagane zgodnie z Kodeksem Pracy	50 lat [art. 51u ust 1 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 t.j.)]	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań.
3.	Zgłoszenia pracownika i członków jego rodziny do ZUS, ich aktualizacja oraz przekazywanie informacji o zwolnieniach.	Pracownicy pomocniczy (recepcjonisci, sprzątaczki, pracownicy gospodarczy), administracyjni oraz nauczyciele	Dane identyfikacyjne, dane adresowe, dane o Odziale NFZ oraz inne dane wymagane w formularzu zgłoszenia ZUS ZUA - zgłoszenie, ZUS IUA - zmiana danych, ZUS ZWUA - wyrejestrowanie, ZUS ZCNA -zgłoszenie członka rodziny, ZAS - wniosek o ustalenie okresu zasiłkowego, OL-2 - wniosek o kontrolę zaśw. lekarskiego, Z15a - zgłoszenie opieki nad dzieckiem, Z15B - zgłoszenie opieki nad innym członkiem rodziny	50 lat [art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]	Nie dotyczy	ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.

4.	Prowadzenie rozliczeń z pracownikami, naliczanie potrąceń, obliczanie składek ZUS	Pracownicy pomocniczy (recepcjonisci, sprzątaczki, pracownicy gospodarczy), administracyjni oraz nauczyciele	Dane identyfikacyjne, dane adresowe, dane kadrowe (wysługa lat pracy, stawka wynagrodzeń), dane o czasie pracy, przyznanych nagrodach, potrąceniach (składki związkowe, zajęcia komornicze itp.) numery kont dla przelewów bankowych pracownika	50 lat [art. 125a ust 4 ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz.U.z 2017 r., poz.1383)]	Nie dotyczy	Banki, urzędy skarbowe, ZUS, inne firmy ubezpieczeniowe - dotyczy tylko osób posiadających polisy ubezpieczeniowe,	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy, system wykrywania włamań. Szyfrowana transmisja podczas przekazywania danych.

5	Prowadzenie księgi uczestników szkoleń	Uczestnicy szkoleń	Dane identyfikacyjne ucznia (imię, nazwiskodatav i miejsce urodzenia, numer PESEL), Adres zamieszkania ucznia, Dane o rodzicach (imię, nazwisko adres zamieszkania - jeżeli są rózne od adresu zamieszkania ucznia, Datę rozpoczęcia nauki, oddział do którego przyjęto oraz datę ukończenia szkoły albo datęi przyczyne jej opuszczenia.	10 lat	Firma XYZ z siedzibą we Wrocławiu przy ul. Xyz 15. Zakres powierzenia obejmuje udostępnieni e poprzez sieć internet Systemu Szkła Net - moduł Sekretariat wraz z usługą zapewnienia ciagłości działania, konfigurachją zabezpieczeń oraz zapewnienie m kobpp bezpieczeńst wa	Dane są przekazywane do Systemu Informacji Oświarowej na podstawie art. 14 Ustawy z dnia 15 kwietnia 2011 r. o Systemie Informacji Oświatowej Dz. U. 2017, poz. 2159)	Ścisle kontrolowany dostęp do danych - dostęp tylko dla uprawnionych, zarejestrowanych uzytkowników. Komputery używane do dostępu do danych zabezpieczono przed atakami z sieci zewnętrznej systemem antywirusowym. Transmisja danych do oraz z serwera bazy danych systemu zabezpieczona jest kryptograficznie. Serwer i dostęp do baz danych zabezpieczony jest przez dostawce usługi wdrożeniem środków ochrony fizycznej i logicznej poprzez zastosowanie firewalli i innych narzędzi zabezpieczajacych.

6	Rejestracja tematyów zajęć i wyników nauczania	Uczestnicy szkoleń, wykładowcy	Dane identyfikacyjne ucznia (nazwisko, imiona, data i mieksce urodzenia) Adres zamieszkania, Dane o rodzicach (imię, nazwisko adres zamieszkania, adresy poczty elektronicznej, numery telefonów). Imiona i nazwiska nauczycieli prowadzących zajęcia, tygodniowy plan zajęć) Tematy zajeć i obecnosci, nieobecności (usprawiedliwione i nieusprawiedliw). Oceny (bieżące, śródroczne, roczne (semestralne) Śródroczne i roczne oceny klasyfikacyjne z zachowania, Świadectwa, Arkusze ocen, Wyniki egzaminów.	10 lat	Firma XYZ z siedzibą we Wrocławiu przy ul. Xyz 15. Zakres powierzenia obejmuje udostępnieni e poprzez sieć internet Systemu Szkła Net - moduł Sekretariat wraz z usługą zapewnienia ciagłości działania, konfigurachją zabezpieczeń oraz zapewnienie kopii bezpieczeństwa	Dane są przekazywane wyłącznie uprawnionym rodzicom.	Ścisle kontrolowany dostęp do danych - dostęp tylko dla uprawnionych, zarejestrowanych uzytkowników. Transmisja danych do oraz z serwera bazy danych systemu zabezpieczona jest kryptograficznie. Serwer i dostęp do baz danych zabezpieczony jest przez dostawce usługi wdrożeniem środków ochrony fizycznej i logicznej poprzez zastosowanie firewalli i innych narzędzi zabezpieczajacych.

Załącznik nr 1.7

Wykaz osób, które zapoznały się z Polityką Bezpieczeństwa Danych Osobowych w Krajowej Radzie Spółdzielczej

Lp.	Imię i Nazwisko	Data zapoznania się z Polityką Bezpieczeństwa Danych Osobowych KRS	Podpis
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			

RADCA PRAWNY
Dominik Niszczak

13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			
21.			
22.			
23.			

Załącznik nr 2 do uchwały nr 20/2021.. Zarządu Krajowej Rady Spółdzielczej z dnia 14 maja 2021 r

Instrukcja zarządzania systemem informatycznym służącym do przetwarzana danych osobowych w Krajowej Radzie Spółdzielczej

§1

Podstawa prawna

Niniejszy dokument zgodny jest z następującymi aktami prawnymi:

1. Rozporządzeniem 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; RODO; Dziennik Urzędowy Unii Europejskiej L z 2016 r. nr 119, str. 1);

2. Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000).

§2

Postanowienia ogólne

1. Ilekroć mowa w niniejszym dokumencie o Instrukcji, należy przez to rozumieć „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Krajowej Radzie Spółdzielczej".

2. Ilekroć mowa w niniejszym dokumencie o KRS należy przez to rozumieć Krajową Radę Spółdzielczą.

§ 3

Zagadnienia organizacyjne

1. Pracownicy upoważnieni do przetwarzania danych osobowych w systemie informatycznym i ręcznym, zobowiązani są do zapoznania się z treścią Instrukcji i jej przestrzegania

2. Fakt zapoznania się z Instrukcją pracownik potwierdza własnoręcznym podpisem na stosownym wykazie, którego wzór stanowi Załącznik nr 2 do Polityki Bezpieczeństwa KRS

§4

Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie

1. Przed rozpoczęciem pracy z systemem informatycznym oraz w trakcie pracy każdy pracownik zobowiązany jest do sprawdzenia, czy nie wystąpiły symptomy mogące świadczyć o naruszeniu ochrony danych osobowych. W przypadku ich wykrycia

RADCA PRAWNY
Dominik Niszczak

należy niezwłocznie powiadomić o tym fakcie Administratora Danych Osobowych lub Administratora Systemu Informatycznego.

2. W celu rozpoczęcia pracy użytkownik wykonuje logowanie do systemu używając nadanego loginu i hasła.

3. Podczas nieobecności przy stanowisku komputerowym należy wylogować się z systemu lub uruchomić wygaszacz ekranu chroniony hasłem.

4. Po zakończeniu pracy w systemie należy wylogować się z systemu i wyłączyć stację roboczą.

5. Zawieszenie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone informacją dla pracowników KRS przekazaną w imieniu ADO przez Pełnomocnika lub ASI (w formie wiadomości e-mail lub osobiście), na co najmniej 30 minut przed planowanym zawieszeniem.

§5

Nadawanie uprawnień

I. Przetwarzać dane osobowe w systemach może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych, którego wzór stanowi Załącznik nr 2 do Polityki Bezpieczeństwa.

2. Uprawnienia do przetwarzania danych osobowych w systemie informatycznym KRS nadaje Administrator Danych Osobowych.

3. Za rejestrowanie uprawnień do przetwarzania danych osobowych w systemie informatycznym odpowiada Administrator Danych Osobowych i Administrator Systemów Informatycznych.

§6

Zabezpieczenia

I. Oprogramowanie wykorzystywane do przetwarzania danych osobowych posiada własny system kont (zabezpieczonych hasłem) i uprawnień. Za okresową (przynajmniej raz na 3 miesiące) zmianę haseł odpowiada użytkownik oprogramowania.

2. Stosuje się aktywną ochronę antywirusową przy pomocy specjalistycznego oprogramowania. Poza tym stosuje się przynajmniej raz w miesiącu skanowanie całego systemu (w poszukiwaniu „złośliwego oprogramowania") na każdym komputerze, na którym przetwarzane są dane osobowe. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania i aktualizację bazy wirusów odpowiada użytkownik komputera.

3. Administrator Systemu Informatycznego raz na kwartał dokonuje przeglądu systemu informatycznego oraz zainstalowanego oprogramowania na każdym stanowisku komputerowym pod kątem aktualności i ważności licencji na ich użytkowanie.

4. Wykaz systemów informatycznych oraz zainstalowanego oprogramowania na każdym stanowisku komputerowym stanowi załącznik nr 1 do Instrukcji.

5. Wykaz kluczy licencyjnych i haseł do zainstalowanego na każdym stanowisku komputerowym oprogramowania stanowi poufny załącznik nr 2 do Instrukcji. Dostęp do w/w załącznika ma Pracodawca i Administrator Systemu Informatycznego

§7

Procedury tworzenia kopii zapasowych

I. Dane systemów kopiowane są w trybie miesięcznym. Odpowiedzialnym za wykonywanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane.

2. Kopie zbiorów umieszczonych na serwerze wykonywane są automatycznie dedykowanym oprogramowaniem wytworzonym we własnym zakresie .

3. Dodatkowe kopie wynikające z np. zmiany platformy sprzętowej przechowywane są w raz z poniższymi.

4. Kopie awaryjne są przechowywane w szafie metalowej lub w zabezpieczonych zamkami regałach w siedzibie KRS.

§8

Odnotowywanie udostępnienia danych

System informatyczny przetwarzający dane osobowe musi posiadać mechanizmy pozwalające na odnotowanie faktu wykonywania operacji na danych. W szczególności zapis ten powinien obejmować:

a) rozpoczęcie i zakończenie pracy przez użytkownika systemu,

b) operacje wykonywane na przetwarzanych danych,

c) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,

d) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonywania operacji na danych osobowych,

e) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.

§9

Procedury wykonywania przeglądów i konserwacji systemów

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników KRS lub przez upoważnionych przedstawicieli wykonawców.

2. Prace wymienione w ust. 1 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

3. Przed rozpoczęciem prac wymienionych w ust. 1 przez osoby niebędące pracownikami KRS należy dokonać potwierdzenia tożsamości tych osób.

§10

Niszczenie wydruków i nośników danych

1. Usuwanie zapisów powinno odbywać się poprzez wymazywanie informacji oraz formatowanie nośnika. Poprawność przygotowania nośnika powinna być sprawdzona przez Administratora Systemu Informatycznego.

2. Uszkodzone nośniki magnetyczne przed ich wyrzuceniem należy fizycznie zniszczyć (przeciąć, przełamać, itp.).

3. Po wykorzystaniu wydruki zawierające dane osobowe powinny być niszczone w niszczarce.

Załączniki:

2.1. Wykaz systemów informatycznych oraz zainstalowanego oprogramowania na każdym stanowisku komputerowym
2.2. Wykaz kluczy licencyjnych i haseł do oprogramowania zainstalowanego na każdym stanowisku komputerowym

Załącznik nr 2.1

Wykaz systemów informatycznych oraz zainstalowanego oprogramowania

Lp.	nr pokoju	nr stanowiska	Nazwa oprogramowania	Data wygaśnięcia licencji	Uwagi
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					
21.					
22.					
23.					
24.					
25.					
26.					
27.					
28.					
29.					

RADCA PRAWNY
Dominik Niszczak

Załącznik nr 2.2

Wykaz kluczy licencyjnych i haseł do oprogramowania zainstalowanego na każdym stanowisku komputerowym

Lp.	nr pokoju	nr stanowiska	Nazwa oprogramowania	Klucz licencyjny/hasło	Uwagi
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					
15.					
16.					
17.					
18.					
19.					
20.					
21.					
22.					
23.					
24.					
25.					
26.					
27.					
28.					
29.					

RADCA PRAWNY
Dominik Niszczak