

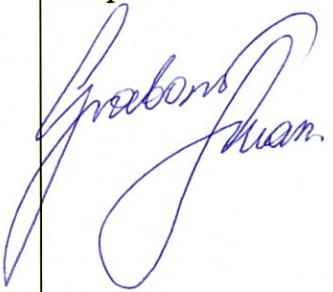
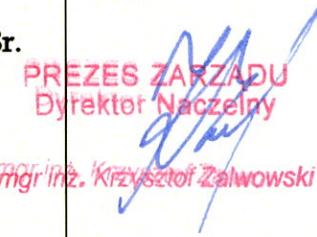


POLITYKA BEZPIECZEŃSTWA INFORMACJI W RPWIK TYCHY S.A.

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

Listopad 2018



Tytuł dokumentu	Polityka Bezpieczeństwa Informacji RPWiK Tychy S.A.		
Opracował	Imię Nazwisko: Łukasz Grabowski Pieczętka: Inspektor Ochrony Danych Łukasz Grabowski	Data: 22.11.2018r.	Podpis: 
Zatwierdził	Imię Nazwisko: Krzysztof Zalwowski Pieczętka:	Data: 22.11.2018r.	Podpis: PREZES ZARZĄDU Dyrektor Naczelnny <i>mgr inż. Krzysztof Zalwowski</i> 
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



Historia zmian

Data	Versja	Utworzona przez	Opis zmiany
22.11.2018	01/2018	Łukasz Grabowski	Podstawowy szablon dokumentu

wersja 01/2018 z 22.11.2018 r.

Strona 3 z 65



Spis treści

1.	Postanowienia ogólne	6
2.	Definicje.....	9
3.	Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO)	14
4.	Kontekst organizacji.....	20
5.	Polityka bezpieczeństwa informacji.....	23
6.	Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe	26
7.	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych – Rejestr zbiorów danych osobowych.....	27
8.	Sposób przepływu danych pomiędzy poszczególnymi systemami.....	28
9.	Odpowiedzialności i uprawnienia.....	29
9.1.	Kontrola dostępu.....	33
10.	Przetwarzanie danych.....	35
11.	Osoby upoważnione do przetwarzania danych osobowych oraz ewidencja osób upoważnionych	37
12.	Plan sprawdeń oraz dokonywanie sprawdeń.....	38
13.	Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych	40



14.	Praca zdalna.....	42
15.	Bezpieczeństwo zasobów ludzkich	43
15.1.	Etap wyboru pracownika.....	43
15.2.	Zatrudnienie	45
15.3.	Zakończenie lub zmiana zatrudnienia	47
16.	Zarządzanie zasobami	49
17.	Procedura postępowania z incydentami ochrony danych osobowych, zarządzanie ciągłością działania, kontakt z organami władzy.....	51
18.	Zarządzanie ryzykiem utraty bezpieczeństwa danych osobowych	53
19.	Podsumowanie	60
20.	Postanowienia końcowe	62



1. Postanowienia ogólne

Realizując obowiązki wynikające z przepisów dotyczących ochrony danych osobowych, Rejonowe Przedsiębiorstwo Wodociągów i Kanalizacji w Tychach Spółka Akcyjna (dalej: „RPWiK Tychy S.A.”) spełnienia wymagania chroniące prywatność i godność każdego pracownika firmy oraz jej kontrahentów i dostawców.

Sposób przetwarzania danych osobowych w RPWiK Tychy S.A. oraz środki techniczne i organizacyjne, zapewniające ochronę przetwarzanych danych osobowych, ujęte zostały zbiorczo w niniejszym dokumencie określającym **Politykę Bezpieczeństwa Informacji** (dalej: PBI). PBI wraz z jej wszystkimi załącznikami należy rozumieć jako zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji, zarówno wewnętrz jak i na zewnątrz organizacji. Zwraca ona uwagę na konsekwencje, jakie mogą ponosić osoby przekraczające określone granice oraz procedury postępowania dla zapobiegania i minimalizowania skutków zagrożeń.

Celem opracowania Polityki Bezpieczeństwa Informacji jest określenie zasad ochrony danych osobowych przetwarzanych w RPWiK Tychy S.A., a co za tym idzie organizacyjne, fizyczne i logiczne, zabezpieczenie posiadanych danych osobowych. Zasady określone w Polityce Bezpieczeństwa Informacji mają zastosowanie do wszystkich osób, które zostały upoważnione do przetwarzania danych osobowych, niezależnie od formy ich zatrudnienia. Utrzymanie bezpieczeństwa przetwarzanych przez RPWiK Tychy S.A. danych osobowych oraz informacji, rozumiane jest jako zapewnienie ich poufności, integralności i dostępności oraz rozliczalności, na jak najwyższym, możliwym do uzyskania w danym czasie, poziomie. Pośrednim celem PBI jest systematyczne edukowanie użytkowników systemu ochrony danych osobowych. Jednocześnie, polityka ta zawiera jasną deklarację zaangażowania kierownictwa firmy i wyznacza jej procesowe podejście do Zarządzania Bezpieczeństwem Informacji.



Polityka Bezpieczeństwa Informacji zapewnia:

- **poufność** – informacja nie jest udostępniana lub ujawniana nieupoważnionym osobom, podmiotom i procesom;
- **integralność** – dane nie zostają zmienione lub zniszczone w sposób nieautoryzowany;
- **dostępność** – istnieje możliwość wykorzystania ich na żądanie, w założonym czasie, przez autoryzowany podmiot;
- **rozliczalność** – możliwość jednoznacznego przypisania działań poszczególnym osobom;
- **autentyczność** – zapewnienie, że tożsamość podmiotu lub zasobu jest zgodna z zadeklarowaną;
- **niezaprzecjalność** – uczestnictwo w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie jest niepodważalne;
- **niezawodność** – zamierzone zachowania i skutki są spójne.

Niniejszy dokument został:

- zatwierdzony (opatrzony stosownym podpisem) przez najwyższe kierownictwo;
- opublikowany i podany do wiadomości wszystkim pracownikom (wraz z załącznikami dotyczącymi konkretnych stanowisk i funkcji pracowniczych) oraz upoważnionym stronom zewnętrznym, we właściwej, dostępnej i zrozumiałej formie.

Wszyscy pracownicy oraz podmioty zewnętrzne zobowiązani są przestrzegać Zasad Bezpieczeństwa Informacji określonych w Polityce Bezpieczeństwa Informacji, a także współpracować we wdrażaniu oraz doskonaleniu procedur ochrony informacji, poprzez m.in. zgłoszenie uwag i opiniowanie zastosowanych rozwiązań.

Odpowiedzialność za realizację ochrony danych ponoszą wszyscy użytkownicy, proporcjonalnie do nadanych uprawnień.

wersja 01/2018 z 22.11.2018 r.

Strona 7 z 65



Polityka Bezpieczeństwa Informacji została opracowana na podstawie:

- Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
- Normy PN-EN ISO/IEC 27001 dotyczącej zarządzania bezpieczeństwem informacji,
- Normy PN-ISO/IEC 17799 dotyczącej praktycznych zasad zarządzania bezpieczeństwem informacji,
- Normy PN-EN ISO/IEC 27002 dotyczącej praktycznych zasad zabezpieczania informacji,
- Normy PN-EN ISO/IEC 27005 dotyczącej zarządzania ryzykiem w bezpieczeństwie informacji,
- Normy PN-ISO 31000 dotyczącej zarządzania ryzykiem,
- Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r. poz. 1000),
- Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne, służące do przetwarzania danych osobowych (Dz. U. 2004 poz. 1024).



2. Definicje

Użyte w niniejszej dokumentacji przetwarzania danych osobowych definicje i pojęcia, są wspólne dla wszystkich pozostałych dokumentów, które zostały przyjęte przez Administratora w zakresie ochrony danych osobowych.

Tabela 1. Zbiór definicji i pojęć używanych w dokumencie

Administrator danych	Organ, jednostka organizacyjna, podmiot lub osoba, którzy decydują o celach i środkach przetwarzania danych osobowych. W niniejszej dokumentacji przez Administratora danych rozumie się RPWiK Tychy S.A.
Akceptowanie ryzyka	Decyzja, aby zaakceptować ryzyko [źródło: PKN-ISO Guide 73].
Analiza ryzyka	Systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka [źródło PKN-ISO Guide 73].
Bezpieczeństwo danych osobowych	Zachowanie poufności, integralności i dostępności danych osobowych oraz odporności systemów i usług przetwarzania.
Dane osobowe (lub „dane”)	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby.
Dokumentacja przetwarzania danych osobowych	Polityka bezpieczeństwa przetwarzania danych osobowych oraz instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.
Dostępność	Właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu [źródło ISO/IEC 27000].
Działanie korygujące	Działanie w celu wyeliminowania przyczyny wykrytej niezgodności lub innej niepożądanej sytuacji [źródło: ISO 9000].



Działanie zapobiegawcze	Działanie w celu wyeliminowania przyczyny potencjalnej niezgodności lub innej potencjalnej sytuacji niepożądanej [źródło: ISO 9000].
Grupa zasobów	Zbiór zasobów rozpatrywanych wspólnie ze względu na podobny charakter i funkcjonalność.
Incydent związany z bezpieczeństwem danych osobowych	Pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, związanych z bezpieczeństwem danych osobowych, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych, w tym zgodności z RODO, i zagrażają bezpieczeństwu danych osobowych.
Informowanie o ryzyku	Wymiana lub dzielenie się informacjami o ryzyku między decydentami, a innymi uczestnikami [źródło: PKN-ISO Guide 73].
Integralność	Właściwość polegająca na zapewnieniu dokładności i kompletności zasobów [źródło: ISO/IEC 27000].
Kryteria ryzyka	Odniesienia, względem których szacowana jest istotność ryzyka [źródło: PKN-ISO Guide 73].
Monitorowanie ryzyka	Ciągłe sprawdzanie, nadzorowanie, krytyczne obserwowanie lub określanie stanu, prowadzone w celu zidentyfikowania zmian w zakresie wymaganego lub oczekiwanej poziomu skuteczności [źródło: PN-ISO 31000].
Ocena ryzyka	Proces porównywania oszacowanego ryzyka, z określonymi kryteriami, w celu określenia znaczenia ryzyka [źródło: PKN-ISO Guide 73].
Osoba fizyczna możliwa do zidentyfikowania	Osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności poprzez powołanie się na numer identyfikacyjny lub specyficzny czynnik/czynniki określające



	jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.
Osoba upoważniona	Osoba, która otrzymała od Administratora upoważnienie do przetwarzania danych.
Podatność	Słabość zasobu lub zabezpieczenia, która może być wykorzystana przez zagrożenie [źródło: ISO/IEC 27000].
Postępowanie z ryzykiem	Proces wyboru i wdrażania środków modyfikujących ryzyko [źródło: PKN-ISO Guide 73].
Poufność	Właściwość polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom [źródło: ISO/IEC 27000].
Przegląd	Działanie podejmowane w celu określenia przydatności, adekwatności oraz skuteczności przedmiotu rozważań do osiągnięcia ustalonych celów [źródło: PN-ISO 31000].
Przetwarzanie danych	Jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te operacje, które wykonuje się w systemach informatycznych.
RODO	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.
RPWiK Tychy S.A.	W tym dokumencie jest rozumiane jako Rejonowe Przedsiębiorstwo Wodociągów i Kanalizacji Spółka Akcyjna, zlokalizowane przy ul. Sadowej 4 w Tychach.



Ryzyko	Kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji [źródło: PKN-ISO Guide 73].
Ryzyko bezpieczeństwa danych osobowych	Potencjalna sytuacja, w której określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, powodując w ten sposób szkodę oraz w rezultacie negatywne / niepożądane konsekwencje.
Ryzyko akceptowalne	Poziom ryzyka uznany za zgodny z wymaganymi RODO i bezpieczny dla realizacji celów związanych z przetwarzaniem danych.
Ryzyko szczegółowe	Ryzyko pozostające po zastosowaniu działań określonych w postępowaniu z ryzykiem [źródło: PN-ISO 31000].
Skuteczność	Stopień, w jakim zaplanowane działania są realizowane, a zaplanowane rezultaty osiągnięte [źródło: ISO 9000].
Skutek	Negatywna zmiana w odniesieniu do poziomu osiągania zgodności z RODO.
Szacowanie ryzyka	Całościowy proces analizy i oceny ryzyka [źródło: PKN-ISO Guide 73].
Upoważnienie	Oświadczenie nadawane przez Administratora, wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane we wskazanym zakresie.
Urząd Ochrony Danych Osobowych (UODO)	Organ nadzorczy zajmujący się ochroną danych osobowych.
Właściciel zasobu	Osoba lub podmiot, mające zatwierdzoną kierowniczą odpowiedzialność w organizacji, za: nadzorowanie produkcji, rozwój, utrzymanie, korzystanie i bezpieczeństwo zasobów. Pojęcie to nie oznacza, że osoba ta rzeczywiście posiada jakiekolwiek prawa własności do zasobu.



Zabezpieczenie	Środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną [źródło: ISO/IEC 27000].
Załączniki	Wzory dokumentów. Administrator może przedmiotowe wzory zastąpić wydrukami z systemów komputerowych lub innymi dokumentami o treści zgodnej z przepisami powszechnie obowiązującego prawa.
Zbiór danych	Każdy posiadający strukturę zestaw danych, o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony, czy podzielony funkcjonalnie.
Zasoby	Wszystko, co ma wartość dla każdego, kto zajmuje się przetwarzaniem informacji umożliwiających identyfikację osoby fizycznej [źródło: ISO/IEC 29134:2017].
Zagrożenie	Potencjalna przyczyna niepożądanego incydentu, który może wywołać naruszenie praw lub wolności osób fizycznych.
Zarządzanie ryzykiem	Skoordynowane działania kierowania i zarządzania organizacją, z uwzględnieniem ryzyka [źródło: PKN-ISO Guide 73].
Zasada "need to know"	Zasada wiedzy koniecznej, tzn. udzielanie tylko informacji potrzebnych do realizacji powierzonych zadań.
Zdarzenie	Wystąpienie szczególnego zbioru okoliczności [źródło: PKN-ISO Guide 73].
Zdarzenie związane z bezpieczeństwem danych osobowych	Określony stan wskazujący na możliwość naruszenia bezpieczeństwa danych osobowych, błąd zabezpieczenia lub zajścia nieznanej dotychczas sytuacji, która może być związana z bezpieczeństwem danych osobowych.

Źródło: Opracowanie własne



3. Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO)

Parlament Europejski i Rada przyjęły 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 w skrócie RODO. W polskim porządku prawnym jest ono stosowane bezpośrednio, od dnia 25 maja 2018 r., bez konieczności implementowania go ustawą.

Po wejściu w życie RODO przetwarzanie danych osobowych odbywa się w nowym otoczeniu prawnym. W związku z tym, że wprowadzane zmiany niosą za sobą daleko idące konsekwencje prawne i biznesowe, warto cyklicznie wykonać audyt, a następnie przyjąć w firmie szereg zmian, w tym organizacyjnych i proceduralnych.

Celem niniejszego wprowadzenia jest jak najbardziej przystępne i syntetyczne objaśnienie zmian w dziedzinie ochrony danych osobowych, w taki sposób, aby każdy pracownik firmy posiadał podstawową wiedzę o tym, w jaki sposób wprowadzić i przestrzegać zasady RODO.

We wprowadzeniu zostaną zasygnalizowane następujące kwestie:

- zgody na przetwarzanie danych osobowych,
- obowiązek informacyjny,
- Inspektor Ochrony Danych (IOD),
- nowe praw podmiotów, których dane są przetwarzane,
- rejestr czynności przetwarzania danych,
- zgłoszanie naruszeń ochrony danych osobowych,
- powierzanie przetwarzania danych,
- kodeksy i certyfikaty zgodności przetwarzania danych.

W świetle zmian wprowadzanych przez RODO, przedsiębiorcy (czyli administratorzy danych) w pierwszej kolejności powinni dokonać audytu zbiorów



danych osobowych i podstaw prawnych stosowanych w ich organizacjach, do przetwarzania danych.

Z uwagi na to, że jedną z najczęściej stosowanych podstaw przetwarzania danych jest zgoda osoby, której dane dotyczą (czyli podmiotu danych), RODO szczególnie odnosi się do kształtu zgody i jej założeń.

Zgodnie z RODO zgoda osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych, w formie ustnej, pisemnej lub elektronicznej. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu, bądź zachowaniu, które w danym kontekście jasno wskazuje, że podmiot danych zaakceptował proponowane przetwarzanie jego danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania, nie mogą być traktowane jako wyrażenie zgody.

Dla osób fizycznych przetwarzanie ich danych osobowych powinno być jasne, przejrzyste i rzetelne. W celu realizacji wymienionych przymiotów legalnego przetwarzania danych, podmiot powinien posiadać wiedzę w przedmiocie tego kto i po co przetwarza jego dane osobowe. Jednym z narzędzi zapewniających legalność przetwarzania jest obowiązek informacyjny, tj. zakres informacji, które administrator danych powinien przekazać podmiotowi danych, w związku z przetwarzaniem jego danych osobowych.

Zgodnie z RODO, administrator danych, w przypadku pozyskiwania informacji od osoby, której one dotyczą, jest zobowiązany do podania:

- swojej tożsamości (pełnej nazwy) i danych kontaktowych;
- danych kontaktowych Inspektora Ochrony Danych (IOD), jeżeli został powołany;
- celu i podstawy przetwarzania danych osobowych;



- prawnie uzasadnionego interesu/-ów administratora danych (jeżeli takowy istnieje);
- informacji o odbiorcach danych osobowych lub o kategoriach odbiorców;
- informacji o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;
- okresu przechowywania danych;
- informacji o prawach podmiotu (dostęp do danych, ich przenoszenie, sprzeciw, sprostowanie, usunięcie etc.);
- informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (w tym o zasadach podejmowania, znaczeniach i konsekwencjach).

Regulacje RODO wprowadzają instytucję Inspektora Ochrony Danych, dalej zwanego także IOD, którego powołanie w określonych sytuacjach jest obowiązkowe dla administratora danych.

IOD powinien podlegać jedynie najwyższemu kierownictwu przedsiębiorstwa (np. Zarząowi). Nie musi być on pracownikiem administratora danych. Funkcja ta może zostać powierzona osobie zewnętrznej, na podstawie umowy o świadczenie usług (outsourcing).

W ramach swojej działalności IOD powinien być właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych w przedsiębiorstwie, wspierany przez administratora w wypełnianiu zadań, poprzez zapewnienie mu zasobów niezbędnych do wykonania tych zadań, np. powołania odpowiedniego zespołu wsparcia IOD oraz dostęp do danych osobowych i operacji przetwarzania.

Zgodnie z brzmieniem rozporządzenia, od 25 maja 2018 r. podmioty danych zostają wyposażone w takie uprawnienia, jak:

- prawo do bycia zapomnianym – podmiot danych ma prawo zażądać od administratora niezwłocznego usunięcia jego danych osobowych, jeżeli zajdzie



jedna z enumeratywnie wymienionych okoliczności z art. 17 ust. 1 pkt. a-f RODO;

- prawo do sprostowania danych – podmiot ma prawo żądać od administratora danych niezwłocznego sprostowania dotyczących jego danych osobowych, które są nieprawidłowe;
- prawo do ograniczenia przetwarzania – osoba, której dane dotyczą, ma prawo żądania od administratora danych ograniczenia przetwarzania jej danych osobowych, w przypadkach wymienionych w art. 18 ust. 1 pkt. a-d RODO;
- 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 odbywa się na podstawie zgody lub wykonania umowy czy też odbywa się w sposób zautomatyzowany (np. *scoring* kredytowy);
- 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.

Co do zasady, realizacja wspomnianych praw przysługujących podmiotowi danych, powinna być bezpłatna. Jednak, jeśli żądania osoby, której dane dotyczą, wymagają od administratora dużych nakładów finansowych i czasowych, są ewidentnie nieuzasadnione, lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może pobrać opłatę, adekwatną do trudności przedsięwzięcia związanego z żądaniem.

wersja 01/2018 z 22.11.2018 r.

Strona 17 z 65



Administrator powinien zapewnić podmiotom danych możliwość skorzystania ze swoich praw, również drogą elektroniczną, szczególnie kiedy przetwarzanie danych odbywa się elektronicznie.

Administrator danych, bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania żądania, powinien odnieść się do wniosku osoby, której dane dotyczą, w zakresie realizacji przysługujących jej praw. Jeżeli administrator nie spełni żądania podmiotu danych, powinien podać tego przyczyny.

Celem ułatwienia administratorom wypełniania obowiązków związanych z przetwarzaniem danych osobowych i jednoczesnym ograniczeniem biurokracji w tej materii, RODO wprowadza zupełnie nowe rozwiązanie, które zastępuje obowiązek rejestracji zbiorów danych – rejestr czynności przetwarzania danych osobowych.

Obowiązek posiadania takiego rejestru spoczywa zarówno na administratorze danych, jak i na podmiocie, któremu powierzono przetwarzanie danych.

Rejestr może być prowadzony w formie pisemnej lub elektronicznej. Administrator lub podmiot przetwarzający dane ma obowiązek udostępnić rejestr na każde żądanie organu nadzorczego. Organ nadzorczy dokonuje kontroli tych rejestrów w celu monitorowania operacji przetwarzania.

Obowiązek posiadania rejestru dotyczy podmiotów zatrudniających powyżej 250 osób, jednakowoż sugerowane jest implementowanie rejestru u każdego administratora danych, choćby dla celów ewentualnej kontroli przez organ nadzorczy.

„Rejestr czynności przetwarzania danych osobowych” stanowi załącznik nr 1 do Polityki Bezpieczeństwa Informacji przedsiębiorstwa.

RODO przewiduje również obowiązek zgłoszenia naruszeń ochrony danych osobowych do organu nadzorczego. O naruszeniu administrator powinien poinformować organ niezwłocznie, nie później niż 72 godziny od wykrycia naruszenia.

Zgłoszenie musi zawierać informacje wskazane w art. 33 ust. 3 pkt. 2-d RODO, czyli m.in. charakter naruszenia, wskazywać kategorię i przybliżoną liczbę osób, których dotyczy naruszenie, możliwe konsekwencje czy dane kontaktowe IOD. Jeżeli naruszenie może



powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki powinien również zawiadomić o naruszeniu osobę, której dane dotyczą.

Z uwagi na nieprzerwanie rozwijający się segment usług outsourcingowych i coraz powszechniejsze korzystanie z tych usług przez administratorów danych, konieczne stało się bardziej precyzyjne uregulowanie współpracy pomiędzy administratorem danych osobowych, a podmiotem, na rzecz którego dochodzi do powierzenia przetwarzania danych.

Regulacje RODO zawierają obligatoryjne elementy umowy powierzenia przetwarzania danych, która zgodnie z nowymi przepisami powinna zawierać: przedmiot powierzenia, czas powierzenia, charakter powierzenia, cel powierzenia, rodzaj danych osobowych podlegających powierzeniu, kategorie osób, których powierzane dane dotyczą, obowiązki i prawa administratora (prawo dokonywania kontroli warunków przetwarzania danych osobowych/obowiązek cyklicznego sprawdzania merytorycznej poprawności powierzanych danych osobowych), obowiązki procesora (m.in. zobowiązanie do zachowania poufności w zakresie przetwarzanych danych, podjęcie środków bezpieczeństwa w stosunku do przetwarzanych danych, legalne korzystanie z usług innego podmiotu przetwarzającego). „Wzór umowy powierzenia danych” stanowi załącznik nr 2 do Polityki Bezpieczeństwa Informacji.

Dodatkowym dokumentem jest „Klauzula poufności informacji wraz z deklaracją poufności”, który stanowi załącznik nr 3 do Polityki Bezpieczeństwa Informacji przedsiębiorstwa.



4. Kontekst organizacji

Niniejszy dokument wprowadza w RPWiK Tychy S.A. nowy system – System Zarządzania Bezpieczeństwem Informacji (SZBI, ISMS), który będzie ustanowiony, wdrożony, utrzymywany i ciągle doskonalony na każdym szczeblu organizacji. System ten oparty jest na podejściu procesowym zgodnie z cyklem Deminga, tj.: Planuj – Wykonuj – Sprawdzaj –Działaj (ang. *Plan – Do – Check – Act*, tj.: *PDCA*) przedstawionym na rysunku 1.

1. Ustalenie zewnętrznych i wewnętrznych kwestii, które oddziałują na zdolność osiągnięcia oczekiwanej rezultatu w SZBI oraz zrozumienie potrzeb i oczekiwania zainteresowanych stron jest kluczowe dla określenia zakresu SZBI. Kontekst zewnętrzny obejmuje ogólne powiązania firmy z otoczeniem – zobowiązania zawarte w umowach z klientami. Natomiast kontekst wewnętrzny obejmuje środowisko wewnętrzne, tzn. obejmuje aspekty organizacyjne i prawne funkcjonowania firmy – ład i strukturę organizacyjną, polityki i procedury opisujące realizację procesów, zasoby ludzkie i jego kompetencje (wiedza), poziom kultury organizacyjnej, świadomość pracowników (w tym w zakresie bezpieczeństwa), przepływy informacji (formy komunikacji), przyjęte normy, wytyczne, stosowane technologie oraz relacje z podwykonawcami i innymi stronami wewnętrz firm.

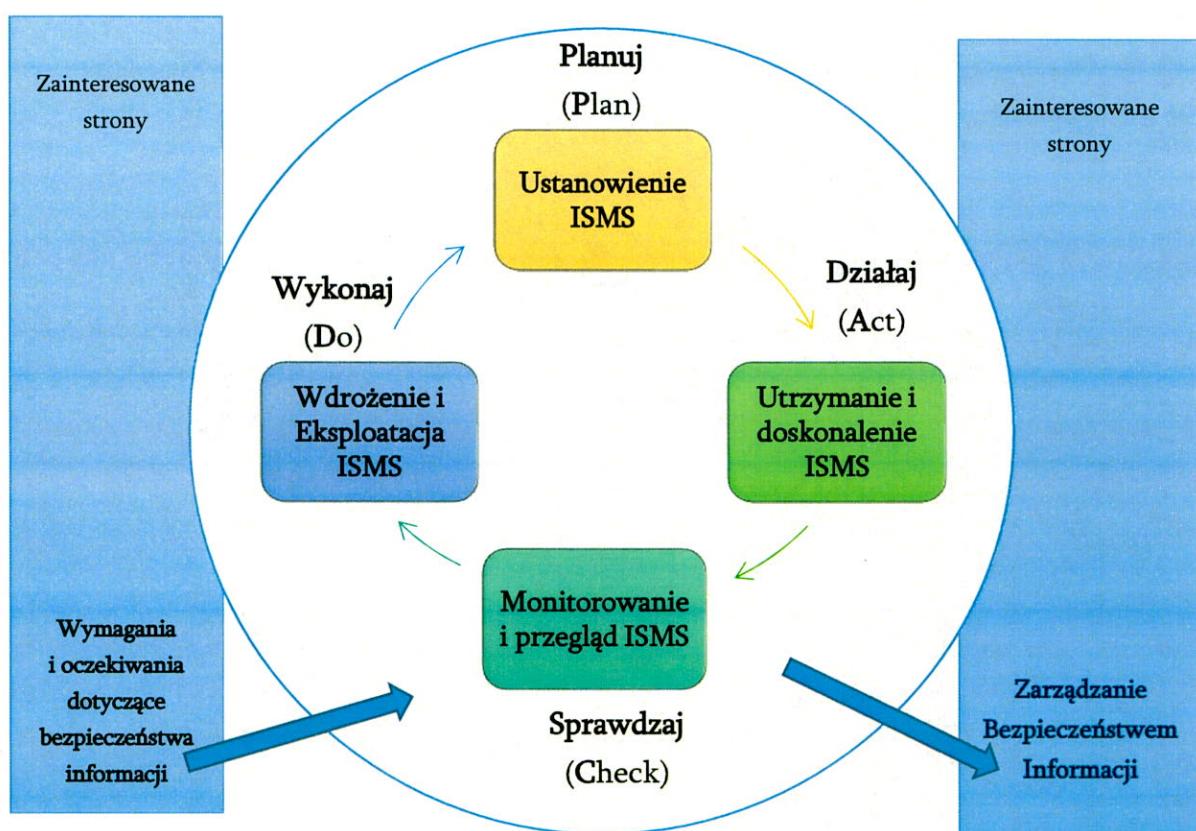
Zainteresowane strony w przypadku RPWiK Tychy S.A. stanowią przede wszystkim:

- klienci, którzy wymagają od firmy ochrony przekazanych informacji;
- właściciele (Zarząd), którzy wymagają, aby zarządzanie informacją odbywało się w sposób kontrolowany, bez naruszania bezpieczeństwa przedsiębiorstwa oraz podmiotów zainteresowanych, a co za tym idzie nie spowodowało strat finansowych firmy, mając na uwadze potrzebę szkolenia pracowników, którzy w przypadku wystąpienia sytuacji kryzysowej ograniczą jej negatywny wpływ na przedsiębiorstwo;
- pracownicy, wymagający ochrony ich danych osobowych, zwłaszcza danych szczególnych kategorii, dotyczących m.in. ich stanu zdrowia, wraz z oczekiwaniem

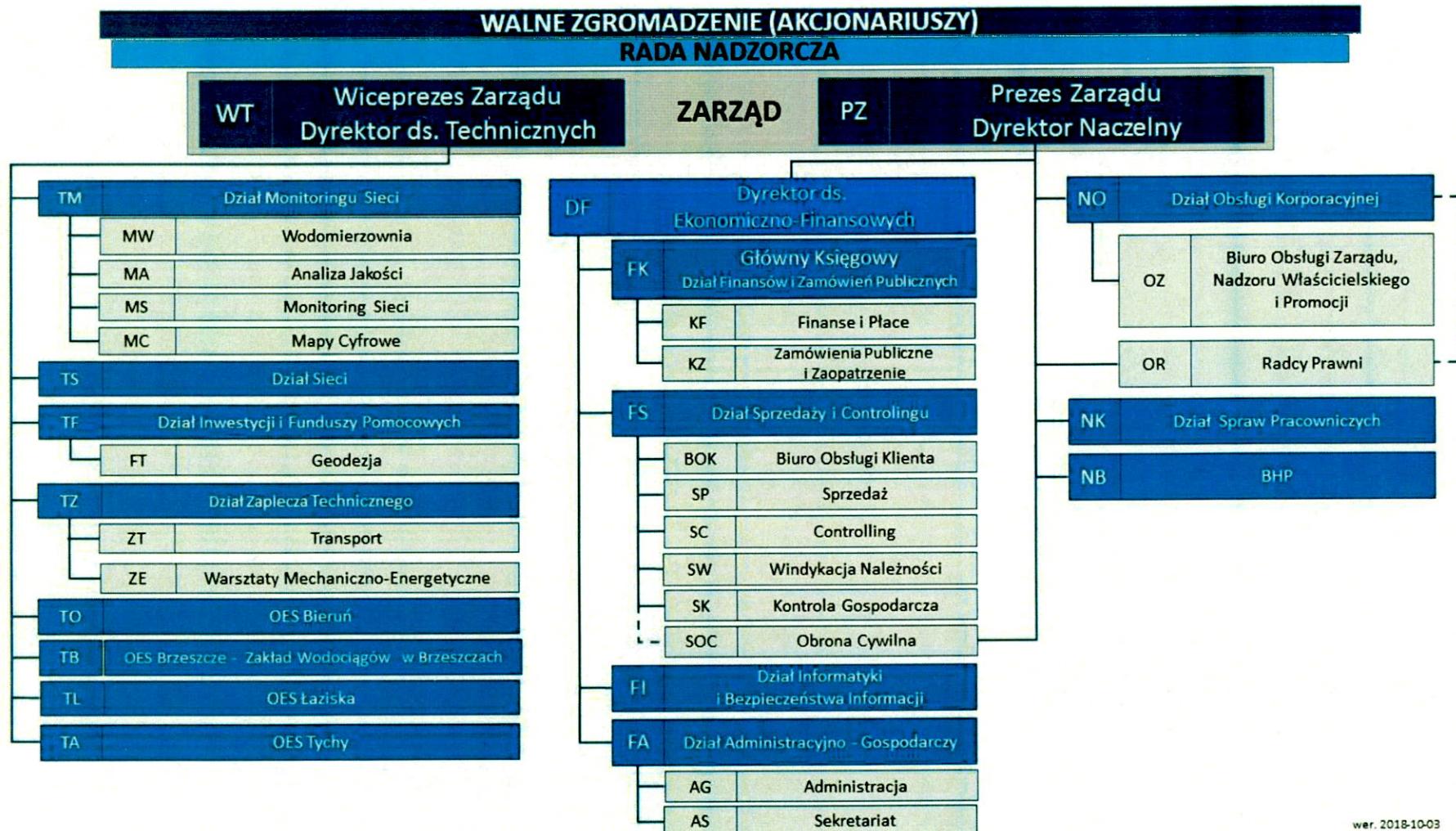
na odpowiednie przeszkolenie i narzędzia, dzięki którym będą mogli skutecznie i bezpiecznie zarządzać informacją;

- ustawodawcy, którzy wymagają przestrzegania, mających zastosowanie, wymagań prawnych.

W związku z powyższym ustanawia się zakres Systemu Zarządzania Bezpieczeństwem Informacji obejmujący całą strukturę organizacyjną RPWiK Tychy S.A. przedstawioną na rysunku 2.



Rysunek 1. Model PDCA stosowany w procesach systemu zarządzania bezpieczeństwem informacji ISMS (ang. *Information Security Management System*) [źródło: opracowanie własne]



Rysunek 2. Schemat organizacyjny przedsiębiorstwa



5. Polityka bezpieczeństwa informacji

Polityka Bezpieczeństwa Informacji RPWiK Tychy S.A. przedstawiona jest w formie dokumentu, wraz z załącznikami, opublikowanego i dostępnego dla wszystkich pracowników, wykonawców lub podwykonawców firmy. Dokument ten podlega ciągłej aktualizacji i udoskonalaniu, w celu dostosowania go do zmieniających się warunków działalności przedsiębiorstwa.

PBI przedsiębiorstwa została przygotowana w celu:

- ograniczenia możliwości nieautoryzowanego udostępnienia informacji oraz danych osobowych przetwarzanych przez pracowników lub kontrahentów;
- ograniczenia naruszeń przepisów prawa oraz innych regulacji;
- zapobiegania obniżenia reputacji RPWiK Tychy S.A.;
- ograniczenia strat finansowych;
- ograniczenia zakłóceń występujących w przedsiębiorstwie.

Polityka Bezpieczeństwa Informacji przedsiębiorstwa, w odniesieniu do ochrony danych osobowych zakłada:

- zbieranie danych osobowych w jasno określonych celach;
- przetwarzanie danych osobowych, które jest zgodne tylko z wcześniej ustalonymi celami;
- przechowywanie danych osobowych przez określony czas, przeznaczony na realizację poszczególnych zadań;
- przedstawienie danych osobowych w sposób sformalizowany, umożliwiający łatwą identyfikację;
- przetwarzanie danych osobowych w sposób zgodny z obowiązującymi przepisami prawa.



Niniejsza Polityka Bezpieczeństwa Informacji zawiera zestaw załączników, określających szczegółowo procedury postępowania z danymi osobowymi w RPWiK Tychy.

S.A. Zestaw ten składa się z następujących załączników:

- 1) Rejestr i wykazy prowadzone przez Administratora Danych Osobowych oraz Inspektora Ochrony Danych;
- 2) Wzór umowy powierzenia danych osobowych;
- 3) Klauzula poufności informacji wraz z deklaracją poufności;
- 4) Sposób przepływu danych pomiędzy poszczególnymi systemami;
- 5) Regulamin ochrony danych osobowych;
- 6) Procedura nadawania uprawnień do przetwarzania danych osobowych;
- 7) Upoważnienie do przetwarzania danych osobowych;
- 8) Polityka pracy zdalnej oraz systemu informatycznego:
 - 8a) Raport z naruszenia ochrony danych osobowych;
- 9) Procedura przewozu dokumentów:
 - 9a) Wzór raportu z naruszenia ochrony danych w trakcie transportu;
- 10) Kwestionariusz osobowy dla osoby ubiegającej się o zatrudnienie;
- 11) Klauzula informacyjna przy formularzu rekrutacyjnym na stronie internetowej pracodawcy;
- 12) Procedura postępowania z danymi osobowymi podczas rekrutacji i w trakcie zatrudnienia;
- 13) Zgoda pracownika na przetwarzanie danych osobowych;
- 14) Kwestionariusz osobowy dla pracownika;
- 15) Zgoda na przetwarzanie danych biometrycznych pracownika;
- 16) Informacja o działającym na terenie zakładu systemu monitoringu;
- 17) Zgoda pracownika na przetwarzanie danych w postaci wizerunku;
- 18) Zgoda na przetwarzanie danych osobowych pracownika tymczasowego;
- 19) Formularz realizacji żądań podmiotu danych;
- 20) Informacja dla pracownika o dokumentacji pracowniczej;



- 21) Polityka Bezpieczeństwa Teleinformatycznego;
- 22) Schemat nadawania uprawnień IT;
- 23) Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji:
 - 23a) Katalog zagrożeń i incydentów zagrażających bezpieczeństwu informacji;
 - 23b) Zgłoszenie naruszenia danych osobowych organowi nadzorcemu;
 - 23c) Raport z naruszenia ochrony danych;
 - 23d) Protokół zabezpieczenia materiału dowodowego;
- 24) Zawiadomienie o zastosowaniu kary porządkowej;
- 25) Oświadczenie o zapoznaniu się z przepisami bezpieczeństwa danych osobowych;
- 26) Plan odtworzenia po katastrofie.



6. Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Przy wyznaczaniu pomieszczeń przeznaczonych do przechowywania danych osobowych należy brać pod uwagę miejsca przetwarzania:

- dokumentacji papierowej,
- stacji komputerowych,
- serwerów,
- przenośnych nośników danych,
- macierzy dyskowych,
- sejfów,
- innych urządzeń przetwarzających dane osobowe.

Powyższe warunki spełniają również miejsca składowania wszelkiego rodzaju uszkodzonych nośników danych (komputerów, dysków, taśm itp.).

Miejsce przetwarzania danych osobowych należy określić poprzez wskazanie budynków, pomieszczeń bądź ich części, w których dokonuje się wyżej wymienionej operacji.

Dane osobowe są przetwarzane przez Administratora jedynie w pomieszczeniach do tego przeznaczonych, w sposób uniemożliwiający dostęp do danych osobom nieuprawnionym.

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe zawarty został w Załączniku nr 1 do Polityki Bezpieczeństwa Informacji przedsiębiorstwa.



7. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych – Rejestr zbiorów danych osobowych

Wykaz wszystkich dostępnych zbiorów danych osobowych prowadzi Administrator. Przy opisie każdego ze zbiorów wskazuje się programy zastosowane do przetwarzania danych. Norma nie wymaga dodawania określania „forma papierowa” w zbiorach, informacja ta może być jednak istotna z punktu widzenia pracowników, sugeruje się więc jej używanie.

Do zbiorów danych można zaliczyć między innymi:

- osoby zatrudnione na podstawie umowy cywilno-prawnej;
- osoby korzystające z Zakładowego Funduszu Świadczeń Socjalnych;
- osoby realizujące zadania w ramach wolontariatu, stażu czy praktyk;
- bazę kontaktów;
- książkę korespondencyjną;
- sponsorów i darczyńców;
- uczestników przetargów;
- osoby, których wizerunek utrwalono za pomocą monitoringu wizyjnego;
- kandydatów do pracy.

Zbiory danych osobowych posiadane przez Administratora wraz z programami zastosowanymi do przetwarzania zawartych w nich danych wymienione zostały w Załączniku nr 1 do Polityki Bezpieczeństwa Informacji przedsiębiorstwa.



8. Sposób przepływu danych pomiędzy poszczególnymi systemami

Poprzez sposób przepływu danych pomiędzy poszczególnymi systemami rozumie się sposób współpracy między różnymi systemami informatycznymi. Sposób przepływu danych pomiędzy poszczególnymi systemami to również relacje istniejące między danymi zgromadzonymi w zbiorach, do przetwarzania których systemy te są wykorzystywane. Jego przygotowanie ma za zadanie lepiej zobrazować ten przepływ, co w konsekwencji ułatwi kontrolę nad tym jakie dane osobowe są przetwarzane, w jakich zbiorach i systemach oraz w jaki sposób migrują one pomiędzy tymi zbiorami i systemami.

Przepływ informacji pomiędzy systemami i powiązania pomiędzy nimi wskazane zostały w Załączniku nr 4: „Sposób przepływu danych pomiędzy poszczególnymi systemami” do Polityki Bezpieczeństwa Informacji przedsiębiorstwa.



9. Odpowiedzialności i uprawnienia

Za bezpieczeństwo przetwarzanych danych osobowych odpowiedzialne jest **RPWiK Tychy S.A.**, zwane dalej Administratorem Danych Osobowych (ADO), oraz każda osoba przez niego upoważniona, niezależnie od formy zatrudnienia. Administrator Danych Osobowych, upoważniając osoby do przetwarzania danych osobowych, zachowuje zasadę, że dostęp do danych osobowych będą miały tylko te osoby, którym jest to niezbędne do realizacji powierzonych im zadań (np. realizacji konkretnego projektu), oraz tylko w takim zakresie, jaki jest konieczny do realizacji powierzonych zadań. Każda z osób upoważnionych do przetwarzania danych osobowych zostanie, przed dopuszczeniem do przetwarzania danych osobowych, przeszkolona z wymagań ochrony danych osobowych oraz poinformowana o konsekwencjach prawnych jakie jej grożą za naruszenie tych zasad. Pomimo upoważnienia poszczególnych osób do przetwarzania danych osobowych, ADO dalej jest odpowiedzialny za poprawność procesu przetwarzania danych.

Odpowiedzialność Administratora Danych Osobowych została wskazana w ustawie o ochronie danych osobowych, wraz z aktami wykonawczymi do niej. Nie mniej, z uwagi na obowiązek znajomości Polityki Bezpieczeństwa Informacji przez wszystkich pracowników **RPWiK Tychy S.A.**, poniżej, zgodnie z RODO, wskazuje się na podstawowe obowiązki Administratora Danych Osobowych:

- zapewnienie przetwarzania zgodnego z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
- zbieranie danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
- zapewnienie adekwatności, stosowności oraz ograniczenie przetwarzania tylko do niezbędnych celów wskazanych w PBI;
- zapewnienie prawidłowości przetwarzania danych osobowych i w razie potrzeby, ich uaktualniania;



- zapewnienie przechowywania danych osobowych w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane;
- zapewnienie przetwarzania danych osobowych w sposób gwarantujący odpowiedni poziom bezpieczeństwa, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych;
- deklarację pełnego zaangażowania w celu zapewnienia bezpieczeństwa przetwarzania danych osobowych, a także prawidłowego zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych;
- nadzór określający jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, bądź z tych zbiorów usunięte oraz komu są przekazywane;
- bieżące dostosowywanie systemów informatycznych służących do przetwarzania danych i wszelkie systemy zabezpieczeń przetwarzania danych osobowych do wymogów określonych w rozporządzeniu (RODO).

Obowiązkiem Administratora jest zapewnienie:

- środków technicznych i organizacyjnych niezbędnych dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;
- systemu i sprzętu informatycznego umożliwiającego bezpieczne przetwarzanie danych;
- dopuszczenia do przetwarzania danych osobowych wyłącznie osób posiadających stosowne upoważnienie;
- zapoznania z przepisami o ochronie danych osobowych każdej osoby upoważnionej do przetwarzania danych osobowych;
- prowadzenia ewidencji osób upoważnionych;



- należytego i terminowego udzielenia informacji na wniosek osób, których dane są przetwarzane i które zwróciły się z wnioskiem o udzielenie informacji;
- kontroli nad tym jakie dane, kiedy i przez kogo zostały do zbiorów Administratora wprowadzone, ze zbiorów usunięte oraz komu i przez kogo przekazane.

W razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, dla którego zostały zebrane, Administrator jest zobowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru.

Administrator jest zobowiązany poinformować, bez zbędnej zwłoki, innych administratorów, którym udostępnił zbiór danych, o dokonanym uaktualnieniu lub sprostowaniu danych.

Dodatkowo, ADO zobligowany jest, zgodnie z RODO, w razie jakichkolwiek wątpliwości do wykazania przestrzegania powyższych obowiązków.

Za rozwój i nadzór wdrażania systemu zarządzania bezpieczeństwem informacji oraz wsparcie w określaniu zabezpieczeń, w RPWiK Tychy S.A. odpowiada, po 25 maja 2018 roku – Inspektor Ochrony Danych (IOD).

Inspektor Ochrony Danych ma następujące zadania:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość,



szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie;
- współpracę z odpowiednim organem nadzorczym;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach;
- wydawanie upoważnień do przetwarzania danych osobowych określając w nich zakres i termin ważności;
- prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
- ewidencjonowanie oświadczeń osób upoważnionych o zaznajomieniu się z zasadami zachowania bezpieczeństwa danych;
- prowadzenie rejestru naruszeń ochrony danych osobowych;
- prowadzenie rejestru czynności przetwarzania danych osobowych;
- prowadzenie rejestru wszystkich kategorii czynności przetwarzania danych osobowych dokonywanych w imieniu ADO.

Administrator danych może powierzyć IOD wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania przez IOD obowiązków wynikających z RODO.

Inspektor Ochrony Danych podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej Administratorem.

Administrator zapewnia środki i organizacyjną odrębność IOD niezbędne do niezależnego wykonywania przez niego zadań.



Inspektor Ochrony Danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

9.1. Kontrola dostępu

Każdy z pracowników, wykonawców oraz podwykonawców RPWiK Tychy S.A. posiada dostęp tylko do takich informacji, danych osobowych oraz zasobów, które są niezbędne z punktu widzenia wykonywanych przez każdego z nich zadań, pełnionych ról, czy posiadanej wiedzy.

Polityka Bezpieczeństwa Informacji jest dokumentem wewnętrznym, poufnym i nie może być udostępniana podmiotom trzecim bez uprzedniej zgody Administratora. Dla codziennych potrzeb pracowników i współpracowników stworzony został Regulamin Ochrony Danych Osobowych (załącznik nr 5 do Polityki Bezpieczeństwa Informacji przedsiębiorstwa) zawierający zasady przetwarzania danych osobowych obowiązujące u Administratora.

Każdemu z pracowników, wykonawców lub podwykonawców firmy, podczas podpisywania umowy z przedsiębiorstwem, nadawane jest prawo dostępu do pewnego zakresu informacji, danych osobowych oraz zasobów przedsiębiorstwa. Prawo dostępu otrzymywane jest na podstawie upoważnienia wydanego przez Administratora lub IOD, w którym zawarte są informacje o jego zakresie i terminie ważności (załącznik nr 6 – „Procedura nadawania uprawnień do przetwarzania danych osobowych”). Na podstawie tego upoważnienia osoba odpowiedzialna za zarządzanie środowiskiem sieciowym, dokonuje utworzenia i aktywacji konta użytkownika, z unikalnym loginem i hasłem, które stanowią podstawę do autoryzacji dostępu. Tylko użytkownicy z aktywnym kontem, posiadają możliwość korzystania z zasobów RPWiK Tychy S.A. (m.in. systemów operacyjnych, aplikacji systemowych, oprogramowania dodatkowego).

Inspektor Ochrony Danych zobowiązany jest do prowadzenia rejestru wyżej wymienionych upoważnień wydanych dla pracowników, wykonawców lub podwykonawców.



Każdy z pracowników, wykonawców lub podwykonawców RPWiK Tychy S.A. informowany jest również, podczas udzielania mu dostępu do informacji, o sankcjach, które będą egzekwowane w przypadku nieautoryzowanego ich udostępnienia.

Osoba odpowiedzialna za środowisko sieciowe w firmie zobowiązana jest do wykonywania systematycznego, nie rzadziej niż raz na miesiąc, przeglądu praw dostępu użytkowników do danych osobowych, informacji i zasobów, a co za tym idzie, do systematycznego ich aktualizowania (dodawania lub usuwania).

Każdy z pracowników, wykonawców lub podwykonawców może wystąpić z wnioskiem o poszerzenie dostępu do większej ilości informacji i danych osobowych. Wniosek ten powinien zostać skierowany do wyznaczonego IOD, który dokonuje analizy konieczności poszerzenia dostępu dla użytkownika i wydaje odpowiednią decyzję, w postaci upoważnienia.

Każdy z pracowników zobowiązany jest do nieudostępniania swojego loginu i hasła do konta osobom postronnym (innym użytkownikom, osobom trzecim). Każdorazowe zalogowanie się do systemu powinno nastąpić, tylko i wyłącznie, na urządzeniach, które należą do RPWiK Tychy S.A. (zabrania się logowania na urządzeniach ogólnodostępnych), chyba że firma udzieli stosownego upoważnienia w tej sprawie.

W przypadku zmiany stanowiska pracy przez pracownika, Administrator, w porozumieniu z IOD, może zmienić jego zakres dostępu. Zmiana ta musi być zgodna z zakresem pełnionych przez tego pracownika obowiązków, ról i odpowiedzialności (może ona polegać na usunięciu dostępu do danych, z których, po awansie, pracownik nie będzie już korzystał oraz udzieleniu mu dostępu do nowych informacji).

W przypadku rozwiązania umowy z pracownikiem, wykonawcą lub podwykonawcą RPWiK Tychy S.A., osoba odpowiedzialna za środowisko sieciowe zobowiązana jest do niezwłocznego usunięcia konta użytkownika, wraz z udzielonym mu dostępem do informacji.



10. Przetwarzanie danych

Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy:

- osoba, której dane dotyczą wyrazi na to zgodę, chyba, że chodzi o usunięcie dotyczących jej danych;
- jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą;
- jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;
- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez Administratora albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Za prawnie uzasadniony cel Administratora uznaje się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności oraz marketing bezpośredni własnych produktów lub usług, przy czym przy podejmowaniu działań marketingowych za pomocą środków komunikacji elektronicznej należy stosować przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r. poz. 1422) oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243), które przewidują dalej idącą ochronę.

Zgoda na przetwarzanie danych osobowych:

- nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
- może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania;
- może zostać odwołana w każdym czasie. W przypadku odwołania zgody na przetwarzanie danych osobowych Administrator zobowiązany jest usunąć



wszystkie dane osobowe osoby, która zgodę cofnęła, chyba, że istnieje inne podstawa prawa upoważniająca Administratora do dalszego przetwarzania tych danych dla innych celów niż wskazany w cofniętej zgodzie;

- powinna być odebrana w postaci możliwej do późniejszego udowodnienia (np. pisemnie w ramach systemu informatycznego po zastosowaniu metody dwustopniowego uwiarygodniania, jako nagranie przeprowadzonej rozmowy telefonicznej – po poinformowaniu rozmówcy o prowadzonej rejestracji).

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.

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.



11. Osoby upoważnione do przetwarzania danych osobowych oraz ewidencja osób upoważnionych

Administrator zobowiązany jest nadać upoważnienie do przetwarzania danych każdej osobie, która do przetwarzania danych będzie dopuszczona.

Upoważnienie powinno zawierać:

- datę, z którą zostało nadane,
- datę, z którą upoważnienie wygasza, jeżeli jest ono nadane na czas określony,
- zakres upoważnienia.

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.

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.

Wzór upoważnienia do przetwarzania danych stanowi Załącznik 7 do Polityki Bezpieczeństwa Informacji – „Upoważnienie do przetwarzania danych osobowych”.

Administrator zobowiązany jest do prowadzenia ewidencji osób upoważnionych. Ewidencja ta może być prowadzona w wersji papierowej lub elektronicznej z możliwością jej wydruku i powinna zawierać:

- imię i nazwisko osoby upoważnionej;
- datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
- identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

Wzór ewidencji stanowi załącznik 1 do Polityki Bezpieczeństwa Informacji. Ewidencja prowadzona jest w systemie informatycznym należącym do ADO.



12. Plan sprawdzeń oraz dokonywanie sprawdzeń

Inspektor Ochrony Danych, jeżeli został wyznaczony i zgłoszony do rejestru prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych (PUODO), lub osoba odpowiedzialna w spółce za bezpieczeństwo danych osobowych, celem zapewnienia zgodnego z prawem przetwarzania danych osobowych, dokonuje sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowuje sprawozdanie w tym zakresie.

Sprawozdanie jest dokonywane dla Administratora.

Przebieg sprawdzenia:

IOD zawiadamia Administratora o rozpoczęciu sprawdzenia doraźnego lub sprawdzenia na żądanie Prezesa Urzędu Ochrony Danych Osobowych przed podjęciem pierwszej czynności, następnie zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

Zawiadomienia nie przekazuje się w przypadku:

- sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce;
- sprawdzenia, o którego dokonanie zwrócił się PUODO, jeżeli na zawiadomienie nie pozwala wyznaczony przez niego termin;
- jeżeli kierownik jednostki organizacyjnej objętej sprawdzeniem posiada informacje o zakresie planowanych czynności.

IOD przygotowuje plan sprawdzenia planowego, który powinien zawierać: przedmiot, zakres, termin sprawdzeń oraz sposób i zakres ich dokumentowania. Plan ten jest przygotowywany na okres nie krótszy niż kwartał i nie dłuższy niż rok. Plan sprawdzeń jest przedstawiony Administratorowi nie później niż na dwa tygodnie przed dniem



rozpoczęcia okresu objętego planem. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

Zbiory danych oraz systemy informatyczne służące do przetwarzania lub zabezpieczania danych osobowych podlegają sprawdzeniu nie rzadziej niż raz na pięć lat.

Po zakończeniu sprawdzenia IOD przygotowuje sprawozdanie, które sporządza w postaci elektronicznej bądź papierowej.

IOD przekazuje Administratorowi sprawozdanie:

- ze sprawdzenia planowego – nie później niż w terminie 30 dni od zakończenia sprawdzenia;
- ze sprawdzenia doraźnego – niezwłocznie po zakończeniu sprawdzenia;
- ze sprawdzenia, o którego dokonanie zwrócił się Prezes Urzędu Ochrony Danych Osobowych – zachowując termin wskazany przez ww. Instytucję.



13. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Każdy kto przetwarza dane osobowe zobowiązany jest zachować w tajemnicy dane osobowe, do których posiada dostęp, sposoby zabezpieczania danych, jak również wszelkie informacje, które powziął w czasie przetwarzania danych, zarówno w sposób zamierzony jak i przypadkowy. Obowiązek zachowania danych w tajemnicy jest bezterminowy.

Podczas przetwarzania danych należy zachować szczególną ostrożność i podając wszelkie możliwe środki umożliwiające zabezpieczenie oraz ochronę danych przed nieuprawnionym dostępem, modyfikacją, zniszczeniem lub ujawnieniem.

Hasła i loginy do systemu informatycznego nie mogą być ujawniane nawet po ich utracie.

Należy dotrzymać należytej staranności podczas przesyłania dokumentów zawierających dane za pomocą środków komunikacji elektronicznej, w szczególności należy upewnić się czy przesyłanie za pomocą poczty elektronicznej dokumenty trafiły do właściwego odbiorcy.

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.

Wszelkie dokumenty zawierające dane osobowe przechowywane są w szafach lub pomieszczeniach zamykanych na klucz. Osoba będąca dysponentem zobowiązana jest nie przekazywać kluczy do budynków i pomieszczeń, w których przetwarzane są dane, osobom nieuprawnionym, a ponadto zobowiązana jest przedsięwziąć działania celem zminimalizowania ryzyka utraty danych. Osoba, która utraciła posiadane klucze do pomieszczeń Administratora w których przetwarzane są dane, niezwłocznie zgłasza tą okoliczność IOD.



Osoba przetwarzająca dane po zakończeniu pracy porządkuje swoje stanowisko zabezpieczając dokumenty i nośniki elektroniczne z danymi w specjalnie do tego przeznaczonych szafach lub pomieszczeniach. Niszczenie dokumentów zawierających dane odbywa się jedynie za pomocą niszczarki gwarantującej odpowiedni stopień rozdrobnienia. Zaleca się, aby niszczarka spełniała wymogi normy DIN 66399 oraz klasę bezpieczeństwa nie niższą niż 3. Alternatywnym rozwiązaniem do celów niszczenia dokumentacji jest zatrudnienie wykwalifikowanej firmy zewnętrznej, zajmującej się profesjonalną utylizacją dokumentów. Wymogiem jest zawarcie z nią umowy o powierzeniu przetwarzania danych osobowych. Każdy dokument zawierający dane, a nieużyteczny niszczy się niezwłocznie. Podczas korzystania z urządzeń wielofunkcyjnych należy zachować szczególną ostrożność. Dokumenty kopowane bądź skanowane wyjmowane są z urządzenia wielofunkcyjnego niezwłocznie po ich użyciu. Dotyczy to również dokumentów powstałych na skutek kopowania bądź skanowania.

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



14. Praca zdalna

Praca zdalna to aktualnie powszechny element stosowany w trakcie zatrudnienia. Pracownik zdalny to jednak, poza wygodą, także szereg zagrożeń związanych z faktem, że dane z założenia są przetwarzane poza firmą w środowisku, któremu często daleko do bezpiecznego. Praca zdalna to często pracownicy rozliczani w systemie zadaniowym jak i na co dzień pracujący w terenie. Pracownik dysponuje zwykle telefonem komórkowym, komputerem lub tabletom zawierającym dane firmowe, z dostępem do sieci firmowej. Dla wielu organizacji głównym problemem w takim przypadku będzie nie tyle utrata laptopa czy tabletu, co utrata zawartych w tych urządzeniach danych - w przypadku danych wrażliwych może się to wiązać z poważnymi konsekwencjami finansowymi.

Na bezpieczeństwo podczas pracy w biurze składają się elementy takie jak kontrola dostępu do pomieszczeń, systemy alarmowe, gaśnicze, niszczarki dokumentów, sejfy czy chociażby firmowa zapora sieciowa, system wykrywania włamań i antywirusowy.

W przypadku pracy zdalnej istotny jest fakt, iż pracownik, który przebywa poza biurem to także element poprawiający ciągłość działania firmy w razie braku dostępu do głównej siedziby przedsiębiorstwa (pożar, zalanie, awaria zasilania).

Szczegółowe wytyczne, co do zachowania bezpieczeństwa informacji przy pracy zdalnej oparte są o normy ISO 27001, ISO 27002 i znajdują się w Załączniku nr 8 do Polityki Bezpieczeństwa Informacji **RPWiK Tychy S.A.** Każdy pracownik będący w posiadaniu urządzeń mobilnych firmy powinien zaznajomić się z zasadami pracy zdalnej i podpisać stosowne oświadczenie o zapoznaniu się z tą dokumentacją.

Nieodzownym elementem pracy zdalnej jest również przewóz dokumentów przedsiębiorstwa oraz różnego rodzaju danych osobowych.

Transport dokumentów reguluje załącznik do Polityki Bezpieczeństwa Informacji przedsiębiorstwa **RPWiK Tychy S.A.** nr 9 – „Procedura przewozu dokumentów”.



15. Bezpieczeństwo zasobów ludzkich

W rozdziale zostało opisane postępowanie z danymi osobowymi pracowników w podziale na trzy etapy:

- etap naboru pracownika;
- etap zatrudnienia;
- etap rozwiązania umowy.

15.1. Etap wyboru pracownika

Wszyscy kandydaci do pracy, wykonawcy oraz podwykonawcy RPWiK Tychy S.A. podlegają szczegółowej weryfikacji, zgodnie z przepisami prawnymi i regulacjami wewnętrznyimi, adekwatnie do wymagań biznesowych, klasyfikacji udostępnionych informacji oraz zidentyfikowanego ryzyka. Weryfikacja ta nie narusza prywatności, ochrony danych osobowych ani regulacji prawnych dotyczących zatrudnienia i obejmuje m.in.:

- sprawdzenie autentyczności referencji osobistych i świadectw pracy;
- sprawdzenie autentyczności przedstawionego życiorysu;
- potwierdzenie deklarowanego wykształcenia i kwalifikacji zawodowych;
- niezależne potwierdzenie tożsamości, np. paszport;
- sprawdzenie zadłużenia i niekaralności.

Każdy z nowo zatrudnionych pracowników podpisuje umowę oraz zaznajamia się z regulaminem pracy, które dokładnie określają odpowiedzialność w zakresie bezpieczeństwa informacji. Role i zakresy odpowiedzialności uwzględniają m.in.:

- działania zgodne z Polityką Bezpieczeństwa Informacji;
- ochronę aktywów przed nieuprawnionym dostępem, ujawnieniem, modyfikacją lub zniszczeniem;
- wykonywanie działań związanych z bezpieczeństwem informacji;



-
- odpowiedzialność pracownika za jego działania lub niepodejmowanie działań;
 - raportowanie zdarzeń związanych z bezpieczeństwem informacji.

Dodatkowo, na każdej z umów znajdują się następujące informacje:

- zapisy o zachowaniu poufności i nieujawnianiu informacji, w przypadku dostępu do informacji wrażliwych;
- prawa i obowiązki w odniesieniu do praw autorskich i ochrony danych osobowych;
- odpowiedzialność w zakresie przetwarzania informacji otrzymywanej z zewnątrz;
- odpowiedzialność w zakresie przetwarzania danych osobowych;
- odpowiedzialność rozszerzona, np. praca w domu, po godzinach pracy;
- konsekwencje nieprzestrzegania procedur bezpieczeństwa.

Rekrutacja i zatrudnianie nowych pracowników w RPWiK Tychy S.A. prowadzona jest na dwa sposoby:

- poprzez kierowników poszczególnych działów,
- poprzez zewnętrzną firmę.

Wewnętrzna rekrutacja odbywa się na poziomie kierownictwa. Kierownicy poszczególnych działów zgłaszają zapotrzebowanie zatrudnienia nowego pracownika do działu kadr. Dział kadr przygotowuje ogłoszenie rekrutacyjne i umieszcza je na stronie internetowej Przedsiębiorstwa. Kandydaci mogą przekazać dokument CV osobiście w siedzibie spółki, a także przesyłać je drogą elektroniczną na specjalnie do tego celu utworzoną skrzynkę rekrutacja@rpwik.tychy.pl, do której dostęp mają jedynie kierownicy. Rozmowy kwalifikacyjne wykonywane są bezpośrednio przez odpowiedniego kierownika działu tutejże osoby o kompetencjach pozwalających na weryfikację umiejętności przyszłego pracownika w kontekście dostępnego stanowiska pracy.



CV lub formularze odrzucone przez kierowników działów/osoby kompetentne, są przez nich niszczone bezpośrednio w niszczarce. CV lub formularze w postaci elektronicznej, przechowywane są do celów przyszłych rekrutacji, tylko i wyłącznie w sytuacji, gdy kandydat wyraził stosowną zgodę, jednak przez okres nie dłuższy niż rok.

CV lub formularz nowozatrudnionego pracownika jest drukowany w jednym egzemplarzu i umieszczany w teczce pracowniczej. Dane nowozatrudnionego pracownika z poczty rekrutacja@rpwik.tychy.pl powinny zostać natychmiast usunięte.

Jeżeli rekrutację na dane stanowisko przeprowadza podmiot zewnętrzny na wszystkich podpisywanych umowach zostaje zamieszczona odpowiednia informacja o odpowiedzialności konkretnej agencji za ten proces. Przy wyborze firmy zewnętrznej dostarczającej pracowników do RPWiK Tychy S.A. decydującym czynnikiem jest spełnianie przez nią wymagań prawnych dotyczących ochrony danych osobowych (weryfikacja pod kątem wdrożenia przez nią RODO).

Załączniki do Polityki Bezpieczeństwa Informacji:

- „Kwestionariusz osobowy dla osoby ubiegającej się o zatrudnienie” – załącznik nr 10;
- „Klauzula informacyjna dotycząca formularza rekrutacyjnego” – załącznik nr 11;
- „Procedura postępowania z danymi osobowymi podczas rekrutacji i w trakcie zatrudnienia” – załącznik nr 12.

15.2. Zatrudnienie

Przestrzeganie zasad PBI w RPWiK Tychy S.A. jest bezwzględnie wymagane przez wszystkich pracowników, wykonawców i podwykonawców.

Pracownicy, wykonawcy i podwykonawcy RPWiK Tychy S.A. są świadomi swoich obowiązków i odpowiedzialności prawnej oraz zagrożeń związanych z bezpieczeństwem informacji. Świadomość ta budowana jest u wszystkich podmiotów poprzez:

- odpowiednie wprowadzenie w obowiązki i zakres kompetencji przed przyznaniem im dostępu do informacji;



- przedstawienie wytycznych dotyczących zależności między procedurami bezpieczeństwa, a zakresem ich czynności;
- stosowanie odpowiednich programów motywacyjnych związanych z przestrzeganiem zapisów PBI;
- cykliczne przeprowadzanie odpowiednich kursów i szkoleń z zakresu PBI;
- podtrzymywanie umiejętności i uzyskiwanie nowych kwalifikacji.

Załączniki do Polityki Bezpieczeństwa Informacji:

- „Zgoda pracownika na przetwarzanie danych” – załącznik nr 13;
- „Kwestionariusz osobowy dla pracownika” – załącznik nr 14;
- „Wzór zgody pracownika na przetwarzanie danych biometrycznych pracownika” – załącznik nr 15;
- „Informacja o działającym na terenie zakładu systemu monitoringu” – załącznik nr 16;
- „Wzór zgody pracownika na przetwarzanie danych w postaci wizerunku” – załącznik nr 17;
- „Klauzula zgody na przetwarzanie danych pracownika tymczasowego” – załącznik nr 18;
- „Formularz do rejestru realizacji żądań podmiotu danych osobowych” – załącznik nr 19;
- „Oświadczenie o zapoznaniu się z przepisami bezpieczeństwa danych osobowych” – załącznik 25.

W przypadku naruszenia zasad bezpieczeństwa informacji oraz danych osobowych przez pracowników, wykonawców i podwykonawców zostaje uruchomione postępowanie dyscyplinarne, w którym gromadzony jest odpowiedni materiał dowodowy. Postępowanie dyscyplinarne uwzględnia przede wszystkim rodzaj i wagę naruszenia zasad



bezpieczeństwa informacji, wpływ na procesy biznesowe oraz charakter naruszenia (czy jest to przypadek incydentalny, czy też jest to kolejne naruszenie).

15.3. Zakończenie lub zmiana zatrudnienia

Rozwiązywanie umowy z pracownikiem, wykonawcą lub podwykonawcą RPWiK Tychy S.A. lub zmiana stanowiska pracy wewnętrz firmy odbywa się w sposób zorganizowany i odpowiednio udokumentowany.

Dokumenty pracownicze, po ustaniu zatrudnienia, przechowywane są przez RPWiK Tychy S.A. przez okres 10 lub 50 lat (poza dokumentami nie związanymi z realizacją przepisów Kodeksu Pracy). Pracownik rozwiązujący umowę, jest zobowiązany podpisać „Informację dla pracownika o dokumentacji pracowniczej”, która stanowi załącznik nr 23 do Polityki Bezpieczeństwa Informacji przedsiębiorstwa RPWiK Tychy S.A..

Po zakończeniu zatrudnienia (zakończenie stosunku pracy lub umowy) pracownicy, wykonawcy lub podwykonawcy są zobowiązani do zwrotu wszystkich posiadanych zasobów firmy (m.in. sprzętu, oprogramowania, akcesoriów komputerowych, kart dostępu i kart kredytowych, podręczników i książek) oraz wszelkich informacji zapisanych na dyskach i nośnikach przenośnych. W przypadku korzystania ze sprzętu będącego własnością wykonawcy lub podwykonawcy wszystkie informacje zostają przekazane RPWiK Tychy S.A. i skutecznie usunięte z tego sprzętu.

W przypadku zmiany stanowiska w firmie podstawową zasadą jest zatrzymanie posiadanego sprzętu i zmiana prawa dostępu stosownie do nowego zakresu czynności.

Jedną z podstawowych zasad bezpieczeństwa informacji w RPWiK Tychy S.A. jest, po każdorazowym zakończeniu zatrudnienia pracownika lub zmianie stanowiska, przegląd prawa dostępu do aktywów i systemów informatycznych. W takich przypadkach zadaniem administratorów sieci jest natychmiastowa aktualizacja rejestrów dostępu oraz zmiana haseł do kont aktywnych. Jeżeli prawa dostępu były przyznane większej liczbie osób niż tylko odchodząącym pracownikom i pracownikom firmy zewnętrznej, osoba odpowiedzialna za



udzielanie dostępów zobowiązana jest do usunięcia odchodzących osób z każdej grupy. Dodatkowo, pozostali pracownicy są informowani na bieżąco na temat zmian w zatrudnieniu w **RPWiK Tychy S.A.** oraz zobowiązani są do zachowania poufności w stosunku do odchodzących pracowników.

Szczegółowe informacje dotyczące systemów informatycznych zawarte zostały w załącznikach:

- „Polityka bezpieczeństwa teleinformatycznego” – załącznik nr 21;
- „Schemat nadawania uprawnień IT” – załącznik nr 22;
- „Wykaz uprawnień do systemów informatycznych” – załącznik nr 1.



16. Zarządzanie zasobami

Wybrani pracownicy, wykonawcy lub podwykonawcy RPWiK Tychy S.A. do realizacji, zawartych w umowie o pracę/współpracy/zlecenie/dzieło, zadań, wykorzystują zasoby, którymi dysponuje przedsiębiorstwo. Za każdy z zasobów przedsiębiorstwa odpowiada osoba, której zostały one przekazane. Podczas przekazywania zasobów danej osobie, spisywany jest odpowiedni protokół zdawczo-odbiorczy, w którym zamieszczane są informacje o udostępnianym zasobie. W protokole tym znajdują się m.in.:

- rodzaj i nazwa zasobu (np. telefon komórkowy, laptop, samochód);
- stan urządzenia (np. nowy, używany, po regeneracji);
- dodatki (np. ładowarka, uchwyt na telefon);
- imię i nazwisko osoby odpowiedzialnej za dany zasób;
- inne.

Każdy z zasobów, udostępniony przez RPWiK Tychy S.A., powinien być użytkowany zgodnie z jego przeznaczeniem, tj. do celów związanych z realizacją zadań wynikających z umowy. Zasoby te powinny być również utrzymywane w stanie pozwalającym na ich bezawaryjne użytkowanie, natomiast każde uszkodzenie zasobu, czy jego podzespołu, powinno być natychmiast, niezwłocznie po jego wykryciu, usunięte.

W momencie zakończenia współpracy pomiędzy RPWiK Tychy S.A., a poszczególnymi pracownikami firmy lub kontrahentami, nakazany jest zwrot zasobów do siedziby przedsiębiorstwa. Zasoby te powinny być zwracane w stanie pozwalającym na ich dalsze wykorzystanie. Podczas ich zwrotu, dokonuje się spisania protokołu zdawczego, który zawiera te same informacje, które umieszczone są w protokole odbiorczym. Za wszelkie wady i uszkodzenia zasobów, które nie zostały w porę zgłoszone do naprawy lub usunięte, odpowiada osoba, która była za nie odpowiedzialna.

Wzór wykazu zasobów wykorzystywanych przez pracowników, wykonawców lub podwykonawców RPWiK Tychy S.A., wraz ze wskazaniem osób odpowiedzialnych za nie, przedstawiony został w załączniku nr 1 do Polityki Bezpieczeństwa Informacji



przedsiębiorstwa. Wykaz prowadzony jest w systemie informatycznym należącym do ADO.



17. Procedura postępowania z incydentami ochrony danych osobowych, zarządzanie ciągłością działania, kontakt z organami władzy

Celem Procedury Zarządzania Incydentami Związanymi z Bezpieczeństwem Informacji jest określenie zadań pracowników w zakresie:

- ochrony wszystkich informacji przed ich modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem, a także utratą oraz ochroną zasobów technicznych;
- prawidłowego reagowania pracowników przy przetwarzaniu danych, w przypadku stwierdzenia ich naruszenia (zwłaszcza naruszenia ochrony danych osobowych) lub naruszenia zabezpieczeń systemu informatycznego;
- ograniczenia ryzyka powstania zagrożeń oraz minimalizacji skutków wystąpienia zagrożeń.

W przypadku naruszenia ochrony danych osobowych, należy oprócz zgłoszenia przełożonemu lub IOD, zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zgłosić to naruszenie właściwemu organowi nadzorczemu, a także w uzasadnionych przypadkach, wszystkim osobom, których to naruszenie dotyczy.

W przypadku naruszenia IOD może zastosować karę wobec pracownika, który dopuścił się wykroczenia. Wzór stanowi „Zawiadomienie o zastosowaniu kary porządkowej” – załącznik nr 24.

Szczegółowe zasady postępowania w przypadku zagrożenia lub naruszenia bezpieczeństwa informacji, przykładowe incydenty ODO oraz wzory zgłoszeń znajdują się w Załączniku nr 23 do Polityki Bezpieczeństwa Informacji – „Procedurze zarządzania incydentami związanymi z bezpieczeństwem informacji”.



Zarządzanie ciągłością działania ma na celu zapewnienie ciągłości realizacji krytycznych dla organizacji procesów biznesowych również w sytuacji kryzysowej, w której nie są dostępne aktywa niezbędne do realizacji tych procesów. Zarządzanie ciągłością działania powinno uwzględniać wszelkie kategorie zdarzeń, które uniemożliwiają realizację krytycznych procesów przez czas dłuższy, niż dopuszczalny dla organizacji – zarówno te, które noszą znamiona katastrofy (pożar, powódź itp.), jak i te, które dotyczą wyłącznie wewnętrznych spraw danej organizacji (np. awaria krytycznego systemu informatycznego, niewywiązanie się dostawcy usług z obowiązków określonych w umowie, itp.). W związku z tym każde przedsiębiorstwo powinno zbudować prawidłowe i skuteczne rozwiązania budujące odporność przedsiębiorstwa na wypadek wystąpienia sytuacji kryzysowej.

Zapewnianie ciągłości działania jest zwykle utożsamiane tylko z wykonywaniem i przechowywaniem tzw. kopii zapasowych (nazywanych także kopiami bezpieczeństwa) oraz w razie potrzeby, odtwarzaniem z nich zasobów informacyjnych organizacji. Jest to w istocie problem znacznie bardziej skomplikowany i wymagający znacznie większej wiedzy i nakładów (organizacyjnych, finansowych, pracy ludzkiej itd.) niż zwykłe wykonywanie kopii zapasowych.

Do środków bezpieczeństwa, które mogą przyczynić się do zmniejszenia strat spowodowanych niedostępnością elementów systemu informatycznego stosowanych w spółce **RPWiK Tychy S.A.** należą m.in.:

- urządzenia podtrzymywania zasilania dla każdego z serwerów (UPS);
- klimatyzatory w pomieszczeniach ze sprzętem komputerowym;
- redundantne rozwiązania sieci oraz sprzętu teleinformatycznego;
- gaśnice.



18. Zarządzanie ryzykiem utraty bezpieczeństwa danych osobowych

Wszelkie informacje zawarte w poniższym opracowaniu są zgodne z obowiązującymi w Unii Europejskiej wymogami, takimi jak:

- 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 (w skrócie RODO);
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępcości, prowadzenia postępowałń przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW;
- Opinia Grupy Roboczej ds. Ochrony danych 29 14/EN WP 218 w sprawie oceny oddziaływania na ochronę danych i określenia czy przetwarzanie "może prowadzić do wysokiego ryzyka" w rozumieniu rozporządzenia 2016/679.

Ochrona bezpieczeństwa danych osobowych w RPWiK Tychy S.A., to nie tylko szereg działań technicznych prawnych i organizacyjnych, ale również zarządzanie zasobami informatycznymi oraz zarządzanie informacją. Wymogi te stawiane są wszystkim przedsiębiorstwom przetwarzającym dane osobowe, bez względu na ich charakter działalności, wielkość czy obrót roczny.

Dobór zabezpieczeń w RPWiK Tychy S.A., z uwagi na koszty, został zaimplementowany stosownie do wartości szkód, które mogłyby ponieść firma w sytuacji ich niezastosowania. Na tej podstawie określone zostały cele bezpieczeństwa przedsiębiorstwa i jego systemów, na które składają się między innymi:

- identyfikacja zasad bezpiecznego przetwarzania danych osobowych;



- szkolenie wstępne oraz systematyczne szkolenia;
- bieżące uświadamianie pracowników o zagrożeniach;
- monitorowanie aktualnego stanu bezpieczeństwa;
- monitorowanie zmian;
- doskonalenie systemów bezpieczeństwa.

Szacowanie ryzyka zostało wykonane z wykorzystaniem autorsko opracowanej Tabeli szacowania ryzyka. Proces szacowania ryzyka każdorazowo koordynowany jest przez Inspektora Ochrony Danych oraz realizowany poprzez właściwą identyfikację zagrożeń i podatności dla właścicieli aktywów, natomiast szacowanie konsekwencji oraz prawdopodobieństwa wykonywane jest przez właścicieli ryzyka – w przypadku RPWiK Tychy S.A. właściciele aktywów, są jednocześnie właścicielami ryzyka.

Aktywa, podatności i zagrożenia

Pierwszym krokiem w szacowaniu ryzyka jest zidentyfikowanie wszystkich aktywów będących w zakresie SZBI kompatybilnym z wymaganiami RODO – oznacza to wszystkie aktywa, które mogą wpływać na poufność, integralność i dostępność informacji w organizacji. Aktywami mogą być dokumenty w postaci papierowej lub elektronicznej, aplikacje i bazy danych, ludzie, sprzęt IT, infrastruktura oraz usługi zewnętrzne / procesy zlecane na zewnątrz. Podczas identyfikacji aktywów, konieczne jest także określenie ich właścicieli – osób lub jednostek organizacyjnych odpowiedzialnych za poszczególne aktywa.

Kolejnym krokiem jest identyfikacja wszystkich zagrożeń i podatności związanych z poszczególnymi aktywami. Identyfikacji zagrożeń i podatności dokonuje się z użyciem katalogów zgodnych z wymaganiami zawartymi w zespole norm ISO 2700x. Poszczególne aktywa mogą być związane z więcej niż jednym zagrożeniem, a każde zagrożenie może być związane z więcej niż jedną podatnością.



Określanie właścicieli ryzyka

Dla każdego ryzyka należy określić właściciela ryzyka, czyli osobę lub jednostkę organizacyjną odpowiedzialną za to ryzyko. Osoba ta w przypadku RPWiK Tychy S.A. jest jednocześnie właścicielem aktywu.

Konsekwencje i prawdopodobieństwo

Gdy właściciele ryzyk zostali już określeni, należy dla każdego aktywu oraz każdej kombinacji zagrożenie-podatność oszacować liczbowo znaczenie skutków zdarzenia, w którym dana podatność została wykorzystana przez dane zagrożenie.

Skutki niewielkie	0	Utrata poufności, dostępności lub integralności nie wpływa na przepływy pieniężne w organizacji, zobowiązania umowne lub prawne lub jej reputację.
Skutki średnie	1	Utrata poufności, dostępności lub integralności powoduje konsekwencje finansowe oraz ma niski lub średni wpływ na zobowiązania prawne, umowne lub reputację organizacji.
Skutki znaczące	2	Utrata poufności, dostępności lub integralności ma znaczący i/lub natychmiastowy wpływ na przepływy pieniężne w organizacji, jej działanie, zobowiązania prawne lub umowne i/lub jej reputację.

Źródło: Opracowanie własne

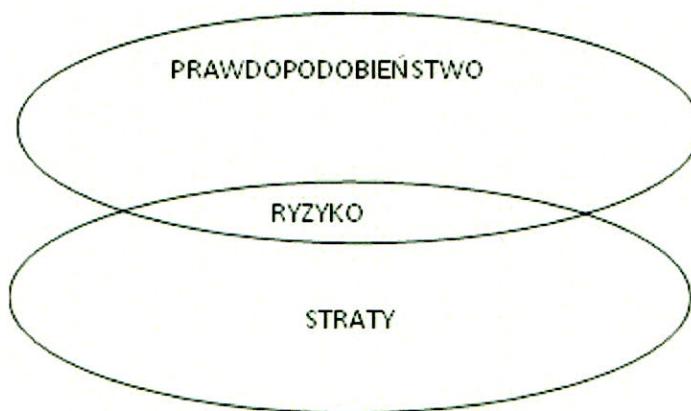
Po oszacowaniu skutków konieczne jest określenie prawdopodobieństwa zdarzenia, tj. prawdopodobieństwa, że dane zagrożenie wykorzysta podatność danego aktywu.

Prawdopodobieństwo niskie	0	Istniejące zabezpieczenia są silne i zapewniały dotychczas odpowiedni poziom ochrony. Nie oczekuje się w przyszłości nowych incydentów.
Prawdopodobieństwo średnie	1	Istniejące zabezpieczenia w większości przypadków zapewniały odpowiedni poziom ochrony. Nowe incydenty są możliwe, ale nie są wysoce prawdopodobne.
Prawdopodobieństwo wysokie	2	Istniejące zabezpieczenia są nieefektywne. Prawdopodobieństwo incydentów w przyszłości jest wysokie.

Źródło: Opracowanie własne

Po wprowadzeniu wartości skutków oraz prawdopodobieństwa do Tabeli szacowania ryzyka, poziom ryzyka jest obliczany automatycznie. Wynik jest sumą skutków oraz prawdopodobieństwa. Kalkulacja określa poziom określonego ryzyka. Istniejące zabezpieczenia wpisuje się w ostatniej kolumnie Tabeli szacowania ryzyka.

Graficzną interpretację ryzyka przedstawia rysunek 3, z którego wynika, że ryzyko jest zbiorowym elementem prawdopodobieństwa i strat. Ryzyko jest tym większe im większy jest jego obszar.



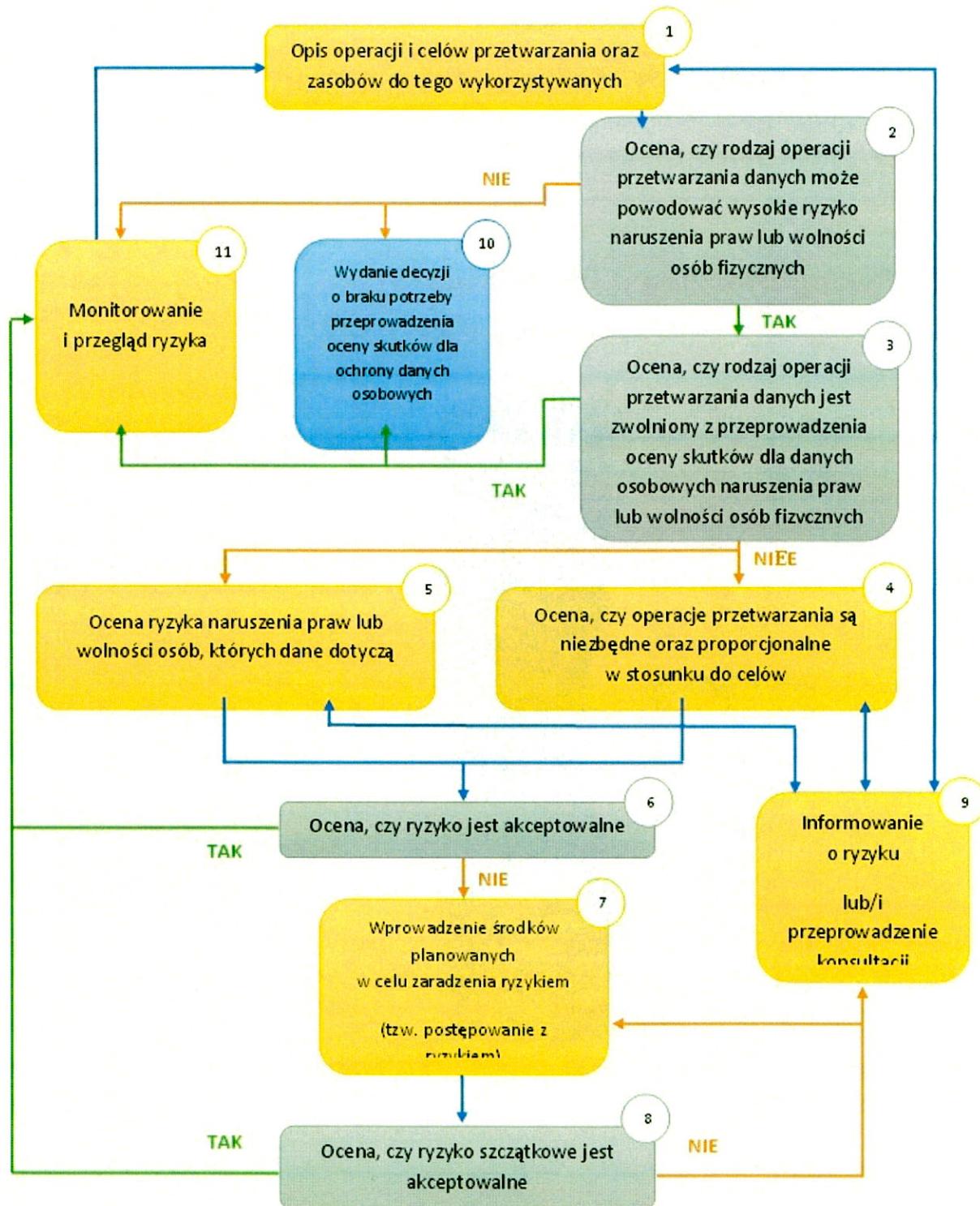
Rysunek 3. Graficzna interpretacja pojęcia ryzyka [źródło: opracowanie własne na podstawie RODO]



Podejście do ryzyka, wynikające z powyższego schematu wymaga od organizacji porównania wartości ryzyka z możliwością pokrycia prawdopodobnych strat wynikających z urzeczywistnienia się tego ryzyka. W zależności od otrzymanego wyniku organizacja powinna określić strategię działania i politykę postępowania w zakresie zarządzania ryzykiem. Profil ryzyka każdej organizacji jest inny i wymaga dostosowania metody łagodzenia go. Zależy to od specyfiki korzystania z systemów informacyjnych oraz woli zdolności organizacji do przeciwdziałania ryzyku w przyszłości. Oznacza to, że nie ma jednego poprawnego podejścia do przeciwdziałania ryzyku.

Szczegółowe informacje odnośnie kalkulacji ryzyka w przedsiębiorstwie wraz z macierzą rozkładu oceny ryzyka zawarte są w dokumencie "Metodyka Zarządzania Ryzykiem".

Poniżej przedstawiono szczegółowy proces zarządzania ryzykiem w przedsiębiorstwie w odniesieniu do ochrony danych osobowych. Schemat ten jest zgodny z założeniami nowego Rozporządzenia oraz wytycznymi w sprawie oddziaływania na ochronę danych.



Rysunek 4. Proces zarządzania ryzykiem w odniesieniu do ochrony danych osobowych
[źródło: opracowanie własne na podstawie RODO]



Głównym celem RPWiK Tychy S.A. w rozumieniu Polityki Bezpieczeństwa Informacji jest jak najskuteczniejsze minimalizowanie ryzyka wycieku danych osobowych. Gwarantuje to wzrost wiarygodności przedsiębiorstwa co przekłada się w bezpośredni sposób na uzyskanie stabilnej pozycji rynkowej. Odpowiednio prowadzony proces zarządzania ryzykiem w firmie gwarantuje bezpieczeństwo finansowe nie tylko z punktu widzenia utraty wiarygodności, ale również w zakresie kar przewidzianych w rozporządzeniu RODO.

Według ustawy o finansach publicznych z dnia 27 sierpnia 2009 zarządzanie ryzykiem jest jednym z elementów kontroli zarządczej, która definiowana jest jako ogólna działań zapewniających realizację celów i zadań w sposób terminowy, efektywny, a przede wszystkim zgodny z prawem.

Zarządzanie ryzykiem przedstawione na rysunku numer 4 uwzględnia poszczególne elementy całościowego procesu, a nie pojedynczego etapu. Proces ten pomaga identyfikować poszczególne zagrożenia, a także planować zabezpieczenia odpowiednie do występującego ryzyka w celu jego minimalizacji.

Skuteczne zarządzanie ryzykiem w rozumieniu Polityki Bezpieczeństwa RPWiK Tychy S.A. to podejmowanie regularnych działań pozwalających na ciągłe monitorowanie, kontrolowanie i udoskonalanie praktyk weryfikacji istniejących i nowo pojawiających się zagrożeń oraz weryfikacja podatności na nie. Jest to bezpośrednio związane ze zmniejszaniem prawdopodobieństwa zaistnienia zagrożenia wyciekami danych w przedsiębiorstwie i jednocześnie ograniczania negatywnych skutków jakie niosą za sobą rzeczone. Przy podejmowaniu strategicznych decyzji dotyczących bezpieczeństwa danych osobowych należy w pierwszej kolejności dochować staranności w wyprzedzaniu przyszłych zdarzeń, co spowoduje zminimalizowanie potencjalnych, szeroko rozumianych strat dla przedsiębiorstwa oraz nie dopuści do utraty jego wiarygodności.

Strategia analizy ryzyka, w przypadku przedsiębiorstwa RPWiK Tychy S.A. została dostosowana do charakteru działalności spółki, tak aby móc zapewnić przedsiębiorstwu odpowiedni poziom bezpieczeństwa dostosowany do wymogów rozporządzenia RODO.



19. Podsumowanie

Niniejsza wysokopoziomowa Polityka określa podstawowe cele, zasady, kierunki zarządzania bezpieczeństwem informacji. Stanowi ona jednocześnie pewnego rodzaju podręcznik dla osób odpowiedzialnych za przetwarzanie danych w RPWiK Tychy S.A.

Niniejszą Politykę stosuje się do całości Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), zgodnie z dokumentem Zakres SZBI.

Użytkownikami niniejszego dokumentu są wszyscy pracownicy RPWiK Tychy S.A., jak również odnośne podmioty zewnętrzne.

Ogólnym celem zarządzania bezpieczeństwem informacji jest, m.in.: redukcja strat związanych z wyciekiem lub incydentem w zakresie danych osobowych a także troska o ww. dane w obrębie zatrudnianej kadry pracowniczej i wśród kooperantów / klientów. Inspektor Ochrony Danych Osobowych odpowiedzialny jest za cykliczne przeglądy wymienionych celów ogólnych SZBI oraz za ustalanie nowych celów.

Cele konkretnych wdrażanych zabezpieczeń lub grup zabezpieczeń będą proponowane przez Administratora (w reprezentacji Zarządu RPWiK Tychy S.A.), Administratora Sieci Komputerowej oraz Inspektora Ochrony Danych Osobowych.

Przegląd wszystkich celów będzie dokonywany co najmniej raz w roku. Za utrzymanie cykliczności odpowiedzialny jest Inspektor Ochrony Danych Osobowych oraz Zarząd.

Wdrożenia będą realizowane poprzez uprzednio przygotowaną przez Inspektora Ochrony Danych Osobowych analizę ryzyka i opracowaną we współpracy z Zarządem Deklarację Stosowania.

Inspektor Ochrony Danych Osobowych odpowiada za zapewnienie zgodności wdrożenia i obsługi SZBI z niniejszą Polityką oraz jej bieżące aktualizacje. Dodatkowo, ww. reprezentant RPWiK Tychy S.A. odpowiada za jego właściwe funkcjonowanie.

Zarząd dokonuje przeglądu SZBI co najmniej raz do roku lub każdorazowo na wniosek Inspektora Ochrony Danych Osobowych w przypadku istotnych zmian,



dostosowań, zakończenia inwestycji lub przedsięwzięć nie inwestycyjnych z przyjętej Deklaracji Stosowania.

Za ochronę integralności, dostępności oraz poufności zasobów odpowiada właściciel danego zasobu.

Wszystkie incydenty związane z bezpieczeństwem informacji każdorazowo powinny być zgłaszane do Inspektora Ochrony Danych Osobowych.

Inspektor Ochrony Danych Osobowych odpowiedzialny jest za wdrożenie Planu szkolenia i uświadamiania pracowników w zakresie bezpieczeństwa informacji. Plan ten dotyczy wszystkich osób, które objęte są SZBI. Ponadto, jest on odpowiedzialny za to, aby treść niniejszej polityki była znana wszystkim podmiotom przetwarzającym dane osobowe w RPWiK Tychy S.A.



20. Postanowienia końcowe

- Dokumentacja przetwarzania danych osobowych stanowi wewnętrzną regulację Administratora i obowiązuje wszystkich pracowników i współpracowników Administratora;
- Dokumentacja przetwarzania danych osobowych obowiązuje od dnia jej wprowadzenia w życie w sposób przyjęty u Administratora. Wszelkie zmiany Dokumentacji przetwarzania danych osobowych obowiązują od dnia ich wprowadzenia w życie w sposób przyjęty u Administratora;
- Każdy kto przetwarza dane posiadane przez Administratora zobowiązany jest do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Dokumentacji przetwarzania danych osobowych;
- 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;
- W sprawach nieuregulowanych w niniejszej polityce bezpieczeństwa mają zastosowanie przepisy powszechnie obowiązującego prawa, w tym w szczególności przepisy ustawy.



21. Ważność oraz zarządzanie niniejszym dokumentem

Stwierdza się ważność niniejszego dokumentu na dzień 25.06.2018 r.

Właścicielem niniejszego dokumentu jest Inspektor Ochrony Danych Osobowych, który jest odpowiedzialny za weryfikację oraz w razie konieczności aktualizację co najmniej raz w roku.

.....
Inspektor Ochrony Danych Osobowych

.....
Członek Zarządu

.....
Członek Zarządu

wersja 01/2018 z 22.11.2018 r.

Strona 63 z 65

**Kontakt do Inspektora Ochrony Danych (IOD):****Łukasz Grabowski**Adres e-mail: odo@rpwik.tychy.pl

Telefon: 48 883-942-060

Kontakt do kierowników komórek organizacyjnych:

Lp.	Dział:	Imię i nazwisko:	Adres e-mail:	Telefon:
1	Dział Monitoringu Sieci	Joanna Banasz	j.banasz@rpwik.tychy.pl	(32) 325-70-91
2	Dział Sieci	Monika Siejka	m.siejka@rpwik.tychy.pl	(32) 325-70-39
3	Dział Inwestycji i Funduszy Pomocowych	Dorota Kowalska	d.kowalska@rpwik.tychy.pl	(32) 325-70-19
4	Dział Zaplecza Technicznego	Ireneusz Pustelnik	i.pustelnik@rpwik.tychy.pl	(32) 325-70-73
5	OES Bieruń	Mateusz Susek	m.susek@rpwik.tychy.pl	(32) 326-96-32
6	OES Brzeszcze	Krystian Czypek	k.czypek@rpwik.tychy.pl	(32) 211-14-66
7	OES Łaziska	Krzysztof Cugowski	k.cugowski@rpwik.tychy.pl	(32) 224-18-37
8	OES Tychy	Marcin Korzus	m.korzus@rpwik.tychy.pl	(32) 325-70-72
9	Dział Finansów i Zamówień Publicznych	Dariusz Wojtal	d.wojtal@rpwik.tychy.pl	(32) 325-70-30
10	Dział Sprzedaży i Controlingu	Damian Maguda	d.maguda@rpwik.tychy.pl	(32) 325-70-23
11	Dział Informatyki i Bezpieczeństwa Informacji	Dariusz Mrowiec	d.mrowiec@rpwik.tychy.pl	(32) 325-70-89



Polityka Bezpieczeństwa Informacji

12	Dział Administracyjno-Gospodarczy	Barbara Długajczyk	<u>b.dlugajczyk-wroblewska@rpwik.tychy.pl</u>	(32) 325-70-26
13	Dział Obsługi Korporacyjnej	Zofia Góra	<u>z.gora@rpwik.tychy.pl</u>	(32) 325-70-22
14	Dział Spraw Pracowniczych	Agnieszka Kałuża	<u>a.kaluza@rpwik.tychy.pl</u>	(32) 325-70-55
15	Dział BHP	Joanna Sikora	<u>j.sikora@rpwik.tychy.pl</u>	(32) 325-70-69