

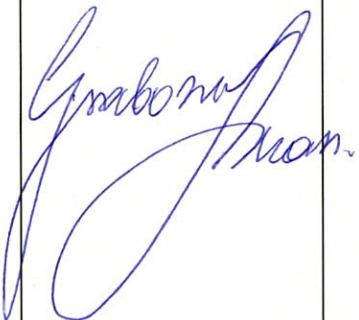


REGULAMIN OCHRONY DANYCH OSOBOWYCH W RPWIK TYCHY S.A.

Wersja:	01/2018
Data wersji:	22.11.2018 r.
Utworzony przez:	mgr inż. Łukasz Grabowski
Zatwierdzony przez:	Krzysztof Zalwowski – Prezes Zarządu
Poziom poufności:	1

Niniejszy regulamin reguluje postępowanie pracowników RPWiK Tychy S.A. w związku z bezpieczeństwem danych osobowych. Opisuje sposób przetwarzania danych w przedsiębiorstwie, prawa podmiotów, których dane dotyczą, a także środki bezpieczeństwa przy pracy z danymi osobowymi.



Tytuł dokumentu	Regulamin ochrony danych osobowych w RPWiK Tychy S.A.		
Opracował	Imię Nazwisko: Łukasz Grabowski	Data: 22.11.2018	Podpis: 
	Pieczętka: Inspektor Ochrony Danych Łukasz Grabowski		
Dokument obowiązuje od dnia podpisania dokumentu przez wskazane powyżej strony			

RPWiK Tychy S. A.
Kierownik Działu Informatyki
i Bezpieczeństwa Informacji
mgr inż. Dariusz Mrowiec

WICEPREZES ZARZĄDU
Dyrektor ds. Technicznych

mgr inż. Marek Dygoń



Spis treści

DEFINICJE.....	4
POSTANOWIENIA OGÓLNE	7
INSPEKTOR OCHRONY DANYCH I ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH	7
OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH.....	8
ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH.....	9
ZGODY I OBOWIĄZEK INFORMACYJNY.....	11
PRAWA PODMIOTÓW DANYCH OSOBOWYCH.....	12
OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNYCH DLA ZAPEWNENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH.....	14
ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI	14
POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH.....	15
PROCEDURY NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRWANIEŃ W SYSTEMIE INFORMATYCZNYM.....	16
POLITYKA HASEŁ.....	16
PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY	18
ZASADY KORZYSTANIA ZE SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ	19
ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET).....	21
ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH.....	21
UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, OPROGRAMOWANIA, NOŚNIKÓW DANYCH.....	22
KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ.....	23
OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM	24
POSTANOWIENIA KOŃCOWE	25



DEFINICJE

Ilekroć w niniejszym regulaminie jest mowa o:

1. Inspektorze Ochrony Danych (lub „IOD”) - rozumie się przez to osobę lub podmiot, wyznaczony przez Administratora, który jest odpowiedzialny za zapewnienie przetwarzania danych zgodnie z odpowiednimi przepisami ustawy i rozporządzenia;
2. Administratorze Danych Osobowych - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, które decydują o celach i środkach przetwarzania danych osobowych. W niniejszym Regulaminie przez Administratora rozumie się RPWiK Tychy S.A. dalej zwaną „Administratorem”;
3. Administratorze Systemów Informatycznych (lub „ASI”) - rozumie się przez to osobę wyznaczoną przez Administratora, która odpowiada za zapewnienie sprawności, należytej konserwacji i wdrażania technicznych zabezpieczeń systemów informatycznych oraz odpowiada za to, aby systemy informatyczne, w których przetwarzane są dane osobowe spełniały wymagania przewidziane ustawą i rozporządzeniem;
4. Danych osobowych (lub „dane”) – rozumie się przez to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
5. Danych genetycznych – rozumie się przez to dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają



- niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
6. Danych biometrycznych – rozumie się przez to dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
 7. Danych dotyczących zdrowia – rozumie się przez to dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
 8. Naruszeniu ochrony danych osobowych – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
 9. Osobie upoważnionej - rozumie się przez to osobę, która otrzymała od Administratora pisemne upoważnienie do przetwarzania danych;
 10. Przetwarzaniu danych – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
 11. Pseudonimizacji – rozumie się przez to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi



-
- i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
12. Rozporządzeniu (lub „RODO”) – rozumie się przez to 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);
13. Upoważnieniu - rozumie się przez to oświadczenie nadawane przez Administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu;
14. Ustawie - rozumie się przez to ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018. poz. 1000);
15. Zbiorze danych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.



POSTANOWIENIA OGÓLNE

§1

W celu zapewnienia ochrony przetwarzanych danych osobowych, zarówno za pomocą systemów informatycznych, jak i w wersji papierowej, Administrator wdrożył Politykę Bezpieczeństwa Informacji (w tym przetwarzania danych osobowych) oraz Instrukcję Zarządzania Systemem Informatycznym. Celem jak najlepszego zapoznania pracowników i współpracowników z zasadami ochrony danych osobowych wdraża się również niniejszy Regulamin, na który składają się postanowienia zawarte w Polityce Bezpieczeństwa oraz Instrukcji Zarządzania, przydatne dla każdej osoby przetwarzającej dane podczas codziennego wykonywania obowiązków zawodowych.

INSPEKTOR OCHRONY DANYCH

I ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

§2

1. Administrator może wyznaczyć Inspektora Ochrony Danych (IOD), który jest odpowiedzialny za nadzorowanie przetwarzania danych w przedsiębiorstwie, edukację w zakresie przetwarzania danych osobowych, przygotowywanie i opiniowanie dokumentacji dotyczącej przetwarzania danych.
2. IOD powinien podlegać jedynie najwyższemu kierownictwu przedsiębiorstwa.
3. Administrator może wyznaczyć co najmniej jednego zastępcę IOD.
4. Zastępca IOD wykonuje wszystkie obowiązki należące do zakresu obowiązków IOD podczas jego nieobecności.

§3

Administrator może wyznaczyć Administratatora Systemów Informatycznych (ASI).



§4

W przypadku niewyznaczenia IOD lub ASI, za zapewnienie należytego przestrzegania zasad ochrony danych osobowych odpowiada Administrator.

§5

1. W przypadku powzięcia jakichkolwiek wątpliwości, co do ewentualnej zgodności z prawem planowanych działań w zakresie przetwarzania danych, należy zwrócić się do IOD z wnioskiem o rozstrzygnięcie wątpliwości.
2. Przed udzieleniem przez IOD odpowiedzi w przedmiocie istniejących wątpliwości niedozwolone jest zbieranie danych osobowych i ich utrwalanie, a w przypadku posiadania już danych osobowych, których wątpliwość dotyczy, należy, do czasu rozstrzygnięcia wątpliwości, wstrzymać wszystkie działania na danych osobowych, co do których istnieją wątpliwości, czy są prawnie uzasadnione.

OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

§6

1. Administrator zobowiązany jest nadać upoważnienie do przetwarzania danych każdej osobie, która do przetwarzania danych będzie dopuszczona.
2. Upoważnienie do przetwarzania danych osobowych wygasza z chwilą upływu terminu wypowiedzenia lub rozwiązania umowy zawartej przez Administratora z osobą, której zostało nadane lub w przypadku, gdy zostało nadane na czas określony, z upływem czasu na jaki zostało nadane.
3. Osoba upoważniona przez Administratora nie ma prawa do nadawania dalszych upoważnień, chyba że upoważnienie do przetwarzania danych osobowych nadane przez Administratora zawiera upoważnienie do nadawania dalszych upoważnień.

§7



1. Każdy, kto przetwarza dane osobowe, zobowiązany jest zachować w tajemnicy dane osobowe, do których posiada dostęp zarówno zamierzony jak i przypadkowy, sposoby zabezpieczenia danych, jak również wszelkie informacje, które powiązały w czasie przetwarzania danych. Obowiązek zachowania danych w tajemnicy jest bezterminowy.
2. Podczas przetwarzania danych należy zachować szczególną ostrożność i podjąć wszelkie możliwe środki umożliwiające ich zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.
3. Należy dochować należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się, czy przesyłane za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.
4. W przypadku przesyłania za pomocą środków komunikacji elektronicznej zestawień, spisów, czy innych dokumentów zawierających dane osobowe, przesyłany dokument należy zaszyfrować, a hasło przesłać, w miarę możliwości, innym środkiem komunikacji elektronicznej.

ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

§8

Dane osobowe muszą być:

1. przetwarzane zgodnie z prawem, rzetельnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
2. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”);
3. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);



4. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
5. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania”);
6. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

§9

Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

1. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
2. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
3. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze;
4. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
5. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi;



6. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności, gdy osoba, której dane dotyczą, jest dzieckiem.

ZGODY I OBOWIĄZEK INFORMACYJNY

§10

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, Administrator przechowuje tę zgodę w formie dokumentu, aby być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
2. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę jest przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
3. Wyrażenie zgody, stanowiące podstawę do przetwarzania danych, przez osobę, której dane dotyczą jest dobrowolnym, konkretnym, świadomym i jednoznacznym okazaniem woli w formie oświadczenia pisemnego lub elektronicznego.
4. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody jest równie łatwe jak jej wyrażenie.

§11

Zgodnie z RODO, Administrator Danych Osobowych, w momencie pozyskiwania informacji od osoby, której dane dotyczą, podaje wzór klauzuli informacyjnej oraz:

1. swoją tożsamość, pełną nazwę i dane kontaktowe;
2. dane kontaktowe IOD (jeżeli został powołany);
3. cel i podstawy przetwarzania danych osobowych;



4. prawnie uzasadniony interes Administratora Danych (jeżeli takowy istnieje);
5. informację o odbiorcach danych osobowych lub o kategoriach odbiorców;
6. informację o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej (jeśli taki zamiar istnieje);
7. okres przechowywania danych;
8. informację o prawach podmiotu (dostęp do danych, ich przenoszenie, sprzeciw, sprostowanie, usunięcie etc.);
9. informację czy podanie danych to wymóg ustawowy lub umowny lub warunek zawarcia umowy oraz konsekwencje niepodania danych;
10. informację o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (w tym o zasadach podejmowania, znaczeniach i konsekwencjach).

PRAWA PODMIOTÓW DANYCH OSOBOWYCH

§12

1. Zgodnie z brzmieniem Rozporządzenia, podmiotom danych przysługują następujące prawa:
 - a. prawo do bycia zapomnianym / prawo do usunięcia danych – podmiot danych ma w każdej chwili prawo zażądać od Administratora niezwłocznego usunięcia jego danych osobowych;
 - b. prawo do sprostowania danych – osoba, której dane dotyczą, ma prawo żądać od Administratora Danych, niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe;
 - c. prawo do ograniczenia przetwarzania – osoba, której dane dotyczą, ma prawo żądać od Administratora Danych ograniczenia przetwarzania jej danych osobowych;
 - d. prawo do przenoszenia danych – osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie,



nadającym się do odczytu maszynowego, dane osobowe jej dotyczące oraz ma prawo przesyłać te dane osobowe innemu Administratorowi bez przeszkód ze strony Administratora, któremu dostarczono te dane osobowe. Przeniesienie danych jest możliwe, jeżeli przetwarzanie odbywało się na podstawie zgody lub wykonania umowy;

- e. prawo do niepodlegania przez konkretną osobę fizyczną decyzjom wywołującym wobec niej skutki prawne lub podobnie wpływającym na nią w inny istotny sposób, a opartym na przetwarzaniu jej danych wyłącznie w sposób zautomatyzowany (za pomocą systemów informatycznych), w tym za pomocą profilowania danych. Przepis ten przewiduje również wyjątki od tej zasady, m.in., gdy takie przetwarzanie danych opiera się na wyraźnie udzielonej zgodzie przez osobę, której one dotyczą.
2. Administrator zobowiązuje się przestrzegać powyższe prawa.
3. Realizacja wspomnianych praw przysługujących podmiotowi danych jest bezpłatna.
4. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Administrator pobiera adekwatną w stosunku do nakładu pracy opłatę.
5. Żądanie podmiotów danych powinno być przekazane w formie pisemnej, elektronicznej lub ustnej.
6. W przypadku zgłoszenia należy wypełnić wzór zgłoszenia żądania, który znajduje się w Załączniku.



OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH, NIEZBĘDNYCH DLA ZAPEWNENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH

§13

1. Wszelkie dokumenty zawierające dane osobowe przechowywane są, w miarę możliwości, w szafach lub pomieszczeniach zamkanych na klucz.
2. Osoba będąca dysponentem kluczy jest zobowiązana nie przekazywać kluczy do budynków i pomieszczeń w których przetwarzane są dane, osobom nieuprawnionym, a ponadto zobowiązana jest przedsięwziąć działania celem wykluczenia ryzyka ich utraty.
3. Osoba, która utraciła posiadane klucze do pomieszczeń Administratora, w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność IOD lub Administratorowi.
4. IOD lub Administrator podejmują wszelkie niezbędne środki techniczne organizacyjne w celu zabezpieczenia pomieszczenia, do którego klucze utracono.

ŚRODKI BEZPIECZEŃSTWA STOSOWANE PODCZAS PRACY Z DANYMI

§14

1. Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach.
2. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki lub za pośrednictwem firmy zajmującej się niszczeniem dokumentów, po zawarciu umowy o powierzeniu przetwarzania danych osobowych.
3. Każdy dokument zawierający dane, a nieużyteczny, niszczy się niezwłocznie.
4. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopiowane bądź skanowane wyjmowane są z urządzenia



wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstających na skutek kopiowania bądź skanowania.

5. Przebywanie osób trzecich w obszarze, w którym przetwarzane są dane jest dopuszczalne za zgodą Administratora lub w obecności osoby upoważnionej.

POSTĘPOWANIE W RAZIE ZAISTNIENIA ZAGROŻENIA DLA BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH LUB NARUSZENIA ZASAD PRZETWARZANIA DANYCH OSOBOWYCH

§15

1. W przypadku podejrzenia naruszenia zasad bezpieczeństwa danych osobowych lub naruszenia zabezpieczeń stosowanych przez Administratora dla ochrony przetwarzanych danych osobowych należy niezwłocznie zawiadomić IOD.
2. W przypadku zagrożenia, naruszenia lub incydentu w zakresie ochrony danych osobowych należy postępować zgodnie z Załącznikiem nr 23 do Polityki Bezpieczeństwa Informacji RPWiK Tychy S.A. – Procedurą zarządzania incydentami związanymi z Bezpieczeństwem Informacji.
3. Przy dokonywaniu sprawdzenia IOD przysługują prawa wskazane w Załączniku nr 23, w tym m.in. prawo do:
 - a. utrwalenia danych z systemu informatycznego służącego do przetwarzania lub zabezpieczania na informatycznym nośniku danych lub dokonania wydruku tych danych;
 - b. odebrania wyjaśnień osoby, której czynności objęto sprawdzeniem;
 - c. sporządzeniu kopii otrzymanego dokumentu;
 - d. sporządzeniu kopii obrazu wyświetlnego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych.



4. Jeżeli IOD nie został wyznaczony, Administrator, w przypadku, o którym mowa w ust. 1 obowiązany jest przeprowadzić postępowanie wyjaśniające i ustalające skutki oraz przyczyny naruszenia lub narażenia na naruszenie zasad bezpieczeństwa, w sposób odpowiadający czynnościom podejmowanym przez IOD w przypadku sprawdzenia doraźnego.

PROCEDURY NADAWANIA UPRAWNIĘ DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRWANIĘ W SYSTEMIE INFORMATYCZNYM

§16

Użytkownikowi systemu informatycznego zostaje nadany dostęp po:

1. zapoznaniu się z Polityką Bezpieczeństwa Informacji (PBI) RPWiK Tychy S.A.;
2. zapoznaniu się ze wszystkimi Załącznikami do PBI;
3. podpisaniu oświadczenia o zapoznaniu się z niniejszą dokumentacją przetwarzania danych osobowych;
4. podpisaniu oświadczenia o zachowaniu informacji (w tym danych osobowych), do których użytkownik będzie miał dostęp podczas wykonywania obowiązków służbowych lub zobowiązań umownych oraz środków ich zabezpieczania w tajemnicy (również po ustaniu łączącej strony umowy), w tym powstrzymanie się od wykorzystywania ich w celach pozasłużbowych;
5. otrzymaniu upoważnienia do przetwarzania danych osobowych.

POLITYKA HASEŁ

§17



1. Każdy użytkownik systemu informatycznego musi posiadać unikalny identyfikator i wprowadzone przez siebie hasło autoryzujące jego osobę w systemie informatycznym.
2. Hasła użytkowników lub inne dane uwierzytelniające podlegają szczególnej ochronie.
3. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła (prócz pierwszego hasła do systemu nadawanego przez Administratora Systemu Informatycznego) i jego przechowywanie.
4. Każdy użytkownik posiadający dostęp do systemów informatycznych Administratora jest zobowiązany do:
 - a. zachowania w poufności wszystkich swoich haseł lub innych danych uwierzytelniających wykorzystanych do pracy w systemie informatycznym;
 - b. niezwłocznej zmiany haseł w przypadkach zaistnienia podejrzenia lub rzeczywistego ujawnienia;
 - c. niezwłocznej zmiany hasła tymczasowego, przekazanego przez Administratora Systemu Informatycznego;
 - d. poinformowania Administratora Systemu Informatycznego oraz IOD o podejrzeniu lub rzeczywistym ujawnieniu hasła;
 - e. stosowania haseł o minimalnej długości 8 znaków, zawierających kombinację małych i dużych liter oraz cyfr lub znaków specjalnych,
 - f. stosowania haseł nie posiadających w swojej strukturze części loginu,
 - g. stosowania haseł nie będących zbliżonymi do poprzednich (np. RPWiK2018 - RPWiK2019),
 - h. zmiany wykorzystywanych haseł nie rzadziej niż raz na 90 dni.
5. Hasła zachowują swoją poufność również po ustaniu ich użyteczności
6. Zabronione jest:
 - a. zapisywanie haseł w sposób jawnym i umieszczania ich w miejscach dostępnych dla innych osób;



- b. stosowanie haseł opartych na skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących danej osoby, np. imiona, numery telefonów, daty urodzenia itp.;
- c. używanie tych samych haseł w różnych systemach operacyjnych i aplikacjach;
- d. udostępnianie haseł innym użytkownikom;
- e. przeprowadzanie prób łamania haseł;
- f. wpisywanie haseł „na stałe” (np. w skryptach logowania) oraz wykorzystywania opcji auto - zapamiętywania haseł (np. w przeglądarkach internetowych).

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA, PROWADZENIA I ZAKOŃCZENIA PRACY

§18

1. Rozpoczęcie pracy w systemie informatycznym następuje po wprowadzeniu unikalnego identyfikatora i hasła.
2. Zawieszenie pracy w systemie informatycznym, tj. brak wykonywania jakichkolwiek czynności przez okres 10 minut powoduje automatyczne uruchomienie systemowego wygaszacza ekranu blokowanego hasłem. Zastosowanie powyższego mechanizmu nie zwalnia użytkownika z obowiązku każdorazowego blokowania ekranu wygaszaczem chronionym hasłem po odejściu od stanowiska.
3. Przed zakończeniem pracy należy upewnić się, czy dane zostały zapisane, aby uniknąć utraty danych.
4. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego przetwarzającego dane osobowe i z systemu operacyjnego,



zabezpieczyć nośniki informacji (elektroniczne i papierowe) oraz wyłączyć komputer.

5. W sytuacji, gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa), w sposób uniemożliwiający wgląd w wyświetlana treść.
6. Użytkownik systemu informatycznego przetwarzającego dane osobowe niezwłocznie powiadamia Administratora systemu w przypadku, gdy:
 - a. wygląd systemu, sposób jego działania, zakres danych lub sposób ich przedstawienia przez system informatyczny odbiega od standardowego stanu uznawanego za typowy dla danego systemu informatycznego;
 - b. otrzymał wgląd w szerszy zakres funkcjonalności programów, do których ma dostęp.

ZASADY KORZYSTANIA Z SŁUŻBOWEJ POCZTY ELEKTRONICZNEJ

§19

1. Użytkownikowi zostaje nadany dedykowany adres skrzynki poczty elektronicznej działający w domenie Administratora Danych Osobowych.
2. Informacja o służbowym adresie skrzynki pocztowej jest jawną i dostępną powszechnie. Może być dostępna na łamach witryny internetowej Administratora w postaci książki adresowej.
3. Nadany użytkownikowi adres skrzynki poczty elektronicznej służy wyłącznie do realizacji celów służbowych lub umownych. Korespondencja realizowana drogą elektroniczną z wykorzystaniem systemów informatycznych Administratora danych podlega rejestraniu i może być monitorowana. Informacje przesyłane za pośrednictwem sieci Administratora Danych Osobowych (w tym do i z Internetu), nie stanowią własności prywatnej użytkownika.



4. Wszelka korespondencja elektroniczna, niezwiązana z działalnością Administratora Danych Osobowych, powinna być prowadzona przez prywatną skrzynkę poczty elektronicznej użytkownika.
5. Korzystanie z systemu poczty elektronicznej dla celów prywatnych nie może wpływać na wydajność systemu poczty elektronicznej.
6. Użytkownicy dokonujący wysyłki korespondencji masowej poza organizację, zobowiązani są do ukrywania odbiorów w kopii (pole BCC lub UDW).
7. Zabronione jest:
 - a. wysyłanie materiałów służbowych na konta prywatne (np. celem pracy nad dokumentami w domu);
 - b. wykorzystywanie systemu poczty elektronicznej do działań mogących zaszkodzić wizerunkowi Administratora Danych;
 - c. odbieranie wiadomości z nieznanych źródeł;
 - d. otwieranie załączników z plikami samorozpakowującymi się bądź wykonalnymi typu .exe, .com, itp.;
 - e. przesyłanie pocztą elektroniczną plików wykonywalnych typu: .bat, .com, .exe, plików multimedialnych oraz plików graficznych;
 - f. ukrywanie lub dokonywanie zmian tożsamości nadawcy;
 - g. czytanie, usuwanie, kopiowanie lub zmiana zawartości skrynek pocztowych innego użytkownika;
 - h. odpowiadanie na niezamówione wiadomości reklamowe lub wysyłane łańcuszki oraz na inne formy wymiany danych określanych spamem;
 - i. posługiwanie się adresem służbowym e-mail w celu rejestrowania się na stronach handlowych, informacyjnych, chat'ach lub forach dyskusyjnych, które nie dotyczą zakresu wykonywanej pracy lub obowiązków umownych;
 - j. wykorzystywanie poczty elektronicznej do reklamy prywatnych towarów lub usług, działalności handlowo-usługowej innej niż wynikającej z potrzeb Administratora lub do poszukiwania dodatkowego zatrudnienia.



ZASADY KORZYSTANIA Z SIECI PUBLICZNEJ (INTERNET)

§20

1. Zdalne korzystanie z systemów informatycznych poprzez sieć publiczną może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
2. Zdalny dostęp do serwerów w celach administracyjnych może mieć miejsce po zastosowaniu systemu uwierzytelniania użytkownika i szyfrowanego kanału transmisji.
3. Dostęp użytkowników do sieci publicznej (Internet) powinien być ograniczony do niezbędnego minimum na danym stanowisku pracy.
4. Na stanowiskach komputerowych, na których zbiera się, przetwarza lub przechowuje dane osobowe, a które podłączone są do sieci publicznej (Internet) zabrania się korzystać ze stron internetowych, portali społecznościowych, platform zakupowych i innych serwisów, których odwiedzanie nie jest związane i potrzebne do wykonania obowiązków służbowych, a które może spowodować zagrożenie naruszenia tych danych.
5. Wprowadza się całkowite ograniczenia w dostępie do treści uznanych za pornograficzne, rasistowskie, traktujące o przemocy, przestępstwach, jak również do protokołów umożliwiających wymianę plików w sieciach z naruszeniem przepisów prawa.

ZASADY POSTĘPOWANIA Z NOŚNIKAMI ELEKTRONICZNYMI ORAZ VPN PODCZAS PRACY POZA OBSZAREM PRZETWARZANIA DANYCH

§21

Każdy użytkownik wymiennych nośników elektronicznych oraz użytkownicy zdalnych dostępów do sieci służbowej Administratora (VPN) oraz użytkownicy elektronicznych



kart dostępu ponoszą całkowitą odpowiedzialność za powierzony do użytkowania sprzęt oraz są zobowiązani do stosowania się do poniższych zasad:

1. zabrania się pozostawiania bez opieki, w miejscach publicznych nośników wymiennych przetwarzających informacje Administratora;
2. komputery przenośne należy przewozić jako bagaż podręczny i w miarę możliwości je maskować;
3. użytkownik, wykonując czynności zawodowe lub umowne w domu, powinien zadbać o należyte zabezpieczenie powierzonego sprzętu oraz dostępu do informacji przed nieautoryzowanym dostępem osób trzecich;
4. zabrania się spożywania posiłków i picia podczas pracy z powierzonym sprzętem;
5. zabrania się udostępniania osobom trzecim nośników elektronicznych informacji oraz powierzonego sprzętu będącego własnością Administratora;
6. w przypadku utraty nośnika elektronicznego lub sprzętu komputerowego należy ten fakt bezzwłocznie zgłosić do bezpośredniego przełożonego lub Administratora Systemu Informatycznego. Bezpośredni przełożony lub Administrator Systemu Informatycznego bezzwłocznie zgłaszały taki fakt do IOD (jeśli jest powołany) lub do Administratora Danych Osobowych, ponieważ zgubienie nośnika przetwarzającego dane może wiązać się z utratą poufności informacji chronionych przez Administratora;
7. problemy wynikające z nieprawidłowego funkcjonowania sprzętu komputerowego należy zgłaszać Administratorowi Systemu Informatycznego.

UŻYTKOWANIE SPRZĘTU KOMPUTEROWEGO, ORPOGRAMOWANIA, NOŚNIKÓW DANYCH

§22

1. Do sprzętu komputerowego zalicza się między innymi:
 - a. komputery stacjonarne;



- b. komputery przenośne;
 - c. tablety;
 - d. smartphony;
 - e. drukarki;
 - f. modemy;
 - g. monitory;
 - h. routery;
 - i. sprzęt dostarczony razem z wyżej wymienionym sprzętem lub zakupiony oddzielnie, a w szczególności, zasilacze, torby, klawiatury, myszki komputerowe;
2. Administrator Systemu Informatycznego odpowiada za poprawne działanie sprzętu komputerowego. Czynność tą Administrator Systemu Informatycznego może wykonywać poprzez pracowników lub współpracowników Administratora, lub poprzez podmioty zewnętrzne.
 3. W przypadku niepoprawnego i niezgodnego z przeznaczeniem użytkowania przez użytkownika sprzętu komputerowego, Administrator Systemu Informatycznego informuje o powyższym IOD.
 4. Użytkownik jest zobowiązany do dbałości o sprzęt oraz oprogramowanie, a także odpowiedzialny za zabezpieczenie go przed używaniem przez osoby nieuprawnione oraz do ochrony przed kradzieżą lub zagubieniem.
 5. Użytkownik nie może samodzielnie zmieniać konfiguracji przekazanego sprzętu komputerowego oraz instalować lub usuwać oprogramowania, w tym nie może używać na przekazanym sprzęcie prywatnego oprogramowania.

KORZYSTANIE Z URZĄDZEŃ KOMUNIKACJI GŁOSOWEJ, FAKSOWEJ I WIZYJNEJ

§23



1. Każdy użytkownik zobowiązany jest do przestrzegania zakazu prowadzenia rozmów, podczas których może dochodzić do wymiany informacji danych osobowych lub informacji poufnych u Administratora, jeśli rozmowy te odbywają się w miejscach publicznych, otwartych pomieszczeniach biurowych lub takich, które nie gwarantują zachowania poufności rozmów.
2. Odczytanie wiadomości z faksów, automatycznych sekretarek lub systemów poczty głosowej powinno być możliwe wyłącznie po wprowadzeniu indywidualnego hasła. W przypadku braku takiej możliwości urządzenia należy zabezpieczyć przed dostępem osób nieuprawnionych.
3. Zabronione jest wykorzystywanie domyślnych („fabrycznych”) haseł dla ww. urządzeń.
4. Przekazywanie za pomocą urządzeń faksowych dokumentów zawierających dane osobowe wrażliwe lub informacje poufne u Administratora. Danych jest zabronione.
5. Drukarki nie mogą być pozostawione bez kontroli, jeśli są wykorzystywane (lub wkrótce będą) do drukowania dokumentów zawierających informacje wrażliwe.

OCHRONA PRZED SZKODLIWYM OPROGRAMOWANIEM

§24

1. Zidentyfikowanymi obszarami systemu informatycznego Administratora, narażonymi na ingerencję wirusów oraz innego szkodliwego oprogramowania, są dyski twardye lub karty pamięci urządzeń, pamięć RAM oraz elektroniczne nośniki informacji.
2. Drogą przedostania się wirusów lub szkodliwego oprogramowania może być sieć publiczna, wewnętrzna sieć teleinformatyczna lub elektroniczne nośniki informacji.



3. Stacje robocze, komputery przenośne oraz serwery objęte są ochroną w czasie rzeczywistym za pomocą oprogramowania antywirusowego oraz zapory (firewall), zapewniających integralność zasobów przechowywanych i przetwarzanych w systemie informatycznym Administratora.
4. Za prawidłowe funkcjonowanie oprogramowania antywirusowego odpowiada Administrator Systemu Informatycznego.

POSTANOWIENIA KOŃCOWE

§25

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub niewykonanie zobowiązania w przypadku stosunku prawnego, innego niż stosunek pracy.
2. W sprawach nieuregulowanych w Regulaminie lub Polityce Bezpieczeństwa Informacji mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy.

Kontakt do Inspektora Ochrony Danych (IOD):

Imię i nazwisko: Łukasz Grabowski

Adres e-mail: odo@rpwik.tychy.pl

Telefon: 48 883 942 060

Kontakt do Administratora Systemów Informatycznych (ASI):

Imię i nazwisko: Dariusz Mrowiec

Adres e-mail: d.mrowiec@rpwik.tychy.pl



Telefon: 32 3257-089

Kontakt do Administratora Systemów Informatycznych (ASI):

Imię i nazwisko: Jerzy Trzepała

Adres e-mail: j.trzepala@rpwik.tychy.pl

Telefon: 32 3257-088