ZARZĄDZENIE NR GKG.GPK.0200.104.2023

DYREKTORA POWIATOWEGO OŚRODKA DOKUMENTACJI

GEODEZYJNEJ I KARTOGRAFICZNEJ

z dnia 2 sierpnia 2023r.

w sprawie: wprowadzenia Procedury zarządzania uprawnieniami w Powiatowym Ośrodku Dokumentacji Geodezyjnej i Kartograficznej

Na podstawie §10 ust. 1 pkt 3 Uchwały nr 3606/2022 Zarządu Powiatu w Poznaniu z 23 listopada 2022 roku w sprawie uchwalenia Regulaminu Organizacyjnego Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej, zarządzam co następuje:

§1. Wprowadza się Procedurę zarządzania uprawnieniami w Powiatowym Ośrodku Dokumentacji Geodezyjnej i Kartograficznej, stanowiącą załącznik do niniejszego Zarządzenia.

§2. Nadzór nad niniejszym Zarządzeniem powierza się Inspektorowi Ochrony Danych.

§3. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
GEODETA POWIATOWY
Tomasz Powroźnik

RADCA PRAWNY
Ewa Woroniecka-Andrzejczak

Inspektor Ochrony Danych
Martyna Frąckowiak

Załącznik do Zarządzenia nr GKG.GPK.0200.104.2023
Dyrektora Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej z dnia 2 sierpnia 2023 roku

Procedura zarządzania uprawnieniami
w Powiatowym Ośrodku Dokumentacji Geodezyjnej i Kartograficznej

§ 1
Słownik

1. **PODGiK** – Powiatowy Ośrodek Dokumentacji Geodezyjnej i Kartograficznej.
2. **Dyrektor PODGiK** – Dyrektor Powiatowego Ośrodka Dokumentacji Geodezyjnej i Kartograficznej.
3. **EZD (Elektroniczne Zarządzanie Dokumentacją)** – system wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania spraw, gromadzenia i tworzenia dokumentacji w postaci elektronicznej, realizowany w ramach systemu teleinformatycznego, o którym mowa w przepisach wydanych na podstawie art. 5 ust. 2b ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach. W PODGiK jest to FINN 8 SQL;
4. **SZUiU –** moduł w FINN 8 SQL o nazwie System zarządzania uprawnieniami i upoważnieniami;
5. **Pracownicy –** na potrzeby niniejszej Procedury, w celu uproszczenia terminologii są to:
   a) osoby zatrudnione na podstawie umowy o pracę w PODGiK;
   b) osoby zatrudnione na podstawie umowy zlecenie w PODGiK;
   c) osoby odbywające praktyki w PODGIK w oparciu o umowę o praktyki zawartą pomiędzy uczelnią/szkołą a PODGiK;
   d) osoby odbywające staż w PODGiK o oparciu o umowę zawartą pomiędzy Urzędem Pracy/uczelnią a PODGiK.
6. **Dysponent zasobu** – osoba, która akceptuje wnioski o uprawnienia do zasobu, którego dysponentem jest jego komórka organizacyjna;
7. **OP - Operator (informatyk)** – osoba, która realizuje wnioski będące w jego kompetencji;
8. **AS - Administrator systemu** – osoba, która realizuje wnioski o nadanie uprawnień do systemów, programów lub aplikacji będących pod pieczą komórki organizacyjnej, w której pełni funkcję administratora systemu.

§2
Postanowienia ogólne

1. Procedura została opracowana zgodnie z wymogami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób

fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO).

2. Celem niniejszej procedury jest określenie czynności procesu zarządzania uprawnieniami w PODGiK, który obejmuje nadawanie, zmianę oraz odbieranie uprawnień pracownikom PODGiK z wykorzystaniem SZUiU.
3. Procedura ma na celu zapewnienie posiadania przez pracowników odpowiednich uprawnień umożliwiających wykonywanie czynności służbowych zgodnie z powierzonym zakresem obowiązków pracownika.
4. Proces zarządzania uprawnieniami odbywa się wyłacznie w formie elektronicznej za pomocą elektronicznego wniosku generowanego w SZUiU.
5. Wniosek dotyczący uprawnień pracownika w zależności od rodzaju zmian kadrowych może dotyczyć:
    a) nadania uprawnień – występuje w przypadku potrzeby przydzielenia nowych uprawnień, których do tej pory pracownik nie posiadał lub rozszerzenia przydzielonych uprawnień;
    b) odebrania uprawnień - występuje w przypadku potrzeby odebrania uprawnień, które do tej pory pracownik posiadał lub zmniejszenia przydzielonych uprawnień;
    c) przedłużenia umowy (przedłużenie uprawnień) – występuje w przypadku przedłużenia stosunku pracy, umowy zlecenia, praktyki i stażu;
    d) zmiany stanowiska;
    e) zmiany formy zatrudnienia;
    f) zmiany nazwiska;
    g) zmiany komórki organizacyjnej;
    h) rozwiązania umowy.
6. W przypadku zmiany stanowiska lub zakresu obowiązków, jeśli jest to wymagane w celu umożliwienia prawidłowej realizacji zadań, powinna nastąpić modyfikacja uprawnień nadanych pracownikowi.
7. Zmiana komórki organizacyjnej przez pracownika generuje dwa wnioski:
    a) Wniosek o odebranie aktualnych uprawnień;
    b) Wniosek o nadanie nowych uprawnień.
8. Proces nadawania uprawnień nowemu pracownikowi rozpoczyna Wydział Organizacyjny i Kadr, który rejestruje użytkownika w EZD, a następnie w SZUiU, najpóźniej w pierwszym dniu rozpoczęcia umowy o pracę, umowy zlecenia, stażu lub praktyki.
9. Dostęp do systemów informatycznych służących do przetwarzania danych osobowych może uzyskać wyłącznie osoba uprawniona, która posiada imienne upoważnienie do przetwarzania

danych osobowych wydane przez Dyrektora PODGiK lub w szczególnych przypadkach przez Starostę Poznańskiego.

10. Zakres nadanych uprawnień musi być zgodny z powierzonym zakresem obowiązków pracownika. Zakres czynności realizowanych przez pracownika określa poziom dostępu do danych osobowych, odpowiedzialności za ich ochronę przed niepowołanym dostępem, nieuzasadnioną modyfikacją, zniszczeniem oraz ich nielegalnym ujawnieniem i pozyskaniem.
11. We wniosku o nadanie uprawnień należy określić, do których zasobów i aplikacji Pracownik ma posiadać uprawnienia i w jakim zakresie.
12. Wniosek o nadanie uprawnień sporządza bezpośredni przełożony (lub osoba przez niego upoważniona) w SZUiU:
    a) najpóźniej w pierwszym dniu rozpoczęcia umowy o pracy, umowy zlecenia, stażu lub praktyki;
    b) najpóźniej w pierwszym dniu roboczym następującym po zaistnieniu zdarzenia, o którym mowa w ust. 5 lit. c, d, e, f i g.
13. Do nadania wybranych uprawnień potrzebna jest zgoda *Dysponenta zasobu, Administratora systemu* lub realizacja przez *Operatora(Informatyka),* w zależności od ustawień podczas konfigurowania i definiowania uprawnienia.
14. Każdorazowo informacja o nadawanych uprawnieniach przekazywana jest do Inspektora Ochrony Danych, a w razie nieobecności do jego Zastępcy.
15. *Dysponent zasobu* jest zobowiązany wyrazić zgodę na nadanie uprawnień. W przypadku odmowy nadania uprawnień, w uwagach uzasadnia swoją odmowę.
16. *Operator(informatyk)* lub *Administrator systemu* nadaje uprawnienia zgodnie z wnioskiem.
17. Odebranie uprawnień w przypadku zakończenia umowy o pracę, zlecenia, praktyki lub stażu następuje najpóźniej z końcem ostatniego dnia umowy o pracę, zlecenia, praktyki lub stażu.
18. Odebranie uprawnień użytkownika jest realizowane w zakresie wszystkich systemów, programów i aplikacji PODGiK oraz podmiotów zewnętrznych po zarejestrowaniu przez pracownika Wydziału Organizacyjnego i Kadr w SZUiU rozwiązania umowy.
19. W uzasadnionych przypadkach, na polecenie Dyrektora PODGiK lub osoby przez niego upoważnionej istnieje możliwość natychmiastowego odebrania uprawnień.
20. Szczegółowe aspekty techniczne nadawania uprawnień w SZUiU reguluje wewnętrzna Instrukcja.
21. Wykaz aplikacji, programów i systemów teleinformatycznych znajduje się w SZUiU. Katalog powyższych zasobów jest katalogiem otwartym.
22. W przypadku nadawania dostępów do systemów zewnętrznych stosuje się procedurę uproszczoną. W powyższym przypadku, SZUiU stanowi wyłącznie rejestr uprawnień posiadanych przez użytkownika.

§ 3

Obowiązki pracownika

1. Każdy pracownik odpowiada za wszelkie czynności dokonywane przez niego w systemach, programach i aplikacjach, do których nadano mu uprawnienia.
2. Każdy pracownik zobowiązany jest do zachowania w tajemnicy haseł do systemów, programów i aplikacji, do których nadano mu uprawnienia.
3. Hasła nie mogą być zapisywane w miejscu dostępnym dla osób nieuprawnionych.
4. Hasła, w stosunku, do których zaistniało podejrzenie o ich ujawnieniu, podlegają bezzwłocznej zmianie. Sytuację taką należy zgłosić do *Administratora systemu lub Dysponenta zasobu.*
5. Hasła dostępu powinny składać się z unikatowego zestawu co najmniej ośmiu znaków, zawierać małe i wielkie litery oraz cyfry i znaki specjalne.
6. Hasła nie mogą być: identyczne z identyfikatorem pracownika ani z jego imieniem i nazwiskiem, numerem telefonu, numerem rejestracyjnym samochodu, jego marką, numerem dowodu osobistego, nazwą ulicy oraz składać się z przewidywalnych sekwencji znaków z klawiatury np.: „QWERTY", „12345678",
7. W sytuacji udostępnienia hasła innej osobie, pracownik ponosi odpowiedzialność za skutki i następstwa wynikłe z faktu wykorzystania tego hasła przez osoby trzecie.
8. Pracownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje:
    a) okresowo, zgodnie z wymaganiami dla danego systemu informatycznego;
    b) w przypadku ujawnienia lub podejrzenia ujawnienia hasła.
9. Do obowiązków Pracowników zaangażowanych w przetwarzanie danych osobowych w systemach informatycznych należy podejmowanie współpracy przy ustaleniu przyczyn naruszenia ochrony danych osobowych oraz usuwania skutków tych naruszeń, w tym zapobieganie ich ewentualnemu ponownemu wystąpieniu.
10. Pracownicy przed przystąpieniem do przetwarzania danych osobowych w tym systemie informatycznym, zobowiązani są zapoznać się z wewnętrznymi regulacjami w PODGiK dotyczącymi bezpieczeństwa przetwarzania danych osobowych.
11. Pracownicy przed dopuszczeniem do obsługi systemu informatycznego, w którym przetwarzane są dane osobowe powinni podlegać przeszkoleniu w zakresie obsługi sprzętu informatycznego, oprogramowania systemowego oraz oprogramowania do obsługi aplikacji, którą będą wykorzystywali.
12. Powyższym obowiązkom podlegają również zleceniobiorcy, stażyści i praktykanci przetwarzający dane osobowe w systemach informatycznych.