POLITYKA BEZPIECZEŃSTWA INFORMACJI ENGIE EC SŁUPSK SPÓŁKA Z O.O[1]

Wersja 3

Załącznik do Zarządzenia Prezesa Zarządu nr 6/2019 z dnia 14 maja 2019 r.

Politykę bezpieczeństwa informacji wprowadzono Zarządzeniem Prezesa Zarządu nr 34/2016 z dnia 30 listopada 2016 r.

Aktualizacje:

- Wersja 2 - Zarządzenie Prezesa Zarządu nr 6/2018 z dnia 07 maja 2018 r

ZATWIERDZAM

Prezes Zarządu
Dyrektor Zarządzający

.....Marek Raczkiewicz.....

[1] Opracowano na podstawie:

- UOŚD Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną.
- 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, zwane potocznie Ogólnym Rozporządzeniem w sprawie Ochrony Danych Osobowych (ang. General Data Protection Regulation) – „RODO" (ang. „GDPR").
- PN-EN ISO/IEC 27001-Systemy zarządzania bezpieczeństwem informacji - Wymagania
- PN-EN ISO/IEC 27002 –Praktyczne zasady zabezpieczenia informacji

SPIS TREŚCI:

WSTĘP

Zarząd Spółki, stojąc na stanowisku, że informacja jest priorytetowym zasobem organizacji oraz warunkiem ciągłego jej rozwoju, stosuje **Politykę Bezpieczeństwa Informacji (PBI)** jako gwarancję sprawnej i skutecznej ochrony informacji oraz zapewnienie odpowiedniego poziomu bezpieczeństwa zgodnie z wymaganiami biznesowymi oraz właściwymi normami prawnymi i regulacjami a także jako ciągłe poszerzanie świadomości i wiedzy pracowników w zakresie bezpieczeństwa informacji.

Podejście do bezpieczeństwa informacji w Spółce opiera się na trzech kluczowych regułach:

- **Reguła poufności informacji** - zapewnienie, że informacja jest udostępniana jedynie osobom upoważnionym
- **Reguła integralności informacji** - zapewnienie zupełnej dokładności i kompletności informacji oraz metod jej przetwarzania
- **Reguła dostępności informacji** - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów tylko wtedy, gdy istnieje taka potrzeba.

Informacja stanowi taki sam zasób (aktyw) naszej Spółki jak pracownicy, technologie, środki finansowe. Ponadto, informacje w postaci know-how, bazy danych czy warunków handlowych, stanowią wartość bilansową, dlatego kluczowe jest właściwe zabezpieczenie ich przetwarzania.

Bezpieczeństwo informacji oznacza natomiast, że informacja jest chroniona przed różnymi zagrożeniami w taki sposób, aby:

- zapewnić ciągłość prowadzenia działalności,
- zminimalizować straty,
- maksymalizować zwrot nakładów na inwestycje i działania o charakterze biznesowym.

Oznacza to, że dostępność, poufność i integralność informacji ma podstawowe znaczenie dla utrzymania konkurencyjności, płynności finansowej, zysku, postępowania zgodnego z przepisami prawa i wizerunku Spółki.

Na bezpieczeństwo aktywów informacyjnych Spółki mają wpływ czynniki zewnętrzne i wewnętrzne, które zidentyfikowano następująco:

czynniki zewnętrzne wpływające na przetwarzanie danych (środowisko zewnętrzne, w którym spółka dąży do osiągnięcia swoich celów)	**czynniki wewnętrzne** wpływające na przetwarzanie danych (środowisko wewnętrzne, w którym spółka dąży do osiągnięcia swoich celów)
środowisko prawne	struktura organizacyjna, role i rozliczalność w organizacji
środowisko społeczne	strategie i polityki stosowane w spółce
środowisko regulacyjne	zdolności rozumiane jako zasoby i wiedza (kapitał, czas, ludzie, procesy, systemy i technologie)
środowisko finansowe	systemy informacyjne, przepływ informacji , procesy podejmowania decyzji
środowisko technologiczne	relacje z wewnętrznymi interesariuszami, ich przestrzeganie i wartości
środowisko konkurencyjne	forma i zakres relacji zawartych w umowach
środowisko grupy ENGIE	normy i standardy przyjęte w spółce tzw. Kultura organizacyjna
regulacje z zewnętrznymi interesariuszami i ich przestrzeganie	relacje z wewnętrznymi interesariuszami, ich przestrzeganie i wartości

Określone powyżej środowisko, w którym Spółka dąży do osiągnięcia swoich celów wpływa na nasze działania, dlatego też ważne jest to w jaki sposób zarządzamy informacjami.

Zarządzanie informacjami w Spółce związane jest z zarządzaniem i ochroną informacji stanowiących tajemnicę Spółki i informacji prawnie chronionych, a celem jest osiągnięcie poziomu organizacyjnego i technicznego, który:

- będzie gwarantem pełnej ochrony danych pracowników i klientów,
- zapewni zachowanie poufności, integralności i dostępności informacji chronionych oraz jawnych,

- zagwarantuje odpowiedni poziom bezpieczeństwa informacji, bez względu na jej postać, we wszystkich systemach jej przetwarzania,
- maksymalnie ograniczy występowanie zagrożeń dla bezpieczeństwa informacji, które wynikają z celowej bądź przypadkowej działalności człowieka oraz ich ewentualne wykorzystanie na szkodę Spółki,
- zapewni poprawne i bezpieczne funkcjonowanie wszystkich systemów przetwarzania informacji,
- zapewni gotowość do podjęcia działań w sytuacjach kryzysowych dla bezpieczeństwa Spółki, jej interesów oraz posiadanych i powierzonych jej informacji.

Spółka zarządzając informacjami dąży do osiągnięcia korzyści, m.in. takich jak:
- zwiększenie zaufania do Spółki,
- podniesienie wiarygodność Spółki w oczach klientów,
- dowód na spełnienie wymagań przepisów prawa dotyczących ochrony informacji.

Polityka Bezpieczeństwa Informacji (PBI) jest dokumentem określającym ramy do ustanowienia celów bezpieczeństwa informacji, które Spółka wypracowała i dotyczy całego procesu korzystania z informacji, niezależnie od sposobu jej przetwarzania. Jest dokumentem nadrzędnym nad wszystkimi dokumentami dotyczącymi bezpieczeństwa informacji funkcjonującymi w Spółce i zasady w niej określone mają zastosowanie do całego usystematyzowanego zarządzania bezpieczeństwem informacji, a w szczególności do:
- wszystkich systemów informatycznych, w których są lub będą przetwarzane informacje podlegające ochronie,
- informacji będących w dyspozycji Spółki lub innych podmiotów, o ile zostały przekazane na podstawie umów,
- wszystkich nośników papierowych, magnetycznych, optycznych i innych, na których są lub będą znajdować się informacje podlegające ochronie,
- wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

Dokument podzielono na trzy rozdziały:
Rozdział I – opisujący cel, zasady i zakres stosowania polityki bezpieczeństwa informacji przez Spółkę
Rozdział II – poświęcony jest polityce bezpieczeństwa przetwarzania danych osobowych
Rozdział III – skupiający się na metodach zabezpieczenia sprzętu/systemu informatycznego.

W rozdziale II i III opisano środki i mechanizmy świadczące o tym, że:
- administrator danych osobowych wdraża mechanizmy i rozwiązania zapewniające ochronę danych osobowych (zasada privacy by design),
- wdrożone środki techniczne i organizacyjne zapewniają, że będą przetwarzane tylko te dane osobowe, które są niezbędne z punktu widzenia konkretnego celu przetwarzania (zasada privacy by default).

PBI oraz dokumenty z nią powiązane powinny być aktualizowane wraz ze zmieniającymi się przepisami prawnymi oraz zmianami faktycznymi, które mogą powodować, że zasady ochrony określone w obowiązujących dokumentach będą nieaktualne lub nieadekwatne.
Ustala się termin weryfikacji zapisów dokumentu 1 raz w roku kalendarzowym. Przegląd PBI ma na celu stwierdzenie, czy postanowienia w niej zawarte odpowiadają aktualnej i planowej działalności Spółki oraz stanowi prawnemu, aktualnemu w momencie dokonywania przeglądu.
Zmiany niniejszej Polityki wymagają przeglądu innych dokumentów obowiązujących w Spółce a dotyczących ochrony informacji. Wszelkie zmiany Polityki są zatwierdzone przez Prezesa Zarządu Spółki.
Bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy, zasady określone w niniejszej Polityce oraz w dokumentach powiązanych obowiązują wszystkich pracowników Spółki. W niezbędnym zakresie do współpracy, zasady opisane w PBI są przekazywane współpracownikom/klientom przetwarzającym dane osobowe, których administratorem jest Spółka.

DEFINICJE

Użyte w dokumencie pojęcia są wspólne dla wszystkich dokumentów powiązanych z niniejszą **PBI** oraz dla wszystkich pozostałych dokumentów, które zostały przyjęte przez Spółkę, w zakresie zabezpieczenia informacji.

- **Aktywa (zasoby)** – wszystko, co ma wartość dla Spółki (zasoby ludzkie, finansowe, informacyjne, organizacyjne, technologiczne i fizyczne).
- **Administrator (ADO)** – podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych, reprezentowany przez Prezesa Zarządu.
- **Administrator Systemów Informatycznych (ASI)** - wyznaczona przez administratora osoba, odpowiedzialna za funkcjonowanie infrastruktury informatycznej, na którą składa się cały sprzęt informatyczny oraz systemy i aplikacje.
- **Autentyczność** - właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana; autentyczność dotyczy takich podmiotów, jak użytkownicy, procesy, systemy i informacja
- **Analiza zagrożeń** - badanie działań i zdarzeń, które mogą szkodliwie wpływać na system przetwarzania danych.
- **Anonimizacja** - proces, którego efektem jest nieodwracalna zmiana informacji umożliwiających identyfikację osoby w taki sposób, aby nie istniała możliwość zidentyfikowania podmiotu danych.
- **Bezpieczeństwo Informacji** – zachowanie poufności, integralności i dostępności; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność, które można osiągnąć wdrażając odpowiedni zestaw zabezpieczeń (polityki, procesy, procedury, struktury organizacyjne, funkcje oprogramowania, sprzęt, itp.).
- **Bezpieczeństwo systemu informatycznego** - wszystkie aspekty związane z definiowaniem, osiąganiem i utrzymywaniem poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności systemu informatycznego
- **Bezpieczeństwo przetwarzania danych osobowych** - zachowanie poufności, integralności i rozliczalności danych osobowych; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak dostępność, autentyczność, niezaprzeczalność i niezawodność.
- **Dane Osobowe** - 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. Cechą odróżniającą dane osobowe od innych informacji dotyczących osób jest brak anonimowości, to znaczy: informacja ma charakter osobowy, dopóki jest możliwość ustalenia tożsamości osoby, której ona dotyczy. W kontekście działalności Spółki takimi danymi osobowymi może być w określonych sytuacjach także wolumen zużycia energii przypisany do danej osoby fizycznej, informacja o preferencjach dotyczących danego klienta, a także inne informacje, które mogą być przypisane zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
- **Dane szczególne i dane zwykłe - art. 6 ust. 1 i art. 9 ust. 1 RODO.** Pod pojęciem danych szczególnych rozumie się dane: ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Pozostałe dane mają charakter danych zwykłych.
- **Dostępność**, zwana też dyspozycyjnością - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne lub **dostępność** - właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.
- **DPIA –(**ang. Data protection impact assessment) ocena skutków przetwarzania danych osobowych.
- **Informacja** – wszystko, co posiada logiczne znaczenie, jako przekaz treści i może być praktycznie wykorzystane, skutkując osiągnięciem celu.
- **Integralność** – zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania.
- **Integralność danych** - właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.

- **Incydent związany z bezpieczeństwem informacji** - pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
- **Inspektor Ochrony Danych (IOD)** - osoba wyznaczona przez Prezesa Zarządu i zgłoszona do Prezesa Urzędu (następca GIODO), odpowiadająca za nadzorowanie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie ochrony danych osobowych.
- **Inspektor Bezpieczeństwa Informatycznego (IBI)**- wyznaczona przez Prezesa Zarządu osoba odpowiadająca za ochronę zasobów informacyjnych i technologii.
- **Know-how** – wiedza techniczna i pozatechniczna (handlowa, administracyjna, organizacyjna, finansowa), przydatna do wykonywania konkretnego rodzaju działalności gospodarczej. Całokształt doświadczeń, praktyk i procedur, jakie Spółka zdobyła w trakcie prowadzenia działalności, wpływających na sposób wykonywania usługi, odróżniających ją od usług konkurencyjnych firm.
- **Naruszenie ochrony danych osobowych** - zamierzone lub przypadkowe naruszenie środków technicznych i organizacyjnych zastosowanych w celu ochrony danych osobowych. W szczególności, gdy stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie ochrony danych osobowych.
- **Niezawodność** - właściwość oznaczająca spójne, zamierzone zachowanie i skutki.
- **Odbiorca danych osobowych lub kategorie odbiorców** - (art. 4 pkt 9 RODO) osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Wyjątkiem są wyłącznie organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem UE lub prawem państwa członkowskiego. Definicja ta nie wyłącza z grona „odbiorców" podmiotów, które wykluczone są z niego obecnie na podstawie art. 7 pkt 6 UODO. W szczególności chodzi tu o procesorów oraz osoby, które administrator, bądź procesor, upoważnili do przetwarzania danych.
- **Przetwarzanie Informacji** – jakiekolwiek operacje wykonywane na informacji, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie.
- **Poufność** – właściwość polegająca na tym, że informacja nie jest udostępniana nieupoważnionym osobom, podmiotom lub procesom.
- **Polityka bezpieczeństwa** - zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji informacji wrażliwej wewnątrz określonego systemu.
- **Podmiot przetwarzający (Procesor)** - oznaczona osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane w imieniu administratora.
- **Przetwarzanie danych osobowych** - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.
- **Przetwarzanie danych zwykłych** – przesłanki legalizujące przetwarzanie danych:
- zgoda osoby, której dane dotyczą (na przetwarzanie jej danych osobowych w jednym lub większej liczbie określonych celów);
- niezbędność przetwarzania do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
- niezbędność przetwarzania do wypełnienia obowiązku prawnego ciążącego na Spółce;
- niezbędność przetwarzania do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.
- **Przetwarzanie danych szczególnych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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.

przesłanki legalizujące przetwarzanie danych: niezbędność przetwarzania do wypełnienia obowiązków i wykonywania szczególnych praw przez Spółkę lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (w zakresie przewidzianym prawem UE lub prawem polskim, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą).

- **Podatność** - słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie.
- **Pseudonimizacja** - przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są chronione środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie danej osobie fizycznej.
- **Rozliczalność** - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
- **Ryzyko** - prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów.
- **System informatyczny (SI)** - należy przez to rozumieć system przetwarzania informacji wraz ze związanymi z nim ludźmi oraz zasobami organizacyjnymi ,technicznymi i finansowymi (urządzenia, programy, procedury przetwarzania informacji i narzędzia programowe), który dostarcza i rozprowadza informacje.
- **System Zarządzania Bezpieczeństwem Informacji** (SZBI) - część całościowego systemu zarządzania oparta na podejściu wynikającym z ryzyka biznesowego, odnosząca się do ustanawiania, wdrażania, eksploatacji, monitorowania, utrzymywania i doskonalenia bezpieczeństwa informacji. Obejmuje strukturę organizacyjną, polityki, planowane działania, odpowiedzialności, zasady, procedury, procesy i zasoby (aktywa).
- **Użytkownik systemu** - osoba upoważniona do bezpośredniego dostępu do danych osobowych przetwarzanych w systemie informatycznym, która posiada ustalony identyfikator i hasło.
- **Użytkownik zewnętrzny** - osoba nie będąca pracownikiem lub stażystą Spółki, posiadającą uprawnienia do przetwarzania informacji w związku z wykonywaniem czynności na jej rzecz.
- **Właściciel zasobów** –osoba kierująca komórką organizacyjną/pracownik na samodzielnym stanowisku, odpowiedzialna za ochronę danych osobowych przetwarzanych w podległej komórce. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
- **Właściciel** - osoba odpowiadająca za bezpośrednie zarządzanie aktywami, które ma pod opieką.
- **Zabezpieczenie** – praktyka, procedura lub mechanizm redukujący ryzyko
- **Zagrożenie** – potencjalna przyczyna mogąca wywołać incydent bezpieczeństwa.
- **Zdarzenie związane z bezpieczeństwem informacji** - jest określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe przełamanie polityki bezpieczeństwa informacji, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem.
- **Zgoda osoby, której dane dotyczą** Art. 4 Rozporządzenia UE - 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.
- **Zbiór danych osobowych** - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy zestawów danych, jest istnienie cechy (cech) pozwalającej na odnalezienie informacji bez potrzeby przeglądania całego zestawu.
- **Zbiór nieinformatyczny** - każdy posiadający strukturę zestaw danych o charakterze osobowym dostępnych według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie, prowadzony poza systemem informatycznym, w szczególności w formie kartoteki, księgi, wykazu lub innego zbioru ewidencyjnego.

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI

INFORMACJE PODLEGAJĄCE OCHRONIE

Konieczność stosowania **PBI** wynika z dwóch aspektów: biznesowego i prawnego.

1. **Aspekt biznesowy** - to dbałość o interesy Spółki, a przede wszystkim ochrona jej tajemnic. Kluczową sprawą jest tutaj ochrona tzw. tajemnicy przedsiębiorstwa, zdefiniowanej w Ustawie z 16 kwietnia 1993r. o zwalczaniu nieuczciwej konkurencji (Dz.U., Nr 47, poz.211, zwanej dalej uznik): ***Art. 11 ust. 4 Ustawy o zwalczaniu nieuczciwej konkurencji*** *„Przez Tajemnicę przedsiębiorstwa rozumie się: Nie ujawnione do wiadomości publicznej informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności".*

Jako **tajemnicę przedsiębiorstwa** określa się:
- know-how Spółki,
- informacje o stanie majątkowym i zobowiązaniach finansowych Spółki,
- dane pracowników i szczegóły zawieranych z nimi umów,
- dane klientów i szczegóły zawieranych z nimi umów.

Do informacji **know-how Spółki** należą wiedza i doświadczenie posiadające następujące cechy:
- **niejawność** - dane nie są powszechnie znane, nie można zdobyć ich z łatwo dostępnych źródeł,
- **istotność dla procesu produkcji lub wykonywania usługi** - określona wiedza jest niezbędna i w znaczący sposób odróżnia usługę od tych wykonywanych przez konkurencyjne firmy.

Spółka wypracowała know-how poprzez produkcję, przesył i dystrybucję energii cieplnej (w części udokumentowanej i w części pozostającej w posiadaniu pracowników).

Jako **know-how Spółki** określa się:
- bazy danych, w tym bazy klientów,
- wewnętrzne akty prawne,
- procedury i instrukcje zawarte w Zintegrowanym Systemie Zarządzania,
- rozwiązania informatyczne, techniczne i technologiczne opracowane przez pracowników Spółki.

2. **Aspekt prawny** - konieczność stosowania PBI wiąże się z konkretnymi wymaganiami w celu ochrony danego rodzaju informacji, a zarazem z poniesieniem przez Spółkę niezbędnych kosztów.

Regulacje prawne:
- **Informacje zawierające dane osobowe pracowników i klientów** 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.
- **nieuprawnione uzyskanie informacji** na podstawie Kodeksu Karnego: Art. 267 § 1. *„Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. § 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. § 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie".*
- **naruszenie integralności lub zniszczenia zapisu w informacji podlegającej ochronie**: Art. 268 Kodeksu Karnego § 1. *„Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".*
- **w przypadku oszustw komputerowych**: Art. 287 Kodeksu Karnego *„Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo*

wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do 5 lat".

- **dokonanie czynu nieuczciwej konkurencji** na podstawie Ustawy o zwalczaniu nieuczciwej konkurencji: Art. 11 ust.1 *„Czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa albo ich nabycie od osoby nieuprawnionej, jeżeli zagraża lub narusza interes przedsiębiorcy;* Art. 18 :*W razie dokonania czynu nieuczciwej konkurencji przedsiębiorca, którego interes został zagrożony lub naruszony, może żądać: zaniechania niedozwolonych działań, usunięcia skutków niedozwolonych działań, złożenia jednokrotnego lub wielokrotnego oświadczenia o odpowiedniej treści i w odpowiedniej formie, naprawienia wyrządzonej szkody na zasadach ogólnych, wydania bezpodstawnie uzyskanych korzyści na zasadach ogólnych, zasądzenia odpowiedniej sumy pieniężnej na określony cel społeczny związany ze wspieraniem kultury polskiej lub ochroną dziedzictwa narodowego - jeżeli czyn nieuczciwej konkurencji był zawiniony.* Art. 23: 1. *Kto, wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informację stanowiącą tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. 2. Tej samej karze podlega, kto, uzyskawszy bezprawnie informację stanowiącą tajemnicę przedsiębiorstwa, ujawnia ją innej osobie lub wykorzystuje we własnej działalności gospodarczej".*

ROLE I ODPOWIEDZIALNOŚCI ZA BEZPIECZEŃSTWO INFORMACJI

Cel: Ustanowić strukturę zarządzania w celu bezpiecznego przetwarzania informacji. Zapewnić rozliczalność użytkowników.

Odpowiedzialność i obowiązki Administratora[2] Danych Osobowych (ADO)

Administratorem jest ENGIE EC SŁUPSK Spółka z o.o reprezentowana przez PREZESA ZARZĄDU. Poprzez przywództwo i zaangażowanie Administrator zapewnia, że:

- cele bezpieczeństwa są ustanowione i zgodne z kierunkiem strategicznym Spółki,
- wymagania systemu zarządzania bezpieczeństwem informacji (SZBI) są zintegrowane z procesami,
- są dostępne potrzebne zasoby w SZBI.

Administrator ustala cele i sposoby przetwarzania danych osobowych i jest zobowiązany w szczególności do:

- zapewnienia warunków organizacyjnych, administracyjnych i technicznych, gwarantujących ochronę danych osobowych;
- zapewnienia środków organizacyjnych i technicznych, które są w szczególności związane z:
  1. pseudonimizacją i szyfrowaniem danych osobowych;
  2. zdolnością do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
  3. zdolnością do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
  4. regularnym testowaniem, mierzeniem i ocenianiem skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Odpowiedzialność i obowiązki Inspektora Ochrony Danych (IOD)

Administrator wyznacza IOD. Nadzoruje on przestrzeganie zasad dot. bezpieczeństwa informacji ze szczególnym uwzględnieniem ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych w formie papierowej i elektronicznej.

Do obowiązków IOD należy:

- nadzór nad ustanowieniem i wdrażaniem Polityki Bezpieczeństwa Informacji i powiązanych procedur,

[2] W nazewnictwie stosuje się określenia: Administrator ; Administrator danych; Administrator danych osobowych – ADO.

- nadzór nad realizacją zadań w Spółce zgodnie z zapisami zatwierdzonej Polityki Bezpieczeństwa Informacji;
- nadzór nad wdrożeniem stosownych środków organizacyjnych, technicznych i fizycznych w celu ochrony przetwarzanych danych osobowych;
- nadzór nad zapewnieniem, przez właścicieli zasobów danych osobowych, dostosowania funkcjonalności systemów przetwarzających dane osobowe do wymagań prawnych;
- reagowanie na zgłaszane incydenty związane z naruszenie ochrony danych osobowych oraz analizowanie ich przyczyn i kierowanie wniosków dotyczących ukarania winnych naruszeń;
- sprawdzanie wypełniania obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych;
- prowadzenie rejestru przetwarzania danych;
- prowadzenia rejestru naruszeń danych osobowych;
- informowanie ADO oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich i doradzanie im w tej sprawie;
- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
- współpraca z 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.

IOD w zakresie realizacji swoich obowiązków, ma prawo żądania od pozostałych osób, bez względu na rangę ich stanowiska, udzielania natychmiastowej pomocy w razie stwierdzenia, że doszło do naruszenia przepisów o ochronie danych osobowych.

Zakres kompetencji:

- z upoważnienia Administratora Danych Osobowych - nadawanie, zmienianie oraz cofanie uprawnień do przetwarzania danych osobowych na wniosek Właścicieli zasobów dla pracowników oraz użytkowników zewnętrznych;
- monitorowanie przestrzegania przepisów o ochronie danych oraz polityk Spółki 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;
- sprawdzanie wypełniania obowiązków technicznych i organizacyjnych związanych z ochroną danych osobowych.

Odpowiedzialność i obowiązki Inspektora Bezpieczeństwa Informatycznego (IBI)

Funkcję IBI pełni pracownik wyznaczony przez Administratora. IBI odpowiada za ochronę zasobów informacyjnych i technologii. Kieruje personelem w zakresie identyfikowania, opracowywania, wdrażania i utrzymywania procesów w celu ograniczenia ryzyka związanego z technologiami informacyjnymi. Odpowiada na incydenty, ustanawia odpowiednie standardy i kontrole. Zarządza technologiami bezpieczeństwa oraz kieruje ustanowieniem i wdrażaniem Polityki Bezpieczeństwa Informacji i powiązanych procedur.

Odpowiedzialność i obowiązki Administratora Systemów Informatycznych (ASI)

Funkcję ASI pełni pracownik wyznaczony przez Administratora odpowiedzialny za funkcjonowanie infrastruktury informatycznej, na którą składa się cały sprzęt informatyczny oraz systemy i aplikacje, za ich przeglądy, archiwizację i konserwację oraz za stosowanie technicznych i organizacyjnych środków bezpieczeństwa. ASI odpowiada także za wdrażanie i utrzymanie Systemów Informatycznych zgodnych z wymogami Ustawy o ochronie danych osobowych. Prowadzi dokumentację systemów informatycznych zawierającą opis współpracy pomiędzy różnymi systemami informatycznymi oraz sposób przepływu danych pomiędzy systemami, w których dane są przetwarzane. Do obowiązków ASI należy :

- określanie potrzeb w zakresie zabezpieczenia zbiorów danych osobowych;
- bieżący nadzór oraz zapewnienie optymalnej ciągłości działania systemu informatycznego w tym procedur określających zarządzanie systemem informatycznym przetwarzającym dane osobowe;
- monitorowanie Systemów Informatycznych i reagowanie bez zbędnej zwłoki, w przypadku naruszenia

bądź powstania zagrożenia bezpieczeństwa danych osobowych;
- analiza raportów wszelkich zdarzeń, w tym incydentów z bezpieczeństwem systemów przetwarzania danych;
- przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych;
- zapewnienie zgodności wszystkich wdrażanych systemów przetwarzania danych osobowych z Rozporządzeniem o ochronie danych osobowych oraz z niniejszą PBI;
- instalacja i konfiguracja oprogramowania oraz sprzętu sieciowego i serwerowego używanego do przetwarzania danych osobowych;
- konfiguracja i administracja oprogramowaniem systemowym i sieciowym zabezpieczającym dane osobowe przed nieupoważnionym dostępem;
- nadzór nad czynnościami związanymi ze sprawdzaniem systemu pod katem obecności szkodliwego oprogramowania;
- nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji;
- nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
- świadczenie pomocy technicznej w ramach oprogramowania a także serwis sprzętu komputerowego będącego na stanie Spółka Spółki z o.o. w Słupsku, służącego do przetwarzania danych;
- diagnozowanie i usuwanie awarii sprzętu komputerowego oraz realizację umów z firmami świadczącymi usługi serwisu pogwarancyjnego sprzętu komputerowego;
- wykonywanie i zarządzanie kopiami awaryjnymi oprogramowania systemowego (w tym danych osobowych oraz zasobów umożliwiających ich przetwarzanie) i sieciowego;
- wykonywanie i przechowywanie dokumentacji w zakresie kompetencji ASI;
- nadzór nad wdrożeniem i zarządzanie aplikacjami (przeglądanie, nadawanie i odbieranie uprawnień użytkownikom, itp.) , w których przetwarza się dane osobowe;

Do kompetencji ASI należy:
- przyznawanie na wniosek Właściciela zbiorów, za zgodą IOD ściśle określonych praw dostępu do danych osobowych w danym systemie;
- nadawanie uprawnień w celu dostępu zdalnego do systemów informatycznych przetwarzających dane osobowe po uzyskaniu akceptacji Administratora Danych Osobowych;
- zabezpieczenie systemów przetwarzania danych osobowych w zależności od kategorii przetwarzanych w tych systemach danych;
- zapewnienie poufności, integralności i rozliczalności danych przetwarzanych w systemach informatycznych.

Odpowiedzialność i obowiązki Właściciela zasobów

Właściciel zasobów (jest równocześnie właścicielem zasobów danych osobowych) - osoba kierująca komórką organizacyjną lub pracująca na samodzielnym stanowisku, odpowiedzialna za ochronę informacji stanowiącą tajemnicę Spółki jak i za ochronę danych osobowych przetwarzanych w podległej komórce. Jest ona zobowiązana zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

Odpowiada za:
- określenie wymagań bezpieczeństwa dla zasobu;
- podejmowanie decyzji związanych z zarządzaniem uprawnieniami do zasobu;
- realizację zadań z obszaru bezpieczeństwa informacji w zakresie przypisanym do ich jednostki organizacyjnej;
- podejmowanie decyzji związanych z zarządzaniem uprawnieniami podległych pracowników i współpracowników.

W przypadku ochrony danych osobowych, do obowiązków Właścicieli zasobów danych osobowych należy:
- zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia;

- zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu;
- realizację obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane;
- zapewnienie, na żądanie uprawnionych osób, udostępnienia informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione;
- zapewnienie, złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania tajemnicy danych osobowych oraz informacji na temat zabezpieczeń danych osobowych;
- zapewnienie, uzyskania przez pracowników przetwarzających dane osobowe, formalnego upoważnienia do przetwarzania danych osobowych;
- przekazywanie informacji do IOD oraz do ASI w przypadku utworzenia nowego zbioru danych osobowych. Informacja zawiera: ustalenie, kogo dotyczą dane osobowe, jaki jest ich zakres (np. imię i nazwisko, adres zamieszkania, PESEL, itp.), cel przetwarzania oraz komu dane osobowe mają być udostępnione;
- informowanie IOD o wszelkich zauważonych naruszeniach oraz nieprawidłowości w działaniu systemu przetwarzającego dane osobowe.

Ponadto Właściciel zasobów danych osobowych, sprawuje bezpośredni nadzór i kontrolę nad:
- danymi przetwarzanymi w komórce oraz nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane;
- czynnościami związanymi z przetwarzaniem danych osobowych, w szczególności aby dane te były przez podległych pracowników:
  a. przetwarzane zgodnie z prawem;
  b. zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu, niezgodnemu z tymi celami;
  c. merytorycznie poprawne i adekwatne w stosunku do celów, w jakim są przetwarzane;
  d. przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Do kompetencji Właściciela zasobów danych osobowych należy :
- określenie celów, w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych;
- określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych, czy w zbiorach nieinformatycznych);
- ustalenie, czy dane przetwarzane dla określonego celu mają mieć charakter poufny.

Odpowiedzialność i obowiązki pracowników (w tym właścicieli) i innych użytkowników

Pracownicy/użytkownicy zewnętrzni są zobowiązani do:
- prawidłowej realizację zadań w zakresie zarządzania bezpieczeństwem informacji, zleconych im przez przełożonych;
- przestrzegania w trakcie pracy ustanowionych zasad bezpieczeństwa;
- Postępowania zgodnie z PBI;
- wnioskowania o zastosowanie środków technicznych i organizacyjnych zapewniających bezpieczeństwo aktywów informacyjnych przetwarzanych na stanowisku pracy.

Ponadto, w przypadku przetwarzania danych osobowych odpowiedzialni są za:
- zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczeń;
- ochronę danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem, lub zniekształceniem;
- przetwarzania wyłącznie na podstawie wytycznych określonych przez kierownika komórki organizacyjnej (właściciela zasobów) oraz ważnego upoważnienia do przetwarzania danych osobowych;
- przetwarzania na podstawie przesłanek prawnych od chwili zebrania danych osobowych do chwili ich usunięcia,
- zachowanie szczególnej ostrożności w przypadku korzystania z komputera przenośnego, a w szczególności do:
  a. zabezpieczenia dostępu do komputera,

b. nieudostępniania komputera osobom nieupoważnionym,
- przestrzeganie procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych;
- informowanie Inspektora Ochrony Danych o wszelkich zauważonych naruszeniach oraz nieprawidłowości w działaniu systemu przetwarzającego dane osobowe.

ZAKRES I ZASADY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Zakres stosowania dotyczy wszystkich procesów prowadzonej działalności i ma zastosowanie do całego systemu informacyjnego Spółki, w szczególności do:
- wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są informacje podlegające ochronie;
- informacji będących własnością Spółki;
- informacji będących własnością klientów Spółki, uzyskanych na podstawie zawartych umów;
- wszystkich lokalizacji Spółki, czyli budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie;
- wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy, konsultantów, praktykantów/stażystów i innych osób mających dostęp do informacji podlegających ochronie.

1. Bezpieczeństwo zasobów ludzkich

Cel: zapewnić, żeby pracownicy i kontrahenci rozumieli swoją odpowiedzialność i byli odpowiednio przeszkoleni do ról, do których są przewidziani. Byli świadomi swoich obowiązków dotyczących bezpieczeństwa informacji i wypełniali je.

1.1. Każdy nowozatrudniony pracownik, przechodzi szkolenie z podstawowych zasad bezpieczeństwa informacji w pierwszym dniu pracy. Za przeprowadzenie szkolenia i przechowywanie zapisów odpowiada IOD. Pracownik zapoznaje się z dokumentem „Polityka Bezpieczeństwa Informacji" i podpisuje **OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI** stanowiące **Załącznik nr 1_BI**. Podpisane oświadczenie przechowywane jest w aktach osobowych pracownika.

1.2. W przypadku wprowadzanych zmian w zarządzaniu bezpieczeństwem informacji (np. w dokumentacji, w sposobie postępowania), każdy pracownik w swojej komórce organizacyjnej jest zapoznany z wprowadzonymi zmianami oraz w ramach działań przypominających z zasadami stosowanymi w celu ochrony informacji. Odpowiedzialność za przestrzeganie przez pracowników poniższych zasad ponosi kierownik danej komórki organizacyjnej/właściciel zasobów.
- **Zasada uprawnionego dostępu.** Każdy pracownik przeszedł szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisał oświadczenie o zachowaniu poufności **(Załącznik nr 1_BI).**
- **Zasada przywilejów koniecznych**. Każdy pracownik posiada prawa dostępu do informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań.
- **Zasada wiedzy koniecznej**. Każdy pracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań.
- **Zasada usług koniecznych**. Spółka świadczy tylko takie usługi jakich wymaga Klient zgodnie z zawartymi umowami.
- **Zasada świadomości zbiorowej**. Wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych Spółki i aktywnie uczestniczą w tym procesie.
- **Zasada indywidualnej odpowiedzialności**. Za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.
- **Zasada obecności koniecznej**. Prawo przebywania w określonych miejscach mają tylko osoby upoważnione.

1.3. W umowach z nowo zatrudnionymi pracownikami Spółki lub osobami wykonującymi świadczenia na rzecz Spółki na podstawie umów cywilnoprawnych muszą być zawierane zapisy o zachowaniu w poufności oraz nieujawnianiu informacji będących tajemnicą przedsiębiorstwa o treści:

– *"Zobowiązuję się do zachowania w tajemnicy informacji, do których mam lub będę miał(a) dostęp, w szczególności informacji dotyczących danych osobowych, technicznych, technologicznych, organizacyjnych oraz innych posiadających wartość gospodarczą, nieujawnionych do publicznej wiadomości."*

Ponadto zapisy zabezpieczające majątkowe prawa autorskie pracodawcy o treści:

– *„Pracodawca/świadczeniodawca ma prawo do korzystania z wyników pracy wykonywanej przez pracowników/świadczeniobiorców i nabywa majątkowe prawa autorskie do utworów (zgodnie z definicją określoną w Ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych Dz.U. z 2006 r. Nr 90 poz. 631 z późn. zm.)stworzonych przez pracownika w wyniku wykonywania obowiązków ze stosunku pracy/w wyniku wykonywania świadczenia na podstawie umowy cywilnoprawnej".*

Za włączenie powyższych zapisów do umów odpowiada Kierownik Działu Zasobów Ludzkich i Administracji.

1.4. W kartach zadań pracownika zostają dodane następujące zapisy :

1.4.1. w części szczegółowej karty zadań pracownika pkt. III zadania w zakresie stosowania bezpieczeństwa informacji:

1. *Zobowiązanie do zachowania w tajemnicy informacji, do których ma lub będzie miał(a) dostęp, w szczególności informacji dotyczących danych osobowych, technicznych, technologicznych, organizacyjnych oraz innych posiadających wartość gospodarczą, nieujawnionych do publicznej wiadomości.*
2. *Realizacja zadań w zakresie zarządzania bezpieczeństwem informacji, zleconych przez przełożonych.*
3. *Przestrzeganie w trakcie pracy ustanowionych zasad bezpieczeństwa informacji.*
4. *Wnioskowanie o zastosowanie środków technicznych i organizacyjnych zapewniających bezpieczeństwo aktywów informacyjnych przetwarzanych na stanowisku pracy.*
5. *W przypadku przetwarzania danych osobowych, do obowiązków należy:*

– *przetwarzanie wyłącznie na podstawie wytycznych określonych przez kierownika komórki organizacyjnej (właściciela zasobów) oraz ważnego upoważnienia do przetwarzania danych osobowych,*
– *przetwarzanie na podstawie przesłanek prawnych od chwili zebrania danych osobowych do chwili ich usunięcia,*
– *informowanie Inspektora Ochrony Danych o wszelkich zauważonych naruszeniach oraz nieprawidłowości w działaniu systemu przetwarzającego dane osobowe.*

1.4.2. w części szczegółowej karty zadań właściciela zasobów/kierownika komórki organizacyjnej/osoby wykonującej obowiązki na stanowisku samodzielnym pkt. III zadania w zakresie stosowania bezpieczeństwa informacji:

1. Zobowiązanie do zachowania w tajemnicy informacji, do których ma lub będzie miał(a) dostęp, w szczególności informacji dotyczących danych osobowych, technicznych, technologicznych, organizacyjnych oraz innych posiadających wartość gospodarczą, nieujawnionych do publicznej wiadomości.
2. *Realizacja zadań w zakresie zarządzania bezpieczeństwem informacji, zleconych przez przełożonych.*
3. *Wnioskowanie o zastosowanie środków technicznych i organizacyjnych zapewniających bezpieczeństwo aktywów informacyjnych przetwarzanych w podległej komórce organizacyjnej.*
4. *W przypadku ochrony danych osobowych, do obowiązków Właściciela zasobów danych osobowych należy:*

– *zapewnienie podstaw prawnych do przetwarzania danych osobowych od chwili zebrania danych osobowych do chwili ich usunięcia;*
– *zapewnienie aktualności, adekwatności oraz merytorycznej poprawności danych osobowych przetwarzanych w określonym przez nich celu;*
– *realizacja obowiązku informowania o przetwarzaniu danych osobowych osób, których dane osobowe są pozyskiwane;*

- *zapewnienie, na żądanie uprawnionych osób, udostępnienia informacji o przetwarzanych danych osobowych oraz podmiotach, którym zostały one udostępnione;*
- *zapewnienie, złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania tajemnicy danych osobowych oraz informacji na temat zabezpieczeń danych osobowych;*
- *zapewnienie, uzyskania przez pracowników przetwarzających dane osobowe, formalnego upoważnienia do przetwarzania danych osobowych;*
- *przekazywanie informacji do Inspektora Ochrony Danych oraz do Administratora Systemów Informatycznych w przypadku utworzenia nowego zbioru danych osobowych.*
- *informowanie IOD o wszelkich zauważonych naruszeniach oraz nieprawidłowości w działaniu systemu przetwarzającego dane osobowe.*

Do kompetencji Właściciela zasobów danych osobowych należy :

- *Określenie celów, w jakich mają być przetwarzane dane osobowe, zakresu oraz czasu trwania przetwarzania danych osobowych;*
- *Określenie sposobu przetwarzania danych osobowych (czy w systemach informatycznych, czy w zbiorach nieinformatycznych) ;*
- *Ustalenie, czy dane przetwarzane dla określonego celu mają mieć charakter poufny.*

Nadzór i kontrola:

Właściciel zasobów danych osobowych, sprawuje bezpośredni nadzór i kontrolę nad:

- *danymi przetwarzanymi w komórce oraz nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane;*
- *czynnościami związanymi z przetwarzaniem danych osobowych, w szczególności aby dane te były przez podległych pracowników:*
  - e. *przetwarzane zgodnie z prawem;*
  - f. *zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu, niezgodnemu z tymi celami;*
  - g. *merytorycznie poprawne i adekwatne w stosunku do celów, w jakim są przetwarzane;*
  - h. *przechowywane w postaci uniemożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.*

Odpowiada za:

- *określenie wymagań bezpieczeństwa dla zasobu;*
- *podejmowanie decyzji związanych z zarządzaniem uprawnieniami do zasobu;*
- *realizację zadań z obszaru bezpieczeństwa informacji w zakresie przypisanym do komórki organizacyjnej;*
- *podejmowanie decyzji związanych z zarządzaniem uprawnieniami podległych pracowników i współpracowników;*

1.4.3. (w części szczegółowej karty zadań wszystkich pracowników IV„INFORMACJA PRACODAWCY): *Pracodawca ma prawo do korzystania z wyników pracy wykonywanej przez pracownika i nabywa majątkowe prawa autorskie do utworów (zgodnie z definicją określoną w Ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych Dz.U. 2016 poz. 666 stworzonych przez pracownika w wyniku wykonywania obowiązków ze stosunku pracy".*

Opracowane według nowego wzoru Karty zadań pracownika będą podlegały wymianie wraz ze zmianą zakresu obowiązków pracownika.

2. Bezpieczeństwo informacji

Cel: zapewnić bezpieczeństwo aktywom informacyjnym Spółki w relacjach z interesariuszami.

- W przypadku udostępnienia informacji stanowiących tajemnicę spółki osobom współpracującym lub stażystom/praktykantom wymagane jest przeprowadzenie szkolenia i podpisanie **ZOBOWIĄZANIA DO ZACHOWANIA BEZPIECZEŃSTWA INFORMACJI stanowiące Załącznik nr 2_BI.** Szkolenie przeprowadza IOD. Dokumentacja jest przechowywana przez IOD. Za skierowanie osoby na szkolenie odpowiada w przypadku praktykantów/stażystów – pracownik działu HR nadzorujący w Spółce proces szkolenia praktykantów/stażystów,

- w przypadku współpracowników/dostawców Spółki – właściciel aktywów (kierownik komórki organizacyjnej, pracownik na samodzielnym stanowisku), które ma pod bezpośrednią opieką i które zostaną udostępnione.

2.1. Kontrahentom należy udostępniać tylko te informacje, które są niezbędne do wykonania umowy.

2.2. W przypadku udostępnienia informacji stanowiących tajemnicę spółki osobom współpracującym w trakcie spotkań grupowych wymagane jest podpisanie **ZOBOWIĄZANIA DO ZACHOWANIA POUFNOŚCI INFORMACJI stanowiące Załącznik nr 3_BI.** Dokumentacja jest przechowywana przez IOD natomiast odpowiedzialność za dopełnienie formalności spoczywa na osobie organizującej spotkanie.

2.3. **Umowy o zachowaniu poufności/ Umowy o wymianie informacji.** W uzasadnionych przepisami prawa bądź względami bezpieczeństwa, wymiana informacji i oprogramowania pomiędzy Spółką a stronami zewnętrznymi podlega regulacji w drodze umowy. W umowach z Podmiotami zewnętrznymi należy zawierać zapisy o zachowaniu w poufności i nieujawnianiu informacji o treści:
" Zobowiązuję się do zachowania w tajemnicy informacji, do których mam lub będę miał(a) dostęp, w szczególności informacji dotyczących danych osobowych, technicznych, technologicznych, organizacyjnych oraz innych posiadających wartość gospodarczą, nieujawnionych do publicznej wiadomości." **Za włączenie do treści umowy zapisów o zachowaniu w poufności odpowiada Kierownik komórki organizacyjnej sporządzającej umowę.**

3. Bezpieczeństwo fizyczne i środowiskowe

Cel: zapobiec nieuprawnionemu fizycznemu dostępowi, szkodom i zakłóceniom w informacjach należących do Spółki.

3.1. Aktywa informacyjne w tym dane osobowe mogą być przetwarzane wyłącznie w bezpiecznych pomieszczeniach zgodnie z zasadą wiedzy koniecznej i w sposób uniemożliwiający złośliwe działania. Do pomieszczeń przetwarzania danych osobowych zalicza się :
- Serwerownie;
- pomieszczenia biurowe, w których zlokalizowane są stacje robocze;
- pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe;
- pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego;
- pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.

W przypadku konieczności przetwarzania danych w innych miejscach niż w.wym. konieczna jest zgoda Administratora.

3.2. Przebywanie wewnątrz obszarów bezpiecznych, osób nieuprawnionych do przetwarzania danych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych za zgodą Właściciela zasobów.

3.3. Budynki lub pomieszczenia, w których przetwarzane są dane, są zamykane podczas nieobecności osób upoważnionych.

3.4. Stosuje się **politykę kluczy** polegającą na tym, że:
- Klucze do pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych.
- Klucze do pomieszczeń szczególnie chronionych tj. serwerowni/archiwum wydawane są za pobraniem i pozostają pod osobistym nadzorem osób upoważnionych.
- Klucze zapasowe przechowywane są w zamkniętej szafce na poziomie I kotłowni KR-1.
- Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą Właścicieli zasobów. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu.

- Klucze służące do zabezpieczenia biurek i szaf w godzinach pracy pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie
- Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
- Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń a w szczególności (wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi, inne).

3.5. Zakazane jest przetwarzanie danych w tych pomieszczeniach, w których osoby Trzecie wykonują prace techniczne.

3.6. Sprzęt do przetwarzania danych w pomieszczeniach bezpiecznych należy umieszczać w takich miejscach, aby zminimalizować niepotrzebny dostęp do obszarów pracy.

3.7. Zabrania się spożywania posiłków i napojów w bliskim sąsiedztwie środków przetwarzania informacji.

3.8. Sprzęt, informacje lub oprogramowanie mogą być wynoszone poza siedzibę Spółki wyłącznie za zgodą Administratora i należy je zabezpieczyć przed wystąpieniem różnych ryzyk związanych z pracą poza miejscami bezpiecznymi.

3.9. Zgoda na użytkowanie komputera przenośnego, do wykonywania czynności służbowych poza obszarami bezpiecznymi (tj. poza siedzibą Spółki) wyrażona jest w formie pisemnej. Wniosek o wyrażenie zgody/wycofanie zgody składa kierownik działu Użytkownika/właściciel zasobów za pośrednictwem IOD. Podpisana przez Prezesa Zarządu zgoda przekazana jest Użytkownikowi (2 egz. przechowywany jest przez IOD). Informację o wyrażonej zgodzie IOD przekazuje kierownikowi działu/właścicielowi zasobów oraz do działu IT w celu wprowadzenia odpowiednich zabezpieczeń.

3.10. Sprzęt, przed zbyciem lub przekazaniem do ponownego użycia należy przekazać ASI w celu sprawdzenia wszystkich jego składników zawierających nośniki informacji, dla zapewnienia, że wszystkie dane i licencjonowane programy zostały usunięte lub bezpiecznie nadpisane.

3.11. Każdy pracownik zobowiązany jest do stosowania **polityki czystego biurka dla dokumentów papierowych i czystego ekranu** dla środków przetwarzania informacji, polegających na tym że:
- po zakończonym dniu pracy bieżąca dokumentacja w formie papierowej oraz nośniki elektroniczne są przechowywane w zamkniętych szafach/biurkach lub w innym bezpiecznym miejscu wskazanym przez właściciela aktywów (kierownika komórki organizacyjnej),
- na biurku pozostaje jedynie telefon, materiały biurowe, organizer na dokumenty powszechnie używane.
- W sytuacjach nagłych, związanych w szczególności ze stanem zdrowia pracownika lub przedłużającą się nieobecnością w biurze, za realizację Polityki w jego imieniu odpowiada właściciel zasobów (kierownik komórki organizacyjnej) lub solidarnie pracownicy, których stanowiska pracy znajdują się najbliżej.
- Dokumentacja przechowywana w formie elektronicznej jest zabezpieczona poprzez wyłączenie komputera (zabezpieczonego indywidualnym hasłem i przy zachowaniu zasad określonych w części III PBI - Zarządzanie bezpieczeństwem informatycznym- Zasady bezpieczeństwa podczas pracy w systemie informatycznym).
- W przypadku czasowego opuszczenia stanowiska pracy, pracownik jest zobowiązany do każdorazowego blokowania komputera poprzez włączenie wygaszacza ekranu.

3.12. Każdorazowe uchybienie zabezpieczeń fizycznych chroniących dane osobowe musi być zgłaszane do IOD.

3.13. Wszyscy pracownicy i użytkownicy podmiotów zewnętrznych, w momencie zakończenia zatrudnienia, umowy lub porozumienia zobowiązani są do zwrotu aktywów związanych z informacją i środkami przetwarzania informacji.

4. Postępowanie dyscyplinarne

4.1. W przypadku naruszenia zasad bezpieczeństwa informacji przez Pracownika zastosowanie znajdują przepisy Kodeksu Pracy i obowiązującego prawa oraz Regulaminu Pracy obowiązującego w Spółce. Za wszczęcie postępowania dyscyplinarnego z powodu naruszenia zasad bezpieczeństwa odpowiada kierownik komórki organizacyjnej. W postępowaniu dyscyplinarnym uwzględnia się takie czynniki jak:

- rodzaj i waga naruszenia bezpieczeństwa informacji;
- wpływ naruszenia na biznes;
- częstotliwość występowania (czy jest to pierwsze czy kolejne naruszenie);
- czy winny był prawidłowo przeszkolony;
- inne stosowne do okoliczności czynniki.

4.2. Naruszenie zasad ochrony danych przez pracownika/użytkownika zewnętrznego może skutkować postawieniem mu zarzutu, określonego w art. 266-269c Kodeksu Karnego (Rozdział XXXIII Przestępstwa przeciwko ochronie informacji).

4.3. Zgodnie z art. 100 §2 pkt 5 Kodeksu Pracy, pracownik jest obowiązany do przestrzegania tajemnicy określonej w odrębnych przepisach. Dane osobowe, którym Spółka nadaje charakter poufny mają charakter takiej tajemnicy, a jej ujawnienie w zależności od zakresu ujawnionych danych osobowych oraz nastawienia pracownika dopuszczającego się nieuprawnionego ujawnienia danych, może mieć charakter naruszenia lub ciężkiego naruszenia obowiązków pracowniczych.

4.4. Pracownik dopuszczający się nieuprawnionego ujawnienia lub wykorzystania danych osobowych w sposób sprzeczny z ich przeznaczeniem (np. wykorzystania danych osobowych do celów prywatnych) czy też ich przetwarzania w sposób niezgodny z przyjętymi w Spółce procedurami może zostać ukarany karą upomnienia lub nagany.

4.5. W razie ciężkiego naruszenia obowiązku zachowania danych osobowych w tajemnicy lub przetwarzania ich w sposób rażąco sprzeczny z przyjętymi zasadami i procedurami, Administrator może rozwiązać bez wypowiedzenia umowę o pracę z winy pracownika.

4.6. Sankcje dotyczące ujawnienia poufnych danych stosuje się analogicznie do ujawnienia przez pracownika informacji dotyczących stosowanych zabezpieczeń.

5. Postępowanie w przypadku naruszenia zasad ochrony danych

W przypadku naruszenia zasad ochrony danych prowadzących do **incydentu bezpieczeństwa** informacji należy postępować zgodnie z instrukcjami zawartymi w **PBI** oraz w Planie Reagowania Kryzysowego – wydawanym Zarządzeniem Prezesa Spółki. Zarządzanie incydentem kryzysowym prowadzone jest w oparciu o wypracowane i wdrożone postępowanie:

- Wykrycie incydentu;
- Regularne monitorowanie incydentu;
- Prowadzenie wewnętrznej komunikacji oraz reagowanie na komunikaty zewnętrzne;
- Zapewnienie dostępności środków komunikacji podczas incydentu, który zakłóca działanie;
- Ułatwienie zorganizowanej komunikacji z instytucjami reagowania kryzysowego;
- Rejestrowania kluczowych informacji na temat incydentu, podjętych działań i decyzji;
- Informowania osób, których dane dotyczą, o zaistniałym lub nadchodzącym incydencie.

STOSOWANE ZABEZPIECZENIA W PRZEPŁYWIE INFORMACJI

Szczegółowy opis występujących zagrożeń oraz stosowanych zabezpieczeń zawarto w RAPORCIE dotyczącym podejścia Spółki do przetwarzania aktywów informacyjnych w tym danych osobowych, opartym na ryzyku, będącym załącznikiem do PBI.

Uwzględniając zagrożenia mogące mieć wpływ na bezpieczeństwo aktywów informacyjnych Spółki, w tym na bezpieczeństwo danych osobowych zastosowano szereg zabezpieczeń klasyfikując je następująco:

TYPY ZABEZPIECZEŃ	LISTA ZABEZPIECZEŃ
ORGANIZACYJNE	Regulamin Pracy, Regulamin Organizacyjny
	Polityka Bezpieczeństwa Informacji
	Instrukcja Bezpiecznego Zarządzania Systemem Informatycznym
	Plan Reagowania Kryzysowego
	Zarządzenia wewnętrzne dot. bezpieczeństwa informacji
	dokumentacja wdrożonych rozwiązań technicznych i fizycznych
	wyniki przeprowadzonych audytów
	instrukcje
PERSONALNE	weryfikacja uprawnień
	umowy/oświadczenia o zachowaniu poufności informacji
	umowy powierzenia przetwarzania danych osobowych
	zgody na przetwarzanie danych osobowych
TECHNICZNE	system antywirusowy, zabezpieczenia opisane w dokumencie poufnym "Instrukcja Bezpiecznego Zarządzania Systemem Informatycznym"
FIZYCZNE	wyznaczenie pomieszczeń bezpiecznych do przetwarzania danych
	określenie praw dostępu do miejsc bezpiecznych
	zabezpieczenie przed nieuprawnionym dostępem
	wprowadzenie zasady "czystych biurek", „politykę kluczy”

Na stosowane zabezpieczenia składają się m.in.:

- **infrastruktura informatyczna** – podzielona jest na biurową i przemysłową. Sprzęt jest regularnie przeglądany i rozbudowywany w zależności od potrzeb, a systemy informatyczne aktualizowane według zaleceń producentów – z wyjątkiem niektórych systemów przemysłowych których aktualizacja nie jest uzasadniona biznesowo.
- **Struktura organizacyjna** - umożliwia bezpośredni kontakt Zarządu z pracownikami. Nie funkcjonują zasady korporacyjne.
- **Zasoby ludzkie i kompetencje –** Spółka charakteryzuje się niewielką rotacją personelu, co przekłada się na wysoką świadomość i znajomość procesów z zakresu bezpieczeństwa informacji. Bezpieczeństwo zapewniają umowy na czas nieokreślony.
- **Procedury i wytyczne pracy** – istnieje udokumentowany Zintegrowany System Zarządzania zgodny z wymaganiami ISO 9001:2008; ISO 14001:2004; OHSAS 18001:2007. Funkcjonuje Regulamin Organizacyjny oraz Regulamin Pracy określający obowiązki i prawa pracowników.
- **Usługi bankowości elektronicznej oraz wydruki faktur** – w transakcjach bankowości elektronicznej oraz przy wymianie informacji w ramach usługi wydruku faktur wykorzystywany jest podpis elektroniczny, który cechuje się wysokim poziomem bezpieczeństwa informacji poprzez zapewnienie wykrywalności wszelkiej zmiany w danych transakcji (integralność transakcji), uniemożliwienie podszywanie się innych pod daną osobę (uwierzytelnienie osoby) oraz niezaprzeczalnym dowodem wykonania transakcji przez konkretną osobę.
- **Aspekty prawne** – Spółka spełnia wymagania Ustawy o Ochronie Danych Osobowych oraz RODO.

KONTROLA PROCESU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Realizacja procesu zarządzania bezpieczeństwem informacji poddawana jest corocznej kontroli przy wykorzystaniu m.in. poniższych miar:

Skala oceny:	**lp**	**stan procesu**
1 = Brak procesów / NIE	1	nowozatrudniony pracownik, przechodzi szkolenie z zasad bezpieczeństwa informacji w pierwszym dniu pracy
	2	pracownik składa oświadczenie o zachowaniu poufności - załącznik nr 1 do **PBI**
2 = Istnieje proces nieformalny / OPRACOWAĆ PONOWNIE	3	istnieją zapisy w umowach o pracę o zachowaniu w poufności oraz nieujawnianiu informacji będących tajemnicą przedsiębiorstwa
	4	istnieją zapisy w kartach zadań pracowników określające obowiązki/uprawnienia odnoszące się do zarządzania przetwarzanymi informacjami i danymi osobowymi
3 = Istnieje formalny, udokumentowany proces/ POPRAWIĆ	5	zobowiązania do zachowania bezpieczeństwa informacji - załącznik nr 2 wymagane w stosunku do osób współpracujących ze Spółką
	6	reagowanie na nowe sytuacje w zakresie bezpieczeństwa informacji,
4 = Istnieje formalny, udokumentowany proces, a ponadto mierzone są najważniejsze parametry / DOBRZE	7	dokonywanie okresowej oceny skuteczności wdrożonych zabezpieczeń,
	8	prowadzenie rejestru incydentów bezpieczeństwa informacji
5 = Istnieje formalny, udokumentowany proces, mierzone są najważniejsze parametry, a ponadto proces jest stale doskonalony na podstawie wyników pomiarów / BARDZO DOBRZE	9	opracowywanie rocznych raportów dotyczących stanu bezpieczeństwa informacji w obszarze bezpieczeństwa organizacyjnego.
	10	w przypadku incydentów - postępowanie zgodne z Planem reagowania kryzysowego

ZARZĄDZENIE BEZPIECZEŃSTWEM RZETWARZANIA DANYCH OSOBOWYCH

CEL ZARZĄDZANIA BEZPIECZEŃSTWEM PRZETWARZANIA DANYCH OSOBWYCH

Procesy przetwarzania danych osobowych podejmowane w Spółce są złożone i angażują wiele podmiotów, co wynika z konieczności m.in. dużej ilości kontrahentów, będących osobami fizycznymi, korzystania z nieruchomości osób trzecich, konieczności uzyskiwania licznych pozwoleń, uzgodnień i opinii. Celem zarządzania bezpieczeństwem przetwarzania danych osobowych w Spółce jest osiągnięcie poziomu organizacyjnego i technicznego, który pozwoli na właściwe wykonanie obowiązków Administratora Danych Osobowych (ADO) w zakresie zabezpieczenia i prawidłowej ochrony przetwarzanych danych osobowych.

Zarządzanie bezpieczeństwem danych osobowych pozwala na określenie:

- zasad przetwarzania danych osobowych oraz ich zabezpieczeń, jako zestawu praw, reguł i zaleceń służących ochronie i dystrybucji wewnątrz Spółki;
- procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń technicznych i organizacyjnych.

Ma zagwarantować, że :

1. na każdym etapie dane osobowe są przetwarzane w niezbędnym zakresie oraz w sposób integralny, poufny i rozliczalny;
2. pracownicy, wykonawcy oraz użytkownicy zewnętrzni:

- są odpowiednio wprowadzeni w swoje obowiązki i odpowiedzialności związane z ochroną danych osobowych i ich przetwarzaniem, przed przyznaniem im dostępu do danych osobowych;
- otrzymali zalecenia określające wymagania w zakresie bezpieczeństwa ochrony danych osobowych, związane z ich obowiązkami;
- wypełniają zalecenia i warunki zatrudnienia, które uwzględniają zasady ochrony danych osobowych oraz właściwe metody pracy;
- w sposób ciągły utrzymują odpowiednie umiejętności i kwalifikacje.

3. Za bieżącą, operacyjną ochronę danych osobowych odpowiada osoba przetwarzająca te dane w zakresie zgodnym z zakresem upoważnienia, kompetencjami lub rolą sprawowaną w procesie przetwarzania danych.

DANE OSOBOWE - KRYTERIA OCENY INFORMACJI

Podczas stosowania oceny, czy określona informacja lub zestaw informacji stanowią dane osobowe, osoby przetwarzające dane osobowe powinny brać pod uwagę następujące wytyczne:

1. przepisy RODO nie dotyczą przetwarzania danych (informacji) dotyczących osób zmarłych, osób prawnych oraz tzw. ułomnych osób prawnych (jednostek organizacyjnych nieposiadających osobowości prawnej), w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej lub ułomnej osoby prawnej;
2. w zależności od okoliczności konkretnego procesu przetwarzania danych osobowych, ta sama kategoria informacji (np. adres, imię i nazwisko) może stanowić dane osobowe lub też nie. W przypadkach braku pewności, czy określona kategoria danych stanowi daną osobową, należy z ostrożności stosować do tych informacji zasady ochrony danych osobowych określone w RODO;
3. dane zagregowane, które nie odnoszą się do jednej osoby, ale do całej grupy osób, nie stanowią danych osobowych, o ile nie można w takim agregacie danych zidentyfikować określonych osób fizycznych, których dane dotyczą. Przykładowo, informacja o adresie (danych adresowych mieszkania) może nie stanowić danej osobowej, jeżeli Spółka nie dysponuje dodatkowymi informacjami, które mógłby powiązać z tą informacją w taki sposób, aby zidentyfikować chociaż jeden podmiot danych (nawet pośrednio);
4. Spółka rozróżnia pseudonimizację od anonimizacji. Anonimizacja jest nieodwracalna, a pseudonimizacja jest procesem możliwym do odwrócenia z wykorzystaniem dodatkowych informacji (np. kluczy szyfrujących, danych źródłowych itp.).

ZASADY SŁUŻACE OCHRONIE PRZETWARZANYCH DANYCH OSOBOWYCH

Spółka, dbając o skuteczność ochrony danych osobowych stosuje m.in.:

- przeszkolenie pracowników dopuszczonych do przetwarzania danych w zakresie bezpieczeństwa danych osobowych;
- przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację w systemach informatycznych (np. hasła, identyfikatory), umożliwiających im dostęp do danych osobowych - stosownie do zakresu upoważnienia i indywidualnych poziomów dostępu;
- okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych;
- podejmowanie niezbędnych działań, w celu likwidacji słabych ogniw w systemie ochrony danych osobowych;
- śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i w miarę możliwości organizacyjnych i techniczno-finansowych wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, służących wzmocnieniu bezpieczeństwa przetwarzania danych osobowych.

Pracownicy spółki oraz użytkownicy zewnętrzni zobowiązani są do:

- wykorzystywania technik kryptograficznych do ochrony poufności, integralności i rozliczalności danych osobowych przesyłanych publicznymi sieciami telekomunikacyjnymi;
- ochrony danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji i zniszczeniem;
- stosowania zabezpieczeń i ograniczeń związanych z możliwością przekazywania wiadomości za pomocą środków komunikacji, np. automatyczne przekazywanie poczty elektronicznej na zewnątrz;
- niepozostawiania informacji zawierających dane osobowe przy urządzeniach drukujących, np. kopiarkach, drukarkach, faksach, do których mogą mieć dostęp osoby nieupoważnione;
- upewnienia się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych;
- zachowania szczególnej ostrożności w trakcie rozmów telefonicznych, unikając podsłuchania danych osobowych przez osoby nieupoważnione;
- niepozostawiania wiadomości zawierających dane osobowe w automatycznych sekretarkach;
- transportu danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane w sposób ograniczający możliwość ich pozyskania i odczytu przez osoby nieupoważnione.

Ponadto, Spółka przetwarzając dane osobowe kieruje się następującymi zasadami, służącymi ochronie praw osoby, której dane osobowe są przetwarzane i w poszanowaniu jej dóbr osobistych[3] i jako Administrator jest odpowiedzialny za przestrzeganie poniższych przepisów oraz musi być w stanie wykazać ich przestrzeganie („**rozliczalność**"). Dane muszą być[4]:

- przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą **(„zgodność z prawem, rzetelność i przejrzystość")**;
- zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („**ograniczenie celu**");
- adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („**minimalizacja danych**");
- 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**");
- przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których te dane są przetwarzane; dane osobowe można

[3] Wywiązując się z obowiązków wynikających z Rozporządzenia RODO wdrożono wzory dokumentów stanowiące załączniki do rozdziału II niniejszej Polityki na podstawie RAPORTU Z AUDYTU W ZAKRESIE NOWYCH PRZEPISÓW O ODO z dnia 09.11.2017r.

[4] Rozporządzenie RODO Rozdział II art.5 zasady dotyczące przetwarzania danych osobowych

przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust.1 („**ograniczenie przechowywania**");
- 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**").

1. Zgodność przetwarzania z prawem (art. 6 RODO)

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

a) **osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;**

b) **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** - (nie wymaga zgody na przetwarzanie danych) np.:
- przetwarzanie danych osobowych właściciela lokalu mieszkalnego w ramach wykonania umowy przez Spółkę na rzecz wspólnoty mieszkaniowej
- wnioski o zawarcie umowy (np. umowy kompleksowej lub umowy o przyłączenie do sieci) składane przez odbiorców ciepła i potencjalnych kontrahentów;

c)**przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze** - (nie wymaga zgody na przetwarzanie danych) np.:
- przetwarzanie danych osobowych właściciela nieruchomości w ramach wykonania dyspozycji normy art. 7 ust. 5 Prawa energetycznego w zakresie realizacji i finansowania budowy i rozbudowy sieci w przypadku, w którym na nieruchomości rzeczonego właściciela mają zostać posadowione urządzenia przesyłowe,
- przetwarzanie danych osobowych różnych podmiotów w zakresie sporządzania planów rozwoju w zakresie zaspokojenia obecnego i przyszłego zapotrzebowania na paliwa gazowe lub energię;

d) **przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej** - (nie wymaga zgody na przetwarzanie danych) np.:
- przetwarzanie danych osobowych właściciela nieruchomości, który zgłosił awarię urządzeń przesyłowych posadowionych na jego nieruchomości, która to awaria zagraża jego żywotnym interesom;

e) **przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi** - (nie wymaga zgody na przetwarzanie danych) np.:
- przetwarzanie danych osobowych różnych podmiotów w zakresie w realizacji i finansowania budowy i rozbudowy sieci ciepłowniczej;

f) **przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny 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 –** (nie wymaga zgody na przetwarzanie danych) np.:
- przetwarzanie danych osobowych w związku z koniecznością obsługi zgłoszeń awaryjnych różnymi kanałami komunikacji;
- przetwarzanie danych osobowych w związku ze zgłaszanymi roszczeniami lub reklamacjami;
- przetwarzanie danych osobowych przez podmiot trzeci w celu windykacji należności;
- marketing bezpośredni np. poprzez wysyłkę papierowych lub elektronicznych broszur informacyjnych i reklamowych dotyczących produktów i usług;
- telefoniczne pogotowie ciepłownicze, czyli telefon alarmowy, który pozwala każdej osobie na zgłaszanie awarii i usterek infrastruktury ciepłowniczej;
- przetwarzanie danych osobowych podmiotów danych związanych z nieruchomościami, na których posadowione zostały urządzenia przesyłowe;
- przetwarzanie danych osobowych podmiotów danych związanych z procesem uzyskiwania tytułu prawnego do nieruchomości, na której mają zostać posadowione urządzenia przesyłowe;
- przetwarzanie danych osobowych podmiotów danych w związku z uzasadnioną koniecznością kontaktu z

podmiotem danych w przypadku odłączenia ciepła z uwagi na zaleganie podmiotu danych z płatnościami, w przypadku, gdy odbiorcami ciepła są spółdzielnie mieszkaniowe, domki wielorodzinne czy wspólnoty mieszkaniowe;
- kontakt z administratorami, zarządcami nieruchomości, wspólnotami mieszkaniowymi.

1.2. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1.1. lit. e) – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym. Jeżeli przetwarzanie w celu innym niż cel, w którym dane osobowe zostały zebrane, nie odbywa się na podstawie zgody osoby, której dane dotyczą, Administrator – aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane – bierze pod uwagę między innymi:

a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;
b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;
c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10;
d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;
e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

2. Warunki wyrażenia zgody (art. 7 RODO)

2.1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.

2.2. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii.

2.3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

Stosowane wzory:

- **Załącznik nr 1 - Wzór zgody na przetwarzanie danych osobowych.**
- **Załącznik nr 2 - Wzór zgody na otrzymanie informacji handlowej za pomocą środków komunikacji elektronicznej.**
- **Załącznik nr 3 - Wzór zgody na używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego**

Każde przetwarzanie danych osobowych w Spółce odbywa się na podstawie określonej przesłanki legalizującej przetwarzanie. Zmiana celu przetwarzania danych wymaga zastosowania procedury - **Załącznik nr 21 - procedura postępowania w przypadku zmiany celu przetwarzania danych.**
Każde cofnięcie zgody na przetwarzanie danych osobowych przez osobę, której dane dotyczą podlega postępowaniu zgodnie z procedurą - **Załącznik nr 22 - procedura postępowania w przypadku cofnięcia zgody na przetwarzanie danych.**

3. Udostępnienie danych osobowych

- Dane osobowe mogą być udostępnione podmiotom uprawnionym do ich otrzymywania na mocy przepisów prawa i osobom, których dotyczą.
- Udostępnienie danych osobowych osobie nieupoważnionej do przetwarzania danych osobowych może nastąpić wyłącznie za zgodą Właściciela zasobów danych osobowych. Decyzję o wyrażeniu zgody podejmuje ADO. Zarówno wniosek jak i zgoda powinny być wystosowane z zachowaniem formy pisemnej.
- Udostępniając dane osobowe należy zaznaczać, że można je wykorzystać wyłącznie zgodnie z przeznaczeniem, dla którego zostały udostępnione.
- Za przygotowanie danych osobowych do udostępnienia w zakresie wskazanym we wniosku jest odpowiedzialny Właściciel zasobów danych (kierownik komórki organizacyjnej).
- Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom lub osobom za

potwierdzeniem odbioru.

4. Obowiązki Administratora w zakresie obsługiwania wniosków/żądań (motyw 59 RODO)

RODO nakłada na administratorów następujące obowiązki w zakresie obsługiwania wniosków/żądań składanych w związku z realizacją przez osoby, których dane dotyczą przysługujących im uprawnień:

1. na każdy wniosek/żądanie należy odpowiedzieć; w przypadku gdy administrator nie będzie realizował wniosku/żądań (np. z uwagi na wyjątek od danego uprawnienia), informuje osobę, której dane dotyczą, w terminie miesiąca o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem;
2. administrator winien zrealizować uprawnienie bez zbędnej zwłoki, a w każdym razie w terminie miesiąca od otrzymania wniosku/żądania; termin ten może być przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań (w takiej sytuacji, w terminie miesiąca od otrzymania żądania administrator informuje osobę, której dane dotyczą o przedłużeniu terminu, z podaniem przyczyn opóźnienia);
3. jeżeli osoba, które dane dotyczą przekazała swoje żądanie elektronicznie (np. e-mailem, wówczas – w miarę możliwości – stosowne informacje należy jej również przekazać elektronicznie, chyba że żąda ona innej formy).

UPRAWNIENIA OSÓB, KTÓRYCH DANE SĄ PRZETWARZANE

1. Obowiązek informacyjny (art. 12-14 RODO)

Każda osoba, której dane dotyczą musi być poinformowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator zobowiązany jest do podania informacji zapewniających rzetelność i przejrzystość przetwarzania, uwzględniając konkretne okoliczności i cel (motyw 60 RODO).

Stosowane wzory:

- **Załącznik nr 4 - Wzór klauzuli informacyjnej (w przypadku pozyskiwania danych osobowych od osoby, której dane dotyczą).**
- **Załącznik nr 5 - Wzór klauzuli informacyjnej (w przypadku pozyskiwania danych osobowych z innych źródeł niż od osoby, której dane dotyczą).**

2. Prawo dostępu do danych osobowych (art. 15 RODO)

Prawo to obejmuje:

- uzyskanie potwierdzenia, czy dane są przetwarzane;
- jeżeli dane są przetwarzane, uzyskanie dostępu do nich oraz informacji wskazanych w art. 15 ust. 1 RODO. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną (np. odpowiednio zabezpieczony e-mail).

Załącznik nr 15 - procedura postępowania w przypadku otrzymania żądania dostępu do danych.

3. Prawo do sprostowania danych osobowych (art. 16 RODO).

Osoba, której dane są przetwarzane ma prawo żądania niezwłocznego sprostowania danych nieprawidłowych. Realizacja żądania sprostowania polega – w zależności od jego treści – na sprostowaniu nieprawidłowych danych osobowych, aktualizacji tych danych (np. w przypadku zmiany adresu, zmiany nazwiska) lub uzupełnienia danych niekompletnych (o ile będzie to zgodne z celem w jakim te dane są przetwarzane). Administrator informuje o dokonanym sprostowaniu danych osobowych (sprostowanie nieprawidłowych danych, aktualizacja danych, uzupełnienie danych niekompletnych), każdego odbiorcę, któremu ujawniono dane osobowe, w tym każdy podmiot, któremu administrator powierzył przetwarzanie tych danych.

Załącznik nr 16 - procedura postępowania w przypadku otrzymania żądania sprostowania danych.

4. Prawo do usunięcia danych - „prawo do bycia zapomnianym" (art. 17 RODO).

Osoba której dane dotyczą ma prawo do żądania niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma je wówczas bez zbędnej zwłoki usunąć. Wspomniane prawo przysługuje, gdy:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania jej danych;
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego;
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego w stosunku do dziecka.

RODO przewiduje w art. 17 ust. 3 wyjątki od prawa do bycia zapomnianym. Prawo takie nie przysługuje, gdy przetwarzanie danych jest niezbędne w szczególności do:

- korzystania z prawa do wolności wypowiedzi i informacji
- wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa UE lub prawa państwa członkowskiego,.
- ustalenia, dochodzenia lub obrony roszczeń.

Załącznik nr 17 - procedura postępowania w przypadku otrzymania żądania usunięcia danych

5. Prawo do ograniczenia przetwarzania (art. 18 RODO).

„Ograniczenie przetwarzania" oznacza przechowywanie danych w celu ograniczenia ich przyszłego przetwarzania (art. 4 ust. 3 RODO). Oznacza to, że dane nie są trwale usuwane, lecz pozostają w systemie, ale są w nim oznaczone w celu zmiany zakresu i formy przetwarzania. W zautomatyzowanych zbiorach danych przetwarzanie należy zasadniczo ograniczyć środkami technicznymi w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane. Prawo przysługuje gdy:

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych;
- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- osoba, której dane dotyczą, wniosła sprzeciw wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Gdy przetwarzanie danych zostanie ograniczone, mogą one być wyłącznie przechowywane i nie mogą być przedmiotem innych operacji. Administrator informuje o dokonanym ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, w tym każdy podmiot, któremu administrator powierzył przetwarzanie tych danych.

Załącznik nr 18 - procedura postępowania w przypadku otrzymania żądania ograniczenia dostępu do danych.

6. Prawo do przenoszenia danych (art. 20 RODO).

RODO uprawnia, osobę której dane dotyczą, do otrzymania od administratora i przesłania do innego administratora dotyczących jej danych osobowych, w „ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego" (np. pliki XML, CSV). Nie należy używać formatów, do których odczytania konieczne jest otrzymanie płatnych licencji. Prawo do przenoszenia danych przysługuje

wówczas, gdy:

- przetwarzanie odbywa się w sposób zautomatyzowany (prawo to nie dotyczy przetwarzania w zbiorach tradycyjnych, np. segregatorach) i
- podstawą przetwarzania była zgoda osoby, której dane dotyczą.

Prawo do przenoszenia danych obejmuje tylko te z nich, które osoba dostarczyła administratorowi.

Załącznik nr 19 - procedura postępowania w przypadku otrzymania żądania przeniesienia danych

7. Prawo do sprzeciwu (art. 21 RODO).

Osoba, której dane dotyczą, ma prawo wniesienia sprzeciwu, gdy:

- podstawą przetwarzania była jego niezbędność do wykonania zadania realizowanego w interesie publicznym;
- podstawą jego przetwarzania była niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią;
- dane są przetwarzane w celu marketingu bezpośredniego (bezwzględne prawo do sprzeciwu).

Warunkiem uwzględnienia sprzeciwu w dwóch pierwszych, wskazanych powyżej przypadkach (względne prawo do sprzeciwu) jest wskazanie, przez osobę, której dane dotyczą, że za uwzględnieniem jej żądania przemawia jej szczególna sytuacja (np. przetwarzanie grozi ujawnieniem danych związanych ze sferą prywatności lub życia rodzinnego. W przypadku sprzeciwu wobec marketingu bezpośredniego, administrator musi zaprzestać przetwarzania tych danych bez dalszych warunków (bezwzględne prawo do sprzeciwu).

Załącznik nr 20 - procedura postępowania w przypadku otrzymania sprzeciwu wobec przetwarzania danych.

OBOWIĄZKI ADMINISTRATORA (ART. 24 RODO).

Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z Rozporządzeniem i aby móc to wykazać.

1. Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych

Spółka stosuje się do poniższych zasad określonych w art. 24 i art. 25 RODO. Przeprowadzana ocena skutków oraz jej wyniki przedstawiono w RAPORCIE dotyczącym podejścia Spółki do przetwarzania aktywów informacyjnych w tym danych osobowych, opartym na ryzyku (data zatwierdzenia Raportu 05.10.2018 r.). Raport obejmuje planowane środki, zabezpieczenia i mechanizmy mające minimalizować to ryzyko, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie RODO.

- **zasada *„privacy by design"* (prywatność powinna być zaprojektowana)** (art. 25 ust. 1 RODO), nakazująca przy określaniu sposobów przetwarzania, jak i w czasie przetwarzania, wdrożenie odpowiednich środków technicznych i organizacyjnych w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by chronić prawa osób, których dane dotyczą.
- **zasada *„privacy by default"* (prywatność domyślnie)**, (art. 25 ust. 2 RODO), polegająca na konieczności wdrożenia odpowiednich środków technicznych i organizacyjnych, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.
- **zasada rozliczalności** w połączeniu z ww. zasadami *„privacy by default"* i *„privacy by design"*, sprawia, że konieczne jest – niezależnie od wdrożenia i udokumentowania stosownych procedur - by każde analizy i decyzje podejmowane w odniesieniu do procesów przetwarzania danych osobowych, a to np. w zakresie stosowanych środków organizacyjnych i technicznych, zapewniających bezpieczeństwo przetwarzania danych, były dokumentowane, w celu zapewnienia realizacji obowiązku rozliczalności się Spółki z działaniami zgodnie z RODO.

2. Powierzenie przetwarzania danych osobowych (art. 26-28 RODO)

Przetwarzanie danych osobowych, których administratorem jest Spółka może być zlecone podmiotom zewnętrznym pod warunkiem dokonania jasnego podziału obowiązków. Przetwarzanie przez podmiot przetwarzający może odbywać się wyłącznie poprzez zawarcie na piśmie umowy powierzenia przetwarzania danych lub umowy o współadministrowanie lub poprzez zastosowanie innych instrumentów prawnych, który wiążą podmiot przetwarzający z administratorem, określają przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz które powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą.

Właściciel zasobów (kierownik komórki organizacyjnej) jest odpowiedzialny za zgłoszenie IOD konieczności podpisania umowy powierzenia przetwarzania danych osobowych. IOD prowadzi dalsze procedowanie.

Stosowane wzory: Załącznik nr 7 - Wzór umowy powierzenia przetwarzania danych osobowych.

3. Rejestrowanie czynności przetwarzania (art. 30 RODO)

Spółka przetwarza dane osobowe określone w **Rejestrze czynności przetwarzania** prowadzonym przez IOD. Jest to dokument, który ma pokazywać w szczególności w jakich procesach są przetwarzane dane osobowe, w jakim celu, kogo dotyczą oraz jak są zabezpieczane. Prowadzony jest również rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.

Stosowane wzory:

Załącznik nr 11 – wzór rejestru czynności przetwarzanych.

W przypadku przetwarzania danych osobowych w imieniu administratora zastosowanie ma **Załącznik nr 12 – wzór rejestru czynności przetwarzanych przez procesora.**

BEZPIECZEŃSTWO PRZETWARZANIA

1. Środki techniczne i organizacyjne

Dane osobowe gromadzone są w zbiorach a przetwarzane w systemach informatycznych oraz w kartotekach ewidencyjnych. Prowadzona jest polityka „czystego biurka" dla dokumentów papierowych i przenośnych nośników pamięci i „czystego ekranu" dla środków przetwarzania informacji.

Zbiory nieinformatyczne są zabezpieczone przed dostępem i zniszczeniem:

- dokumenty i wydruki, zawierające dane osobowe, przechowuje się w zamykanych szafach biurowych lub zamykanych szufladach;
- dokumenty są archiwizowane i przechowywane w zamkniętym pomieszczeniu, do których dostęp mają jedynie uprawnione osoby;
- wydruki robocze, błędne lub zdezaktualizowane są niezwłocznie niszczone przy użyciu niszczarki do papieru lub w inny sposób zapewniający skuteczne ich usunięcie;
- w przypadku likwidacji zbiorów archiwalnych, stosuje się przepisy dot. zasad archiwizacji i brakowania dokumentacji Spółki.

Wdrożono:

- pseudonimizację i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Spółka stosuje odpowiednie i adekwatne zabezpieczenia organizacyjne:

- Odpowiednia organizacja - istnienie struktury organizacyjnej zdolnej do kierowania i nadzorowania ochrony danych osobowych (wyznaczenie IOD);
- PBI - dokumentacja wyznaczająca formalnie cele i zasady, które są stosowane dla ochrony danych osobowych (plan działania, regularne przeglądy polityki, ryzyka, itd.) oraz adresatów (użytkownicy, dział IT, itd.);

- Zarządzanie ryzykiem - polityka wyznaczająca proces kontroli ryzyka czynności przetwarzania w Spółce, które mogą wpłynąć na prawa i wolności podmiotów danych (rejestr czynności przetwarzania danych osobowych, danych, Nośników danych, ocena ryzyka, ustalenie istniejących i planowanych środków, itd.);
- Uwzględnianie ochrony prywatności w fazie projektowania - wprowadzenie procedur opisujących metody uwzględniania ochrony danych osobowych w przypadku każdej nowej czynności przetwarzania;
- Zarządzanie naruszeniami ochrony danych osobowych - wprowadzenie operacyjnej struktury organizacyjnej pozwalającej wykrywać i obsługiwać zdarzenia, które mogą mieć wpływ na prawa i wolności podmiotów danych (określenie odpowiedzialności, plan reagowania, klasyfikacja naruszeń, itd.);
- Zarządzanie HR - prowadzenie planu wyznaczającego sposoby uświadamiania podejmowane w stosunku do nowego pracownika oraz procedury opisującej środki podejmowane w stosunku do osób odchodzących z pracy;
- Relacje z osobami trzecimi - wprowadzenie procedury mającej na celu ograniczenie ryzyka nieuprawnionego dostępu osób trzecich do danych osobowych, które może skutkować naruszeniem praw lub wolności osób, których dane dotyczą (identyfikacja osób trzecich, umowy powierzenia, itd.).
- Nadzór - wprowadzenie środków pozwalających uzyskiwać całościową i aktualną wizję stanu ochrony danych i zgodności z RODO (kontrola zgodności czynności przetwarzania, celów i wskaźników, zakresy odpowiedzialności, itd.).

2. Dokumentacja dotycząca ochrony danych osobowych

Na dokumentację ochrony danych osobowych w Spółka składają się:

- dokumentacja prowadzona przez IOD:
  a) Ewidencja osób upoważnionych do przetwarzania danych osobowych;
  b) Rejestr czynności przetwarzania danych osobowych oraz programów zastosowanych do ich przetwarzania;
  c) Rejestr kategorii czynności przetwarzania danych osobowych;
  d) Oryginały i Kopie dokumentów dotyczących ochrony danych osobowych oraz uchwały, zarządzenia, polityki itd. dotyczące ochrony danych osobowych;
  e) Protokoły z przeprowadzonych kontroli wewnętrznych i zewnętrznych w zakresie ochrony danych osobowych.
- dokumentacja prowadzona przez ASI:
  a) Instrukcja Bezpiecznego Zarządzania Systemami Informatycznymi;
  b) Opisy struktury zbiorów osobowych;
  c) Wykaz systemów i aplikacji zastosowanych do przetwarzania danych osobowych;
  d) Opisy sposobów przepływu danych pomiędzy systemami;
  e) Plany archiwizacji danych osobowych i programów służących do ich przetwarzania;
  f) Ewidencje przenośnych nośników danych używanych w poszczególnych komórkach organizacyjnych.

3. Szkolenie w zakresie ochrony danych osobowych

Cel: zapewnić, żeby pracownicy i kontrahenci byli świadomi swoich obowiązków dotyczących bezpieczeństwa danych osobowych i wypełniali je.

Przed rozpoczęciem przetwarzania danych osobowych każdy pracownik Spółki zostaje przeszkolony.

Szkolenie prowadzone przez IOD obejmuje następujące zagadnienia :

- przepisy o ochronie danych osobowych,
- zasady przetwarzania danych osobowych,
- zagrożenia, na jakie może być narażone przetwarzanie danych osobowych,
- zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
- sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego,
- odpowiedzialność z tytułu naruszenia ochrony danych osobowych.

Szkolenia pracowników tzw. przypominające, powtarzane są przez IOD cyklicznie 1 raz w roku oraz na żądanie, gdy zaistnieje taka potrzeba.

Szkolenie prowadzone przez ASI obejmuje:
- procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych,
- zasady użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych,
- zagrożenia, na jakie może być narażone przetwarzanie danych osobowych w systemach informatycznych.

Użytkownicy reprezentujący osoby trzecie (użytkownicy zewnętrzni) przechodzą szkolenie w zakresie :
- zasad wynikających z Polityki.
- poprawnego użytkowania urządzeń i systemów informatycznych służących do przetwarzania danych osobowych.

4. Dopuszczenie osób do przetwarzania danych osobowych

Cel: ograniczyć dostęp do danych osobowych.

Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez pracownika/użytkownika zewnętrznego formalnego upoważnienia do przetwarzania danych osobowych wystawionego przez IOD.

W tym celu właściciel zasobów (przełożony pracownika/użytkownika zewnętrznego) przed dopuszczeniem pracownika do pracy przy przetwarzaniu danych osobowych wnioskuje do IOD o nadanie uprawnień podając według zasady potrzeby koniecznej i indywidualnego przypadku: cel, okres, sposób (papierowy/ informatyczny) i zakres przetwarzania danych oraz ich kategorię. Wniosek zgodny z **Załącznikiem nr 6 – Wzór upoważnienia do przetwarzania danych** przesyła drogą elektroniczną (podając zakres należy wskazać proces i nr zbioru, w którym dane są przetwarzane np. Proces ZAKUPY , nr zbioru Z_1).

W przypadku przetwarzania danych w systemie informatycznym należy wskazać również system/moduł/folder. Zarządzanie prawami dostępu do systemu informatycznego prowadzone jest przez ASI, dlatego w takim przypadku, IOD przesyła wniosek do ASI.

5. Ewidencja osób upoważnionych do przetwarzania danych osobowych

Cel: zapobiec nieuprawnionemu dostępowi.

Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi IOD.

Ewidencja prowadzona jest na elektronicznych nośnikach informacji, które są zabezpieczone hasłem uniemożliwiającym ich usuwanie lub modyfikowanie. Jakakolwiek zmiana w zakresie informacji zawartych w ewidencji podlega natychmiastowemu odnotowaniu.

Właściciele zbiorów danych osobowych (kierownicy komórek organizacyjnych) odpowiadają za natychmiastowe zgłoszenie do IOD osób, które utraciły uprawnienia dostępu do danych osobowych. IOD w oparciu o otrzymane informacje, wyrejestrowuje je z ewidencji i informuje ASI. Procedury nadawania, modyfikacji i anulowania uprawnień do przetwarzania danych osobowych w systemach informatycznych opisano szczegółowo w Rozdziale III.

6. Naruszenie ochrony danych osobowych (art. 33 – 34 RODO)

Poniższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych przetwarzanych w systemach informatycznych, jak i w zbiorach nieinformatycznych.

6.1. Przed przystąpieniem do pracy pracownicy/użytkownicy zewnętrzni są zobowiązani dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.

6.2. Za naruszenie zasad bezpieczeństwa danych osobowych uważa się w szczególności:

lp.	Opis naruszenia
1	Nieupoważniony dostęp danych osobowych lub innych informacji z nośnika danych (tradycyjny lub elektroniczny).
2	Udostępnienie danych osobowych osobom lub podmiotom nieupoważnionym.
3	Nieautoryzowany dostęp do danych osobowych przez połączenie sieciowe.

4	Nieautoryzowany dostęp do pomieszczenia, w którym przetwarza się dane osobowe.
5	Nieupoważnione zniszczenie danych osobowych lub innych informacji z nośnika danych (tradycyjny lub elektroniczny).
6	Nieupoważniona modyfikacja danych osobowych lub innych informacji z nośnika danych (tradycyjny lub elektroniczny).
7	Nieodpowiednie zabezpieczenie systemu IT i związany z tym nieupoważniony dostęp do danych osobowych.
8	Zamierzone i nielegalne ujawnienie danych osobowych przez pracowników.
9	Pozyskiwanie danych osobowych z nielegalnych źródeł.
10	Przetwarzanie danych osobowych niezgodnie z celem.
11	Odnotowanie wystąpienia złośliwego oprogramowania na sprzęcie komputerowym, na którym są przechowywane lub przetwarzane dane osobowe.
12	Nieupoważniony dostęp do haseł służących zabezpieczeniu dostępu do systemu.
13	Przesyłanie danych osobowych bez odpowiednich zabezpieczeń.
14	Wykonanie kopii danych osobowych.
15	Kradzież, zagubienie lub inne naruszenie bezpieczeństwa nośników zawierających dane osobowe.
16	Naruszenie bezpieczeństwa kopii zapasowych zawierających zgromadzone dane osobowe.
17	Niewłaściwe zniszczenie nośników danych osobowych.
18	Naruszenie bezpieczeństwa danych osobowych poprzez nienależytą ochronę fizyczną pomieszczeń, w których przetwarzane lub przechowywane są dane osobowe, przed nieuprawnionym dostępem.
19	Przetwarzanie danych osobowych przez pracowników nieposiadających odpowiednich upoważnień.
20	Inne sytuacje, które wskazują na naruszenie bezpieczeństwa danych osobowych.

W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych przetwarzanych w systemach teleinformatycznych lub poza systemami teleinformatycznymi każdy, kto uzyskał informacje o takim zdarzeniu zobowiązany jest do:

- powstrzymania się od wszelkich działań mogących spowodować zatarcie śladów bądź dowodów naruszenia,
- powiadomienia bezpośredniego przełożonego o tym zdarzeniu,
- powiadomienia IOD,
- postępowania zgodnego z Planem Reagowania Kryzysowego.

Inspektor niezwłocznie informuje ADO o powzięciu informacji na temat podejrzenia naruszenia ochrony danych.

W przypadku stwierdzenia naruszenia ochrony danych osobowych należy postępować zgodnie z procedurą postępowania w przypadku naruszenia ochrony danych – **załącznik nr 8, 9 i 10.**

W przypadku zaklasyfikowania naruszenia ochrony danych jako naruszenia o średnim stopniu ryzyka:

- IOD, działając w imieniu Administratora, zgłasza naruszenie Organowi nadzorczemu, bez zbędnej zwłoki, a o ile to możliwe nie później niż w czasie 72 godzin od stwierdzenia naruszenia;
- użytkownik może kontynuować pracę dopiero po otrzymaniu zgody od IOD.

Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem incydentu związanego z naruszeniem ochrony danych osobowych.

7. Ocena skutków przetwarzania danych –DPIA (art.35 RODO)

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (ang. Data Protection Impact Assessment, DPIA)

Operacje przetwarzania, które wiążą się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych (art. 35 ust. 3 RODO), obejmują w szczególności operacje, które:

- wiążą się z użyciem nowych technologii;
- są nowe i nie zostały jeszcze poddane przez administratora ocenie skutków dla ochrony danych; lub
- stały się niezbędne z uwagi na upływ czasu od pierwotnego przetwarzania.

Kiedy nie musimy stosować DPIA? Obowiązek oceny skutków dla ochrony danych nie zachodzi, jeżeli dana operacja przetwarzania lub zestaw operacji jest niezbędna do wypełnienia obowiązku prawnego ciążącego na administratorze.

Przed podjęciem jakichkolwiek nowych operacji na danych osobowych, a w szczególności przed rozpoczęciem zbierania nowych danych, wprowadzeniem danych do systemu informatycznego lub ich przekopiowaniem w systemie informatycznym, rozważyć należy – w szczególności poprzez konsultację z IOD - czy konieczne jest w związku z tym przeprowadzenie DPIA. Konsultacja taka jest w szczególności wymagana w przypadku planowanego zastosowania nowych technologii (nowych rozwiązań technicznych.

Wdrożenie procedury oceny skutków dla ochrony danych osobowych, której wzór stanowi **załącznik nr 13 - procedura oceny skutków dla ochrony danych osobowych.**

Zgodnie z art. 36 ust. 1 RODO, jeżeli DPIA wykaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym. **Wzór wniosku konsultacyjnego do organu nadzorczego z uwagi na wysokie ryzyko planowanego przetwarzania stanowi załącznik nr 14 .**

KONTROLA PROCESU ZARZĄDZANIA BEZPIECZEŃSTWEM OCHRONY DANYCH OSOBOWYCH

Realizacja procesu zarządzania bezpieczeństwem ochrony danych osobowych poddawana jest corocznej kontroli przy wykorzystaniu m.in. poniższych miar.

Skala oceny:	lp	stan procesu
1 = Brak procesów. / NIE 2 = Istnieje proces nieformalny. / OPRACOWAĆ PONOWNIE 3 = Istnieje formalny, udokumentowany proces. / POPRAWIĆ 4 = Istnieje formalny, udokumentowany proces, a ponadto mierzone są najważniejsze parametry. / DOBRZE 5 = Istnieje formalny, udokumentowany proces, mierzone są najważniejsze parametry, a ponadto proces jest stale doskonalony na podstawie wyników pomiarów. / BARDZO DOBRZE	1	IOD- Zapoznawanie pracowników oraz współpracowników Spółki z przepisami i zasadami ochrony danych osobowych
	2	Właściciel zbioru- zapewnienie, złożenia przez pracowników oświadczenia o znajomości przepisów o ochronie danych osobowych oraz zobowiązania do zachowania tajemnicy danych osobowych oraz informacji na temat zabezpieczeń danych osobowych.
	3	IOD- Raporty z naruszenia bezpieczeństwa danych osobowych
	4	IOD - Ewidencja osób upoważnionych do przetwarzania danych osobowych
	5	IOD – Rejestr czynności przetwarzania danych osobowych w Spółce oraz programów zastosowanych do ich przetwarzania
	6	ASI– Opisy struktury zbiorów osobowych
	7	ASI–Opisy sposobów przepływu danych pomiędzy systemami
	8	ASI -Ewidencja przenośnych nośników danych używanych w poszczególnych komórkach organizacyjnych
	9	IOD Upoważnienie do przetwarzania danych osobowych

ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMATYCZNYM

CEL ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMATYCZNYM

Celem zarządzania bezpieczeństwem informatycznym w Spółce jest osiągnięcie poziomu organizacyjnego i technicznego, który pozwoli na optymalne zabezpieczenie środków przetwarzania informacji.

1. Stosuje się najlepsze systemy informatyczne, które umożliwiają uzyskanie potrzebnych informacji (trafność, jakość, czas realizacji).
2. Kierownictwo dokonuje przeglądu by upewnić się, że zmiany odnośnie systemów komputerowych są stale wprowadzane tak, by dostosować się do zmian/potrzeb.
3. Obiekty centrum danych (serwerownie) są wyposażone w urządzenia kontroli środowiskowej (nieprzerwana obsługa zasilania, klimatyzacja itp.) Dostęp do centrum danych jest ograniczony do uprawnionego personelu. Zdefiniowano krytyczne aplikacje procesowe i powiązane systemy sterowania.
4. Implementowany jest ograniczony dostęp do krytycznych transakcji.
5. Plan tworzenia kopii zapasowych i Plan Odbudowy Odpadów są wdrażane i są okresowo testowane.
6. Opracowano i wdrożono procedury archiwizacji (w tym role i zakres odpowiedzialności) w zależności od potrzeb biznesowych i przepisów prawa - procesu tworzenia kopii zapasowych i przywracania z codzienną kontrolą (dzienniki).
7. Zasady bezpieczeństwa są realizowane zgodnie z wymaganiami Grupy ENGIE:
   7.1. Sprzęt i sieci komputerowe są skonfigurowane by zapewnić optymalny poziom bezpieczeństwa wykorzystując zaporę sieciową - firewall,
   7.2. Ochrona przed wirusami w formie oprogramowania wykrywającego i neutralizującego szkodliwe oprogramowanie, które jest zarządzane przez konsolę systemu zabezpieczeń stacji roboczych - z codzienną kontrolą (dzienniki).
   7.3. Ochrona przed wszelkiego rodzaju niedoskonałościami w oprogramowaniu, (mogące umożliwić penetrację systemów) poprzez aktualizację oprogramowania, w szczególności podnoszące poziomy bezpieczeństwa.
8. Systemy informacyjne generują informacje o wystarczającej jakości, aby obsługiwać skuteczne zarządzanie nimi.
9. Pracownicy działu IT w razie potrzeb, przesyłają użytkownikom informacje przypominające (w formie krótkich instrukcji) z zakresu zasad korzystania ze sprzętu jego obsługi oraz dot. środków bezpieczeństwa informatycznego.

W Spółce wypracowano **Instrukcję bezpiecznego zarządzania systemem informatycznym**[5], która jest dokumentem integralnym z PBI i określa:

- sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
- warunki techniczne i organizacyjne, jakim odpowiadają urządzenia i systemy informatyczne służące do przetwarzania danych;
- wymagania w zakresie odnotowywania udostępniania danych i bezpieczeństwa przetwarzania danych.

W celu zachowania bezpieczeństwa informacji dokument określono jako POUFNY, który udostępniony zostaje wyłącznie:

- Zarządowi Spółki
- Inspektorowi Ochrony Danych (IOD)
- Inspektorowi Bezpieczeństwa Informacji (IBI)
- Administratorowi Systemów Informatycznych (ASI)
- Kierownikowi Działu IT
- Audytorowi wewnętrznemu/zewnętrznemu – po uzyskaniu zgody Zarządu Spółki.

[5] zgodnie z: Rozporządzeniem 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

ZASTOSOWANY POZIOM BEZPIECZEŃSTWA PRZETWARZANIA DANYCH

Uwzględniając kategorie przetwarzanych danych, ich sposób magazynowania, udostępniania oraz zagrożenia stosuje się w Spółce **wysoki poziom bezpieczeństwa** przetwarzania danych w systemie informatycznym w rozumieniu zawartym w Rozporządzeniu ministra spraw wewnętrznych i administracji z dnia 29 kwietnia 2004r. 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. z 2004 r. Nr 100, poz. 1024).

Poziom wysoki stosuje się, gdy przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych, połączone jest z siecią publiczną. Na poziomie tym zastosowanie mają również środki bezpieczeństwa na poziomie podstawowym i podwyższonym.

Środki bezpieczeństwa na poziomie podstawowym:

1. Jeżeli dostęp do danych przetwarzanych posiadają co najmniej dwie osoby, wówczas zapewnia się, aby:
- w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator;
- dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.
2. System informatyczny zabezpiecza się, w szczególności przed:
- działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
- Inne ryzyka środowiskowe (np. zalanie, huragan, wojna itd.)
3. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.
4. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni. Hasło składa się co najmniej z 6 znaków.
5. Dane przetwarzane zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.
6. Kopie zapasowe:
- przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;
- usuwa się niezwłocznie po ustaniu ich użyteczności.
7. Osoba użytkująca komputer przenośny zawierający dane zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych.
8. Urządzenia, dyski lub inne elektroniczne nośniki informacji, przeznaczone do:
- likwidacji — pozbawia się wcześniej zapisu danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
- naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI.

Środki bezpieczeństwa na poziomie podwyższonym:

1. Zawiera elementy poziomy podstawowego oraz:
2. W przypadku gdy do uwierzytelniania użytkowników używa się hasła, składa się ono co najmniej z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.
3. Urządzenia i nośniki zawierające dane osobowe zabezpiecza się w sposób zapewniający poufność i integralność tych danych.

Środki bezpieczeństwa na poziomie wysokim:

Zawiera elementy poziomu podwyższonego oraz:

1. System informatyczny służący do przetwarzania danych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.
2. Logiczne zabezpieczenia obejmują:
- kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią

publiczną;
- kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.

3. Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

ZARZĄDZANIE AKTYWAMI[6]

1. Postępowanie z nośnikami

Cel: Zapobiec nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu informacji zapisanych na nośnikach.

1.1. Nośniki zawierające informację przechowywane są w bezpiecznych miejscach zgodnie z zaleceniami producenta.
1.2. Dane z nośników ze stacji roboczych niszczone są poprzez zastosowanie odpowiedniego oprogramowania.
1.3. Na nośnikach wymiennych stosuje się techniki kryptograficzne jeżeli istotna jest poufność lub integralność danych.
1.4. Na oddzielnych nośnikach przechowywane są kopie cennych danych w celu zmniejszenia ryzyka przypadkowego zniszczenia danych lub ich utraty.
1.5. Tam, gdzie jest niezbędne użycie nośnika wymiennego wprowadzono monitorowanie kopiowania informacji.
1.6. Likwidacja nośników danych polega na zniszczeniu fizycznym w sposób uniemożliwiający jakiekolwiek odtworzenie danych.

2. Zasady korzystania ze sprzętu komputerowego

2.1. Służbowy komputer służy do wykonywania czynności służbowych na stanowisku pracy lub poza siedzibą Spółki w uzasadnionych przypadkach (komputer przenośny).
2.2. Ze służbowego komputera przenośnego może korzystać każdy pracownik (użytkownik), który uzasadni taką potrzebę.
2.3. Użytkownikom systemu informatycznego nie wolno samowolnie rozłączać, przemieszczać ani podłączać urządzeń informatycznych. W razie wystąpienia takiej konieczności należy powiadomić o tym pracownika działu IT.
2.4. Użytkownik ponosi pełną odpowiedzialność za komputer, jego stan techniczny, oprogramowanie a także za dane zgromadzone na twardym dysku komputera, w szczególności za dane osobowe.
2.5. Nadzór i opiekę nad komputerem, w szczególności nad jego stanem technicznym i poprawnością wykorzystywania sprawuje pracownik działu IT.
2.6. Komputer przenośny jest urządzeniem bardzo delikatnym. Jego transport i obsługa powinny odbywać się z zachowaniem szczególnej ostrożności. Niedopuszczalny jest transport komputera niezamkniętego w odpowiedniej torbie.
2.7. Komputer przenośny jest urządzeniem podatnym na kradzież, dlatego pracownik powinien dołożyć wszelkiej staranności w zabezpieczeniu go przed takim zdarzeniem.
2.8. Użytkownikom nie wolno wykonywać żadnych czynności naprawczych przy sprzęcie komputerowym. W razie zaistnienia takiej potrzeby należy poinformować o tym dział IT.
2.9. Użytkownicy sprzętu komputerowego mają obowiązek utrzymywać go w czystości poprzez regularne czyszczenie stacji roboczej, monitora ekranowego oraz innych urządzeń peryferyjnych podłączonych do stacji roboczej.
2.10. Instrukcje dotyczące sposobu czyszczenia jak również odpowiednie środki czystości przekazuje pracownik działu IT odpowiedzialny za infrastrukturę informatyczną.
2.11. Zabronione jest spożywanie posiłków i napojów przy stanowisku komputerowym oraz w bliskim sąsiedztwie urządzeń informatycznych.

[6] Na podstawie PN-EN ISO/IEC 2700 ZAŁACZNIK A i PN-EN ISO/IEC 27002

3. Zarządzanie dostępem użytkowników

Cel: Ograniczyć dostęp do informacji i środków przetwarzania informacji. Zapewnić dostęp uprawnionym użytkownikom i zapobiec nieuprawnionemu dostępowi do systemów i usług.

3.1. Dostęp do sieci i usług sieciowych

3.1.1. Dostęp do systemów informatycznych mogą posiadać zgodnie z zasadą „wszystko jest zabronione, dopóki nie jest wyraźnie dozwolone":
- pracownicy – niezbędny do wykonywania powierzonych im czynności służbowych,
- wykonawcy usług oraz dostawcy sprzętu lub oprogramowania – w zakresie koniecznym do realizowania danej usługi lub wykonania określonych czynności w systemie.

3.1.2. Korzystanie z usług sieciowych jest monitorowane.

3.1.3. Dostęp do usług sieciowych wymaga uwierzytelnienia użytkownika.

3.2. Rejestrowanie i wyrejestrowanie użytkowników.

3.2.1. Rejestrowanie i wyrejestrowanie użytkowników dokonywane jest przez ASI na wniosek właściciela zasobów (kierownika komórki organizacyjnej).

3.2.2. ASI wprowadza unikalny identyfikator użytkownika i przyznaje dostępy do danych i operacji zgodnych z zakresem uprawnień użytkownika.

3.2.3. Ustanowione hasło dostępu ASI przekazuje użytkownikowi. Każdy z użytkowników systemu posiada własne hasło i identyfikator.

3.2.4. Hasło ustanowione podczas przyznawania uprawnień wymaga zmiany na indywidualne, podczas pierwszego logowania się w systemie informatycznym. Następna zmiana hasła użytkownika następuje nie rzadziej niż co 90 dni.

3.2.5. Identyfikatora użytkownika nie należy zmieniać bez wyraźnej przyczyny, a po wyrejestrowaniu użytkownika z systemu nie powinien być on przydzielany innej osobie.

3.2.6. Użytkownicy są odpowiedzialni za zachowanie poufności swoich haseł.

3.2.7. Hasła użytkownika utrzymuje się w tajemnicy również po upływie ich ważności, nie wolno ich udostępniać, ani zapisywać w sposób jawny.

3.2.8. Hasło należy wprowadzać w sposób, który uniemożliwia innym osobom jego poznanie.

3.2.9. W sytuacji kiedy zachodzi podejrzenie, że ktoś poznał hasło w sposób nieuprawniony, użytkownik zobowiązany jest do jego natychmiastowej zmiany.

3.2.10. Przy wyborze hasła obowiązują następujące zasady:
- minimalna długość hasła – 8 znaków;
- właściwa złożoność hasła - litery duże i małe oraz cyfry i znaki specjalne, o ile system informatyczny na to pozwala.

Zakazuje się stosować haseł:
- które użytkownik stosował uprzednio (do dziesięciu haseł wstecz);
- będących nazwą użytkownika w jakiejkolwiek formie (np. pisanej dużymi literami);
- analogicznych jak identyfikator;
- zawierających ogólnie dostępne informacje takie jak: imię, nazwisko, numer rejestracyjny samochodu, numer telefonu, imiona dzieci itp.;
- stanowiących wyrazy słownikowe lub przewidywalne sekwencje znaków np. 12345678 lub abcdefgh.

3.2.11. Zmiany hasła nie należy zlecać innym osobom.

3.2.12. W systemach umożliwiających zapamiętanie nazwy użytkownika lub jego hasła nie należy korzystać z tego ułatwienia.

3.2.13. Użytkownik ponosi odpowiedzialność za wszelkie operacje wykonywane przy użyciu jego identyfikatora i hasła.

3.2.14. W systemie informatycznym stosuje się uwierzytelnienie dwustopniowe: na poziomie dostępu do sieci lokalnej (w przypadku komputerów niepowiązanych z siecią – do systemu operacyjnego) oraz dostępu do aplikacji.

3.2.15. W przypadku anulowania uprawnień użytkownika jego identyfikator zostaje zablokowany a hasło unieważnione.

3.2.16. W zależności od potrzeb nie rzadziej niż 1 raz na kwartał, ASI dokonuje przeglądu wykazu zarejestrowanych użytkowników.

3.2.17. W przypadkach awaryjnych (np. nieobecność użytkownika) hasło może być przekazane decyzją właściciela zasobów osobie zastępującej. Po ustaniu sytuacji awaryjnej, użytkownik jest zobowiązany do zmiany hasła.

3.2.18. Komputery Engie EC Słupsk są podpięte do domeny AD o nazwie d54.tes.local, która jest częścią domeny AD właściciela spółki. Aby uzyskać dostęp do zasobów sieci LAN i WAN Spółki użytkownik musi posiadać login w domenie.

3.2.19. Dla nowych pracowników w ramach Instrukcji zatrudnienia IZ-03 zakładane jest konto AD. Administrator dokonuje rejestracji nowego użytkownika w domenie d54.tes.local, nadając mu unikatowy 6-znakowy identyfikator tzw. login (GID – unikalny identyfikator pracownika w ENGIE)

3.2.20. Dla nowych pracowników w ramach Instrukcji zatrudnienia IZ-03 zakładane jest konto Office 365. Konta office365 tworzone są w oparciu o zasadę: imię.nazwisko@engie.com (forma adresu e-mail może ulec zmianie ze względu na możliwości techniczne – np. konto pożądane już istnieje dla innej osoby w strukturze ENGIE). Konto Office 365 jest zmapowanym kontem użytkownika AD za pomocą interfejsu OKTA.

3.2.21. Konta do Systemy IMPULS EVO tworzone są w oparciu o zasadę: Pierwsza litera imienia||Nazwisko (forma może ulec zmianie, patrz jw.)

3.3. Przydzielanie dostępu do systemów

3.3.1. Użytkownik ma prawo do wykonywania w systemie tylko tych czynności, do których został upoważniony. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.

3.3.2. Nadawanie praw dostępu związanych z każdym systemem lub procesem (np. systemem operacyjnym, systemem zarządzania bazami danymi, aplikacjami, folderami) dokonywane jest przez ASI na wniosek właściciela zasobów według zasady potrzeby koniecznej i indywidualnego przypadku. Właściciel zasobu przesyła drogą elektroniczną wniosek **o nadanie/zmianę/pozbawienie upoważnienia do przetwarzania danych**. Sposób postępowania określono w rozdziale II pkt. 64.4.- **Dopuszczenie osób do przetwarzania danych osobowych.**

3.3.3. ASI prowadzi rejestr użytkowników systemu, w którym odnotowuje imię i nazwisko, identyfikator, zakres uprawnień użytkownika oraz datę nadania, modyfikacji i anulowania uprawnień.

3.3.4. Za opracowanie szczegółowych zasad nadawania, modyfikacji i anulowania uprawnień do systemów informatycznych wykorzystywanych w firmie oraz dostępu do sieci chronionej, jak również wdrożenie i nadzór nad przestrzeganiem przedmiotowych zasad odpowiedzialny jest Kierownik Działu IT.

3.3.5. Jeśli kierownik komórki lub właściciel zasobu wnioskuje o nadanie uprawnień dotyczących zbiorów danych osobowych ASI sprawdza w rejestrze „REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH" czy pracownik posiada upoważnienie nadane przez IOD do przetwarzania danych osobowych w danym obszarze. Pracownik nie posiadający uprawnień jest odsyłany do IOD, który decyduje o nadaniu upoważnienia Po nadaniu upoważnienia przez IOD, ASI nadaje właściwe uprawnienia.

3.3.6. Pracownicy EC zostali podzieleni na grupy uprawnień. Ich wykaz znajduje się "Z:\Organizacyjny BJ\Uprawnienia do systemów informatycznych\Grupy pracowników\Grupy pracowników.xlsx" . O przypisaniu pracownika do odpowiedniej grupy decyduje kierownik komórki w której pracuje użytkownik. Złożenie wniosku do Administratora o dodanie/usunięcie użytkownika w grupie odbywa się przez wysłanie w wiadomości email pliku excel wypełnionego wg. opisu znajdującego się pliku.

3.3.7. Foldery na serwerze plików posiadają swoich właścicieli, którzy decydują jakie uprawnienia dostępu ma posiadać określona grupa pracowników. Właściciel folderu identyfikowany jest poprzez inicjały w nazwie folderu. Właściciel folderu zleca nadanie uprawnień Administratorowi przekazując mu za pomocą email plik excel wypełniony wg. wzoru: "Z:\Organizacyjny BJ\Uprawnienia do systemów informatycznych\Serwer plików\Dostępy do folderów i plików- wzór.xlsx"

3.3.8. Nadawanie uprawnień do podsystemów Impuls EVO odbywa się w systemie ERP. Kierownik komórki zleca nadanie uprawnień Administratorowi przekazując mu za pomocą email wypełniony wg, wzoru plik excel, w którym wskazuje uprawnienia grup za które jest odpowiedzialny. Nowym pracownikom

w ramach procedury zatrudnienia (procedura) zostaje domyślnie przyznany zestaw uprawnień pozwalający na dostęp do portalu pracowniczego. Wykaz uprawnień znajduje się pod adresem: "Z:\Organizacyjny BJ\Uprawnienia do systemów informatycznych\Impuls\Uprawnienia Impuls.xlsx". Instrukcja nadawania uprawnień zapisana jest w pliku.

3.3.9. Konta Office 365 domyślnie po uruchomieniu posiadają dostęp do aplikacji Teams, Skype ,OneDrive, Yammer i indywidualnej skrzynki pocztowej. Zakładanie i dostęp do skrzynki współdzielonej przez pracowników realizowany jest na przesłany do Administratora drogą elektroniczną wniosek kierownika komórki.

3.3.10. Użytkownik Teams może samodzielnie założyć swój własny zespół w którym sam nadaje uprawnienia.

BEZPIECZNA EKSPLOATACJA

Cel: Zapewnić poprawną i bezpieczną eksploatację środków przetwarzania informacji.

1. Zarządzanie zmianami

Zarządzanie bezpieczeństwem informatycznym jest nadzorowane przez Inspektora Bezpieczeństwa Informacji (IBI) i Administratora Systemów Informatycznych (ASI). Każda wprowadzana zmiana w środkach i systemach służących do przetwarzania informacji podlega kontroli IBI i ASI. Pracownicy działu IT zobowiązani są również do:

- identyfikowania i rejestrowania znaczących zmian,
- planowania i testowania zmian w środowiskach informatycznych,
- szacowania potencjalnego wpływu zmian, także na bezpieczeństwo informacji,
- przekazania informacji o zmianach wszystkim właściwym osobom,
- szybkiego i nadzorowanego wprowadzania zmian niezbędnych do rozwiązania incydentu związanego z bezpieczeństwem informacji.

2. Zabezpieczenia przed szkodliwym oprogramowaniem

2.1. Oprogramowanie stosowane w firmie może pochodzić wyłącznie ze źródeł legalnych i sprawdzonych, obowiązkowo posiadać łatwo dostępną informację o identyfikatorze, wersji i numerze licencji.

2.2. Wdrożenie modyfikacji istniejącego lub stworzenie albo zakup nowego oprogramowania przetwarzającego dane osobowe możliwe jest wyłącznie w przypadku spełnienia przez przedmiotowe oprogramowanie wymogów z zakresu bezpieczeństwa wynikających z obowiązujących przepisów prawa dotyczących ochrony danych osobowych.

2.3. Zabronione jest uruchamianie lub instalowanie i uruchamianie oprogramowania niezwiązanego merytorycznie z wykonywaną pracą.

2.4. Korzystanie z zasobów firmy poprzez sieć publiczną winno mieć miejsce po zastosowaniu koniecznych systemów zabezpieczeń i mechanizmów ochronnych, w szczególności firewall-i oraz systemu uwierzytelniania użytkowników i szyfrowania danych, a także kompleksowego oprogramowania antywirusowego.

2.5. Sieć wewnętrzna firmy odseparowana jest od sieci publicznej za pomocą uaktywnionych firewalli sprzętowych i programowych.

2.6. Dostęp do sieci rozległej mogą posiadać, przy zastosowaniu zasad dopuszczenia do zasobów informatycznych obowiązujących firmie:

- pracownicy firmy,
- osoby lub podmioty, z którymi firma współpracuje na podstawie zawartych umów oraz ich pracownicy w zakresie przewidzianym umową.
- Za techniczne umożliwienie użytkownikom korzystania z zasobów internetowych odpowiedzialny jest pracownik działu IT.

2.7. W przypadku konieczności dokonania rejestracji w Internecie zabronione jest wykorzystywanie do tego celu identyfikatorów i haseł używanych do dostępu do zasobów Firmy.

2.8. W celu ochrony systemów przed szkodliwym oprogramowaniem, oprogramowanie antywirusowe podlegające systematycznej aktualizacji musi być zainstalowane na każdym stanowisku komputerowym.
2.9. Sprawdzanie dostępności baz wirusów oprogramowania antywirusowego odbywa się automatycznie nie rzadziej niż raz na dobę. Zaleca się okresowe monitorowanie czy aktualizacja ta przebiega bez zakłóceń.
2.10. Użytkownicy zobowiązani są do niezwłocznego zgłaszania do pracownika działu IT każdej stwierdzonej nieprawidłowości dotyczącej profilaktyki antywirusowej (np. braku zainstalowanego oprogramowania antywirusowego, nieaktualności sygnatur wirusów).
2.11. Programy antywirusowe winny być uaktywnione cały czas podczas pracy danego systemu.
2.12. Wszystkie pliki otrzymywane z zewnętrz, jak również wysyłane na zewnątrz, należy sprawdzać pod kątem występowania wirusów najnowszą dostępną wersją programu antywirusowego.
2.13. Każdy użytkownik zobowiązany jest do ochrony przed szkodliwym oprogramowaniem powierzonego mu stanowiska komputerowego.
2.14. Zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje użytkownik, który nośnik zamierza użyć.
2.15. Zabrania się pobierania z Internetu plików niewiadomego pochodzenia. Każdy plik pobrany z Internetu musi być sprawdzony programem antywirusowym. Sprawdzenia dokonuje użytkownik, który pobrał plik.
2.16. Zabrania się odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym. Sprawdzenia dokonuje pracownik, który pocztę otrzymał.
2.17. W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien:
- odłączyć stanowisko komputerowe od sieci,
- zawiadomić pracownika działu IT o zaistniałym zdarzeniu,
- zanotować nazwę wirusa, uruchomić program antywirusowy celem wykonania skanu dysku twardego.

2.18. W przypadku uszkodzenia danych lub programów ASI zobowiązany jest do przywrócenia sprawności systemu korzystając z kopii zapasowych.
2.19. W firmie przeprowadzone są cykliczne kontrole antywirusowe na wszystkich wykorzystywanych komputerach.
2.20. Kontrola antywirusowa przeprowadzana jest również na wybranym komputerze w przypadku zgłoszenia nieprawidłowości w funkcjonowaniu sprzętu komputerowego lub oprogramowania.
2.21. W przypadku wykrycia wirusów komputerowych sprawdzane jest stanowisko komputerowe, na którym wirusa wykryto, jak również wszystkie repozytoria danych, do których ten komputer miał dostęp.

3. Zabezpieczenie telefonów komórkowych przed atakami szkodliwego oprogramowania

- Telefony służbowe są przydzielane pracownikom na podstawie Zarządzenia Prezesa Zarządu w sprawie zasad korzystania ze służbowych telefonów komórkowych.
- Przed przekazaniem telefonu pracownikowi, dział IT dostosowuje oprogramowanie mające na celu zabezpieczenie przed naruszeniem danych.

4. Kopie zapasowe

W celu ochrony przed utratą danych regularnie wykonywane są i testowane kopie informacji i oprogramowania (kopie bezpieczeństwa i archiwalne). Za opracowanie i wdrożenie szczegółowych zasad i trybu wykonywania kopii zapasowych oraz ich systematyczne przygotowanie odpowiedzialny jest ASI.
Kopie bezpieczeństwa wykonywane są w szczególności:

- przed dokonaniem zmian w konfiguracji systemów lub oprogramowania,
- przed dokonaniem zmian w programach (np. zmiana wersji),
- po każdej istotnej zmianie danych w bazie danych.

Oprócz kopii bezpieczeństwa wykonywane są okresowo kopie archiwalne istotnych danych dla działalności Spółki. Szczegółowy harmonogram wykonywania kopii zapasowych został opisany w Instrukcji

bezpiecznego zarządzania systemem informatycznym oraz w planie działania na lata 2018-2019 zawartym w Raporcie.[7]

5. Przeglądy i konserwacja systemów oraz nośników informacji

5.1. Przeglądy, konserwacje lub naprawy systemów i nośników wykorzystywanych w firmie dokonywane są przez osobę upoważnioną do tego typu czynności, w szczególności przez ASI.

5.2. Dopuszcza się realizację czynności określonych w ustępie 1 przez specjalistyczne firmy świadczące usługi z zakresu IT. W przypadku korzystania z usług specjalistycznej firmy konieczne jest zawarcie stosownej umowy cywilnoprawnej.

5.3. Umowy dotyczące świadczenia usług teleinformatycznych, w tym zakupu, modernizacji, sprzedaży lub serwisu urządzeń komputerowych, systemów informatycznych i oprogramowania powinny zawierać niezbędne klauzule określające wzajemne prawa i obowiązki stron umowy, a w szczególności wymagania dotyczące bezpieczeństwa, dostępu i ochrony danych oraz zakresu odpowiedzialności stron umowy w tym względzie.

5.4. Pracownicy firm świadczących usługi w oparciu o zawarte z firmą ENGIE umowy wykonują zlecone zadania tylko za zgodą ASI lub innego uprawnionego pracownika i pod jego nadzorem.

5.5. W przypadku zdalnego dostępu do komputera (np. w celu wykonywania czynności serwisowych na komputerze) użytkownik komputera musi potwierdzić przejęcie pulpitu komputera oraz nadzorować wszelkie czynności wykonywane przez ASI lub osobę przejmującą pulpit komputera, której zostały zlecone stosowne działania.

6. Korzystanie z oprogramowania

6.1. Spółka posiada licencjonowane egzemplarze oprogramowania komputerowego opracowanego przez różnych producentów. Licencjonowane i zarejestrowane egzemplarze oprogramowania komputerowego zostały zainstalowane na komputerach oraz wykonano właściwe kopie zapasowe zgodnie z postanowieniami umów Licencyjnych. Stosuje się zakaz wykonywania innych kopii tego oprogramowania ani też dokumentacji bez zgody producenta oprogramowania.

6.2. Spółka dostarcza kopie legalnie nabytego oprogramowania by terminowo i we właściwych ilościach zapewnić oprogramowanie dla wszystkich stacji roboczych w firmie, w sposób zgodny z prawem.

6.3. Używanie oprogramowania uzyskanego z jakiegokolwiek innego źródła może stanowić zagrożenie dla bezpieczeństwa Spółki oraz groźbę postępowania prawnego, dlatego też używanie takiego oprogramowania jest ściśle bezwzględnie zabronione.

6.4. W niektórych przypadkach umowa licencyjna może pozwalać na zainstalowanie określonego programu komputerowego na komputerze przenośnym lub komputerze domowym wykorzystywanym do celów służbowych. Pracownicy nie mogą wykonywać dodatkowych żadnych kopii oprogramowania lub dokumentacji bez zgody działu IT.

6.5. Niedozwolone kopiowanie oprogramowania lub dokumentacji objętych prawem autorskim stanowi naruszenie prawa i jest sprzeczne z ustalonymi normami postępowania dla pracowników Spółki.

6.6. Spółka zastrzega sobie prawo do ochrony swojej reputacji i inwestycji w oprogramowanie komputerowe poprzez zastosowanie skutecznych wewnętrznych mechanizmów kontroli w celu zapobieżenia wykonywania niedozwolonych kopii oprogramowania lub używania takowych. Mechanizmy te obejmują częste i okresowe kontrole wykorzystania oprogramowania, zapowiedziane i niezapowiedziane przeglądy stacji roboczych w celu stwierdzenia zgodności oprogramowania z umowami licencyjnymi, usuwanie oprogramowania znalezionego na komputerach, dla którego nie można określić ważnej licencji lub dowodu.

6.7. Wszyscy pracownicy mogą wykorzystywać jedynie legalne oprogramowanie. za które odpowiedzialny jest ASI.

6.8. Autoryzowana instalacja oprogramowania na stanowiskach pracowniczych może być dokonywana przez pracowników (lub osoby współpracujące) tylko i wyłącznie po wydaniu zgody przez dział IT.

6.9. Zabronione jest:

[7] Raport_ dotyczący podejścia ENGIE EC SŁUPSK SPÓŁKA Z O.O do przetwarzania aktywów informacyjnych w tym danych osobowych, opartym na ryzyku zatwierdzonym w dniu 05.10.2018 r.

- samowolne instalowanie w systemie informatycznym, bez zgody administratora systemu, jakichkolwiek programów komputerowych
- odinstalowanie programów zainstalowanych w systemie.

6.10. Oprogramowanie w wersjach testowych lub w jakikolwiek inny sposób ograniczony umowami licencyjnymi może być użytkowane wyłącznie zgodnie z jego przeznaczeniem jedynie przez osoby upoważnione przez ASI.

6.11. Zabrania się wnoszenia na teren Spółki prywatnych kopii oprogramowania oraz kopiowania i pobierania z Internetu „utworów" będących przedmiotem ochrony praw autorskich (programy komputerowe, utwory muzyczne, filmy, gry komputerowe, itp.).

6.12. Konieczne zakupy oprogramowania lub instalowanie oprogramowania niebędącego w zasobach Spółki wykonuje pracownik działu IT. Instalacja i korzystanie z produktów w wersjach ewaluacyjnych, testowych lub w jakikolwiek inny sposób ograniczony umowami licencyjnymi może być użytkowane zgodnie z ich przeznaczeniem.

6.13. Wszelkie wątpliwości rozstrzygane są przez ASI.

BEZPIECZEŃSTWO KOMUNIKACJI

Cel: zapewnić ochronę informacji w sieciach oraz wspomagających je środkach przetwarzania komunikacji. Utrzymać bezpieczeństwo informacji przesyłanych wewnątrz Spółki i wymienianych z podmiotami zewnętrznymi.

1. Korzystanie z łącza internetowego

1.1. Zakładowe łącze internetowe jest przeznaczone do korzystania z usług internetowych, takich jak przeglądanie witryn www, wysyłanie i odbiór poczty elektronicznej, transfer plików, itp.

1.2. Łącze internetowe może być wykorzystywane jedynie do celów związanych z wykonywaną pracą.

1.3. Korzystanie z łącza internetowego jest dozwolone jedynie w wyznaczonych godzinach pracy.

1.4. Dostęp do Internetu na poszczególnych stacjach roboczych przydziela pracownik działu IT.

2. Sposoby przesyłania dużych plików

Wszystkie wrażliwe dane udostępnione na zewnątrz Spółki ~~powinny być~~ muszą być spakowane do pliku **rar** zaszyfrowanego hasłem z opcją zaszyfruj nazwy plików.

Hasło do pliku powinno być przesłane w osobnym mailu, wysłane sms na numer telefonu odbiorcy lub przekazane w rozmowie telefonicznej.

2.1. Dysk Google. Wykorzystuje konto Google pracowników działu IT. Wielkość danych do 15 GB. Ilość danych można powiększyć do 100 GB przez wykupienie abonamentu w Google. Pracownik wskazuje specjaliście IT pliki lub foldery które mają być przekazane na zewnątrz oraz podaje adres email osoby, która ma odebrać dane. IT przenosi je na dysk Google i przesyła link z udostępnionym zasobem do odbierającego. Dane nie mogą być edytowane przez odbierającego. Link może być przesłany przez odbierającego dalej. Należy zaszyfrować zasób i usunąć go po odebraniu. Wymagana współpraca z IT.

2.2. Dysk OneDrive. Narzędzie do wykorzystania tylko w ramach ENGIE, wykorzystuje Office 365. Każdy pracownik ENGIE może udostępnić folder innemu pracownikowi, który znajduje się na liście adresowej ENGIE. Dane mogą być edytowane w folderze przez odbierającego. Zaletą jest ogromna wygoda i możliwość edycji przez odbierającego. Niewymagana współpraca z IT.

2.3. Firmowy Serwer. Możliwość pobierania i zapisywania plików przez zdalnych odbiorców. Administrator ma możliwość śledzenia kto i kiedy zapisywał i pobierał pliki. Rozwiązanie dobre dla ogromnych plików i stałej współpracy z odbiorcą. Wymagana współpraca z IT.

2.4. Przesłanie email. Większe pliki można również skompresować za pomocą rar dzieląc je na paczki po 10 MB i wysyłać osobno w oddzielnych wiadomościach email. Odbiorca scala w całość wszystkie paczki po kliknięciu na jedną z nich. Rozwiązanie dobre dla plików do 40 MB. Niewymagana współpraca z IT.

3. Dostęp do portali społecznościowych grupy ENGIE

W ramach Grupy ENGIE pracownicy mają dostęp do wewnętrznej strony internetowej HORIZON pod adresem https://engie.sharepoint.com/sites/E024/en-us i możliwość wykorzystywania zawartych tam materiałów.

Udostępniono również wewnętrzny portal społecznościowy YAMMER, aby usprawnić współpracę między pracownikami Grupy oraz z upoważnionymi stronami trzecimi współpracującymi w dziedzinach będących przedmiotem wspólnego zainteresowania. Portal społecznościowy Grupy jest narzędziem wymiany informacji, którego celem jest w szczególności:

- ułatwienie współpracy przy realizacji projektów, wymianie know-how, organizacji imprez lub wymianie dobrych praktyk,
- dzielenie się fachową wiedzą,
- wymiana informacji na temat aktualnego stanu realizacji projektu lub usługi,
- odnalezienie właściwego eksperta lub współpracownika.

Wszyscy pracownicy Spółka korzystający z portalu społecznościowego YAMMER zobligowani są do przestrzegania reguł dopuszczalnych działań ,określonych przez grupę ENGIE w dokumencie stanowiącym **załącznik nr 1_PSI POLITYKA YAMMER Portal społecznościowy Grupy ENGIE - Reguły dopuszczalnych działań**.

PRACA W SYSTEMIE INFORMATYCZNYM

1. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

1.1. Przed rozpoczęciem pracy w systemie komputerowym należy zalogować się do systemu przy użyciu indywidualnego identyfikatora oraz hasła.

1.2. Przy opuszczeniu stanowiska pracy na odległość uniemożliwiającą jego obserwację należy wykonać opcję wylogowania z systemu, zablokowania dostępu poprzez zabezpieczony hasłem wygaszacz ekranu lub jeżeli taka możliwość nie istnieje wyjść z programu.

1.3. Osoba udostępniająca stanowisko komputerowe innemu upoważnionemu pracownikowi zobowiązana jest wykonać funkcję wylogowania z systemu.

1.4. Przed wyłączeniem komputera należy bezwzględnie zakończyć pracę uruchomionych programów, wykonać zamknięcie systemu i wylogować się z sieci komputerowej.

1.5. Niedopuszczalne jest wyłączanie komputera przed zamknięciem oprogramowania oraz zakończeniem pracy w sieci.

1.6. Przypadki stwierdzenia nieprawidłowości w zakresie działania systemu należy zgłaszać do ASI, który zdarzenia stanowiące incydenty bezpieczeństwa rejestruje w dzienniku Awarii Systemu Informatycznego.

1.7. Zabronione jest podejmowanie działań mogących być zagrożeniem dla systemu, a w tym:

- łamanie haseł;
- dokonywanie włamań na konta innych użytkowników;
- nieprawne uzyskiwanie dostępu do kont administracyjnych;
- zakłócanie działania usług;
- omijanie i badanie zabezpieczeń (nie dotyczy czynności wykonywanych w ramach audytu, czynności kontrolnych lub testowania wykonywanych przez osoby upoważnione);
- doprowadzanie do rozprowadzania wirusów, robaków i koni trojańskich oraz niechcianej poczty;
- praca na koncie innego użytkownika;
- samowolne umieszczanie w systemie informatycznym jakichkolwiek plików niezwiązanych bezpośrednio z wykonywaną pracą;
- samowolna zmiana ustawień sieciowych i systemowych stacji roboczych;
- uruchamianie na stacjach roboczych, bez ASI, jakichkolwiek programów komputerowych znajdujących się na przenośnych nośnikach danych.

2. Zasady bezpieczeństwa podczas pracy w systemie informatycznym

1. Opuszczając stanowisko komputerowe, jego użytkownik ma obowiązek zabezpieczyć to stanowisko w sposób wymagający ponownego uwierzytelnienia.
2. Zabronione jest udostępnianie stacji roboczej osobie nieposiadającej uprawnień do korzystania z systemu informatycznego.
3. Zabronione jest pozostawienie zalogowanego i nie zabezpieczonego stanowiska komputerowego bez nadzoru osoby uprawnionej do korzystania z systemu informatycznego.
4. Zabronione jest zdradzanie osobom postronnym identyfikatorów użytkowników systemu, nazw serwerów oraz innych szczegółów dotyczących funkcjonowania i budowy systemu informatycznego oraz systemu zabezpieczeń.
5. Zabronione jest wprowadzanie na prośbę niezweryfikowanej osoby jakichkolwiek poleceń do komputera (szczególnie poleceń dla siebie niezrozumiałych).
6. Użytkownikom systemu nie wolno otwierać załączników w podejrzanych listach e-mail, w szczególności we wszystkich listach o tematyce niezwiązanej z wykonywaną pracą, listach reklamujących niezamawiane usługi czy produkty, listach o niezrozumiałe] treści. W razie konieczności otwarcia takiego załącznika należy powiadomić administratora systemu.
7. Wszelkie przesyłki realizowane drogą elektroniczną zawierające dane niejawne powinny być zaszyfrowane za pomocą uzgodnionego z korespondentem narzędzia kryptograficznego.
8. Podczas przesyłania informacji przez formularze znajdujące się na stronach internetowych należy wszędzie gdzie jest to możliwe korzystać z szyfrowanego połączenia (SSL).

3. Zasady monitorowania przez pracodawcę: pracowników, sprzętu komputerowego i oprogramowania stanowiącego własność firmy.

3.1. Pracodawca jest uprawniony do kontrolowania przebiegu pracy oraz jej efektów. Pracodawca ma także prawo monitorować sposób wykonywania przez pracownika obowiązków wynikających ze stosunku pracy, a także badać i oceniać jej efektywność.

3.2. W ramach monitoringu kontrolowane mogą być wyłącznie:

- czas aktywności użytkownika (czas pracy z godziną rozpoczęcia i zakończenia pracy z przerwami);
- czas procesów (całkowity czas działania a czas wykorzystania przez użytkownika);
- rzeczywiste użytkowanie programów (procentowa wartość wykorzystywania zainstalowanych na stacji roboczej aplikacji) oraz edytowanych dokumentów;
- rodzaj aktywności pracowników (raporty przedstawiające czas pracy, czas przeglądania Internetu, czas grania w gry komputerowe, czas zakupów online, itp.);
- odwiedzane strony internetowe (nagłówki stron, liczba i czas wizyt);
- transfer sieciowy użytkowników (ruch sieciowy lokalny i transfer internetowy wygenerowany przez pracowników);
- wydruki komputerowe (nazwa użytkownika i nazwa stacji roboczej, data wydruku;
- wykorzystana drukarka, drukowany dokument),koszty wydruków, operacje na urządzeniach przenośnych odczyt i kopiowanie plików.

3.3. W ramach monitoringu zabrania się: zdalnie podglądać pulpit użytkownika, z wyłączeniem sytuacji gdy pracownik sam zwróci się do osoby posiadającej uprawnienia do monitorowania z prośbą o podgląd pulpitu w celach serwisowych i kontrolnych (np. prośba o sprawdzenie, czy prawidłowo wykonywane są operacje na stacji roboczej lub zbadanie przyczyny usterki).

3.4. Pracodawca ma prawo wglądu w służbową skrzynkę mailową pracownika.

3.5. Pracodawca jest zobowiązany poinformować każdego użytkownika systemu informatycznego o stosowaniu monitoringu a użytkownik systemu informatycznego zobowiązany jest zapoznać się z „Zasadami pracy z komputerem i oprogramowaniem służbowym w sieci teleinformatycznej, oraz zasadami monitorowania przez pracodawcę: pracowników, sprzętu komputerowego i oprogramowania stanowiącego własność firmy. Powyższe potwierdza złożone przez użytkownika systemu informatycznego oświadczenie. Informacja Pracodawcy o stosowaniu monitoringu podawana jest pracownikom odrębnym Zarządzeniem Prezesa Zarządu (Zarządzenie nr 2/2019 z dnia 16.04.2019 r.).

Ze względu na konieczność dokumentowania dopełnienia obowiązku informacyjnego wynikającego z Art. 13, Art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 – RODO: pracownik pozostający w stosunku pracy na dzień wejścia w życie zarządzenia podpisuje oświadczenie u IOD (Inspektor Ochrony Danych), które następnie przechowywane jest w aktach osobowych pracownika,

1. nowozatrudniony pracownik podpisuje oświadczenie u IOD, które następnie przechowywane jest w aktach osobowych pracownika.

KONTROLA POLITYKI BEZPIECZEŃSTWA INFORMATYCZNEGO

1. Bezpieczeństwo informatyczne jest monitorowane na bieżąco a zapisy w Polityce i w **Instrukcji bezpiecznego zarządzania systemem informatycznym** są weryfikowane przynajmniej jeden raz w roku i aktualizowane w razie potrzeby.
2. Bezpieczeństwo w relacjach z podmiotami zewnętrznymi:

– wymagania w dziedzinie bezpieczeństwa są elementem wszystkich umów prawnych z podmiotami zewnętrznymi,
– wykonawcy zewnętrzni są zobowiązani do przestrzegania Polityki Bezpieczeństwa Informacji obowiązującej w Spółce.

3. W relacjach z osobami postronnymi (gośćmi, wykonawcami itd.) stosuje się specjalne procesy kontroli w odniesieniu do dostępu fizycznego i logicznego na terenie Spółki oraz dostępu zdalnego.
4. Jeden raz w roku ABI/IOD przeprowadza ocenę stanu procesów zarządzania zabezpieczeniami logicznymi stosowanych w odniesieniu do newralgicznych aplikacji. Do oceny wykorzystywane jest poniższe miary:

Skala oceny:	lp	stan procesu
	1	Przygotowanie komputerów i korzystających z zasobów sieciowych przed oddaniem do użytkowania
	2	Zabezpieczenie przed utratą lub skokiem napięcia w elektrycznej sieci zasilającej
1 = Brak procesów. / NIE	3	Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym
2 = Istnieje proces nieformalny. / OPRACOWAĆ PONOWNIE	4	Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
3 = Istnieje formalny, udokumentowany proces. / POPRAWIĆ	5	Dostęp użytkowników zdalnych do zasobów spółki
4 = Istnieje formalny, udokumentowany proces, a ponadto mierzone są najważniejsze parametry. / DOBRZE	6	Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania
5 = Istnieje formalny, udokumentowany proces, mierzone są najważniejsze parametry, a ponadto proces jest stale doskonalony na podstawie wyników pomiarów/BARDZO DOBRZE	7	Postępowanie ze sprzętem na którym przechowywane były dane firmowe w tym dane osobowe w przypadku jego likwidacji lub sprzedaży.
	8	Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania
	9	Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Uzyskany wynik wskazuje kierunki doskonalenia procesu.

PODSUMOWANIE

Polityka Bezpieczeństwa Informacji zawiera zbiór reguł i sposobów postępowania mających na celu jak najlepsze zabezpieczenie aktywów informacyjnych. Obejmuje trzy ściśle powiązane ze sobą obszary: informację, ochronę danych osobowych i systemy informatyczne.

Wszyscy pracownicy są zobowiązani do zapoznania się z jej treścią i przestrzegania, podpisując **załącznik nr 1_PBI – oświadczenie pracownika.**

Dokumentację powiązaną z niniejszym dokumentem stanowią:

1. Raport dotyczący podejścia ENGIE EC SŁUPSK SPÓŁKA Z O.O do przetwarzania aktywów informacyjnych w tym danych osobowych, opartym na ryzyku z dnia 05.10.2018 roku.
2. Plan Reagowania Kryzysowego – wydawany Zarządzeniem Prezesa Spółki.
3. Regulamin Pracy Spółki.
4. Zarządzenie nr 7/2018 Prezesa Zarządu ENGIE EC Słupsk Sp. z o. o. w Słupsku z dnia 07 maja 2018 roku
5. w sprawie: zasad przestrzegania bezpieczeństwa informacji w ENGIE EC Słupsk w zakresie monitoringu wizyjnego
6. Zarządzenie nr 2 /2019 Prezesa Zarządu ENGIE EC Słupsk Sp. z o. o. w Słupsku z dnia 16.04.2019 roku w sprawie: procedury zapoznania pracowników z zasadami stosowania monitoringu

LISTA ZAŁĄCZNIKÓW:

Rozdział I:

Załącznik_BI_ nr:

1. Oświadczenie o zachowaniu poufności (oświadczenie pracownika)
2. Zobowiązanie do zachowania bezpieczeństwa informacji (oświadczenie osoby współpracującej)
3. Zobowiązanie do zachowania poufności informacji (spotkanie grupowe)

Rozdział II:

Załącznik nr..._RODO:

1. Wzór zgody na przetwarzanie danych osobowych.
2. Wzór zgody na otrzymanie informacji handlowej za pomocą środków komunikacji elektronicznej.
3. Wzór zgody na używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego.
4. Wzór klauzuli informacyjnej (w przypadku pozyskiwania danych osobowych od osoby, której dane dotyczą).
5. Wzór klauzuli informacyjnej (w przypadku pozyskiwania danych osobowych z innych źródeł niż od osoby, której dane dotyczą).
6. Wzór upoważnienia do przetwarzania danych.
7. Wzór umowy powierzenia przetwarzania danych osobowych.
8. Wzór procedury w przypadku naruszenia ochrony danych
9. Wzór powiadomienia o naruszeniu ochrony danych osobowych – zgłoszenia do organu nadzorczego.
10. Wzór zawiadomienia o naruszeniu ochrony danych osobowych osoby, której dane dotyczą.
11. Wzór rejestru czynności przetwarzania przez administratora.
12. Wzór rejestru czynności przetwarzania przez procesora.
13. Wzór procedury oceny skutków dla ochrony danych osobowych
14. Wzór wniosku konsultacyjnego do organu nadzorczego z uwagi na wysokie ryzyko planowanego przetwarzania
15. Wzór procedury postępowania w przypadku otrzymania żądania dostępu do danych.
16. Wzór procedury postępowania w przypadku otrzymania żądania sprostowania danych.
17. Wzór procedury postępowania w przypadku otrzymania żądania usunięcia danych.
18. Wzór procedury postępowania w przypadku otrzymania żądania ograniczenia dostępu do danych.
19. Wzór procedury postępowania w przypadku otrzymania żądania przeniesienia danych
20. Wzór procedury postępowania w przypadku otrzymania sprzeciwu wobec przetwarzania danych
21. Wzór procedury postępowania w przypadku zmiany celu przetwarzania danych.
22. Wzór procedury postępowania w przypadku cofnięcia zgody na przetwarzanie danych.

Rozdział III:

Załącznik _BSI_nr 1 POLITYKA YAMMER Portal społecznościowy Grupy ENGIE - Reguły dopuszczalnych działań