Centrum Usług Wspólnych
ul. 1 Maja 18, 78-200 Białogard
NIP 672-20-97-265 REGON 387416976
tel. (94) 3579 350
e-mail:cuw@bialogard.info

Centrum Usług Wspólnych

Zarządzenie nr 48/IV/2026

Dyrektora Centrum Usług Wspólnych w Białogardzie

z dnia 20 kwietnia 2026 r.

w sprawie wprowadzenia zmiany do Regulaminu pracy Centrum Usług Wspólnych w Białogardzie

Na podstawie art. 22^3 § 1–4 w zw. z art. 22^2 § 6–10, art. 104^2 § 1–2 oraz art. 104^3 § 1 ustawy z dnia 26 czerwca 1974 r. – Kodeks pracy zarządza się, co następuje:

§ 1. W Regulaminie pracy Centrum Usług Wspólnych w Białogardzie, stanowiącym załącznik do Zarządzenia nr 31/V/2023 Dyrektora Centrum Usług Wspólnych w Białogardzie z dnia 18 maja 2023 r., wprowadza się zmianę określoną w załączniku do niniejszego zarządzenia.

§ 2. Wykonanie zarządzenia powierza się Starszemu specjaliście ds. kadr Centrum Usług Wspólnych w Białogardzie.

§ 3. Zarządzenie wchodzi w życie po upływie 2 tygodni od dnia podania go do wiadomości pracowników.

Załącznik
do Zarządzenia nr 48/IV/2026
Dyrektora CUW w Białogardzie
z dnia 20 kwietnia 2026 r.

Zmiana Regulaminu pracy Centrum Usług Wspólnych w Białogardzie

W Regulaminie pracy Centrum Usług Wspólnych w Białogardzie, stanowiącym załącznik do Zarządzenia nr 31/V/2023 Dyrektora Centrum Usług Wspólnych w Białogardzie z dnia 18 maja 2023 r., w Rozdziale IV „Organizacja pracy", po § 8 dodaje się § 8a w następującym brzmieniu:

§ 8a

Monitorowanie służbowego sprzętu komputerowego, systemów informatycznych i sieci teleinformatycznej

1. Pracodawca stosuje monitorowanie służbowego sprzętu komputerowego, systemów informatycznych, służbowych kont użytkowników oraz sieci teleinformatycznej wykorzystywanych przez pracowników przy wykonywaniu obowiązków służbowych.
2. Monitorowanie, o którym mowa w ust. 1, stosuje się wyłącznie w zakresie niezbędnym do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikom narzędzi pracy, w tym służbowego sprzętu komputerowego, systemów informatycznych, służbowych kont użytkowników oraz sieci teleinformatycznej. W ramach powyższych celów monitorowanie może służyć w szczególności weryfikacji prawidłowego i bezpiecznego korzystania z narzędzi pracy, ochronie integralności i dostępności systemów informatycznych, ochronie danych przetwarzanych w tych systemach oraz wyjaśnianiu zdarzeń mogących świadczyć o nieprawidłowym użyciu narzędzi pracy lub naruszeniu bezpieczeństwa informacji.
3. Monitorowanie obejmuje następujące kategorie danych technicznych i eksploatacyjnych:
    1. identyfikację komputera, użytkownika oraz służbowego konta użytkownika;
    2. datę i godzinę logowania oraz wylogowania użytkownika;
    3. informacje o aktywności służbowego komputera;
    4. informacje o zainstalowanym i uruchamianym oprogramowaniu;

5. informacje o wykorzystaniu aplikacji, zasobów systemowych i zasobów sieciowych;
6. informacje o korzystaniu ze służbowej sieci teleinformatycznej, w tym adresy odwiedzanych stron internetowych, z zastrzeżeniem ust. 6;
7. informacje o podłączanych urządzeniach zewnętrznych;
8. informacje o zdarzeniach mogących mieć znaczenie dla bezpieczeństwa systemów informatycznych, danych osobowych, informacji lub mienia pracodawcy;
9. oraz inne techniczne dane eksploatacyjne o podobnym charakterze, jeżeli ich przetwarzanie jest niezbędne do realizacji celów określonych w ust. 2 i mieści się w sposobie monitorowania określonym w niniejszym paragrafie.

4. Monitorowanie jest prowadzone przy użyciu narzędzi informatycznych służących do zarządzania infrastrukturą informatyczną, w szczególności systemu Axence nVision lub innego równoważnego systemu stosowanego przez pracodawcę.
5. Monitorowanie prowadzone jest w sposób proporcjonalny do celów, dla których zostało wprowadzone, z poszanowaniem godności, prywatności, tajemnicy korespondencji oraz innych dóbr osobistych pracownika.
6. Monitorowanie nie obejmuje treści prywatnej korespondencji pracownika ani treści prywatnych plików. Pracodawca nie prowadzi monitorowania w sposób wykraczający poza cele określone w ust. 2.
7. Dane pozyskane w wyniku monitorowania mogą być wykorzystywane wyłącznie do celów określonych w ust. 2, w szczególności do wyjaśniania incydentów bezpieczeństwa, kontroli prawidłowego użytkowania sprzętu służbowego, ochrony danych osobowych, ochrony informacji, ochrony mienia pracodawcy oraz zapewnienia prawidłowej organizacji pracy.
8. Dostęp do danych pozyskanych w wyniku monitorowania mają wyłącznie osoby imiennie upoważnione przez pracodawcę, w zakresie niezbędnym do realizacji powierzonych im zadań. Inspektor Ochrony Danych może uzyskiwać dostęp do informacji niezbędnych do wykonywania zadań określonych w przepisach o ochronie danych osobowych, w szczególności w zakresie opiniowania, monitorowania zgodności i wyjaśniania incydentów.

9. Dane pozyskane w wyniku monitorowania przechowywane są przez okres niezbędny do realizacji celów, dla których zostały zebrane, nie dłużej jednak niż przez 3 miesiące od dnia ich zarejestrowania, chyba że dane te stanowią dowód w postępowaniu prowadzonym na podstawie prawa albo pracodawca powziął wiadomość, że mogą one stanowić dowód w takim postępowaniu. W takim przypadku okres ich przechowywania ulega przedłużeniu do czasu prawomocnego zakończenia postępowania. Po upływie okresów, o których mowa w niniejszym ustępie, dane pozyskane w wyniku monitorowania podlegają usunięciu albo trwałej anonimizacji, chyba że odrębne przepisy prawa wymagają ich dalszego przechowywania.
10. W razie ujawnienia danych mogących wskazywać na prywatny charakter korespondencji lub plików, pracodawca odstępuje od zapoznawania się z ich treścią, chyba że jest to niezbędne do ochrony ważnego interesu pracodawcy lub wykonania obowiązku wynikającego z przepisów prawa. W takim przypadku czynność powinna być ograniczona do niezbędnego zakresu i udokumentowana.
11. Pracodawca informuje pracowników o wprowadzeniu monitorowania w sposób przyjęty u pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem.
12. Przed dopuszczeniem pracownika do pracy pracodawca przekazuje mu, w postaci papierowej lub elektronicznej, informację o celu, zakresie oraz sposobie stosowania monitorowania.

Załącznik nr 1

…….
imię i nazwisko pracownika

…….
stanowisko

Białogard, dnia …… r.

Wzór oświadczenia pracownika

Ja, niżej podpisana/podpisany

……, oświadczam, że zapoznałam/zapoznałem się z:

1. Zarządzeniem nr 48/IV/2026 Dyrektora Centrum Usług Wspólnych w Białogardzie z dnia 20 kwietnia 2026 r. w sprawie wprowadzenia zmiany do Regulaminu pracy Centrum Usług Wspólnych w Białogardzie;
2. treścią § 8a Regulaminu pracy Centrum Usług Wspólnych w Białogardzie dotyczącą monitorowania służbowego sprzętu komputerowego, systemów informatycznych i sieci teleinformatycznej;
3. informacją o celu, zakresie oraz sposobie stosowania monitorowania służbowego sprzętu komputerowego, systemów informatycznych i sieci teleinformatycznej.

Przyjmuję do wiadomości, że monitorowanie służbowego sprzętu komputerowego, systemów informatycznych i sieci teleinformatycznej będzie prowadzone na zasadach określonych w Regulaminie pracy Centrum Usług Wspólnych w Białogardzie.

……
czytelny podpis pracownika

Załącznik nr 2

KLAUZULA INFORMACYJNA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH W ZWIĄZKU Z MONITOROWANIEM SŁUŻBOWEGO SPRZĘTU KOMPUTEROWEGO, SYSTEMÓW INFORMATYCZNYCH I SIECI TELEINFORMATYCZNEJ

Na podstawie art. 13 ust. 1 i ust. 2 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 oraz swobodnego przepływu tych danych (RODO), informuję, że:

1. Tożsamość Administratora
Administratorem Pani / Pana*) danych osobowych jest CUW Usług Wspólnych, z siedzibą przy ul. 1 Maja 18, 78- 200 Białogard, e-mail: cuw@bialogard.info, tel. 94 35 79 351, reprezentowane przez Dyrektora.

2. Inspektor Ochrony Danych
Z Inspektorem Ochrony Danych można skontaktować się pod adresem e-mail: cuw.iod@bialogard.info lub telefonicznie: 94 35 79 350.

3. Cele i podstawa prawna przetwarzania danych
Pani/Pana*) dane osobowe są przetwarzane w związku ze stosowaniem przez pracodawcę monitorowania służbowego sprzętu komputerowego, systemów informatycznych, służbowych kont użytkowników oraz sieci teleinformatycznej wykorzystywanych przy wykonywaniu obowiązków służbowych.
Dane osobowe są przetwarzane w celu:
1. zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy,
2. zapewnienia prawidłowego i bezpiecznego korzystania z narzędzi pracy, w tym służbowego sprzętu komputerowego, systemów informatycznych, służbowych kont użytkowników oraz sieci teleinformatycznej
3. zapewnienia bezpieczeństwa systemów informatycznych, w tym ich integralności i dostępności,
4. ochrony danych osobowych oraz innych informacji przetwarzanych w tych systemach informatycznych,
5. wyjaśniania zdarzeń mogących świadczyć o nieprawidłowym użyciu narzędzi pracy lub naruszeniu bezpieczeństwa informacji,
6. ochrony mienia pracodawcy,
7. ustalenia, dochodzenia lub obrony roszczeń.

Podstawą prawną przetwarzania danych osobowych jest:
1. art. 6 ust. 1 lit. c RODO — wypełnienie obowiązku prawnego ciążącego na Administratorze, wynikającego z przepisów prawa pracy, w szczególności art. 22^3 § 1–4 w związku z art. 22^2 § 6–10 Kodeksu pracy,
2. art. 6 ust. 1 lit. e RODO — wykonywanie zadania realizowanego w interesie publicznym, w zakresie, w jakim Administrator realizuje zadania publiczne,
3. art. 6 ust. 1 lit. f RODO — prawnie uzasadniony interes Administratora polegający na ochronie mienia, zapewnieniu bezpieczeństwa systemów informatycznych i informacji oraz dochodzeniu lub obronie roszczeń — w zakresie, w jakim przetwarzanie nie jest realizowane w ramach wykonywania zadań publicznych ani nie znajduje oparcia w podstawach wskazanych w pkt 1–2.

4. Odbiorcy danych
Pani/Pana*) dane osobowe mogą zostać przekazywane:
1. podmiotom uprawnionym do ich otrzymania na podstawie przepisów prawa, w szczególności sądom, prokuraturze, Policji lub innym uprawnionym organom,
2. podmiotom świadczącym na rzecz Administratora usługi informatyczne, serwisowe, techniczne, prawne lub doradcze — wyłącznie w zakresie niezbędnym do realizacji tych usług i na podstawie stosownych umów,

5. Okres przechowywania danych
Dane pozyskane w wyniku monitorowania są przechowywane przez okres niezbędny do realizacji celów, dla których zostały zebrane, nie dłużej jednak niż przez **3 miesiące od dnia ich pozyskania**.

Jeżeli dane stanowią dowód w postępowaniu prowadzonym na podstawie prawa albo Administrator powziął wiadomość, że mogą one stanowić dowód w takim postępowaniu, okres ich przechowywania ulega przedłużeniu do czasu prawomocnego zakończenia postępowania albo ustania potrzeby ich zabezpieczenia.
Po upływie okresów przechowywania dane podlegają usunięciu, chyba że odrębne przepisy prawa wymagają ich dalszego przechowywania.

6. Prawa osoby, której dane dotyczą
W związku z przetwarzaniem danych osobowych w celach określonych w pkt 3 przysługują Pani / Panu*) następujące prawa wynikające z RODO:
a) **prawo dostępu** do treści swoich danych osobowych (art. 15 RODO),
b) **prawo do sprostowania** danych osobowych (art. 16 RODO),
c) **prawo do usunięcia danych** (art. 17 RODO) – z wyłączeniem przypadków, gdy przetwarzanie odbywa się na podstawie obowiązujących przepisów prawa (w szczególności ustawy o Kodeks Pracy) lub jest niezbędne do:
• wywiązania się przez Administratora z obowiązku prawnego,
• celów archiwalnych realizowanych w interesie publicznym,
• ustalenia, dochodzenia lub obrony roszczeń,
d) **prawo do ograniczenia przetwarzania danych** (art. 18 RODO), w następujących przypadkach:
• osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych,
• przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
• administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
• osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania,
e) **prawo do przenoszenia danych** (art. 20 RODO), o ile przetwarzanie odbywa się na podstawie zgody lub umowy oraz w sposób zautomatyzowany – w przypadku przetwarzania danych osobowych na podstawie przepisów prawa oraz bez zastosowania zautomatyzowanego przetwarzania danych – prawo do przenoszenia danych nie ma zastosowania,

7. Prawo do wniesienia skargi do organu nadzorczego
W przypadku uznania, że przetwarzanie danych narusza przepisy RODO, przysługuje Pani / Panu*) prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

8. Informacja o charakterze obowiązku podania danych i skutkach jego niewypełnienia
Przetwarzanie danych osobowych w związku ze stosowaniem monitorowania służbowego sprzętu komputerowego, systemów informatycznych, służbowych kont użytkowników oraz sieci teleinformatycznej wynika z korzystania przez pracownika z narzędzi pracy udostępnionych przez pracodawcę.
Brak możliwości przetwarzania danych w tym zakresie może uniemożliwić prawidłowe korzystanie ze służbowego sprzętu komputerowego, systemów informatycznych, służbowych kont użytkowników lub sieci teleinformatycznej, a tym samym może utrudnić albo uniemożliwić wykonywanie obowiązków służbowych przy użyciu tych narzędzi.

9. Zautomatyzowane podejmowanie decyzji
Dane osobowe nie będą przetwarzane w sposób zautomatyzowany, w tym nie będą profilowane.

POTWIERDZENIE ZAPOZNANIA SIĘ Z KLAUZULĄ INFORMACYJNĄ

Potwierdzam, że zapoznałam/zapoznałem*) się z klauzulą informacyjną dotyczącą przetwarzania danych osobowych w związku ze stosowaniem przez Centrum Usług Wspólnych w Białogardzie monitorowania służbowego sprzętu komputerowego, systemów informatycznych, służbowych kont użytkowników oraz sieci teleinformatycznej.

.....
Data i czytelny podpis pracownika

*) niepotrzebne skreślić