Uchwała Nr 7/24

Zarządu Przedsiębiorstwa Wodociągów i Kanalizacji Sp. z o.o. w Olsztynie

z dnia 8 kwietnia 2024 r.

w sprawie wprowadzenia „Instrukcji zarządzania systemami informatycznymi oraz danymi przetwarzanymi w PWiK Sp. z o.o. Olsztyn"

Na podstawie §6 pkt 1 ust. 8 Regulaminu Zarządu Przedsiębiorstwa Wodociągów i Kanalizacji Spółka z o.o. w Olsztynie, Zarząd Spółki:

§1

Wprowadza „Instrukcję zarządzania systemami informatycznymi oraz danymi przetwarzanymi w PWIK Sp. z o.o. Olsztyn" w brzmieniu określonym w Załączniku.

§2

„Instrukcja zarządzania systemami informatycznymi oraz danymi przetwarzanymi w PWIK Sp. z o.o. Olsztyn" zamieszczona jest na serwerze Spółki w katalogu: \\file\zasob\pb w folderze „Instrukcje".

§3

Uchwała wchodzi w życie z dniem 8 kwietnia 2024 r.

Wiceprezes Zarządu

Jarosław Słoma

Prezes Zarządu

Wiesław Pancer

Instrukcja zarządzania systemami informatycznymi oraz danymi przetwarzanymi w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

	Imię i nazwisko/stanowisko	data/podpis
Opracował:	**Anita Chudzińska** *Inspektor Ochrony Danych* **Adam Szymański** *Główny Informatyk Audytor IT* **Andrzej Piotrowicz** *Kierownik Działu Informatyki*	8.04.2024 ..... 8.04.2024 A. Szymański 08.04.2024 A.P.
Zatwierdził:	**Wiesław Pancer** *Prezes Zarządu* **Jarosław Słoma** *Wiceprezes Zarządu*	....

ORYGINAŁ

Obowiązuje od dnia:
8.04.2024 r.
Wycofano dnia: *)
.....
Ver. 3.0.

Egzemplarz roboczy podlega aktualizacji

*) wypełniać wyłącznie na oryginale procedury

Spis treści

Wstęp

Niniejszy dokument jest instrukcją postępowania dla pracowników zatrudnionych w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn (PWiK) w celu realizacji polityki ochrony danych osobowych oraz ochrony informacji przetwarzanych w Spółce.

Regulacje zawarte w opracowaniu (zwanym w dalszej części „Instrukcją") mają zastosowanie do wszystkich informacji przetwarzanych w PWiK niezależnie od zastosowanych środków technicznych przetwarzania, w tym: elektronicznych oraz tradycyjnych (papierowych) ze szczególnym uwzględnieniem danych osobowych, danych prawnie chronionych oraz innych informacji stanowiących zasób przedsiębiorstwa.

Podstawę prawną opracowania Instrukcji stanowią w szczególności:

- Rozporządzenie 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) - zwane dalej RODO;
- Ustawa o ochronie danych osobowych z dnia 10.05.2018 r. - zwana dalej UODO;
- Norma PN-EN ISO/IEC 27001:2023-08 - System Zarządzania Bezpieczeństwem Informacji;
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych;
- Zatwierdzone kodeksy postępowania uwzględniające specyfikę działalności Administratora Danych - na mocy art. 40 RODO;
- Wytyczne opublikowane przez organ nadzorczy powołany w celu monitorowania stosowania Rozporządzenia - na mocy art. 51 RODO;
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Zakres rozpowszechniania dokumentu

Instrukcja jest rozpowszechniona wśród pracowników PWIK odpowiedzialnych za przetwarzanie danych oraz pracowników, którzy korzystają ze sprzętu teleinformatycznego znajdującego się w zasobach PWiK.

Do stosowania się do wytycznych zawartych w Instrukcji zobowiązani są również pracownicy podmiotów współpracujących z PWiK, bądź wykonujących zadania na rzecz PWiK, w przypadkach, kiedy posiadają dostęp do danych przetwarzanych w PWiK (ze szczególnym uwzględnieniem danych osobowych, danych prawnie chronionych oraz innych informacji stanowiących zasób przedsiębiorstwa.

Dostęp do Instrukcji dla pracowników/współpracowników PWiK jest powszechny, dokument przechowywany jest w każdej komórce organizacyjnej i udostępniany na żądanie pracownika/współpracownika. Ponadto elektroniczna wersja instrukcji jest opublikowana na serwerze \\file\zasob\instrukcje. Powielanie, dystrybuowanie, udostępnianie Instrukcji innym osobom jest zabronione.

Powołanie służb odpowiedzialnych za bezpieczeństwo danych osobowych

W celu nadzoru nad bezpieczeństwem danych osobowych, Zarząd PWiK z dniem 27.05.2019 r. powołuje Zarządzeniem Prezesa Zarządu Zespół ds. Ochrony Danych Osobowych w składzie:

- Anita Chudzińska - Inspektor Ochrony Danych;
- Adam Szymański - monitoring oraz wdrażanie metod zabezpieczeń informatycznych systemów przetwarzania danych;
- Bogusława Rurka - monitoring oraz wdrażanie metod zabezpieczeń zbiorów danych osobowych;
- Cezary Kowalewski - monitoring oraz wdrażanie metod zabezpieczeń zbiorów danych osobowych klientów zewnętrznych;
- Adam Królak - nadzór nad dokumentacją przetwarzania danych.

Zespół jest odpowiedzialny za wdrożenie wymogów określonych w RODO, UODO oraz zapewnienie ich przestrzegania na stanowiskach pracy w PWiK.

Zespół jest zobowiązany do:

- przeprowadzania audytów w zakresie sprawdzenia przestrzegania ochrony danych osobowych w PWiK (min. 1 raz w roku) oraz raportowania ich wyników do Administratora Danych;
- inicjowania oraz wdrażania środków ochrony danych osobowych wraz z dokonywaniem analizy ich adekwatności;
- prowadzenia i aktualizowania rejestru osób upoważnionych do przetwarzania danych osobowych;
- prowadzenia rejestru czynności przetwarzania danych osobowych;
- szacowania ryzyka w kontekście przetwarzanych danych osobowych;
- organizowania szkoleń pracowników z zakresu ochrony danych osobowych;
- reprezentowania Administratora Danych przed organem nadzorczym;
- rozstrzyganie spraw w kontekście obowiązków Administratora Danych wynikających z RODO/UODO;
- opiniowania spraw dotyczących ochrony danych osobowych;
- prowadzenia nadzoru nad aktualnością niniejszej Instrukcji oraz Polityki Bezpieczeństwa Informacji.

Metody realizacji zasad bezpieczeństwa przy przetwarzaniu danych osobowych oraz danych elektronicznych w PWiK

W niniejszym opracowaniu dokonano podziału środków ochrony systemów informatycznych eksploatowanych w PWiK na nw. części:

- organizacyjno-prawna;
- techniczna.

W poszczególnych grupach określono podstawowe zasady ochrony informacji, jakie należy przedsięwziąć na stanowiskach pracy PWiK podczas przetwarzania informacji.

Część organizacyjno-prawna

1. Wszyscy pracownicy PWiK oraz pracownicy reprezentujący podmiot zewnętrzny realizujący zadania na rzecz PWiK, zobowiązani są do przestrzegania regulacji wewnętrznych związanych

z bezpieczeństwem informacji, w szczególności zapisów niniejszej Instrukcji oraz Polityki bezpieczeństwa informacji (łącznie zwane dalej „Dokumentacją Bezpieczeństwa").

2. Podstawę i zasady przetwarzania zarówno danych osobowych, jak i danych niezbędnych do realizacji celów statutowych PWiK, stanowią przepisy prawa w tym, przepisy wyszczególnione we Wstępie do niniejszego dokumentu oraz instrukcje, regulaminy, procedury przyjęte przez PWiK.

3. Upoważnionymi pracownikami do przetwarzania danych są wyłącznie osoby posiadające upoważnienie (polecenie) przetwarzania danych podpisane przez Administratora Danych. Odpowiedzialnym za wystąpienie z wnioskiem o wystawienie upoważnienia jest:

- dla nowozatrudnionych pracowników, pracowników już zatrudnionych w PWiK lub pracowników firm realizujących zadania na rzecz PWiK - Kierownik Działu, w którym dany pracownik jest zatrudniony lub nadzorujący wykonanie zadań przydzielonych firmie zewnętrznej;
- dla stanowisk kierowniczych/samodzielnych - Dział Spraw Pracowniczych.

Wzory upoważnień stanowią Załączniki nr 4 i 5 do Instrukcji.

4. Odpowiedzialnym za wystąpienie z wnioskiem o cofnięcie upoważnienia dla stanowisk kierowniczych/samodzielnych jest Dział Spraw Pracowniczych, dla pozostałych pracowników, w tym pracowników podmiotów zewnętrznych - Kierownik Działu (jak w pkt 3). Wzór cofnięcia upoważnienia stanowi Załącznik nr 4a i 5a do Instrukcji.

5. Czynności dotyczące wydania lub cofnięcia upoważnień winny być realizowane przez strony wskazane w pkt 3 i 4 niezwłocznie.

6. Kierownicy działów PWiK oraz Dział Spraw Pracowniczych w przypadkach stanowisk kierowniczych i samodzielnych, zobowiązani są do niezwłocznego pisemnego zgłaszania Kierownikowi Działu Informatyki lub osobie przez niego wyznaczonej, wszelkich zmian uprawnień pracowników do systemów informatycznych (utworzenia nowych, modyfikacji oraz usunięcia istniejących uprawnień). Wzory dokumentów o nadanie lub usunięcie uprawnień do systemu informatycznego stanową Załączniki nr 1 i 2 do Instrukcji.

7. W uzasadnionych przypadkach związanych z koniecznością zapewnienia natychmiastowego bezpieczeństwa danych elektronicznych, informację o konieczności zablokowania dostępu do danych dla wskazanego pracownika PWiK/pracownika podmiotu zewnętrznego, niezwłocznie strony przekazują bezpośrednio Kierownikowi Działu Informatyki lub osobie go zastępującej,

który podejmuje kroki zmierzające do natychmiastowego zablokowania konta pracownika w celu uniemożliwienia mu dostępu do zasobów informatycznych PWiK.

8. Pracownicy/współpracownicy mają obowiązek zgłaszania Inspektorowi Ochrony Danych, Kierownikowi Działu Informatyki lub w przypadku ich nieobecności członkowi Zespołu ds. Ochrony Danych Osobowych - wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa, zapisy Dokumentacji Bezpieczeństwa oraz innych instrukcji, regulaminów i procedur przyjętych przez PWiK w zakresie bezpieczeństwa informacji.

9. W sytuacji, gdy stwierdzone zostanie naruszenie bezpieczeństwa systemu informatycznego, użytkownik zobowiązany jest do zastosowania się do wytycznych „Procedury zgłaszania naruszenia/incydentu bezpieczeństwa teleinformatycznego" (str. 27). Ponadto pracownik zobowiązany jest do:

- zawiadomienia o powyższym osób wskazanych w pkt 8 lub kierownika komórki organizacyjnej;
- zablokowania komputera w sposób uniemożliwiający dalszą pracę w systemie;
- utrzymania sprzętu w taki sposób, aby uniemożliwić do niego dostęp innym osobom.

10. Dla skuteczności przestrzegania zasad bezpiecznego przetwarzania danych w PWiK wymagana jest powszechna znajomość przez pracowników przepisów dotyczących ochrony danych.

11. Kierownicy Działów oraz Dział Spraw Pracowniczych są zobowiązani do dostarczenia lub wskazania ścieżki dostępu pracownikowi przetwarzającemu dane (bądź pracownikowi podmiotu zewnętrznego realizującego usługi na rzecz PWiK) do Rozporządzenia RODO, Ustawy o ochronie danych osobowych, Dokumentacji Bezpieczeństwa. Dział Spraw Pracowniczych zobowiązany jest przyjąć oświadczenie pracownika o zapoznaniu się z wytycznymi ww. przepisów wraz z zobowiązaniem do ich stosowania. Oświadczenie należy przechowywać w aktach osobowych pracownika. Treść oświadczenia zawierającego pożądany zapis uwzględniona jest w Załączniku nr 4 i 5 do Instrukcji.

12. Przetwarzanie danych osobowych w PWiK może mieć miejsce wyłącznie w przypadkach określonych w art. 6 i 9 RODO.

13. Powierzenie przetwarzania danych osobowych innym podmiotom może mieć miejsce wyłącznie w przypadkach określonych w art. 28 RODO wg wzoru umowy powierzenia stanowiącego Załącznik nr 10 do Instrukcji.

14. Za zawarcie umowy powierzenia odpowiedzialni są kierownicy działów lub samodzielne stanowiska nadzorujące wykonanie umowy.

15. Wzór umowy powierzenia przed jej podpisaniem przez osoby upoważnione do reprezentacji PWiK podlega akceptacji Radcy Prawnego oraz Inspektora Ochrony Danych.

16. Udostępnienie danych osobowych, źródło danych osobowych, data sprzeciwu wobec przetwarzania danych jest odnotowywane w systemie informatycznym przez osobę wyznaczoną przez Kierownika działu upoważnionego do zarządzania kartoteką podmiotów. Formularze służące do odnotowania udostępnienia/wstrzymania dostępu do danych (w tym danych osobowych) wskazane są na str. 38-41 Instrukcji.

17. W PWiK zezwala się na instalację wyłącznie legalnego oprogramowania użytkowanego zgodnie z jego licencją oraz instrukcją, nabytego z oficjalnych kanałów dystrybucyjnych.

18. Do instalacji oprogramowania upoważniony jest wyłącznie pracownik Działu Informatyki zatrudniony w PWiK.

19. W PWiK będzie przechowywana faktura zakupu oprogramowania, potwierdzająca źródło jego pochodzenia.

20. Zakres użytkowania oprogramowania na stanowiskach komputerowych nie może wykraczać poza obszar określony w umowie licencyjnej.

21. Podczas instalacji, użytkowania oraz dystrybucji oprogramowania muszą być przestrzegane zapisy Ustawy o prawie autorskim i prawach pokrewnych.

22. Kompetencje i obowiązki Inspektora Ochrony Danych oraz Zespołu ds. Ochrony Danych Osobowych określają przepisy prawa wymienione w RODO, UODO oraz przepisy zawarte w Dokumentacji Bezpieczeństwa.

23. Przy zakupie nowych systemów informatycznych, ich wymianie lub modernizacji należy zwrócić szczególną uwagę na ich zgodność z obowiązującymi przepisami prawa, szczególnie RODO.

24. Dostęp do pomieszczenia serwerów jest ograniczony wyłącznie do pracowników Działu Informatyki obsługujących urządzenia.

25. W przypadku konieczności przeprowadzenia prac administracyjnych w serwerowni, dostęp do pomieszczeń innych osób możliwy jest wyłącznie za zgodą Kierownika Działu Informatyki (lub osoby go zastępującej), który wyznaczy osobę odpowiedzialną za nadzór nad bezpieczeństwem sprzętu zainstalowanego w serwerowni.

26. Umiejscowienie serwerów musi zapewnić jak najszybszą reakcję służb informatycznych na wszelkiego rodzaju oznaki wadliwej pracy urządzenia.

27. Urządzenie, na którym przechowywane są dane osobowe, powinno znajdować się na cokole lub innym elemencie konstrukcyjnym uniemożliwiającym bezpośredni kontakt obudowy serwera z posadzką pomieszczenia.

28. Urządzenia przeznaczone do dystrybucji ruchu sieciowego LAN i WAN, powinny być zabezpieczone przed dostępem osób niepowołanych.

29. Serwerownia powinna być zabezpieczona systemem alarmowym oraz systemem monitorującym warunki klimatyczne w pomieszczeniu.

30. Po godzinach pracy dostęp do pomieszczeń, w których przetwarzane są dane osobowe, możliwy jest wyłącznie za zgodą Prezesa Zarządu, Wiceprezesa Zarządu, Prokurenta, Dyrektora lub Inspektora Ochrony Danych.

31. Pracownik podejmujący czynności na stanowisku przetwarzania danych osobowych poza godzinami pracy określonymi przez pracodawcę, musi się odnotować w rejestrze dostępnym na dyżurce, który powinien zawierać następujące informacje:

- nazwisko i imię pracownika;
- komórka organizacyjna;
- godzina wejścia i wyjścia do pomieszczeń firmy;
- cel wejścia;
- wykaz pomieszczeń do których pracownik miał dostęp w czasie realizacji zadań poza godzinami pracy.

32. Dostęp do obiektów należących do PWiK, w tym do pomieszczeń, gdzie przetwarzane są dane osobowe, powinien być zabezpieczony przez agencję ochrony lub inną instytucję posiadającą odpowiednie uprawnienia do świadczenia tego typu usług.

33. Kopie bezpieczeństwa danych z systemów informatycznych muszą być zdeponowane w metalowych szafach zabezpieczonych odpowiedniej klasy zamkami uniemożliwiającymi ich proste sforsowanie. Zabezpieczenia należy dobierać proporcjonalnie, mając na względzie kategorię danych poddanych archiwizacji.

34. W przypadku stwierdzenia naruszenia zasad bezpieczeństwa o znaczeniu krytycznym dla prawidłowego funkcjonowania PWiK, w tym naruszeń ochrony danych osobowych, incydentów bezpieczeństwa, Kierownik Działu Informatyki lub wskazane przez niego osoby

z personelu Działu Informatyki, zobowiązani są do zablokowania dostępu do systemu osobie, u której stwierdzono naruszenie/incydent oraz do sporządzenia Raportu do Administratora Danych na podstawie Załącznika nr 3 do Instrukcji.

35. W sytuacji naruszenia ochrony danych osobowych Zespół ds. Ochrony Danych Osobowych podejmie kroki w celu wyjaśnienia natury naruszeń oraz zapobieżenia im w przyszłości oraz przedstawi Administratorowi Danych swoje wnioski w postaci Raportu wg Załącznika nr 3a.

36. Dokumenty papierowe oraz nośniki elektroniczne zawierające dane przetwarzane w PWiK, po ustaniu ich użyteczności należy poddać obróbce, która uniemożliwi zapoznanie się z ich zawartością.

37. W celu niszczenia dokumentów papierowych należy korzystać z niszczarek wg wykazu stanowiącego Załącznik nr 12 do Instrukcji, mając na względzie dobór urządzenia wg klasyfikacji danych podlegających usunięciu.

38. Dane znajdujące się na nośnikach informatycznych wykorzystywanych do przetwarzania danych osobowych oraz informacji stanowiących tajemnicę przedsiębiorstwa, winny być usuwane przy udziale Inspektora Ochrony Danych lub Kierownika Działu Informatyki albo osoby przez nich upoważnionej. Czynność usunięcia danych jest odnotowywana wg wzoru stanowiącego Załącznik nr 11 do Instrukcji.

39. Przed utworzeniem nowego zbioru zawierającego dane osobowe Kierownik komórki organizacyjnej/samodzielne stanowisko zobowiązane jest do jego zarejestrowania u Inspektora Ochrony Danych. Wzór zgłoszenia zbioru stanowi Załącznik nr 9 do Instrukcji.

40. W PWiK dopuszcza się wyłącznie wykorzystywanie szablonów pism/zleceń/umów oraz innych aplikacji (w których przetwarzane są dane osobowe) spełniających wytyczne RODO, zatwierdzonych przez Zespół ds. Ochrony Danych oraz Administratora Danych.

41. Każdy pracownik/współpracownik PWiK zobowiązany jest do przestrzegania tzw. „Zasady czystego biurka" opisanej w Załączniku nr 13 do Instrukcji.

42. Każdy pracownik/współpracownik PWiK jest zobowiązany do zachowania w tajemnicy informacji, które przetwarza, nabył bądź wytworzył w trakcie wykonywania swoich obowiązków pracowniczych, w szczególności: danych osobowych, wszelkich informacji o charakterze technicznym, technologicznym, prawnym, handlowym lub organizacyjnym, jak również informacji odnoszących się do jego strategii, personelu, spraw finansowych lub przyszłych planów, perspektyw lub innych informacji posiadających wartość gospodarczą stanowiącą

tajemnicę przedsiębiorstwa w rozumieniu Ustawy o zwalczaniu nieuczciwej konkurencji z dnia 16 kwietnia 1993 r. (Dz.U. z 2020 r., poz. 1913).

43. Każdy użytkownik systemu informatycznego odpowiada za wiarygodność oraz poprawność wprowadzonych przez siebie danych. Ponadto użytkownik zobowiązany jest do przestrzegania porządku danych poprzez umieszczanie danych osobowych wyłącznie w polach przewidzianych do ich przechowywania.

44. W przedsiębiorstwie został wdrożony Zintegrowany System Informatyczny „ZSI Papirus" umożliwiający obieg dokumentów elektronicznych. Wprowadzony elektroniczny obieg dokumentów zapewnia m.in.:

- trwałą, czytelną postać zapisów;
- nadanie priorytetów spraw;
- możliwość stwierdzenia źródła pochodzenia zapisów oraz ustalenie osoby odpowiedzialnej za ich wprowadzenie i modyfikację;
- możliwość sprawdzenia poprawności i kompletności przetwarzanych danych;
- możliwość eksportu wykazów spraw oraz przypisanych do realizacji zadań;
- możliwość grupowania treści po wykazie JRWA oraz tematycznym;
- możliwość identyfikacji poszczególnych wpisów oraz terminów przekazywania spraw pomiędzy komórkami organizacyjnymi.

Dopuszcza się stosowanie dokumentów elektronicznych zamiast zdefiniowanych druków Zintegrowanego Systemu Zarządzania (wykaz druków znajduje się na serwerze w katalogu \\file\zasob\zsz\druki_zsz) pod warunkiem uzyskania akceptacji Pełnomocnika ZSZ w zakresie uwzględnienia w druku elektronicznym wszystkich wymaganych treści oraz zapewnienia ich rozliczalności.

Dokumenty elektroniczne wymagające podpisu tradycyjnego lub parafek (np. umowy) służą jako szablony do wypełnienia wymaganej treści i nie można ich uznawać za dokumenty w obiegu elektronicznym np. druk D23-10 OT.

Zgodnie z art. 78 Kodeksu cywilnego w PWiK dopuszcza się stosowanie elektronicznego podpisu kwalifikowanego bądź podpisu składanego za pośrednictwem profilu zaufanego w obiegu dokumentów elektronicznych i traktuje je jako tożsame z podpisem własnoręcznym. Obieg takich

dokumentów odbywa się drogą elektroniczną. Dokument źródłowy należy przechowywać w sposób umożliwiający weryfikację złożonego podpisu elektronicznego.

Dokumenty elektroniczne przetwarzane w Zintegrowanym Systemie Informatycznym „ZSI Papirus" muszą rejestrować autora wpisów oraz sygnaturę czasu.

Zatwierdzone do stosowania druki elektroniczne przetwarzane w Zintegrowanym Systemie Informatycznym „ZSI Papirus" traktowane są na równi z dokumentami przetwarzanymi w formie tradycyjnej tzw. papierowej.

Instrukcje odnośnie przetwarzania dokumentów elektronicznych w poszczególnych programach dziedzinowych ZSI Papirus zawarte są na serwerze w katalogu \\file\zasob\instrukcje\SOFTHARD

Zasady obiegu i kontroli dokumentów księgowych za pomocą środków elektronicznych określa „Instrukcja obiegu i kontroli dokumentów księgowych Przedsiębiorstwa Wodociągów i Kanalizacji Spółka z o.o. w Olsztynie"

Część techniczna

1. W zakresie rozwiązań sprzętowo-programowych, w celu zapewnienia realizacji zasad bezpieczeństwa systemów informatycznych, PWiK będzie korzystało wyłącznie ze sprawdzonych na rynku rozwiązań.
2. Każde połączenie z Internetem musi być rejestrowane w logach systemowych routera dostępowego – dostęp do logów mają wyłącznie pracownicy Działu Informatyki PWiK.
3. Dostęp do logów systemowych routera rejestrującego aktywność użytkowników w Internecie może być udostępniony innym osobom po otrzymaniu przez nich zgody członka Zarządu PWiK, po uprzednim określeniu celu dostępu wraz z informacją czy ma być to dostęp jednorazowy czy stały.

4. Logi systemowe muszą umożliwiać pełną identyfikację komputera, z którego nawiązano połączenie z Internetem oraz powinien być w nich podany adres komputera docelowego wraz z sygnaturą czasu połączenia.

5. Komputery należące do PWiK będą poddawane dokonywanej przez pracowników Działu Informatyki kontroli sprzętowej, programowej oraz danych, w zakres której wchodzi sprawdzenie sprawności, podatności na zagrożenia, wydajności sprzętu oraz przestrzegania zasad przetwarzania danych przyjętych przez PWiK.

6. Całość oprogramowania powinna być aktualizowana na bieżąco pod kątem instalacji, nowych uaktualnień programów operacyjnych, użytkowych, narzędziowych o znaczeniu krytycznym oraz znaczącym dla utrzymania bezpieczeństwa systemów informatycznych PWiK.

7. W przypadku wybranych stanowisk lub gdy aktualizacja oprogramowania jest niewskazana ze względu na destabilizację stanowisk komputerowych bądź innych urządzeń IT, stanowisko komputerowe nie powinno mieć bezpośredniego dostępu do Internetu.

8. Całościowe kopie wprowadzanych danych do Zintegrowanego Systemu Informatycznego, muszą być wykonywane w cyklu codziennym.

9. Kopie bezpieczeństwa danych muszą być zapisywane na nośnikach zapewniających prawidłowe ich odtworzenie w przypadku awarii nośników podstawowych.

10. Kopie danych z serwerów wykonywane są przez pracowników Działu Informatyki.

11. Pracownicy PWiK zobowiązani są do bieżącej klasyfikacji posiadanych danych elektronicznych przetwarzanych na dostępnym dla nich sprzęcie informatycznym (w szczególności katalogów, plików, programów, baz danych, multimediów, widomości e-mail oraz innych danych agregowanych zarówno na stacjonarnych jak i przenośnych nośnikach informacji) w kontekście ich przydatności dla celów realizowanych przez PWiK oraz ze względu na konieczność zapewnienia rozliczalności prowadzonych spraw. Na postawie ww. klasyfikacji pracownicy zobowiązani się niezwłocznie zgłaszać potrzebę archiwizacji tych danych do Działu Informatyki - wg Załącznika nr 6 do Instrukcji.

12. Archiwizacja danych musi być dokonywana za pomocą skryptu umożliwiającego jej automatyczne przeprowadzenie, w czasie, kiedy serwer nie jest obciążony dodatkowymi zadaniami, mogącymi mieć istotny wpływ na prawidłowy przebieg procesu wykonywania kopii bezpieczeństwa.

13. Każdy nowo instalowany program lub dostarczone na stanowisko dane, muszą być poddane sprawdzeniu aktualnym (z aktualną bazą wirusów) oprogramowaniem antywirusowym przed pierwszym ich użyciem.

14. Pracownicy zobowiązani są do sprawdzenia dostępnych dla nich danych lokalnych (poza danymi zlokalizowanymi na serwerach) oprogramowaniem antywirusowym przynajmniej 1 raz w tygodniu.

15. Lokalne systemy informatyczne mające dostęp do sieci publicznej należy chronić zaporą ogniową (tzw. firewall) oraz oprogramowaniem antywirusowym z aktualną bazą wirusów.

16. Użytkownik komputera zobowiązany jest każdorazowo do sprawdzenia oprogramowaniem antywirusowym wszelkich nośników pamięci lub pobranych za pomocą Internetu zasobów przed ich użyciem.

17. Stacja robocza przetwarzająca dane osobowe musi zostać zabezpieczona hasłem dostępowym (BIOS) oraz hasłem logującym użytkownika do systemu operacyjnego.

18. Dostęp do podsystemów informatycznych, w których przetwarzane są dane osobowe może być możliwy jedynie w przypadku wprowadzenia hasła dostępowego do BIOS, poprawnej nazwy logowania oraz hasła użytkownika.

19. Hasła użytkowników w systemach informatycznych muszą spełniać następujące warunki:
    - minimalna długość hasła – co najmniej 14 znaków;
    - hasło powinno stanowić kombinację: dużych liter, małych liter, cyfr, znaków specjalnych;
    - okres ważności hasła – 1 rok.

20. Za nadanie haseł inicjujących (startowych) do systemów informatycznych, oprogramowania świadczącego usługi, oprogramowania narzędziowego niezbędnego do monitorowania bezpieczeństwa, urządzeń aktywnych sieci LAN i WAN, serwisów www, skrzynek e-mail, pozostałych urządzeń oraz oprogramowania podlegającego nadzorowi przez Dział Informatyki odpowiedzialni są pracownicy wyznaczeni przez Kierownika Działu Informatyki.

21. Procedurę nadania uprawnień określa Procedura opisana na str. 23 Instrukcji.

22. Hasła nie mogą posiadać cech czyniących je podatnymi na odkrycie metodą ataków słownikowych (np. składać się ze słów lub fraz znajdujących się w słownikach); składać się z: danych osobowych (np. daty urodzenia, numeru PESEL, nazwiska panieńskiego matki, itp.), osobistych upodobań (np. ulubiony: kolor, sport, potrawa, itp.), imion zwierząt domowych, itp.

23. W przypadku chwilowej nieobecności pracownika na stanowisku pracy, jest on zobowiązany do zabezpieczenia dostępu osobom nieupoważnionym - do systemów informatycznych poprzez zablokowanie/wylogowanie stacji roboczej; do zbiorów danych osobowych gromadzonych w formie papierowej oraz innych nośników, w tym elektronicznych poprzez składowanie ich w miejscach zabezpieczonych przed dostępem osób niepowołanych.

24. Korzystając ze stacji roboczej użytkownik ma obowiązek zastosowania się do wytycznych Procedury rozpoczęcia, zawieszenia i zakończenia pracy na stanowiskach komputerowych, opisanej na str. 26 Instrukcji.

25. Na komputerach przetwarzających dane osobowe, mechanizm automatycznego zablokowania/wylogowania stacji/użytkownika, powinien włączać się samoistnie w przypadkach, kiedy czas bezczynności stacji wynosi 15 minut.

26. Architektura sieci komputerowej powinna uwzględniać stosowanie jak najmniejszych domen kolizyjnych.

27. Brzegowe urządzenia sieciowe powinny umożliwiać bezpieczne przesyłanie danych.

28. Dane osobowe przesyłane poprzez sieć publiczną powinny być zabezpieczone środkami kryptograficznymi uzgodnionymi z Działem Informatyki.

29. Transmisję za pośrednictwem sieci bezprzewodowych należy zabezpieczyć środkami kryptograficznymi uzgodnionymi z Działem Informatyki, odpowiednimi do rodzaju przesyłanych w nich danych.

30. Urządzenia kluczowe dla prawidłowego funkcjonowania systemu (serwer, szafy dystrybucyjne) muszą być podłączone do urządzeń podtrzymujących napięcie – zasilaczy awaryjnych UPS.

31. Korzystanie z nośników informatycznych w postaci pamięci przenośnych przez pracowników PWiK, wymaga uprzednio uzyskania zgody Prezesa / Dyrektora oraz Inspektora Ochrony Danych wyrażonej w formularzu stanowiącym Załącznik nr 8 do Instrukcji.

32. Dane osobowe przetwarzane na nośnikach pamięci przenośnych muszą uprzednio zostać poddane szyfrowaniu mechanizmami uzgodnionymi z Działem Informatyki.

33. Sprzęt komputerowy w tym serwery, stanowiska robocze, drukarki, urządzenia peryferyjne i sieciowe są zasilane z wydzielonej sieci elektrycznej odpowiednio zabezpieczonej. Niedopuszczalne jest używanie sieci komputerowej do podłączania innych urządzeń, zwłaszcza urządzeń dużej mocy (czajniki, urządzenia grzewcze).

34. Obwód zasilający sprzęt komputerowy musi zostać zabezpieczony przed możliwością podłączenia do niego innych urządzeń elektrycznych (np. czajnika, odkurzacza itd.).

35. Przeglądy i konserwacje systemu i zbiorów danych dokonywane są przez pracowników Działu Informatyki lub w przypadku uzasadnionej potrzeby przez osoby posiadające odpowiednie kwalifikacje w tym zakresie, pod nadzorem pracownika uprawnionego do wykonywania tych czynności przez Kierownika Działu Informatyki lub Administratora Danych.

36. Użytkownik zobowiązany jest do zgłaszania Kierownikowi działu (w przypadku stanowisk samodzielnych zgłoszenie należy wystosować do Kierownika Działu Informatyki) potrzebę likwidacji lub zgłoszenia do zagospodarowania nieużytkowanego sprzętu IT oraz wszelkich nośników danych. Wyznaczony pracownik Działu Informatyki - po uprzednim dostarczeniu mu urządzenia/nośnika przez użytkownika – usuwa dane, a gdy jest to niemożliwe uszkadza nośnik w sposób uniemożliwiający jego odczytanie.

37. Każdorazowo Dział/samodzielne stanowisko zgłaszające sprzęt IT bądź oprogramowanie do Komisji Likwidacyjnej lub w innych sytuacjach wymagających trwałego usunięcia danych, winien otrzymać od Działu Informatyki dokument poświadczający usunięcie danych z nośników – wg wzoru zawartego w Załączniku nr 11 do Instrukcji.

38. Monitory w pomieszczeniach, w których przebywają osoby postronne ustawia się w sposób uniemożliwiający tym osobom wgląd do wyświetlonych danych.

39. W przypadku opuszczenia pomieszczeń, w których znajdują się komputery, pomieszczenia te bezwzględnie muszą być zamykane na klucz. Przebywanie w obszarze przetwarzania danych osób nieuprawnionych jest dopuszczalne za zgodą Administratora Danych lub w obecności osoby upoważnionej do przetwarzania danych, w zakresie przewidzianym na danym stanowisku. Niedopuszczalne jest pozostawienie w pomieszczeniu wyłącznie osób postronnych.

40. Wszelkie dokumenty zawierające dane osobowe, informacje istotne z punktu widzenia interesów PWiK, jak również inne informacje prawnie chronione - niezależnie od użytych środków technicznych służących do ich przechowywania - należy zabezpieczyć przed dostępem osób nieuprawnionych przez ich przechowywanie w zamkniętych szafach wyposażonych w zamki uniemożliwiające ich proste sforsowanie. Zabezpieczenia należy dobierać proporcjonalnie, mając na względzie kategorię przechowywanych (przetwarzanych) informacji.

41. Przekazanie komputerów podmiotom zewnętrznym w uzasadnionych przypadkach, za wiedzą Administratora Danych, może odbyć się po trwałym usunięcia danych lub po usunięciu z nich nośników danych przez wyznaczonego pracownika Działu Informatyki.

42. W przypadku zbiorów danych osobowych oraz danych stanowiących tajemnicę przedsiębiorstwa przetwarzanych w postaci plików generowanych w pakietach biurowych (Open Office, Microsoft Office lub innych) lub za pośrednictwem innego oprogramowania dostęp do pliku/zasobu należy dodatkowo zabezpieczyć hasłem z zastosowaniem mechanizmu szyfrowania lub dokonać ich zabezpieczenia uzgodnionego z Działem Informatyki programu zewnętrznego zapewniającego ww. poziom szyfrowania.

43. W uzasadnionych przypadkach - w szczególności w sytuacjach przetwarzania danych osobowych poza siedzibą PWiK - jest wymagane stosowanie mechanizmów szyfrowania nośnika danych. Pracownicy Działu Informatyki na wniosek osoby przetwarzającej, udostępniają program umożliwiający szyfrowanie informatycznych nośników danych.

44. W PWiK zasady funkcjonowania systemu monitoringu określa Regulamin stanowiący Załącznik nr 14 do niniejszej Instrukcji.

Wykaz czynności zabronionych

W celu realizacji zadań przyjętej ochrony danych w PWiK zabrania się:

1. Instalowania programów oraz jakichkolwiek innych zbiorów plików na komputerach przez nieupoważnione osoby, plików niezwiązanych z obowiązującym pracownika zakresem obowiązków na danym stanowisku pracy.
2. Pracy na plikach pochodzących spoza wewnętrznej sieci informatycznej PWiK, niesprawdzonych aktualnym oprogramowaniem antywirusowym.
3. Korzystania z zewnętrznych nośników informatycznych, na korzystanie z których nie uzyskano uprzednio zgody wyrażonej na formularzu stanowiącym Załącznik nr 8 do Instrukcji.
4. Korzystania ze sprzętu informatycznego w sposób wykraczający poza zastosowania wynikające z zakresu obowiązków na danym stanowisku pracy.
5. Realizowania połączeń z Internetem na stanowiskach nie wyposażonych w niezbędne programy zabezpieczające tj. firewall oraz antywirus.

6. Wynoszenia jakiegokolwiek sprzętu informatycznego poza siedzibę PWiK bez wiedzy oraz pisemnej zgody członka Zarządu, Prokurenta, Dyrektora lub Inspektora Ochrony Danych.
7. Udostępniania, kopiowania, wysyłania za pośrednictwem Internetu oraz wynoszenia jakichkolwiek danych niezależnie od formy ich zapisu zawierających dane osobowe lub informacje na temat działalności przedsiębiorstwa poza siedzibę Spółki bez zgody członka Zarządu.
8. Kopiowania i wynoszenia nośników instalacyjnych, kluczy licencyjnych, kluczy zabezpieczających oraz instalacji oprogramowania będącego własnością PWiK poza siedzibę Spółki.
9. Dokonywania jakichkolwiek prób napraw sprzętu komputerowego przez nieupoważnione osoby.
10. Realizowania połączeń z Internetem w celu innym niż dostęp do informacji zawartej na stronie internetowej (WEB), niezbędnej do wykonania czynności przewidzianych na danym stanowisku pracy.
11. Podejmowania działań manipulacyjnych bądź destrukcyjnych w systemie za pomocą technik informatycznych, socjotechnik, używania programów mających na celu zdobycie haseł oraz danych generowanych za pomocą sprzętu IT.
12. Podejmowania działań w celu uzyskania nieautoryzowanego dostępu do Internetu, infrastruktury informatycznej oraz przetwarzanych w niej danych.
13. Podejmowania innych czynności mogących mieć wpływ na zmniejszenie bezpieczeństwa systemu informatycznego eksploatowanego w przedsiębiorstwie.
14. Udostępniania stanowisk komputerowych z zainstalowanym oprogramowaniem umożliwiającym dostęp do danych osobowych oraz danych kluczowych do prawidłowego funkcjonowania PWiK pracownikom nie upoważnionym/osobom postronnym.
15. Udostępniania stanowisk komputerowych osobom nie zatrudnionym w PWiK.
16. Przynoszenia i instalacji na komputerach oraz innych urządzeniach teleinformatycznych (w tym służbowych telefonach komórkowych) PWiK prywatnych danych, oprogramowania.
17. Ujawniania innym osobom indywidualnych haseł dostępowych do systemów/urządzeń uwzględniających proces autoryzacji.
18. Udostępniania osobom nieupoważnionym jakichkolwiek informacji, których właścicielem jest PWiK.

19. Oddalania się od stanowiska pracy bez zabezpieczenia dostępu do danych.
20. Generowania wydruków zawierających dane osobowe lub inne dane kluczowe do prawidłowego funkcjonowania PWiK, w przypadku braku możliwości ich zabezpieczenia przed dostępem osób nieupoważnionych lub postronnych.
21. Wyrzucania wydruków, kartotek i innych zbiorów danych zawierających dane osobowe lub dane kluczowe do prawidłowego funkcjonowania PWiK, bez uprzedniego ich zniszczenia uniemożliwiającego ich odtworzenie.
22. Podłączania prywatnych urządzeń do infrastruktury informatycznej, w tym sieciowej LAN/WAN należącej do PWiK.
23. Udostępniania informacji o systemach eksploatowanych w PWiK, środkach ich zabezpieczenia oraz innych szczegółach technicznych infrastruktury teleinformatycznej.
24. Wykorzystywania jakiegokolwiek sprzętu IT należącego do PWiK do celów prywatnych.
25. Wykorzystywania zasobów internetowych udostępnionych przez PWiK (np. portale internetowe, skrzynki e-mail, serwery FTP, zasoby dostępne za pośrednictwem chmury internetowej) do celów prywatnych.
26. Nieautoryzowanego dostępu lub zakłócania pracy urządzeń IT w sposób uniemożliwiający ich prawidłową eksploatację.
27. Zabezpieczania danych w sposób nie uzgodniony z Działem Informatyki.
28. Przechowywania w zasobach sieciowych komputerów (katalogi ogólnodostępne) danych zawierających: dane osobowe, dane istotne z punktu widzenia interesów PWiK oraz inne dane prawnie chronione.

Procedura wykonywania kopii bezpieczeństwa danych osobowych, danych kluczowych dla prawidłowego funkcjonowania przedsiębiorstwa oraz programów, narzędzi programowych, w których są przetwarzane dane osobowe

Procedura wykonywania kopii bezpieczeństwa danych oraz programów w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn realizowana jest w celu:

- zabezpieczenia przed utratą danych przetwarzanych w systemach informatycznych kluczowych dla niezakłóconego funkcjonowania Spółki;

- zapewnienia wymaganego bezpieczeństwa danych;
- zminimalizowania kosztów ewentualnych awarii sprzętu IT i związanych z tym przestojów.

1. Kopie bezpieczeństwa baz danych ZSI przetwarzanych na serwerach Spółki wykonywane są w cyklu codziennym.
2. Kopie bezpieczeństwa programów i narzędzi programowych służących do przetwarzania danych osobowych wykonywane są przynajmniej raz w miesiącu.
3. Kopie bezpieczeństwa wykonywane są za pomocą skryptów lub oprogramowania narzędziowego umożliwiającego ich wykonanie w czasie najmniejszego obciążenia serwerów.
4. Kopie bezpieczeństwa przechowywane są na nośnikach zapewniających ich prawidłowe odtworzenie, w miejscu zabezpieczonym przed dostępem osób niepowołanych, z dala od źródeł emisji wpływających na zdegradowanie użyteczności nośników.
5. Kopie bezpieczeństwa zawierające dane krytyczne (bazy danych obsługujące oprogramowanie ZSI Papirus) dla prawidłowego funkcjonowania PWiK, przechowywane są dodatkowo w Archiwum Zakładowym zlokalizowanym, w budynku innym niż serwerownia. Aktualizacja danych składowanych w kopiach bezpieczeństwa w tym przypadku nie może być rzadsza niż raz na kwartał.
6. Zbiory kopii bezpieczeństwa przechowuje się do chwili ustania ich użyteczności w zastosowaniu do działań realizowanych przez PWiK.
7. Za wykonywanie kopii bezpieczeństwa zasobów przetwarzanych na serwerach oraz wdrożenie rozwiązań umożliwiających ich przeprowadzenie odpowiedzialni są pracownicy Działu Informatyki.
8. Dział Informatyki wdraża środki umożliwiające wykonanie kopii bezpieczeństwa danych ze stacji roboczych Spółki.
9. Za zgłoszenie do Działu Informatyki potrzeby archiwizacji zbiorów danych osobowych przetwarzanych na stacjach roboczych oraz danych kluczowych do prawidłowego funkcjonowania Spółki odpowiedzialni są użytkownicy stacji roboczych. Wzór zgłoszenia potrzeby archiwizacji stanowi Załącznik nr 6 do Instrukcji.
10. Odtworzenie zbiorów z archiwum możliwe jest w przypadkach: sprawdzenia poprawności wykonywania archiwum, utraty danych na stacji roboczej/serwerach - na wniosek stanowiący Załącznik nr 7 do Instrukcji.

11. Odtworzenie zbiorów kopii bezpieczeństwa danych zawierających dane osobowe, możliwe jest po uzyskaniu akceptacji Prezesa Zarządu PWiK, w uzgodnieniu z Inspektorem Ochrony Danych.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji oraz kopii zapasowych zawierających dane osobowe oraz dane kluczowe dla prawidłowego funkcjonowania PWiK

1. Elektroniczne nośniki informacji zawierające dane osobowe/dane kluczowe dla prawidłowego funkcjonowania PWiK, przechowywane są w zamkniętych szafkach wyposażonych w zabezpieczenia przed dostępem osób nieupoważnionych, adekwatne do kategorii przechowywanych w nich danych.
2. Okres przechowywania nośników zawierających dane osobowe/dane kluczowe dla prawidłowego funkcjonowania PWiK, powinien być ustalony przez kierownika działu/samodzielne stanowisko.
3. Kopie bezpieczeństwa są niezwłocznie niszczone po ustaniu użyteczności danych tam zawartych.
4. Zniszczenia kopii dokonuje się w sposób uniemożliwiający późniejsze odtworzenie danych, poprzez fizyczne zniszczenie nośników danych lub jeśli to niemożliwe, poprzez trwałe usunięcie danych przy pomocy specjalistycznego oprogramowania służącego do tego celu.
5. Kierownik działu/stanowisko samodzielne zobowiązany jest pisemnie poinformować pracownika Działu Informatyki podczas konfiguracji programu do wykonywania archiwizacji o wymaganym czasie przechowywania kopii zapasowych.
6. Kopie zapasowe serwerów powinny być przechowywane z uwzględnieniem zasad redundancji z wykorzystaniem urządzeń znajdujących się w posiadaniu PWiK (macierze dyskowe, dyski twarde, taśmy streamerów).
7. Przechowywanie kopii zapasowych możliwe jest wyłącznie w pomieszczeniach nadzorowanych przez Dział Informatyki oraz w archiwum zakładowym, w oddzielnym sejfie dedykowanym do przechowywania kopii.
8. Zawartość kopii składowanych w archiwum zakładowym musi być opisana elektronicznie (w formie pliku tekstowego zawierającego wykaz zbiorów) oraz w postaci papierowej (w postaci załącznika do nośnika kopii), w sposób umożliwiający szybką lokalizację zbiorów.

Procedura nadania uprawnień do systemu przetwarzającego dane osobowe oraz do pozostałych usług informatycznych obsługujących metody uwierzytelniania w PWiK Olsztyn

Przed przystąpieniem do przetwarzania danych osobowych użytkownik ma obowiązek zapoznać się z następującymi dokumentami określającymi zasady postępowania na stanowisku pracy:

- 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;
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych - zwana dalej UODO;
- Dokumentacją Bezpieczeństwa obowiązującą w PWiK.

1. Zapoznanie się z ww. dokumentami użytkownik potwierdza własnoręcznym podpisem na druku upoważnienia do przetwarzania danych osobowych stanowiącym Załącznik nr 4 do Instrukcji.
2. Przyznanie uprawnień do systemów informatycznych lub innych zasobów informatycznych umożliwiających uwierzytelnianie/autoryzację użytkowników, następuje na podstawie Załącznika nr 1 do Instrukcji zgodnie ze ścieżką zatwierdzeń dokumentu określoną w Załączniku nr 2a do Instrukcji.
3. Uprawnienia do systemu oraz indywidualny identyfikator użytkownika nadawane są przez odpowiedzialnych za tę czynność pracowników Działu Informatyki.
4. Przyjęty format identyfikatora użytkownika to: nazwisko+pierwsza litera imienia np. dla użytkownika **Kowalski Jan** należy nadać identyfikator:

k	**o**	**w**	**a**	**l**	**s**	**k**	**i**	**j**

5. Podczas pierwszego uruchomienia komputera użytkownik z pomocą pracownika Działu Informatyki ustanawia hasło BIOS.
6. Hasło pierwszego logowania do systemu operacyjnego ustala Kierownik Działu Informatyki lub wyznaczony przez niego pracownik, który przekazuje hasło użytkownikowi.

7. W trakcie pierwszego logowania do systemu operacyjnego następuje proces wymuszenia zmiany hasła użytkownika na indywidualne - zgodnie z wytycznymi co do jego złożoności, określonymi w Części technicznej Instrukcji (pkt 19 i 22).

8. Hasła użytkowników uprzywilejowanych (administratorów serwerów, stacji roboczych, urządzeń posiadających mechanizmy uwierzytelniania) powinny być zdeponowane w zalakowanej kopercie lub przechowywane elektronicznie w postaci programu uwzględniającego możliwość ich odpowiedniego zabezpieczenia.

9. Hasła wymienione w pkt 7 muszą być dostępne wyłącznie dla wyznaczonych przez Kierownika Działu Informatyki administratorów systemów informatycznych zatrudnionych w PWiK. W przypadku ich nieobecności decyzję o udostępnieniu zdeponowanych haseł może podjąć wyłącznie Zarząd Spółki lub upoważniona przez Zarząd osoba.

10. Dostęp osób postronnych do systemów informatycznych PWiK bądź danych przetwarzanych w tych systemach, jest zabroniony. W uzasadnionych przypadkach dostępu do systemów może udzielić wyłącznie Administrator Danych - po uzyskaniu opinii Inspektora Ochrony Danych oraz Kierownika Działu Informatyki.

Procedura wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

1. Upoważnionymi do dokonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych są pracownicy Działu Informatyki.
2. Wszelkie czynności serwisowe nie wymagające specjalistycznych napraw wykonywane są w siedzibie PWiK Olsztyn.
3. W przypadku, kiedy dokonanie czynności serwisowej w siedzibie PWiK nie jest możliwe, urządzenia do przetwarzania danych dostarcza się serwisantowi, po uprzednim demontażu nośników zawierających dane osobowe oraz dane newralgiczne dla prawidłowego funkcjonowania PWiK, lub usuwa/zabezpiecza w sposób uniemożliwiający ich odczytanie.
4. O fakcie dokonywania czynności serwisowych musi być poinformowany Kierownik Działu Informatyki.
5. Wykryte błędy w funkcjonowaniu urządzeń przetwarzających dane osobowe usuwa się niezwłocznie.
6. Czynności konserwacyjne serwerów, na których przetwarzane są dane osobowe, dokonuje się nie rzadziej niż 1 raz w roku.
7. Wykaz czynności obejmujących konserwację serwerów:
   - czyszczenie podzespołów;
   - analiza struktury fizycznej i logicznej dysków twardych;
   - analiza pamięci operacyjnej;
   - diagnostyka pozostałych komponentów (m.in. płyta główna, karta sieciowa, napędy);
   - optymalizacja systemu operacyjnego pod kątem wydajności;
   - test zasilaczy UPS.
8. W przypadkach archiwizowania danych na streamerach, czyszczenie napędu odbywa się raz na dwa tygodnie.

Procedura rozpoczęcia, zawieszenia i zakończenia pracy na stanowiskach komputerowych

1. Po uruchomieniu stacji roboczej użytkownik rozpoczyna pracę od wpisaniu hasła BIOS, a następnie hasła do systemu operacyjnego.
2. Przed uwierzytelnieniem w systemie użytkownik powinien się upewnić, czy inna osoba nie ma możliwości odczytania wprowadzonych haseł.
3. Uwierzytelnienie polega na podaniu indywidualnego identyfikatora użytkownika oraz indywidualnego hasła.
4. W przypadku opuszczenia stanowiska pracy na krótki czas, należy zablokować stację roboczą przez naciśnięcie CTRL+L lub CTRL+ALT+DELETE oraz wybranie opcji „Zablokuj Komputer" (Windows 7) lub „Zablokuj" (Windows 10).
5. Po powrocie do swojego stanowiska pracy należy odblokować stację roboczą podając hasło.
6. Zakończenie pracy w systemie odbywa się przez wylogowanie z systemu oraz wyłączenie stacji roboczej po uprzednim zakończeniu pracy w programach użytkowanych na stanowisku.
7. Przed wylogowaniem z systemu należy upewnić się, że wszystkie wyniki pracy zostały zachowane.
8. Przed odejściem od stanowiska pracy należy upewnić się, że proces wylogowania zakończył się pomyślnie oraz nastąpiło wyłączenie stacji roboczej. Użytkownik zobowiązany jest do wyłączenia listwy zasilającej sprzęt komputerowy.
9. W przypadku stwierdzenia nieprawidłowości związanych z przebiegiem procesu logowania/wylogowania, fakt ten należy niezwłocznie zgłosić pracownikowi Działu Informatyki.

Procedura zgłaszania naruszenia/incydentu bezpieczeństwa teleinformatycznego

Rejestrowanie informacji o naruszeniach/incydentach:

1. Pracownicy mają obowiązek zgłaszania Kierownikowi Działu Informatyki/Inspektorowi Ochrony Danych wszelkich zdarzeń, które naruszają lub mogą naruszyć przepisy prawa, zapisy Dokumentacji Bezpieczeństwa oraz innych instrukcji, regulaminów i procedur przyjętych przez PWiK w zakresie bezpieczeństwa informacji/ochrony danych.
2. Kierownik Działu Informatyki po uprzednim dokonaniu działań minimalizujących ryzyko utraty, uszkodzenia, nieautoryzowanej zmiany, niekontrolowanego udostępnienia danych bądź ich usunięcia - niezwłocznie informuje Administratora Danych o wystąpieniu incydentu bezpieczeństwa teleinformatycznego wraz z informacją o jego skutkach wg Załącznika nr 3 do Instrukcji. W przypadku, kiedy incydent bezpieczeństwa informacji dotyczy sprzętu IT, na którym przetwarzano dane osobowe – Kierownik Dział Informatyki niezwłocznie informuje o incydencie bezpieczeństwa członków Komisji ds. Ochrony Danych Osobowych, która rozstrzyga czy incydent nosi znamiona naruszenia podlegającego zgłoszeniu do organu nadzorczego w trybie zgodnym z art. 33 ust. 1 RODO.
3. W przypadku noszącym znamiona naruszenia praw i wolności osób fizycznych, Zespół ds. Ochrony Danych Osobowych niezwłocznie przygotowuje i przedstawia do podpisu Administratorowi Danych zgłoszenie do organu nadzorczego naruszenia, zgodnie z wytycznymi art. 33 ust. 3 RODO. Za wysyłkę zgłoszenia do organu nadzorczego o naruszeniu odpowiedzialny jest Inspektor Ochrony Danych.
4. Zespół ds. Ochrony Danych Osobowych prowadzi Rejestr Naruszeń danych osobowych - na podstawie Załącznika nr 3a do Instrukcji - zawierający następujące informacje:
   - datę i godzinę zgłoszenia podejrzenia o wystąpienie naruszenia/incydentu;
   - dane osoby, u której stwierdzono naruszenie;
   - datę i godzinę zarejestrowania naruszenia;
   - opis naruszenia;
   - ocenę skutków naruszenia;
   - informacje dotyczące klasyfikacji naruszenia w kontekście konieczności wypełnienia obowiązku zgłoszenia naruszenia do organu nadzorczego;

- opis podjętych czynności w celu usunięcia naruszenia bądź zminimalizowania jego skutków;
- w przypadku stwierdzenia ryzyka naruszenia praw i wolności osób fizycznych datę zgłoszenia naruszenia do organu nadzorczego.

5. Zespół ds. Ochrony Danych Osobowych prowadzi analizy i statystyki naruszeń dotyczących danych osobowych.

6. Zespół ds. Ochrony Danych Osobowych zapewnia właściwe wykorzystanie informacji o incydentach związanych z bezpieczeństwem informacji dla doskonalenia systemu zarządzania bezpieczeństwem informacji, zapobieżenia naruszeniom w przyszłości oraz do celów szkoleniowych.

7. Za rejestrowanie naruszeń/incydentów innych niż wskazane w pkt 3 odpowiedzialny jest pracownik wyznaczony przez Kierownika Działu Informatyki.

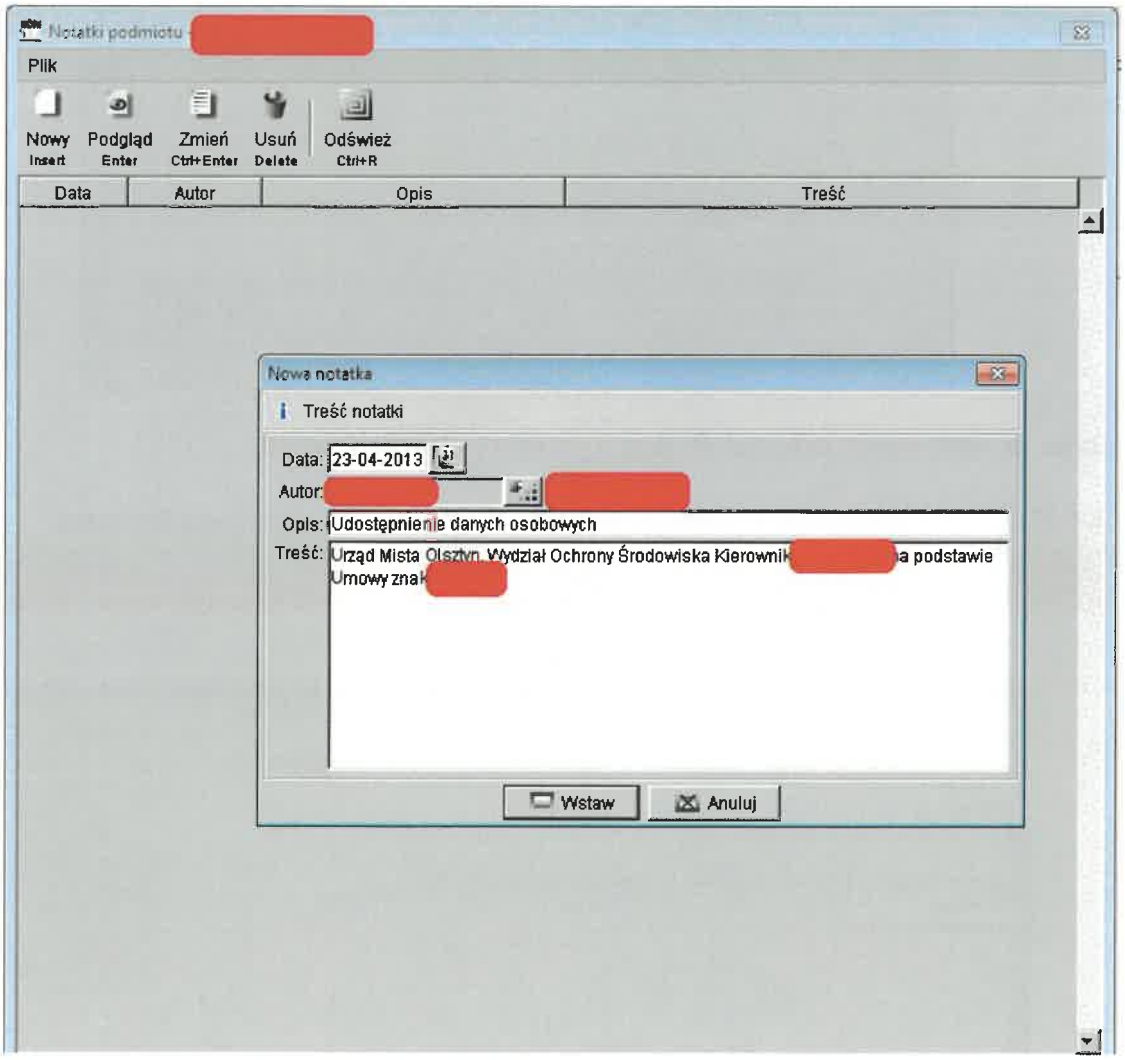
8. Kierownik Działu Informatyki dokonuje analizy zarejestrowanych naruszeń/incydentów (bez związku z danymi osobowymi) i na ich podstawie rekomenduje Administratorowi Danych środki techniczne oraz rozwiązania programowe w celu zminimalizowania ilości oraz skutków naruszeń/incydentów.

Sposób gromadzenia informacji o udostępnieniu danych osobowych, źródle danych oraz historii zamian podmiotu w poszczególnych systemach informatycznych administratora

Informacje o osobach, których dane zostały udostępnione – formularz

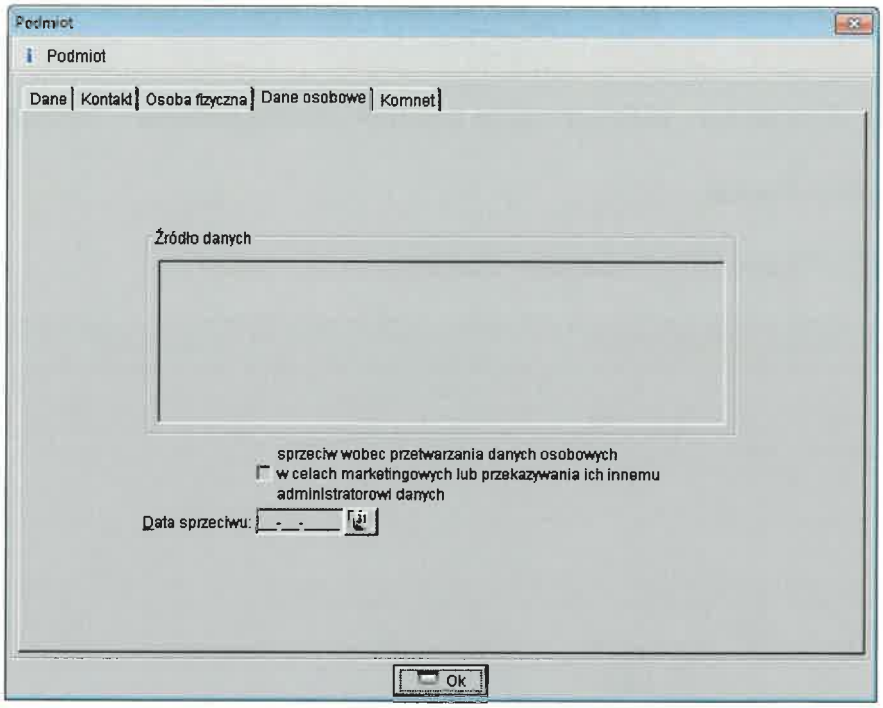
Ścieżka do formularza:

KOM-MEDIA->Kartoteki->Podmioty->Podmioty->Plik>Notatki



Źródło danych osobowych oraz data sprzeciwu – formularz, raport

KOM-MEDIA

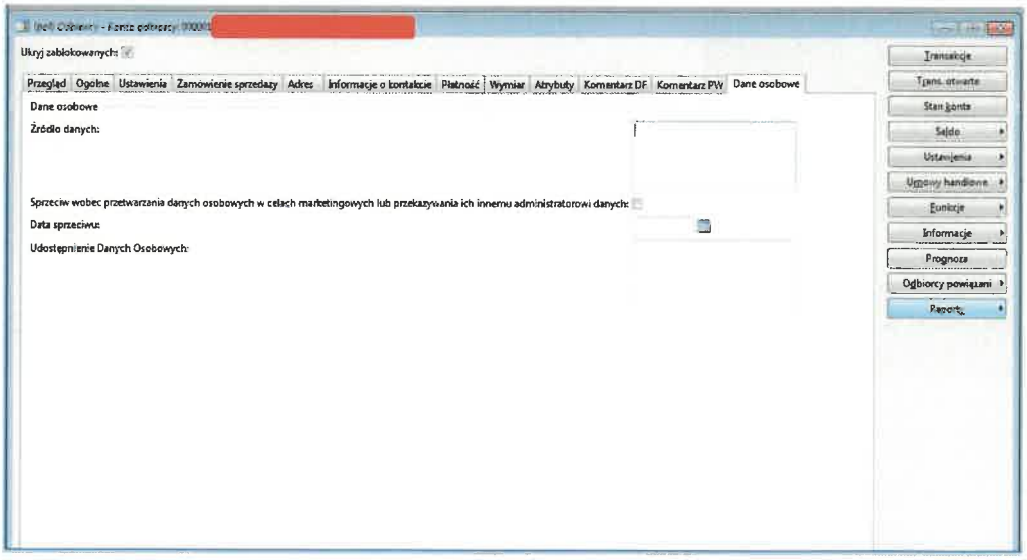


Ścieżka do wykonania raportu nt. daty sprzeciwu, źródła danych:

KOM-MEDIA->Administracja->Grupy zapytań->Zapytania->Raport Dane osobowe

NAZWA_PELNA	ADRES	TELEFON	SPRZECIW	DATA_SPRZECIWU	ZRODLO_DANYCH	ID_PODM_W_RPG

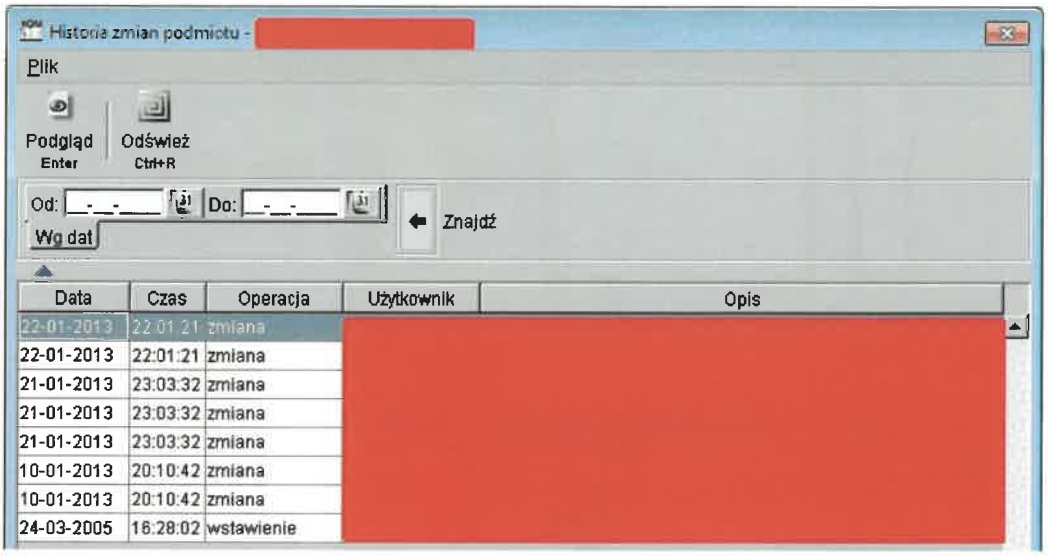
AXAPTA



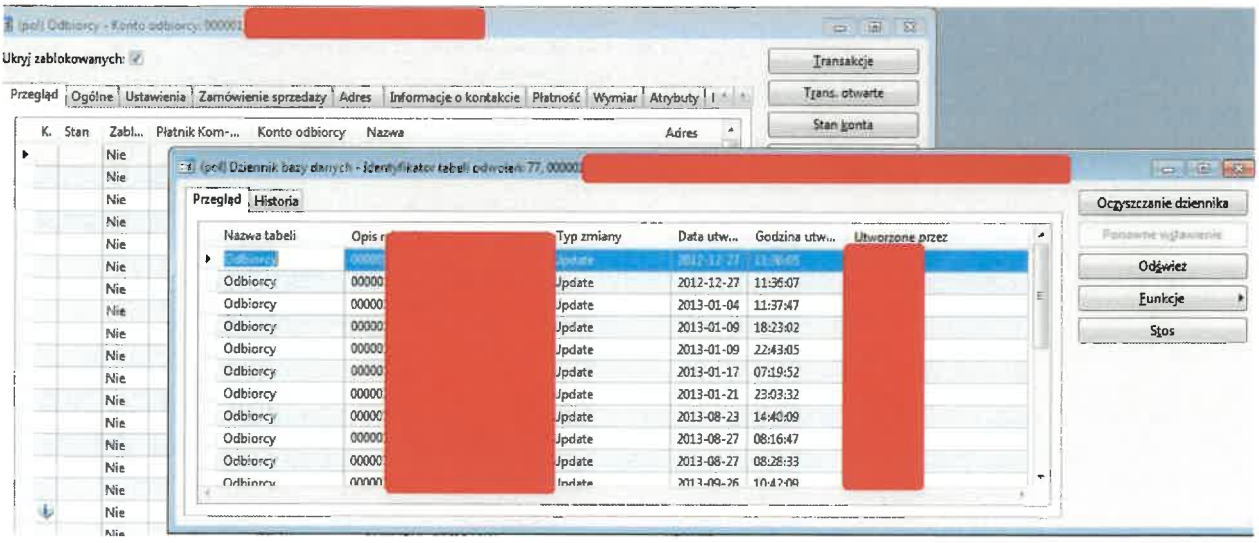
Historia zmian podmiotu – formularz, raport

Ścieżka dostępu do informacji nt. historii zmian podmiotu:

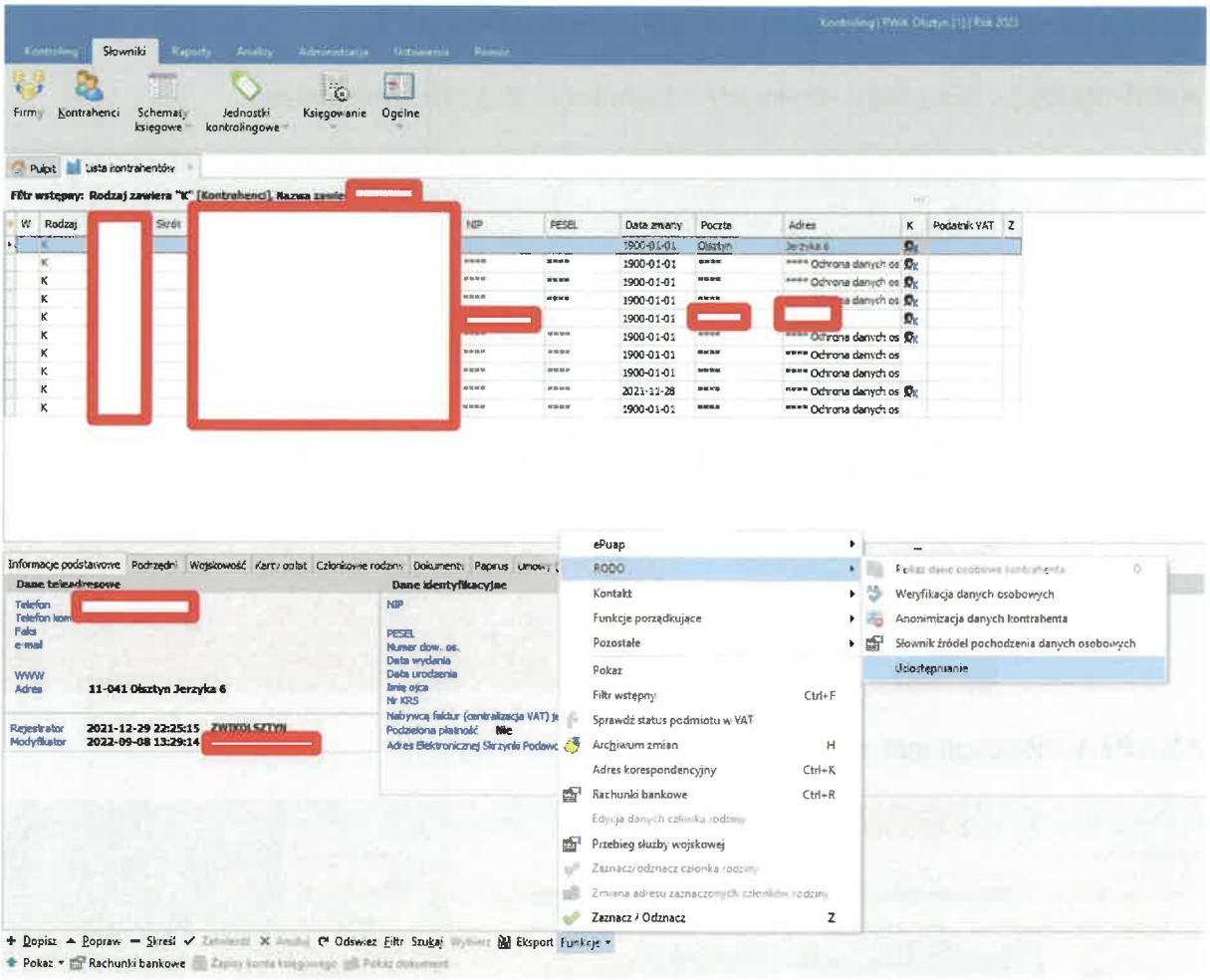
KOM-MEDIA->Kartoteki->Podmioty->Podmioty->Plik>Historia zmian



AXAPTA->Rozrachunki z odbiorcami->Odbiorcy



Dane osobowe w ZSI Papirus



Załącznik nr 1 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Wniosek o nadanie uprawnień do Zintegrowanego Systemu Informatycznego

Zwracam się o nadanie uprawnień obowiązujących od dnia.....

dla pracownika.....
(nazwisko i imię)

zatrudnionego na stanowisku.....w dziale.....
(stanowisko) *(nazwa działu)*

do następujących podsystemów Zintegrowanego Systemu Informatycznego:

	Podsystem[1]	Zakres uprawnień[2]	Uwagi
☐	System Bilingowy		
☐	Obieg Informacji i Dokumentów (OID)		
☐	Zlecenia		
☐	Finanse i Księgowość		
☐	Kasa i Banki		
☐	Środki Trwałe		
☐	Magazyny		
☐	Kadry i Płace		
☐	Rejestry Faktur		
☐	Zaopatrzenie		
☐	Transport		
☐	Remonty		
☐	Kontroling		
☐	eBOK		
☐	Inny[3]		

Sporządził:	Sprawdził:	Zatwierdził:
.....	.....	.....
(Data i podpis)	*(Data i podpis)*	*(Data i podpis)*

[1] Należy zaznaczyć krzyżykiem nazwę podsystemu

[2] W przypadku uprawnień standardowych (np. stanowisko rozliczeń za wodę i ścieki) należy podać nazwę użytkownika posiadającego już konto w podsystemie. W przypadku uprawnień niestandardowych (brak konta w podsystemie, które stanowiłoby szablon uprawnień) należy podać szczegółowy zakres kompetencji np. wystawianie faktur, modyfikacja podmiotów, przeglądanie zleceń

[3] Należy podać nazwę podsystemu

Załącznik nr 2 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Wniosek o usunięcie uprawnień do Zintegrowanego Systemu Informatycznego

Zwracam się o usunięcie uprawnień od dnia..... .....

dla pracownika.....
(nazwisko i imię)

zatrudnionego na stanowisku.....w dziale.....
(stanowisko) *(nazwa działu)*

do następujących podsystemów Zintegrowanego Systemu Informatycznego:

Podsystem[1]	Zakres uprawnień[2]	Uwagi
☐ System Bilingowy		
☐ Obieg Informacji i Dokumentów (OID)		
☐ Zlecenia		
☐ Finanse i Księgowość		
☐ Kasa i Banki		
☐ Środki Trwałe		
☐ Magazyny		
☐ Kadry i Płace		
☐ Rejestry Faktur		
☐ Zaopatrzenie		
☐ Transport		
☐ Remonty		
☐ Kontroling		
☐ eBOK		
☐ Inny[3]		

Sporządził:	Sprawdził:	Zatwierdził:
.....	.....	.....
(Data i podpis)	*(Data i podpis)*	*(Data i podpis)*

[1] Należy zaznaczyć krzyżykiem nazwę podsystemu
[2] W przypadku uprawnień standardowych (np. stanowisko rozliczeń za wodę i ścieki) należy podać nazwę użytkownika posiadającego już konto w podsystemie. W przypadku uprawnień niestandardowych (brak konta w podsystemie, które stanowiłoby szablon uprawnień) należy podać szczegółowy zakres kompetencji np. wystawianie faktur, modyfikacja podmiotów, przeglądanie zleceń
[3] Należy podać nazwę podsystemu

Załącznik nr 2a do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Schemat zatwierdzeń wniosków o nadanie i usunięcie uprawnień do Zintegrowanego Systemu Informatycznego PWiK

1. Nadanie/cofnięcie uprawnień dla pracownika

2. Nadanie/cofnięcie uprawnień dla kierownika/stanowiska samodzielnego

Załącznik nr 3 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Olsztyn, dn. .....

Raport z incydentu bezpieczeństwa informacji

Nr.....

Data i godzina wystąpienia incydentu		
1. Dane osoby, u której stwierdzono incydent bezpieczeństwa informacji	**Imię i nazwisko**	
	Stanowisko	
	Nazwa działu	
	Tel. kontaktowy (służbowy)	
2. Charakterystyka incydentu	**Opis incydentu**	
	Ocena skutków	
3. Opis podjętych czynności w celu usunięcia incydentu bądź zminimalizowania jego skutków dla bezpieczeństwa danych przetwarzanych w PWiK		

Data, podpis osoby, u której stwierdzono incydent bezpieczeństwa informacji

.....

Data, podpis osoby zgłaszającej incydent bezpieczeństwa informacji

.....

Data, podpis osoby wykonującej czynności określone w pkt 3)

.....

Data, podpis Kierownika Działu Informatyki

.....

Załącznik nr 3a do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn
Olsztyn, dn. .....

Raport z naruszenia ochrony danych osobowych

Nr.....

Data i godzina zgłoszenia podejrzenia o wystąpienie naruszenia		**Data i godzina zarejestrowania naruszenia**	
Dane osoby u której stwierdzono naruszenie	**Imię i nazwisko**		
	Stanowisko		
	Nazwa działu		
	Tel. kontaktowy		
Charakterystyka naruszenia	**Opis naruszenia**		
	Ocena skutków		
	Klasyfikacja naruszenia	☐ istnieje ryzyko naruszenia praw i wolności osób fizycznych – wymaga zgłoszenia do organu nadzorczego w terminie max. 72h	
		☐ nie stwierdzono ryzyka naruszenia praw i wolności osób fizycznych	
	Data i godzina zgłoszenia naruszenia do organu nadzorczego		
Opis podjętych czynności w celu usunięcia incydentu bądź zminimalizowania jego skutków dla bezpieczeństwa danych przetwarzanych w PWiK			
	Data i podpis osoby upoważnionej do podjęcia ww. czynności		

Data, podpis osoby, u której stwierdzono naruszenie ochrony danych osobowych

.....
Data, podpis osoby zgłaszającej naruszenie

.....

Data, podpisy Zespołu ds. Ochrony Danych

.....
Data, podpis Administratora Danych

.....

Załącznik nr 4 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 29 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 (RODO) oraz na podstawie Ustawy o Ochronie Danych Osobowych (UODO) niniejszym upoważniam Pana/Panią:

.....	.....
(*Imię, nazwisko Upoważnionego*)	(*Stanowisko*)
.....	.....
(Nazwa działu/stanowiska samodzielnego)	*(Okres ważności upoważnienia od - do)*

do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku. Upoważnienie ma zastosowanie do przetwarzania danych osobowych zawartych w następujących kategoriach danych osobowych oraz wyłącznie we wskazanych celach przetwarzania:

Opis kategorii danych oraz osób, których dane dotyczą	Cel przetwarzania danych	Wykaz zbiorów

Upoważnienie jest ważne do odwołania lub do czasu upłynięcia terminu jego ważności. W przypadku posiadania wcześniej wydanych upoważnień niniejsze upoważnienie odwołuje wszystkie uprzednio wydane upoważnienia.

.....	.....
(Data, podpis Inspektora Ochrony Danych)	*(Data, podpis Administratora Danych)*

Niniejszym potwierdzając własnoręcznym podpisem Upoważniony zobowiązuje się do:

- **przestrzegania zasad określonych w RODO, UODO, Polityce Bezpieczeństwa Informacji i Instrukcji zarządzania systemami informatycznymi oraz danymi w PWiK Sp. z o.o. Olsztyn, procedurach przyjętych przez Spółkę w zakresie przetwarzania i zapewnienia bezpieczeństwa informacji zawierających dane osobowe oraz dane kluczowe do prawidłowego funkcjonowania przedsiębiorstwa;**
- **zachowania wszelkich danych nabytych podczas wypełniania obowiązków pracowniczych w tajemnicy, również po ustaniu zatrudnienia oraz zachowania w tajemnicy informacji o środkach ich zabezpieczenia.**

Upoważniony oświadcza, że zapoznał się z ww. przepisami.

.....
(Data, podpis osoby Upoważnionej)

Załącznik nr 4a do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Niniejszym wnioskuję o odwołanie upoważnienia do przetwarzania danych osobowych dla pracownika:

....
(*Imię, nazwisko Upoważnionego*) (*Stanowisko*)

.....
(Nazwa jednostki organizacyjnej)

w nw. zakresie:

1) ☐ pełnym - wyszczególnionym w druku upoważnienia z dn. .....

2) ☐ wg poniższego wykazu – wyszczególnionego w druku upoważnienia z dn. .....
(w poniższej tabeli należy podać zakres cofnięcia upoważnienia)

Opis kategorii danych oraz osób, których dane dotyczą	Wykaz zbiorów

Powodem wystąpienia o odwołanie upoważnienia do przetwarzania danych osobowych dla ww. pracownika jest:

Data, podpis występującego o odwołanie upoważnienia

.....

Data, podpis Inspektora Ochrony Danych

.....

Data, podpis Administratora Danych

.....

Załącznik nr 5 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH

Na podstawie umowy/zlecenia znak..... niniejszym upoważniam Panią/Pana:

....
(*Imię, nazwisko Upoważnionego*) (*Nazwa jednostki organizacyjnej*)

....
(*Dane kontaktowe*) (*Okres ważności upoważnienia od - do*)

do przetwarzania danych, których dysponentem jest Przedsiębiorstwo Wodociągów i Kanalizacji Sp. z o.o. Olsztyn (PWiK), we wskazanym poniżej zakresie niezbędnym do wypełnienia zobowiązań wobec PWiK.

Zakres danych:

Opis kategorii danych	Cel przetwarzania danych	Wykaz zbiorów

Upoważnienie jest ważne do odwołania lub do czasu upłynięcia terminu jego ważności. W przypadku posiadania wcześniej wydanych upoważnień niniejsze upoważnienie odwołuje wszystkie uprzednio wydane upoważnienia.

....
(*Data, podpis Inspektora Ochrony Danych*) (*Data, podpis Administratora Danych*)

Upoważniony bez zgody Administratora Danych nie ma prawa do powielania, udostępniania ani wykonywania jakichkolwiek innych czynności przetwarzania w innym celu niż wskazany w Upoważnieniu jakichkolwiek informacji, które nabył podczas wypełniania zobowiązania wobec PWiK.

Niniejszym potwierdzając własnoręcznym podpisem Upoważniony zobowiązuje się do przestrzegania zasad określonych w:

- **-Polityce Bezpieczeństwa Informacji i Instrukcji zarządzania systemami informatycznymi oraz danymi obowiązującej w PWiK Sp. z o.o. Olsztyn;**
- **-procedurach przyjętych przez Spółkę w zakresie przetwarzania i zapewnienia bezpieczeństwa informacji zawierających dane osobowe oraz dane kluczowe do prawidłowego funkcjonowania przedsiębiorstwa.**

Upoważniony zobowiązuje się do zachowania w tajemnicy wszelkich danych nabytych podczas wypełniania obowiązków na rzecz PWiK, również po ustaniu zobowiązania oraz do zachowania w tajemnicy informacji o środkach ich zabezpieczenia.

W przypadku przetwarzania danych osobowych, których administratorem jest PWiK Upoważniony oświadcza, że znane mu są przepisy 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 oraz Ustawy o Ochronie Danych Osobowych.

Upoważniony oświadcza, że zapoznał się z ww. przepisami.

.....
(*Data, podpis osoby Upoważnionej*)

Załącznik nr 5a do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH

Niniejszym wnioskuję o odwołanie upoważnienia do przetwarzania danych dla:

....
(*Imię, nazwisko Upoważnionego*) (*Nazwa jednostki organizacyjnej*)

.....
(*Dane kontaktowe*)

w nw. zakresie:

1) ☐ pełnym - wyszczególnionym w druku upoważnienia z dn. .....

2) ☐ wg poniższego wykazu – wyszczególnionego w druku upoważnienia z dn. .....
(w poniższej tabeli należy podać zakres cofnięcia upoważnienia)

Opis kategorii danych	Wykaz zbiorów

Powodem wystąpienia o odwołanie upoważnienia do przetwarzania danych dla ww. osoby jest:

Data, podpis występującego o odwołanie upoważnienia

.....

Data, podpis Inspektora Ochrony Danych

.....

Data, podpis Administratora Danych

.....

Załącznik nr 6 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Olsztyn, dnia .....

Druk zgłoszenia danych do archiwizacji

Nr.....

Zwracam się o archiwizację danych w trybie.....[1] ze stanowiska komputerowego użytkowanego przez .....
w dziale .....w celu.....

Wykaz zbiorów danych objętych archiwizacją:

Lp.	*Rodzaj / Nazwa zbioru[2]*	*(K)atalog/(P)lik[3]*	*Ścieżka do zbioru[4]*

Data, podpis Kierownika Działu

.....

Data, podpis Wnioskodawcy

.....

Opinia Inspektora Ochrony Danych:

[1] Należy podać częstość archiwizacji (np. tydzień, miesiąc, kwartał, rok).
[2] Należy podać rodzaj archiwizowanych danych (np. korespondencja z klientami).
[3] Zgłoszenie archiwizacji dotyczy Katalogu/Pliku. Należy wstawić K lub P.
[4] Wskazanie ścieżki do zbioru w formacie „C:\Users\NazwaUżytkownika\Moje dokumenty"

Załącznik nr 7 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Olsztyn, dnia .....

Wniosek o odtworzenie danych z archiwum

Nr.....

Zwracam się o odtworzenie z archiwum danych ze stanowiska komputerowego użytkowanego przez ..... w dziale .....

w celu .....

Zakres danych do otworzenia:

Data, podpis Kierownika Działu — .....

Data, podpis Wnioskującego — .....

Opinia Inspektora Ochrony Danych:

Data, podpis Inspektora Ochrony Danych — .....

Data, podpis Administratora Danych — .....

Załącznik nr 8 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Olsztyn, dnia .....

Wniosek o wyrażenie zgody na wykorzystywanie nośnika informatycznego

Nr.....

Zwracam się o wyrażenie zgody na wykorzystywanie nośnika informatycznego w postaci pamięci przenośnej na stanowisku komputerowym użytkowanym w dziale.....

przez.....

w celu.....

.....

Data, podpis Kierownika Działu

.....

Rodzaj danych składowanych na nośniku:

Opinia Inspektora Ochrony Danych:	**Charakterystyka Nośnika:**	
	Producent	
	Pojemność	
	S.N.	
Sposób zabezpieczenia nośnika danych (wypełnia pracownik Działu Informatyki):	*Data, podpis pracownika Działu Informatyki*	

Data, podpis Inspektora Ochrony Danych

.....

Data, podpis Prezesa / Dyrektora

.....

Załącznik nr 9 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Informacja o planowanym utworzeniu nowego zbioru danych osobowych

Nazwa Działu/stanowisko	
Nazwa zbioru	
Opis kategorii danych oraz osób, których dane dotyczą	
Podstawa prawna utworzenia zbioru oraz przewidywany termin przetwarzania danych	
Sposób przetwarzania danych w zbiorze (*system informatyczny, przetwarzanie elektroniczne, przetwarzanie w kartotekach papierowych)*	
Zakres przetwarzania danych	
Cel przetwarzania danych	
Kategorie odbiorców, którym dane mogą być przekazywane	
Uzasadnienie potrzeby utworzenia zbioru	

Data, podpis Kierownika Działu/samodzielnego stanowiska	*Data, podpis Inspektora Ochrony Danych*	*Data, podpis Administratora Danych*
.....	.....	.....

Załącznik nr 10 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Wzór umowy powierzenia przetwarzania danych osobowych

zawarta dnia _____ pomiędzy:
(zwana dalej „Umową")

Przedsiębiorstwem Wodociągów i Kanalizacji Sp. z o.o. 10 -218 Olsztyn, ul. Oficerska 16a, zarejestrowanym w Sądzie Rejonowym w Olsztynie VIII Wydział Gospodarczy, KRS: 0000126352, kapitał zakładowy: ..... zł; NIP: 739-040-33-23; Regon: 510620050; posiadającym certyfikat systemu zarządzania jakością (PN-EN ISO 9001:2015), bezpieczeństwa i higieny pracy (PN-ISO 45001:2018) oraz ochrony środowiska (PN-EN ISO 14001:2015)
zwanym w dalszej części umowy **„Administratorem Danych" lub „Administratorem"**
reprezentowanym przez:
Prezesa Zarządu - Wiesława Pancera

a

_____

zwanym w dalszej części umowy **„Podmiotem przetwarzającym"** reprezentowanym przez:

_____

§ 1
Powierzenie przetwarzania danych osobowych

1. Administrator Danych powierza Podmiotowi przetwarzającemu, w trybie 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 (zwanego w dalszej części „Rozporządzeniem"), dane osobowe do przetwarzania, na zasadach i w celu określonym w niniejszej Umowie.
2. Podmiot przetwarzający zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą umową, Rozporządzeniem oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.
3. Podmiot przetwarzający oświadcza, iż stosuje środki bezpieczeństwa spełniające wymogi Rozporządzenia.

§ 2
Zakres i cel przetwarzania danych

1. Podmiot przetwarzający będzie przetwarzał, powierzone na podstawie niniejszej umowy dane osobowe ..... Administratora agregowane w jego Systemie Informatycznym.
2. Zakres przetwarzanych danych:
   a) .....
   b) .....

3. Powierzone przez Administratora Danych dane osobowe będą przetwarzane przez Podmiot przetwarzający wyłącznie w celu realizacji Umowy nr ..... z dnia ..... (zwaną dalej „Umową.....") w zakresie .....

§ 3

Obowiązki podmiotu przetwarzającego

1. Podmiot przetwarzający zobowiązuje się, przy przetwarzaniu powierzonych danych osobowych, do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, o których mowa w art. 32 Rozporządzenia.
2. Podmiot przetwarzający zobowiązuje się dołożyć należytej staranności przy przetwarzaniu powierzonych danych osobowych.
3. Podmiot przetwarzający zobowiązuje się do nadania upoważnień do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone dane w celu realizacji niniejszej Umowy.
4. Podmiot przetwarzający zobowiązuje się zapewnić zachowanie w tajemnicy, (o której mowa w art. 28 ust. 3 pkt b) Rozporządzenia) przetwarzanych danych przez osoby, które upoważnia do przetwarzania danych osobowych w celu realizacji niniejszej Umowy, zarówno w trakcie zatrudnienia ich w Podmiocie przetwarzającym, jak i po jego ustaniu.
5. Podmiot przetwarzający nie jest uprawniony do przetwarzania jakichkolwiek danych osobowych oraz innych danych należących do Administratora w celu innym niż określonym w Umowie, bez jego uprzedniej –pisemnej zgody.
6. Po zakończeniu świadczenia usług związanych z przetwarzaniem danych w zakresie niniejszej Umowy, Podmiot przetwarzający zwraca Administratorowi wszelkie kopie danych osobowych, inne dane należące do Administratora oraz wszelkie dane które zostały wygenerowane przez Podmiot przetwarzający w oparciu o przetwarzane dane osobowe pozyskane od Administratora. Ponadto Podmiot przetwarzający zobowiązany jest do trwałego usunięcia ze wszystkich posiadanych urządzeń danych oraz konfiguracji umożliwiających nawiązanie połączeń zdalnych z Systemem Informatycznym Administratora.
7. W miarę możliwości Podmiot przetwarzający pomaga Administratorowi w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 Rozporządzenia.
8. Podmiot przetwarzający, po stwierdzeniu naruszenia ochrony danych osobowych, bez zbędnej zwłoki zgłasza je Administratorowi w ciągu maksymalnie 24 godzin.

§ 4

Prawo kontroli

1. Administrator danych zgodnie z art. 28 ust. 3 pkt h) Rozporządzenia ma prawo do przeprowadzenia audytów, w tym inspekcji, czy środki zastosowane przez Podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych danych osobowych spełniają postanowienia umowy.

2. Administrator danych realizować będzie prawo kontroli w godzinach pracy Podmiotu przetwarzającego. Jeżeli godziny te nie będą możliwe do ustalenia przez Podmiot przetwarzający, kontrola odbędzie się w godzinach określonych przez Administratora.
3. Podmiot przetwarzający zobowiązuje się do usunięcia uchybień stwierdzonych podczas kontroli w terminie wskazanym przez Administratora Danych nie dłuższym niż 7 dni.
4. Podmiot przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia.

§ 5
Dalsze powierzenie danych do przetwarzania

1. Podmiot przetwarzający może powierzyć dane osobowe objęte niniejszą Umową do dalszego przetwarzania Podwykonawcom jedynie w celu wykonania zadań przewidzianych w Umowie serwisowej po uzyskaniu uprzednio pisemnej zgody Administratora Danych.
2. Podwykonawca, o którym mowa w ust. 1, winien spełniać te same gwarancje i obowiązki jakie zostały nałożone na Podmiot przetwarzający w niniejszej Umowie.
3. Podmiot przetwarzający zaświadcza, że kryteria doboru Podwykonawców do realizacji zadań na rzecz Administratora, dają gwarancję co do przestrzegania przez nich wytycznych Rozporządzenia, przepisów prawa krajowego oraz przyjętych norm i wytycznych zarówno w zakresie ochrony danych osobowych jak i bezpieczeństwa danych teleinformatycznych.
4. Podmiot przetwarzający ponosi pełną odpowiedzialność wobec Administratora za niewywiązanie się ze spoczywających na Podwykonawcy obowiązków ochrony danych.

§ 6
Odpowiedzialność Podmiotu przetwarzającego

1. Podmiot przetwarzający jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z treścią Umowy, a w szczególności za udostępnienie powierzonych do przetwarzania danych osobowych osobom nieupoważnionym.
2. Podmiot przetwarzający zobowiązuje się do niezwłocznego informowania Administratora Danych o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Podmiot przetwarzający (lub Podwykonawców) danych osobowych określonych w Umowie, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Podmiotu przetwarzającego (lub Podwykonawców), a także o wszelkich planowanych, o ile są wiadome, lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania w Podmiocie przetwarzającym (lub Podwykonawców) tych danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Generalnego Inspektora Ochrony Danych Osobowych lub powołanego na mocy Rozporządzenia organu nadzorczego. Niniejszy ustęp dotyczy wyłącznie danych osobowych powierzonych przez Administratora Danych.
3. Podmiot przetwarzający musi informować Administratora o ilości wszczętych bądź prowadzonych przeciwko niemu (lub Podwykonawcom) postępowań sądowych dotyczących naruszenia ochrony danych osobowych, o rozstrzygnięciach zakończonych już postępowań oraz o liczbie naruszeń ochrony danych osobowych, z uwzględnieniem tych które nie zostały zgłoszone do organu nadzorczego.

§ 7
Czas obowiązywania umowy

Niniejsza Umowa obowiązuje od dnia jej zawarcia przez czas obowiązywania Umowy nr/znak .....

§ 8
Rozwiązanie umowy

1. Administrator Danych może rozwiązać niniejszą Umowę ze skutkiem natychmiastowym, gdy Podmiot przetwarzający:
   a) pomimo zobowiązania go do usunięcia uchybień stwierdzonych podczas kontroli nie usunie ich w wyznaczonym terminie;
   b) przetwarza dane osobowe w sposób niezgodny z Umową;
   c) powierzył przetwarzanie danych osobowych innemu podmiotowi bez zgody Administratora Danych;
   d) nie realizuje zapisów § 4 Umowy lub utrudnia bądź uniemożliwia ich realizację przez Administratora Danych.
2. Administrator zastrzega sobie prawo zgłoszenia incydentu naruszenia danych osobowych na zasadach określonych w art. 33 ust. 1 Rozporządzenia na podstawie przesłanek określonych w § 8 ust. 1 Umowy oraz w przypadkach, kiedy czynności podejmowane przez Podmiot przetwarzający (lub Podwykonawcę), będą skutkowały ryzykiem naruszenia praw lub wolności osób fizycznych.

§ 9
Zasady zachowania poufności

1. Podmiot przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji, danych, materiałów, dokumentów i danych osobowych otrzymanych od Administratora Danych i od współpracujących z nim osób oraz danych uzyskanych w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej („dane poufne").
   Podmiot przetwarzający oświadcza, że w związku ze zobowiązaniem do zachowania w tajemnicy danych poufnych nie będą one wykorzystywane, ujawniane ani udostępniane bez pisemnej zgody Administratora Danych w innym celu niż wykonanie Umowy nr/znak .....

§ 10
Postanowienia końcowe

1. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.
2. W sprawach nieuregulowanych zastosowanie będą miały przepisy Kodeksu cywilnego oraz Rozporządzenia.
3. Sądem właściwym dla rozpatrzenia sporów wynikających z niniejszej umowy będzie sąd właściwy dla Administratora Danych.

Administrator danych

Podmiot przetwarzający

Załącznik nr 11 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Olsztyn, dnia .....

Potwierdzenie usunięcia danych z nośnika informatycznego

Nr.....

Zwracam się o usunięcie danych z nośnika informatycznego użytkowanego na stanowisku

.....w dziale.....

przez.....w celu.....

Rodzaj danych składowanych na nośniku:

Data, podpis Kierownika działu/stanowiska samodzielnego

.....

Data, podpis Kierownika Działu Informatyki

.....

Sposób usunięcia danych (wypełnia pracownik Działu Informatyki):

Rodzaj nośnika		*Potwierdzenie usunięcia danych przez pracownika Działu Informatyki (data, podpis)*
S.N.		
Pojemność		.....

Uwaga: druk należy wypełnić 2 egzemplarzach – 1 szt. jako załącznik do zgłoszenia do Komisji Likwidacji, 1 szt. dla Działu Informatyki

Załącznik nr 12 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Wykaz niszczarek zainstalowanych w PWiK

Lp.	Nazwa asortymentu	Ilość [szt.]	Lokalizacja Symbole Działów	Niszczarka może być użytkowana w celu niszczenia dokumentów zawierających dane osobowe (TAK/NIE)
1	Fellowes PS-70	7	RT, PB, PA, ES, RIR	NIE
2	Opus VS 505	4	RT, RUR-M, RZM	NIE
3	HSM Securio B 24 – P-4	4	PB, PA, PK, RWK	TAK
4	HSM Shredstar X 10 – DIN III	4	RTW, RUR-M, VOŚ	NIE
5	ARGO Wallner	5	EP, VJW	NIE
6	Apollo Winer 1000	5	RI, PZK, EF	NIE
7	Rexel P180	1	EF	NIE
8	Cobra S150	3	RIR, PZP, RWK	NIE
9	Ideal 2230	1	EPA	NIE

Załącznik nr 13 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Zasada czystego biurka/stanowiska pracy

1. Zasada czystego biurka/stanowiska pracy jest częścią Instrukcji zarządzania systemami informatycznymi oraz danymi przetwarzanymi w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn i obowiązuje wszystkich pracowników zatrudnionych przez PWiK.
2. Przez pracownika należy rozumieć osobę, o której mowa w art. 2 Kodeksu Pracy, zleceniobiorcę, stażystę, praktykanta, osobę prowadzącą jednoosobową działalność gospodarczą, która współpracuje z PWiK.
3. Pracownik:
   a. zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są mu potrzebne do wykonywanej w danym momencie pracy;
   b. dokumenty zawierające dane osobowe potrzebne do bieżącej pracy, powinny być zabezpieczone przed wglądem do nich osób postronnych/nieuprawnionych do ich przetwarzania;
   c. nie może przetrzymywać na biurku jedzenia oraz picia;
   d. po zakończonej pracy zobowiązany jest do zabezpieczenia dokumentów w zamykanej na klucz szafie, szafce, biurku, itp.;
   e. zobowiązany jest do niszczenia niepotrzebnych dokumentów w najbliższej odpowiedniej niszczarce, w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji.
4. Wykaz niszczarek zawarty jest w Załączniku nr 12.

Załącznik nr 14 do
Instrukcji zarządzania systemem informatycznym oraz danymi przetwarzanymi
w Przedsiębiorstwie Wodociągów i Kanalizacji Sp. z o.o. Olsztyn

Regulamin funkcjonowania monitoringu w Przedsiębiorstwie Wodociągów i Kanalizacji sp. z o.o. w Olsztynie

1. Regulamin określa zasady funkcjonowania systemu monitoringu w Przedsiębiorstwie Wodociągów i Kanalizacji sp. z o.o. w Olsztynie z siedzibą przy ul. Oficerskiej 16a, w tym: systemu monitoringu wizyjnego, systemu monitoringu ruchu, urządzeń IT oraz systemu monitoringu GPS, reguły rejestracji i zapisu informacji oraz sposób ich zabezpieczenia, a także możliwości udostępniania zgromadzonych danych o zdarzeniach.
2. Administratorem danych z systemu monitoringu jest Prezes Zarządu.

PODSTAWA PRAWNA:
-Rozporządzenie 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) (Dz. Urz. UE1119 z 4 maja 2016 r.);
- Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r.
- Kodeks Pracy.

§ 1

1. Celem funkcjonowania systemu monitoringu jest:
a) zapewnienie oraz zwiększenie bezpieczeństwa użytkowników obiektu (ze szczególnym uwzględnieniem pracowników i klientów oraz osób przebywających na terenie obiektu),
b) zapobieganie dewastacjom i kradzieżom mienia;
c) ograniczenie zachowań nagannych, wybryków chuligańskich oraz innych zachowań niepożądanych zagrażających zdrowiu i bezpieczeństwu użytkowników obiektu i osób na nim przebywających;
d) wyjaśnianie sytuacji konfliktowych;
e) ustalanie okoliczności wypadków przy pracy oraz zdarzeń potencjalnie wypadkowych;
f) ograniczanie dostępu do obiektu osób nieuprawnionych i niepożądanych;
g) zwiększenie i zapewnienie ochrony przeciwpożarowej;
h) sprawowanie nadzoru oraz kontroli przez właściciela obiektu;
i) dbanie o efektywność czasu pracy pojazdów Spółki oraz zabezpieczenie ich przed nieuprawnionym wykorzystaniem,
j) świadczenia pomocy zdalnej pracownikom,
h) zapewnienia bezpieczeństwa przetwarzanych danych, przestrzegania zasad rozliczalności oraz przeciwdziałania zagrożeniom, w tym cyberatakom na infrastrukturę informatyczną.

2. Monitoring wizyjny nie stanowi środka kontroli wykonywania pracy przez pracownika.

3. Nie obejmuje się monitoringiem wizyjnym miejsc, które nie są przeznaczone do wykonywania pracy lub przemieszczania się po obiekcie, w tym pomieszczeń sanitarnych, szatni, stołówek lub palarni.

§2

1. System monitoringu funkcjonuje całodobowo.
2. Rejestracji i zapisywaniu na nośniku fizycznym podlega:
- obraz z kamer systemu monitoringu wizyjnego;
- godzina wzbudzenia czujników ruchu oraz ich wyłączenia;
- czas i miejsce przebywania czujnika GPS zamontowanego w pojeździe;
- czas użycia oraz zasoby sprzętu informatycznego, w tym: dane elektroniczne w postaci wykorzystywanych zasobów dyskowych, usługi, procesy, oprogramowanie i urządzenia podłączone do sieci LAN i WAN.

Żaden z systemów monitoringu nie rejestruje dźwięku.
3. Infrastruktura objęta monitoringiem:
- siedziba Spółki przy ul. Oficerskiej 16a;
- Oczyszczalnia Ścieków „Łyna" przy ul. Leśnej;
- Stacje Uzdatniania Wody przy ul.: Wiosennej 1, Pstrowskiego 43, Żeglarskiej 1, Krańcowej 1, Słonecznej 45;
- przepompownie ścieków przy ul. Artyleryjskiej w Olsztynie oraz ul. Jagiełły w Kiełlinach.
4. Siedziba Spółki oraz obszar objęty zasięgiem systemu monitoringu jest oznakowany w widoczny sposób. Wzór informacji w załączeniu.
5. Infrastruktura objęta systemem monitoringu GPS:
- wszystkie pojazdy w Spółce (niezależnie od ich własności).
6. Pojazdy objęte systemem monitoringu GPS są oznakowane w widoczny sposób. Wzór informacji w załączeniu.

§3

1. System monitoringu obiektów Spółki składa się z kamer i czujników ruchu rozmieszczonych wewnątrz i na zewnątrz budynków:
- kamer rejestrujących obraz w kolorze i rozdzielczości umożliwiającej identyfikacje osób, urządzenia i oprogramowania zapisującego obraz oraz czas na nośniku fizycznym oraz pozwalającego na jego odczyt;
- czujników ruchu wykrywających ruch w strefach chronionych, urządzenia i oprogramowania zapisującego czas na nośniku fizycznym oraz pozwalającego na jego odczyt;
-oprogramowania infrastruktury informatycznej tj. sprzętu informatycznego, danych elektronicznych oraz oprogramowania należących do PWiK, urządzeń podłączonych sieci LAN i WAN - w zakresie użytkowania zasobów dyskowych, podejmowanych działań w programach komputerowych, odwiedzanych stron www, pojemności skrzynek e-mail.

2. System monitoringu pojazdów Spółki składa się z urządzeń zamontowanych wewnątrz pojazdu:
- modułów rejestrujących czas i miejsce przebywania pojazdu oraz czujników zbierających informacje o parametrach jazdy, urządzeń umożliwiających nadawanie i odbieranie informacji z systemu drogą radiową, urządzenia i oprogramowania zapisującego dane z systemu na nośniku fizycznym oraz pozwalającego na jego odczyt.

§ 4

1. Odpowiedzialnymi za obsługę oraz prawidłowe funkcjonowanie systemu monitoringu są: Zarządzanie Kryzysowe, kierownik Działu Administracji, pracownicy Działu Transportu, posiadający upoważnienia administratora systemu, którzy mają dostęp do:

a) bezpośredniego podglądu obiektów z kamer w czasie rzeczywistym;

b) bezpośredniego podglądu pojazdów z modułów GPS w czasie rzeczywistym;
c) urządzenia rejestrującego obraz z kamer systemu monitoringu wizyjnego;
d) zapisów z kamer systemu monitoringu wizyjnego;
e) urządzenia rejestrującego dane z systemu monitoringu GPS;
f) zapisów z urządzeń systemu monitoringu GPS.

2. Dostęp do obrazu i zapisu z systemu monitoringu wizyjnego oraz ruchu mają pracownicy firmy ochraniającej obiekty PWIK Sp. z o.o. w Olsztynie oraz firm świadczących usługi konserwacji urządzeń monitorujących, na podstawie umowy powierzenia zawartej ze Spółką.
3. Dostęp do informacji i zapisu z systemu monitoringu GPS mają pracownicy firm świadczących usługi konserwacji urządzeń monitorujących, na podstawie umowy powierzenia zawartej ze Spółką.
4. Dostęp do informacji i zapisu z systemu monitoringu IT mają pracownicy Działu Informatyki.

§5

1. Zapis obrazu z systemów monitoringu może być udostępniony za zgodą Prezesa Zarządu na podstawie pisemnego wniosku, którego wzór stanowi załącznik do niniejszego regulaminu:
a) pracownikom Spółki w ramach czynności wykonywanych w trakcie prowadzenia postępowania wewnętrznego mającego na celu wyjaśnienie okoliczności;
b) wypadków przy pracy;
c) zdarzeń związanych z zachowaniem nagannym, wybrykami chuligańskimi oraz innymi zachowaniami niepożądanymi zagrażającymi zdrowiu i bezpieczeństwu użytkowników obiektu;
d) sytuacji konfliktowych lub związanych z ustalaniem sprawców czynów nagannych (zniszczenia mienia, kradzieże itp.) na terenie należącym do Spółki;
e) właściwym organom (policji, prokuraturze, sądom itp.) w zakresie realizowania przez nie ustawowych zadań.

Kopie nagrania udostępniane są na nośniku elektronicznym i przekazywane za pokwitowaniem.
2. Rejestr udostępnień nagrań z monitoringu prowadzi Inspektor Ochrony Danych.
Okres przechowywania nagrań wynosi 10 dni w przypadku monitoringu wizyjnego. Po tym okresie nagrania są kasowane automatyczne poprzez nadpisanie kolejnymi nagraniami.
3. Osoby, które mają wgląd w informacje zarejestrowane przez systemy monitoringu zostały poinformowane o spoczywającej na nich odpowiedzialności za ochronę danych osobowych oraz posiadają stosowne upoważnienie wydane przez Administratora Danych Osobowych.

§ 6

1. Każda osoba ma prawo dostępu do danych, do żądania sprostowania danych, gdy są niezgodne ze stanem rzeczywistym, a nadto w przypadkach przewidzianych prawem do ich usunięcia lub ograniczenia przetwarzania danych. Wnioski w tych sprawach należy kierować do Administratora.
2. Każda osoba ma prawo do wniesienia skargi do organu nadzorczego.