WÓJT GMINY
GOLUB-DOBRZYŃ

ZARZĄDZENIE Nr 44/2018

Wójta Gminy Golub-Dobrzyń

z dnia 3 września 2018 roku

w sprawie aktualizacji dokumentacji Polityki Bezpieczeństwa

W oparciu o wymagania:

1. Rozporządzenia Parlamentu Europejskiego i Rady UE 2016/672 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
2. Ustawy o ochronie danych osobowych z dnia 10 maja 2018 roku (Dz.U. z 2018 poz. 1000).

zarządza się co następuje:

§ 1

1. W celu zapewnienia ochrony danych osobowych wprowadza się Politykę Ochrony Danych Osobowych.
2. Jednocześnie wprowadza się następujące załączniki do Polityki Ochrony Danych Osobowych:

a) Załącznik nr 1 – Powierzenie przetwarzania danych.
b) Załącznik nr 2 – Zobowiązanie osoby upoważnionej.
c) Załącznik nr 3 – Klauzule informacyjne.
d) Załącznik nr 4 – Procedura zarządzania ryzykiem.
e) Załącznik nr 5 – Formularz analizy ryzyka.
f) Załącznik nr 6 – Protokół zdawczo-odbiorczy.
g) Załącznik nr 7 – Upoważnienie do przetwarzania danych osobowych (PDO)

§ 2

1. Zobowiązuje się **wszystkich** pracowników lub osoby świadczące na podstawie umów cywilnoprawnych do zapoznania się z dokumentami, o których mowa w § 1 ust. 1 i 2 zarządzenia i stosowania się do postanowień niniejszych dokumentów.
2. Przestrzeganie zasad bezpieczeństwa informacji należy do obowiązków wszystkich pracowników i osób świadczących na podstawie umów cywilnoprawnych oraz podmiotów zewnętrznych współpracujących z Urzędem.
3. Procedury i regulacje wewnętrzne przygotowywane przez osoby na samodzielnych stanowiskach i komórki organizacyjne nie mogą naruszać postanowień określonych w niniejszym zarządzeniu.

§ 3

1. Wykonanie zarządzenia w podległych obszarach powierza się kierownikom komórek organizacyjnych.

§ 4

Z dniem wejścia w życie niniejszego zarządzenia przestaje obowiązywać dotychczasowa Polityka bezpieczeństwa wdrożona zarządzeniem Nr 16/2016 Wójta Gminy Golub-Dobrzyń z dnia 1 kwietnia 2016 r. w sprawie wprowadzenia Polityki Bezpieczeństwa i Instrukcji Zarządzania Systemem Informatycznym.

§ 5

Niniejsze Zarządzenie wchodzi w życie z dniem podpisania.

WÓJT
Marek Rygiewicz

Załączniki:

Załącznik nr 1 Polityka Ochrony Danych Osobowych wraz z załącznikami.

Umowa powierzenia przetwarzania danych osobowych

Spis treści

1 Cel dokumentu

Dokument zawiera szablon umowy powierzenia przetwarzania danych osobowych.

2 Zakres stosowania

Umowę powierzenia lub porozumienie należy stosować we wszystkich przypadkach, w których istnieje konieczność przetwarzania danych osobowych przez inną niż administrator jednostkę organizacyjną lub podmiot, w tym np.:

- usługi prawne
- usługi hostingu serwerów czy przestrzeni dyskowej
- usługi niszczenia dokumentów/ nośników danych
- usługi bhp

Wyjątkiem od stosowania niniejszej umowy są sytuacje, w których przetwarzanie danych osobowych odbywa się przez podmiot posiadający uprawnienia z mocy ustawy do przetwarzania danych osobowych, (np. Policja w uzasadnionych przypadkach).

O konieczności podpisania umowy decyduje Administrator.

3 Treść umowy powierzenia

UMOWA
POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Zawarta w dniu ..... w ..... pomiędzy:

URZĄD GMINY

.....

.....

reprezentowaną przez:

.....

zwanym dalej **administratorem**,

a

.....

.....

z siedzibą w ..... przy

ul. .....,

reprezentowaną/nym przez:

.....

.....

Zwaną/nym dalej **podmiotem przetwarzającym**.

Słownik pojęć:

1. "zwykłe dane osobowe" oznaczają 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, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej - za wyjątkiem "szczególnych kategorii danych osobowych";
2. "szczególne kategorie danych osobowych" - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;
3. "dane osobowe dotyczące wyroków skazujących i naruszeń prawa" - dane osobowe dotyczące wyroków skazujących i naruszeń prawa;
4. „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
5. „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie

Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

6. „podmiot przetwarzający" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
7. „dane dotyczące zdrowia" oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

§1

1. **Podmiot przetwarzający** w celu realizacji umowy ..... może przetwarzać w trybie art. 28 ogólnego rozporządzenia o ochronie danych z dnia 27 kwietnia 2016 roku, zwanego dalej RODO następujące dane osobowe:

zwykłe dane osobowe, w tym m.in.: *imię i nazwisko, adres zamieszkania, PESEL, data i miejsce urodzenia, stan cywilny, wynagrodzenie*	☐TAK ☐NIE
szczególne kategorie danych osobowych, w tym: *stan zdrowia*	☐TAK ☐NIE
dane osobowe dotyczące wyroków skazujących i naruszeń prawa	☐TAK ☐NIE

dotyczące:

pracowników lub członków ich rodzin	☐TAK ☐NIE
Interesantów Urzędu	☐TAK ☐NIE
Inne (jakie)	☐TAK ☐NIE

przekazane przez **Administratora** w zakresie niezbędnym realizacji umowy.

§2

1. **Podmiot przetwarzający** jest zobowiązany do przestrzegania przepisów RODO.
2. **Podmiot przetwarzający** oświadcza, iż uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.

§3

1. Dostęp do powierzonych danych osobowych mogą posiadać tylko osoby, którym nadano upoważnienie do przetwarzania danych.
2. Upoważnienie nadaje **podmiot przetwarzający**, który jednocześnie zapewnia, że osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania ich w tajemnicy.
3. **Podmiot przetwarzający** oświadcza, że w celu realizacji umowy, o której mowa w §1 nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody **administratora**.

§4

Podmiot przetwarzający zobowiązuje się:

a) umożliwiać administratorowi, na każde żądanie, dokonania przeglądu stosowanych środków technicznych i organizacyjnych, aby przetwarzanie toczyło się zgodnie z prawem, a także uaktualniać te środki, o ile w opinii administratora są one niewystarczające do tego, aby zapewnić zgodne z prawem przetwarzanie powierzonych danych osobowych;

b) pomagać administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO; w szczególności, zobowiązuje się przekazywać administratorowi informacje oraz wykonywać jego polecenia dotyczące stosowanych środków zabezpieczania danych osobowych, przypadków naruszenia ochrony danych osobowych oraz zawiadamiania o tym organu nadzorczego lub osób, których dane osobowe dotyczą, przeprowadzenia oceny skutków dla ochrony danych, oraz przeprowadzania uprzednich konsultacji z organem nadzorczym i wdrożenia zaleceń organu;

c) przekazywać Administratorowi bez zbędnej zwłoki, najpóźniej w ciągu 24 godzin od wykrycia zdarzenia na adres mailowy ....., informacje o naruszeniu ochrony powierzonych **w związku z realizacją umowy** danych osobowych, w tym informacje niezbędne administratorowi do zgłoszenia naruszenia ochrony danych organowi nadzorczemu, o którym mowa w art. 33 ust. 3 RODO;

d) pomagać administratorowi, poprzez odpowiednie środki techniczne i organizacyjne oraz na podstawie odrębnych ustaleń, w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane dotyczą, w zakresie wykonywania ich praw określonych w rozdziale III RODO;

§5

Podmiot przetwarzający odpowiada za szkody, jakie powstały wobec **administratora** lub osób trzecich w wyniku niezgodnego z Umową przetwarzania danych osobowych.

§6

Administrator może rozwiązać niniejszą umowę w każdym czasie. Niniejsza umowa może być rozwiązana przez **podmiot przetwarzający** z zachowaniem miesięcznego okresu wypowiedzenia. W każdym jednak wypadku niniejsza umowa wygasa w dacie rozwiązania lub wygaśnięcia Umowy, o której mowa w § 1 ust. 1 niniejszej umowy.

§7

Po zakończeniu świadczenia usług związanych z przetwarzaniem, **podmiot przetwarzający** zależnie od decyzji **administratora** usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie przetwarzanych w związku z realizacją umowy o której mowa w §1 danych osobowych.

§8

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

Administrator **Podmiot przetwarzający**

ZOBOWIĄZANIE OSOBY UPOWAŻNIONEJ

Oświadczam, że zapoznałam/zapoznałem się z dokumentami Ochrony danych osobowych, tj.:

☐ Polityka Ochrony Danych Osobowych

Znane mi są przepisy dotyczące przetwarzania i ochrony danych osobowych, w szczególności: ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w zakresie niezbędnym do wykonywania czynności służbowych.

Ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku (Dz.U. z 2018 r. poz. 1000)

Zobowiązuje się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, również po ustaniu stosunku pracy, oraz do przestrzegania instrukcji i procedur związanych z ochroną danych osobowych wynikających z dokumentacji przetwarzania danych osobowych.

.....
Data i czytelny Podpis Pracownika

KLAUZULA INFORMACYJNA DLA PRACOWNIKÓW

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dalej RODO, informuję, że:

1) Administratorem Pani/Pana danych osobowych jest .....
2) Inspektorem Ochrony Danych jest Piotr Juzoń, e-mail puzon@abidata.pl
3) Pani/Pana dane osobowe będą przetwarzane w celu realizacji praw i obowiązków wynikających ze stosunku pracy, na podstawie art.6 ust.1 pkt c RODO, w celu realizacji świadczeń ZFŚS na podstawie zgody na przetwarzanie danych - art.6 ust.1 pkt a RODO.
4) Podanie przez Panią/Pana danych osobowych jest wymogiem ustawowym w zakresie realizacji praw i obowiązków wynikających ze stosunku pracy, a ich nieprzekazanie spowoduje niemożność realizacji zawartej umowy o pracę i związanych z nią obowiązków podatkowo-składkowych. W przypadku realizacji świadczeń ZFŚS podanie danych jest dobrowolne, lecz ich niepodanie uniemożliwi realizację świadczeń.
5) Odbiorcą Pani/Pana danych osobowych będą jednostki nadrzędne, obsługa informatyczne, ...
6) Pani/Pana dane nie będą podlegały zautomatyzowanemu przetwarzaniu.
7) Pani/Pana dane osobowe będą przechowywane przez okres trwania stosunku pracy oraz w obowiązkowym okresie przechowywania dokumentacji związanej ze stosunkiem pracy i akt osobowych, ustalanym zgodnie z odrębnymi przepisami prawa.
8) Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
9) Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

KLAUZULA INFORMACYJNA DLA KANDYDATÓW DO PRACY

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dalej RODO, informuję, że:

1) Administratorem Pani/Pana danych osobowych jest .....
2) Inspektorem Ochrony Danych jest Piotr Juzoń, e-mail puzon@abidata.pl
3) Pani/Pana dane osobowe będą przetwarzane w celu przeprowadzenia procesu rekrutacyjnego, na podstawie art.6 ust.1 pkt a RODO - zgody na przetwarzanie danych i art.6 ust.1 pkt c RODO - jest to niezbędne do realizacji obowiązku prawnego RODO.
4) Podanie przez Panią/Pana danych osobowych jest dobrowolne, a ich nieprzekazanie spowoduje brak możliwości przeprowadzenia postępowania rekrutacyjnego.
5) Administrator nie będzie przekazywał Pani/Pana danych podmiotom innym niż upoważnione na mocy przepisów prawa.
6) Pani/Pana dane nie będą podlegały zautomatyzowanemu przetwarzaniu.
7) Pani/Pana dane osobowe będą przechowywane do momentu zakończenia procesu rekrutacyjnego, nie dłużej jednak niż przez ..... od zakończenia rekrutacji.
8) Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
9) Ma Pani/Pan prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.

KLAUZULA - MONITORING WIZYJNY

Zgodnie z art. 13 ust. 1 i 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dalej RODO, informuję, że:

- Administratorem Pani/Pana danych osobowych jest ....
- Inspektorem Ochrony Danych jest Piotr Juzoń, e-mail puzon@abidata.pl
- Dane osobowe w tym wizerunek osób przebywających na terenie budynku i obszaru wokół budynku objętym monitoringiem wizyjnym będą przetwarzanie w celu zapewnienia bezpieczeństwa osób i mienia - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze
- zapisy monitoringu przechowywane są do ..... dni i będą udostępniane jedynie podmiotom uprawnionym na mocy przepisów prawa;
- Posiada Pani/Pan prawo do:
  - żądania dostępu do swoich danych osobowych sprostowania, usunięcia lub ograniczenia przetwarzania przy uwzględnieniu możliwości technicznych administratora
  - wniesienia sprzeciwu wobec przetwarzania, przenoszenia danych,
  - wniesienia skargi do organu nadzorczego,
- Pani/Pana dane nie będą podlegały zautomatyzowanemu podejmowaniu decyzji.
- przebywanie w granicach obszaru objętego monitoringiem wiąże się z możliwością rejestracji wizerunku na powyższych zasadach.

KLAUZULA INFORMACYJNA (NA STRONĘ WWW I/lub TABLICĘ INFORMACYJNĄ w GMINIE)

ADMINISTRATOR DANYCH

Administratorem Pani/Pana danych osobowych jest Urząd Gminy Golub-Dobrzyń, ul. Plac1000-lecia 25; 87-400 Golub-Dobrzyń

Można się z nim kontaktować listownie, mailowo: sekretariat@golub-dobrzyn.ug.gov.pl

INSPEKTOR OCHRONY DANYCH

Do kontaktów w sprawie ochrony Pani/Pana danych osobowych został także powołany inspektor ochrony danych, z którym możesz się kontaktować wysyłając e-mail na adres .....ZAŁÓŻ MI PROSZĘ SKRZYNKĘ IOD@uggolub-dobrzyn.pl..... lub pismo na adres Urzędu z dopiskiem – Inspektor Ochrony Danych

CEL I PODSTAWY PRZETWARZANIA

Pani/Pana dane osobowe przetwarzane będą w celu wypełnienia przez administratora zadań określonych w przepisach szczególnych np.: nagrywania i transmisji obrad rady gminy (audio i wideo), utrwalania imprez publicznych (wizerunek), wydania decyzji administracyjnej, postanowienia lub innego działania wynikającego z przepisów prawa.

ODBIORCY DANYCH

Dane osobowe możemy przekazywać i udostępniać wyłącznie podmiotom uprawnionym na podstawie obowiązujących przepisów prawa są nimi np.: sądy, organy ścigania, podatkowe oraz inne podmioty publiczne, gdy wystąpią z takim żądaniem oczywiście w oparciu o stosowną podstawę prawną. Pani/Pana dane osobowe możemy także przekazywać podmiotom, które przetwarzają je na zlecenie administratora tzw. podmiotom przetwarzającym, są nimi np.: podmioty świadczące usługi informatyczne, telekomunikacyjne, pocztowe i inne, jednakże przekazanie danych nastąpić może tylko wtedy, gdy zapewnią one odpowiednią ochronę Państwa praw.

Ponadto, z nagrań sesji rady gminy, zgodnie z obowiązującymi przepisami prawa, administrator może prowadzić bezpośrednią transmisję na stronach internetowych Gminy.

Zdjęcia z imprez publicznych mogą pojawić się w mediach, w tym mediach elektronicznych.

OKRES PRZECHOWYWANIA DANYCH

Pani/Pana dane osobowe mogą być przechowywane przez okres wymagany przepisami prawa.

PRAWA OSÓB KTÓRYCH DANE DOTYCZĄ

Posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych oraz do cofnięcia zgody na przetwarzanie danych.

Wymienione prawa mogą być ograniczone w sytuacjach, kiedy Urząd jest zobowiązany prawnie do przetwarzania danych w celu realizacji obowiązku ustawowego.

W przypadku monitoringu wizyjnego ograniczenia wynikać mogą również z braku możliwości technicznych.

Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

INFORMACJA O WYMOGU PODANIA DANYCH

Podanie przez Pana/Panią danych osobowych jest dobrowolne, choć w niektórych przypadkach może być konsekwencją wymogów przepisów prawa.

KLAUZULA INFORMACYJNA – WNIOSKI I DECYZJE

ADMINISTRATOR DANYCH

Administratorem Pani/Pana danych osobowych jest Urząd Gminy Golub-Dobrzyń, ul. Plac1000-lecia 25; 87-400 Golub-Dobrzyń

Można się z nim kontaktować listownie, mailowo: sekretariat@golub-dobrzyn.ug.gov.pl

INSPEKTOR OCHRONY DANYCH

Do kontaktów w sprawie ochrony Pani/Pana danych osobowych został także powołany inspektor ochrony danych, z którym możesz się kontaktować wysyłając e-mail na adres IOD@uggolub-dobrzyn.pl lub pismo na adres Urzędu z dopiskiem – Inspektor Ochrony Danych

CEL I PODSTAWY PRZETWARZANIA

Pani/Pana dane osobowe przetwarzane będą w celu wypełnienia przez administratora zadań określonych w przepisach szczególnych np.: wydania decyzji administracyjnej, postanowienia lub innego działania wynikającego z przepisów prawa.

ODBIORCY DANYCH

Dane osobowe możemy przekazywać i udostępniać wyłącznie podmiotom uprawnionym na podstawie obowiązujących przepisów prawa są nimi np.: sądy, organy ścigania, podatkowe oraz inne podmioty publiczne, gdy wystąpią z takim żądaniem oczywiście w oparciu o stosowną podstawę prawną. Pani/Pana dane osobowe możemy także przekazywać podmiotom, które przetwarzają je na zlecenie administratora tzw. podmiotom przetwarzającym, są nimi np.: podmioty świadczące usługi informatyczne, telekomunikacyjne, pocztowe i inne, jednakże przekazanie danych nastąpić może tylko wtedy, gdy zapewnią one odpowiednią ochronę Państwa praw.

OKRES PRZECHOWYWANIA DANYCH

Pani/Pana dane osobowe mogą być przechowywane przez okres wymagany przepisami prawa.

PRAWA OSÓB KTÓRYCH DANE DOTYCZĄ

Posiada Pani/Pan prawo do żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych oraz do cofnięcia zgody na przetwarzanie danych.

Wymienione prawa mogą być ograniczone w sytuacjach, kiedy Urząd jest zobowiązany prawnie do przetwarzania danych w celu realizacji obowiązku ustawowego.

Ma Pani/Pan prawo wniesienia skargi do organu nadzorczego, gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

INFORMACJA O WYMOGU PODANIA DANYCH

Podanie przez Pana/Panią danych osobowych jest dobrowolne, choć w niektórych przypadkach może być konsekwencją wymogów przepisów prawa.

KLAUZULA INFORMACYJNA

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

- administratorem Pani/Pana danych osobowych jest **Urząd Gminy Golub-Dobrzyń, ul. Plac1000-lecia 25; 87-400 Golub-Dobrzyń, sekretariat@golub-dobrzyn.ug.gov.pl**
- Urząd Gminy Golub-Dobrzyń posiada inspektora ochrony danych osobowych. Kontakt z inspektorem jest możliwy pod adresem e-mail: IOD@uggolub-dobrzyn.pl lub pocztą tradycyjną na adres Urzędu Gminy z dopiskiem – Inspektor Ochrony Danych,
- dane osobowe przekazane przez Wykonawcę przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego *którego przedmiotem jest* ..... prowadzonym w trybie .....;
- odbiorcami danych osobowych przekazanych przez Wykonawcę będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa Pzp";
- dane osobowe przekazane przez Wykonawcę będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres trwania zawartej umowy oraz w okresie przechowywania dokumentacji ustalonym zgodnie z odrębnymi przepisami.
- obowiązek podania przez Wykonawcę danych osobowych bezpośrednio Wykonawcy dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
- w odniesieniu do danych osobowych przekazanych przez Wykonawcę decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
- Wykonawca jak i osoby których dane Wykonawca przekazał w ramach obowiązku informacyjnego wskazanego w art. 14 RODO posiadają:
  - na podstawie art. 15 RODO prawo dostępu do danych osobowych ich dotyczących;
  - na podstawie art. 16 RODO prawo do sprostowania danych osobowych ich dotyczących[1];
  - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO[2];

---

[1] **Wyjaśnienie:** skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmiana postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.

- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

- Wykonawcy jak i osobom których dane Wykonawca przekazał w ramach obowiązku informacyjnego wskazanego w art. 14 RODO nie przysługuje:
  - w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
  - prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
  - na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych Wykonawcy jak i osób których dane Wykonawca Przekazał w ramach obowiązku informacyjnego wskazanego w art. 14 RODO jest art. 6 ust. 1 lit. c RODO.

[2] **Wyjaśnienie:** prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

KLAUZULA INFORMACYJNA – ZAMÓWIENIA PUBLICZNE, KONTRAHENCI

ADMINISTRATOR DANYCH

Administratorem danych osobowych jest Urząd Gminy Golub-Dobrzyń, ul. Plac1000-lecia 25; 87-400 Golub-Dobrzyń

Można się z nim kontaktować listownie, mailowo: sekretariat@golub-dobrzyn.ug.gov.pl

INSPEKTOR OCHRONY DANYCH

Do kontaktów w sprawie ochrony danych osobowych został także powołany inspektor ochrony danych, z którym możesz się kontaktować wysyłając e-mail na adres IOD@uggolub-dobrzyn.pl lub pismo na adres Urzędu z dopiskiem – Inspektor Ochrony Danych

CEL I PODSTAWY PRZETWARZANIA

Dane osobowe osób kontaktowych (zwane dale „dane osobowe") przetwarzane będą w celu realizacji praw i obowiązków związanych z czynnościami przed zawarciem umowy oraz wynikających z zawartej umowy, na podstawie art.6 ust.1 pkt b RODO

ODBIORCY DANYCH

Dane osobowe możemy przekazywać i udostępniać wyłącznie podmiotom uprawnionym na podstawie obowiązujących przepisów prawa są nimi np.: sądy, organy ścigania, podatkowe oraz inne podmioty publiczne, gdy wystąpią z takim żądaniem oczywiście w oparciu o stosowną podstawę prawną. Dane osobowe możemy także przekazywać podmiotom, które przetwarzają je na zlecenie administratora tzw. podmiotom przetwarzającym, są nimi np.: podmioty świadczące usługi informatyczne, telekomunikacyjne, pocztowe i inne, jednakże przekazanie danych nastąpić może tylko wtedy, gdy zapewnią one odpowiednią ochronę Państwa praw.

OKRES PRZECHOWYWANIA DANYCH

Dane osobowe będą przechowywane przez okres trwania zawartej umowy oraz w okresie przechowywania dokumentacji ustalonym zgodnie z odrębnymi przepisami.

PRAWA OSÓB KTÓRYCH DANE DOTYCZĄ

Osoby, których dane dotyczą, mają prawo do żądania od administratora dostępu do danych osobowych, prawo do ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do wniesienia sprzeciwu wobec przetwarzania oraz prawo do przenoszenia danych oraz do cofnięcia zgody na przetwarzanie danych.

Wymienione prawa mogą być ograniczone w sytuacjach, kiedy Urząd jest zobowiązany prawnie do przetwarzania danych w celu realizacji obowiązku ustawowego.

Mają również prawo wniesienia skargi do organu nadzorczego, gdy uznają, iż przetwarzanie danych osobowych narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.

Podane dane osobowe nie będą podlegały zautomatyzowanemu przetwarzaniu (profilowanie).

INFORMACJA O WYMOGU PODANIA DANYCH

Udział w postępowaniu jest dobrowolny. Podanie danych osobowych może być wymogiem ustawowym, a ich nieprzekazanie spowodować może niemożność przygotowania i realizacji zawartej umowy.

.....

Imię i nazwisko

ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH DLA CELÓW ZWIĄZANYCH Z ZFŚS

Ja, niżej podpisany, wyrażam zgodę na przetwarzanie przez .....oraz powołaną *np. komisję* ..... danych osobowych moich i członków mojej rodziny oraz innych osób pozostających ze mną we wspólnym gospodarstwie domowym, które zostały wskazane we wniosku i załączonych dokumentach, a które są niezbędne do ustalenia sytuacji życiowej, rodzinnej i materialnej celem uzyskania świadczenia z ZFŚS.

.....

Data i podpis

PROCEDURA ZARZĄDZANIA RYZYKIEM PRZY PRZETWARZANIU DANYCH OSOBOWYCH

Niniejsza *Instrukcja* ma status dokumentu przeznaczonego do użytku wewnętrznego i może być udostępniona jedynie osobom upoważnionym (lub określonym) przez Administratora. Dopuszcza się wgląd do niniejszego dokumentu osób działających z mocy obowiązującego prawa.

Zawartość

I. Podstawowe informacje

Niniejsza procedura reguluje zasady zarządzania ryzykiem w procesie przetwarzania danych osobowych. Jej przedmiotem jest ustalenie metodyki oceny ryzyka bezpieczeństwa informacji oraz skutecznego pomiaru wyselekcjonowanych zabezpieczeń i grup zabezpieczeń poprzez mierniki oceny skuteczności.

Procedury i zasady określone w niniejszym dokumencie powinny być znane i stosowane przez wszystkie osoby biorące udział w procesie przetwarzania danych osobowych w systemach informatycznych, bez względu na zajmowane stanowisko, miejsce wykonywanej pracy oraz charakter stosunku pracy.

II. Zarządzanie ryzykiem

1. Pojęcie ryzyka

Ryzyko to niepewne zdarzenie lub zbiór zdarzeń, które w przypadku ich wystąpienia będą mieć wpływ na bezpieczeństwo informacji. Zarządzanie ryzykiem odnosi się do systematycznego stosowania procedur dotyczących zadań identyfikowania i oceniania ryzyk, a następnie planowania i wdrażania reakcji na nie.

Ryzyko to wskaźnik stanu lub zdarzenia, które może prowadzić do strat. Jest ono proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat, które może spowodować.

Ryzyko to przyszłe zdarzenie. Sytuacja, w której wybranie danego wariantu decyzyjnego pociąga za sobą możliwości wystąpienia negatywnych i pozytywnych konsekwencji przy znanym prawdopodobieństwie wystąpienia każdej możliwości.

Ryzyko wynika często z funkcjonowania dużej liczby złożonych i zmiennych podmiotów, zachodzących między nimi zależności, zmian w ich otoczeniu, ograniczonej możliwości kontrolowania oraz ich wyników. Głównym kierunkiem działań każdej organizacji powinno być dążenie do ograniczenia, redukowania ryzyka.

Ryzyko jest nieuniknionym czynnikiem, który musi być wzięty pod uwagę w procesie przetwarzania danych osobowych. Bezpieczeństwo informacji jest ważne, zaś środkiem do jego zapewnienia jest skuteczny system zarządzania bezpieczeństwem informacji, którego główną składową jest zarządzanie ryzykiem.

W dobie gdzie komunikowanie odbywa się za pomocą środków przekazu w sposób błyskawiczny, współczesne przedsiębiorstwo jest zobligowane do dbania o swoje informacje, gdyż mogą one w znaczący sposób zaważyć na konkurencyjności wobec innych podmiotów na rynku. Ochrona informacji to nie tylko działanie organizacyjno-techniczne, którego głównym zadaniem jest kontrola dostępu danych ale także zarządzanie informacjami oraz zasobami informatycznymi. Bezpieczeństwo informacji to już nie tylko norma i wymóg czasu ale obowiązek każdej organizacji będącej w posiadaniu informacji. Wymogi prawa nakładają na zarządy organizacji obowiązek podjęcia szeregu działań o charakterze organizacyjno-technicznym z zakresu ochrony przetwarzanych informacji. Dobór zabezpieczeń z uwagi na koszt powinien zostać dobrany stosownie do wartości szkód, które może ponieść organizacja w sytuacji gdy ich nie zastosuje. Wskazane jest wiec określenie celów bezpieczeństwa w instytucji i jej systemów. Jednym z ważniejszych celów to zidentyfikowanie zasad bezpiecznego przetwarzania informacji, szkolenia, uświadamianie pracowników, monitorowanie aktualnego stanu bezpieczeństwa, doskonalenie systemów bezpieczeństwa. Bezpieczeństwo nie jest więc aktem jednorazowym, lecz bardzo złożonym procesem, wymagającym stałego nadzoru i przystosowania się do zmieniających się warunków otoczenia. Bezpieczeństwo procesu informacyjnego jest zapewnione, gdy istnieje możliwość sprawnego i poufnego gromadzenia informacji, ich przetwarzania, przetrzymywania i przesyłania. Zapewnienie opisanego stanu wymaga ciągłego uwzględniania prawdopodobieństwa zajścia niekorzystnych zdarzeń np.: kradzież danych.

Ponieważ ryzyko jest funkcją konsekwencji, która następuje w wyniku niepożądanego zdarzenia i prawdopodobieństwem zajścia określonego zdarzenia, to szacowanie ryzyka polega na:

→ analizie ryzyka obejmującej identyfikację i wycenę ryzyka,

→ ocenie ryzyka.

Szacowanie ryzyka określa wartość zasobów informacyjnych, rozpoznaje zagrożenia i występujące podatności, wskazuje istniejące środki kierowania bezpieczeństwem i ich wpływ na zidentyfikowanie ryzyka. Wybór zastosowania zabezpieczeń powinien ściśle odpowiadać wynikom szacowania i postępowania z ryzykiem, wymaganiach prawnych, wymaganiach nadzoru. Stąd podstawą do budowania skutecznych *zabezpieczeń* jest szacowanie ryzyka.

Administrator/ADO stosuje podejście jakościowe do szacowania ryzyka - jest to najczęściej subiektywna ocena, oparta na dobrych praktykach i doświadczeniu. Wynikiem takiego szacowania są listy zagrożeń wraz z relatywnym rankingowaniem ryzyka (niskie, średnie, wysokie). Metody te są bardzo elastyczne i otwarte na wszelkiego typu modyfikacje. Umożliwiają dzięki temu dostarczenie organizacji szybko i kosztowo efektywne wyniki w zakresie identyfikacji zagrożeń i stosowania zabezpieczeń.

2. Procedura zarządzania ryzykiem

Proces przetwarzania danych osobowych powinien zakładać procedurę zarządzania ryzykiem, której celem będzie wspieranie podejmowania właściwych decyzji poprzez lepsze zrozumienie ryzyk - ich przyczyn, prawdopodobieństwa, wpływu, czasu wystąpienia oraz wyboru możliwych reakcji na nie.

Zarządzanie ryzykiem to proces szacowania ryzyka, mający na celu ograniczenie go do akceptowalnego poziomu. To działanie wykonywane nieustannie w procesie przetwarzania danych osobowych dla uzyskania potwierdzenia, że proces jest bezpieczny, tzn. spełnia jednocześnie kryterium poufności, integralności i dostępności, a także rozliczalności. Poufność to zapewnienie, że dane osobowe nie są udostępniane nieupoważnionym podmiotom. Integralność to zapewnienie, aby wszelkie zmiany wykonywane w systemie informatycznym, w systemie jego katalogów oraz poszczególnych plikach zawierających dane osobowe były skutkiem zaplanowanych działań użytkowników systemu; właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany. Dostępność to właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym. Rozliczalność to właściwość zapewniająca, że działania podmiotu przetwarzającego dane osobowe mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

Zarządzanie ryzykiem uwzględnia poszczególne elementy całościowego procesu, a nie pojedynczego etapu. W działalności gospodarczej zarządzanie ryzykiem stanowi identyfikację zagrożeń mogących spowodować realne zagrożenie dla zysku finansowego przedsiębiorstwa, a także zaplanowanie zabezpieczeń charakterystycznych dla zaistniałego ryzyka. O skutecznym zarządzaniu ryzykiem można mówić wtedy gdy podejmowane są zdecydowane działania związane z ciągłym monitorowaniem i analizą ryzyk coraz to nowszych zagrożeń i podatności. Będzie miało to na celu zmniejszenie prawdopodobieństwa zaistnienia zagrożenia w przedsiębiorstwie oraz ograniczenie jej skutków. Istotnym czynnikiem podejmując decyzję będzie zarówno zminimalizowanie strat jak również wyprzedzenie przyszłych zdarzeń.

Administrator stosuje procedurę zarządzania ryzykiem opartą o cykl PDCA. Cykl PDCA (inaczej cykl/ koło Deminga, z ang. Plan-Do-Check-Act) to schemat ilustrujący podstawową zasadę ciągłego ulepszania/ doskonalenia. Zakłada następującą kolejność działań:

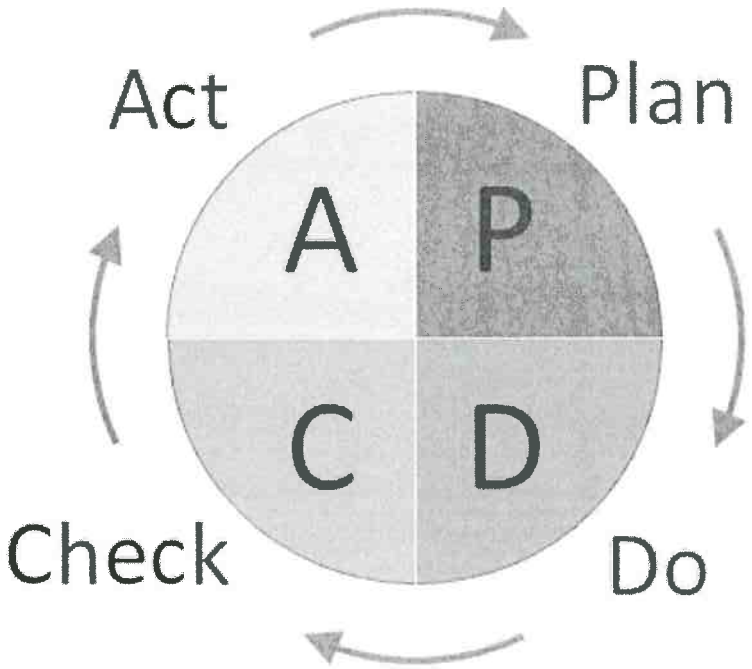
- **P** → PLAN – z j.ang. „planuj" (planuj poprawę swoich działań, najpierw skoncentruj się nad tym co nie funkcjonuje prawidłowo; opracuj pomysły, które mogą ten problem rozwiązać),
- **D** → DO – z j.ang. „wykonaj" (wprowadź zaplanowane zmiany na małą skalę (eksperyment), to pozwoli na późniejsze przetestowanie pomysłu bez wprowadzania zaburzeń w całej organizacji jeżeli pomysł nie będzie dobry),
- **C** → CHECK – z j.ang. „sprawdź" (sprawdź czy wprowadzony eksperyment przyniósł właściwe rezultaty czy nie, sprawdź to dokładnie, czy np. zmiana nie wprowadzi kolejnych

problemów - jeżeli to potrzebne wykonaj testy i walidacje produktu lub procesu zanim stwierdzisz, że zmiana przynosi pozytywny skutek),

- **A** → ACT – z j. ang. „działaj" (wprowadź zmiany na pełną skalę jeżeli eksperyment się udał, podziel się także pomysłem z innymi osobami w organizacji, które mogą na tej zmianie skorzystać i czegoś się nauczyć)

i przedstawiana jest za pomocą koła:

Schemat 1. Cykl *PDCA*



Źródło: http://kdobrowolski.pl/pdca-planuj-wykonuj-sprawdzaj-dzialaj-cykl-deminga-ciagle-doskonalenie/

Analizując pojedynczy cykl takiego koła należy najpierw zaplanować działanie czyli zdefiniować:

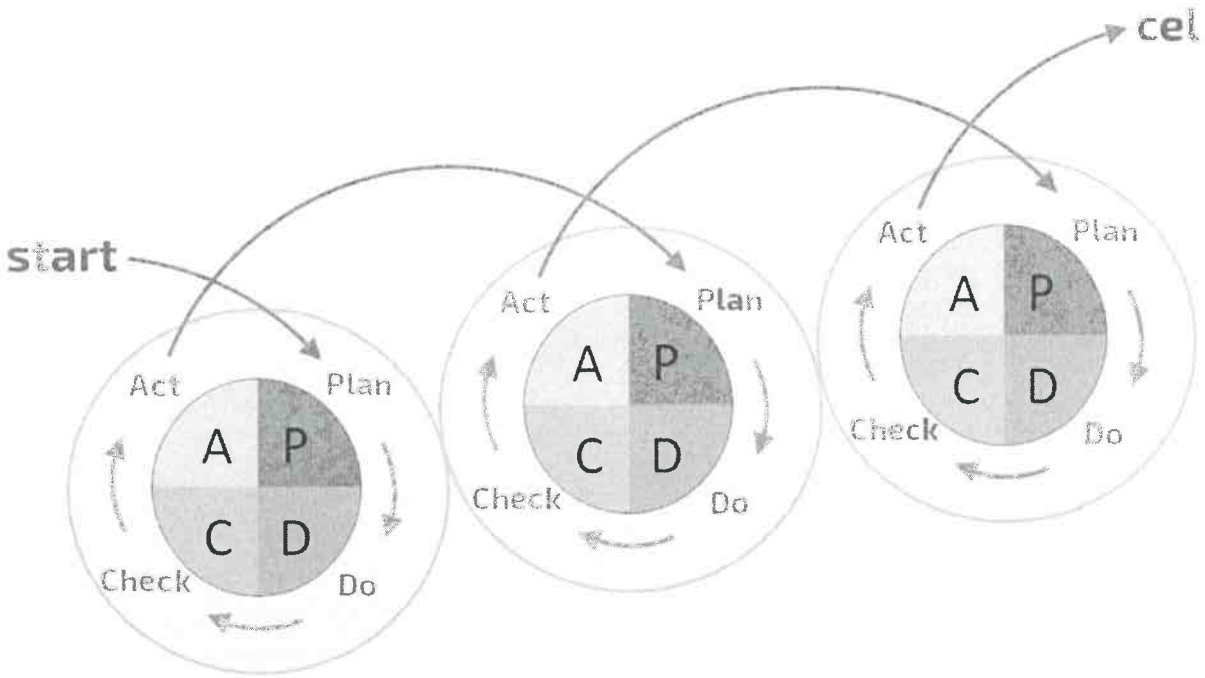
→ co chcemy wykonać – jaki jest cel?
→ co nam do tego będzie potrzebne – jakich zasobów (narzędzi, materiałów) potrzebujemy?
→ kto jest odpowiedzialny za wykonanie danego działania – która konkretnie osoba?
→ jaki termin wyznaczamy na wykonanie zadania – do kiedy (data) konkretnie?

W drugim kroku wykonujemy to, co zaplanowaliśmy. Następnie sprawdzamy, czy osiągnęliśmy zamierzony efekt (mierzymy wartość uzyskaną i porównujemy do oczekiwanej – analizujemy):

→ jeśli tak, to działamy tak, jak coś zostało wdrożone czyli stosujemy nasze rozwiązanie (zamykamy koło PDCA),
→ jeśli nie, to wracamy do planowania i szukamy innego rozwiązania (koło się jeszcze raz „toczy").

Pracy nie powinniśmy kończyć na jednym cyklu. Jeżeli usprawniliśmy naszą metodę pracy wprowadzając dane rozwiązanie, sprawdziliśmy czy działa poprawnie i zaczęliśmy to rozwiązanie stosować na stałe (wprowadzając standard), to możemy zabrać się do jego ulepszania. Uruchamiamy koło PDCA jeszcze raz... i jeszcze raz... i jeszcze raz... Kolejne iteracje (powtarzanie tej samej sekwencji czynności w pętli) prowadzą do celu.

Schemat 2. Cykl *PDCA – ciągłe doskonalenie*



Źródło: http://kdobrowolski.pl/pdca-planuj-wykonuj-sprawdzaj-dzialaj-cykl-deminga-ciagle-doskonalenie/

Po zakończeniu cyklu PDCA możemy rozpocząć kolejny cykl zaczynając od P-Planuj. Jeżeli jednak faza C-Sprawdź wykazała, iż eksperyment nie przyniósł oczekiwanych wyników to należy pominąć etap A-Działaj (bo nie ma sensu na pełną skalę wdrażać złego pomysłu) i przejść do etapu P-Planuj (opracować nowy plan), aby problem rozwiązać.

III. Procedura analizy ryzyka

1. Cel analizy ryzyka

Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Celem procedury jest zapewnienie że:

- proces szacowania ryzyka jest kompletny oraz daje szczegółowe, porównywalne i odtwarzalne rezultaty,
- kryteria oceny ryzyka są ustanowione i spójne z rzeczywistym stanem bezpieczeństwa aktywów oraz dostarczają rzetelnych wyników na temat faktycznego poziomu ryzyka,
- zidentyfikowano potencjalne ryzyko, opisano w kategoriach ilościowych i zarządza się nim świadomie,
- dokumentacja szacowania ryzyka jest poddawana cyklicznym przeglądom oraz jest zatwierdzana przez kompetentny personel.

Głównym celem analizy ryzyka bezpieczeństwa informacji jest wyznaczenie właściwych kierunków działania oraz określenie priorytetów dla zarządzania ryzykami i zabezpieczeniami w jednostce. Wyniki analizy ryzyka prowadzą do opracowania planu postępowania z ryzykiem obejmującego wprowadzenie rozwiązań umożliwiających odpowiednio: unikanie tych ryzyk, ograniczanie ich do akceptowanego poziomu, przeniesienie lub świadomą ich akceptację.

Aby przeprowadzić właściwą analizę ryzyka przetwarzania danych osobowych, należy zidentyfikować zagrożenia i oszacować prawdopodobieństwo ich wystąpienia, które jest związane z procesami przetwarzania danych osobowych realizowanymi w organizacji.

2. Narzędzie do przeprowadzania analizy ryzyka

Administrator analizę ryzyka przeprowadza w oparciu o metodologię jakościową w specjalnym szablonie tj. *Załącznik nr 5 PBDO – Arkusz analizy ryzyka*.

Arkusz analizy ryzyka ma postać tabelaryczną i jest dokumentem sporządzanym w celu rozpoznania i oceny ryzyka oraz jego wyeliminowaniu poprzez wskazane środki. Do elementów arkusza analizy ryzyka należą: aktywa, zagrożenia, prawdopodobieństwo wystąpienia incydentu, skutki wystąpienia incydentu, ryzyko wystąpienia incydentu, zastosowane zabezpieczenia.

Za merytoryczne przygotowanie oraz nadzorowanie, rozpowszechnianie, analizowanie, zatwierdzanie i przechowywanie oryginałów dokumentacji dotyczącej analizy ryzyka odpowiedzialny jest Administrator Danych (ADO). Każdy pracownik zobowiązany jest zgłaszać zaobserwowane lub potencjalne zagrożenie oraz incydenty związane z bezpieczeństwem informacji swojemu bezpośredniemu przełożonemu.

3. Wyznaczenie zbiorów do analizy ryzyka z aktywami

Analizie ryzyka poddawane są zbiory danych osobowych i procesy przetwarzania, dlatego też do analizy wymagane jest zidentyfikowanie aktywów. Aktywa ADO podzielone zostały na 3 główne grupy, tj.:

- → ***dokumentacja tradycyjna***,
- → ***dokumentacja elektroniczna***,
- → ***system informatyczny***.

4. Wyznaczenie zagrożeń

ADO jest odpowiedzialny za określenie listy możliwych zagrożeń, które mogą wystąpić w przetwarzaniu danych w zbiorze lub w procesie przetwarzania. Zagrożenia powinny być identyfikowane w odniesieniu do aktywów. Przy identyfikacji zagrożeń należy przede wszystkim odnieść się do sytuacji, które dotyczą:

- → udostępnienia danych osobom nieupoważnionym – czyli osobom, które nie posiadają nadanego przez ADO lub procesora upoważnienia do przetwarzania danych osobowych,
- → zabrania danych przez osobę nieuprawnioną – przejęcie danych przez osobę nieupoważnioną do przetwarzania danych, w celu ich bezprawnego wykorzystania,
- → przetwarzania danych z naruszeniem prawa – sytuacji naruszenia obowiązków związanych z przetwarzaniem danych określonych w RODO, w szczególności tych, które są zagrożone odpowiedzialnością karną,
- → zmiany, utraty, uszkodzenia lub zniszczenia danych – sytuacji związanych z naruszeniem integralności danych, w tym ich manipulacji, uniemożliwienia odczytu lub zniszczenia zarówno przez osoby upoważnione, jak i osoby nieupoważnione do przetwarzania danych.

Wykaz zidentyfikowanych potencjalnych zagrożeń zawiera zakładka nr 2 Arkuszu analizy ryzyka - Lista potencjalnych zagrożeń.

5. Wyliczenie ryzyka dla zagrożeń

Szacowanie ryzyka związanego z wystąpieniem zagrożeń dla przetwarzania danych osobowych wiąże się z identyfikacją podatności na zagrożenia w procesach przetwarzania danych osobowych. Podatność określa łatwość wyrządzenia szkody dla wskazanego zasobu w kontekście utraty poufności, integralności i dostępności. Identyfikacja podatności ma wskazać, gdzie występują słabe punkty w realizacji działań techniczno-organizacyjnych związanych z ochroną przetwarzanych danych, w tym:

- → brak znajomości przepisów oraz zasad ochrony danych u osób upoważnionych do przetwarzania danych,

- → brak procedur postępowania przy realizacji obowiązków przetwarzania danych (np. przy zbieraniu danych czy ich udostępnianiu innym podmiotom, przy nadawaniu upoważnień do przetwarzania itp.),
- → błędna konfiguracja systemu informatycznego (np. brak indywidualnych identyfikatorów oraz odpowiednich haseł dostępowych, brak odnotowywania identyfikatora osoby, która wprowadza dane czy daty wprowadzenia danych do systemu itp.),
- → brak tworzenia kopii zapasowych z danymi osobowymi,
- → brak redundancji (sprzętowej i osobowej) – zakłócenie dotyczące ciągłości przetwarzania danych.

ADO określa prawdopodobieństwo (P) wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania. Zastosowaną w analizie ryzyka skalę prawdopodobieństwa prezentuje Tabela A.

Tabela A. *Prawdopodobieństwo wystąpienia zagrożenia*

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
brak zagrożenia	0
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

Następnie ADO określa skutki (S) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne. Zastosowaną w analizie ryzyka skalę skutków prezentuje Tabela B.

Tabela B. *Skutki wystąpienia zagrożenia*

SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA (WAGA)
brak skutków	0
małe (do 5000 PLN, incydent prasowy lokalny)	1
średnie (5000-20000 PLN, incydent prasowy ogólnopolski)	2
duże (od 20000 PLN lub naruszenie prawa)	3

W ostatnim kroku ADO wylicza ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły:

$$R = P * S$$

6. Porównanie wyliczonych ryzyk i określenie dalszego postępowania

ADO porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem. Zastosowaną w analizie ryzyka skalę ryzyka prezentuje Tabela C.

Tabela C. *Poziom ryzyka*

POZIOM RYZYKA	WARTOŚĆ [R = P*S]
brak ryzyka	0
ryzyko pomijalne i akceptowalne (akceptacja)	1-2
ryzyko jest opcjonalne (akceptacja lub obniżenie)	3-6
ryzyko jest nieakceptowalne (konieczne obniżenie)	9

Stanowi to początek dla opracowania planu postępowania z ryzykiem. Ryzyka należy podzielić stosownie do ich wielkości i prawdopodobieństwa wystąpienia oraz przyjąć odpowiednią w tym celu strategię postępowania.

7. Reakcja na wartość ryzyka

Jeżeli zabezpieczenia są właściwe i nie ma potrzeby stosowania dodatkowych zabezpieczeń następuje **AKCEPTACJA RYZYKA** - godzimy się z możliwością wystąpienia incydentu, jego skutki są ekonomicznie akceptowalne a koszt wdrożenia zabezpieczeń przewyższa wartość ewentualnych strat. Decyzję o akceptowalnym poziomie ryzyka jak i dopuszczalnego ryzyka szczątkowego podejmuje ADO korzystając z wyników przeprowadzonej analizy ryzyka i uwzględniając monitorowanie incydentów i potencjalne zagrożenia oraz proponowane nowe sposoby zabezpieczeń.

Jeżeli oszacowany poziom ryzyka związanego z danym zagrożeniem okazał się niemożliwy do zaakceptowania konieczne jest podjęcie kroków mających na celu poprawę zastanej sytuacji. Działania obniżające ryzyko, które może zastosować ADO to:

- **REDUKACJA/ MINIMALIZACJA RYZYKA**: zastosowanie zabezpieczeń w celu obniżenia ryzyka (np. zaszyfrowanie pendrivów z danymi wynoszonych poza organizację),
- **UNIKANIE RYZYKA**: unikanie i eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji),
- **PRZENIESIENIE RYZYKA**: przekazanie/ przerzucenie ryzyka na inny podmiot (np. ubezpieczyciel, zewnętrzny dostawca, podwykonawca, outsourcing).

8. Plan postępowania z ryzykiem

Wszędzie, gdzie ADO decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne – zgodnie z *Zakładką - Plan postępowania z ryzykiem*. Plan postępowania z ryzykiem zawiera wykaz zagrożeń do obniżenia z wyszczególnieniem pomocnych temu zabezpieczeń do wdrożenia, osób odpowiedzialnych za ich wdrożenia, przewidywanego terminu wdrożenia oraz oceny wykonania. Wykaz przykładowych zabezpieczeń znajduje się w Zakładce - Lista potencjalnych zabezpieczeń. Ponadto ADO zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

9. Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne). Dokonywanie zmian w ocenie ryzyka odbywa się w wyniku każdorazowego podjęcia działań korygujących i/lub zapobiegawczych, zidentyfikowania nowego - realnego zagrożenia oraz dokonanego incydentu naruszającego bezpieczeństwo informacji.

Zapisy sporządzone w ocenie ryzyka nie ulegają przedawnieniu i są trwałe, w związku z czym każde działanie mające na celu ponowną ocenę ryzyka bezwzględnie dokonuje się w kolejnym cyklu analizy.

Załącznik nr 5	**ARKUSZ ANALIZY RYZYKA**	Nr	
		Wydanie	
		Data wydania:	
		Strona	1 z 1

Rodzaj zagrożeń	R=P*S P - prawdopodobieństwo wystąpienia zagrożenia S - skutki wystąpienia zagrożenia R - poziom ryzyka	DOKUMENTACJA TRADYCYJNA [DT] P	S	R	reakcja na ryzyko	DOKUMENTACJA ELEKTRONICZNA [DE] P	S	R	reakcja na ryzyko	SYSTEM INFORMTYCZNY [SI] P	S	R	reakcja na ryzyko
ATAKI SOCJOTECHNICZNE	phishing	0	0	**0**	brak	1	2	**2**	akceptacja	3	2	**6**	obniżenie
	cybersquatting	0	0	**0**	brak	1	2	**2**	akceptacja	3	2	**6**	obniżenie
	wyłudzanie informacji	0	0	**0**	brak	1	2	**2**	akceptacja	3	2	**6**	obniżenie
	nakłanianie do wykonania czynności	1	3	**3**	akceptacja	2	3	**6**	obniżenie	2	3	**6**	obniżenie
	podrzucanie nośników danych	0	0	**0**	brak	2	3	**6**	obniżenie	2	3	**6**	obniżenie
	ataki telefoniczne	1	1	**1**	akceptacja	0	0	**0**	brak	0	0	**0**	brak
ATAKI NA INFRASTRUKTURĘ	łamanie haseł (słownikowe, siłowe)	0	0	**0**	brak	2	3	**6**	obniżenie	2	3	**6**	obniżenie
	ataki na sprzęt	0	0	**0**	brak	1	2	**2**	akceptacja	0	0	**0**	brak
	ataki na oprogramowanie	0	0	**0**	brak	0	0	**0**	brak	0	0	**0**	brak
	skanowanie sieci i usług	0	0	**0**	brak	0	0	**0**	brak	0	0	**0**	brak
	podsłuchiwanie transmisji (okablowanie, wifi, telefonia, internet)	0	0	**0**	brak	0	0	**0**	brak	2	3	**6**	obniżenie
	ataki man-in-the-middle	0	0	**0**	brak	0	0	**0**	brak	0	0	**0**	brak
	eskalacja uprawnień	0	0	**0**	brak	0	0	**0**	brak	0	0	**0**	brak
	DOS	0	0	**0**	brak	0	0	**0**	brak	0	0	**0**	brak
	DDOS	0	0	**0**	brak	0	0	**0**	brak	0	0	**0**	brak
ZŁOŚLIWE OPROGRAMOWANIE	wirusy / trojany	0	0	**0**	brak	3	2	**6**	obniżenie	3	2	**6**	obniżenie
	backdoory	0	0	**0**	brak	3	2	**6**	obniżenie	3	2	**6**	obniżenie
	keyloggery	0	0	**0**	brak	3	2	**6**	obniżenie	3	2	**6**	obniżenie
	ransomeware	0	0	**0**	brak	3	2	**6**	obniżenie	3	2	**6**	obniżenie
	exploity / exploitpacki	0	0	**0**	brak	3	2	**6**	obniżenie	3	2	**6**	obniżenie
ZAGROŻENIA DLA SPRZĘTU	kradzież / zniszczenie sprzętu	0	0	**0**	brak	2	3	**6**	obniżenie	2	3	**6**	obniżenie
	pożar / eksplozja	0	0	**0**	brak	1	2	**2**	akceptacja	0	0	**0**	brak
	zalanie	0	0	**0**	brak	1	2	**2**	akceptacja	0	0	**0**	brak
	przegrzanie	0	0	**0**	brak	1	2	**2**	akceptacja	0	0	**0**	brak
	awaria zasilania	0	0	**0**	brak	1	2	**2**	akceptacja	0	0	**0**	brak
	awaria sprzętu	0	0	**0**	brak	1	2	**2**	akceptacja	0	0	**0**	brak
ZAGROŻENIA DLA DANYCH	nieuprawniony dostęp	2	2	**4**	akceptacja	1	3	**3**	akceptacja	2	3	**6**	obniżenie
	kradzież tożsamości	1	3	**3**	akceptacja	1	3	**3**	akceptacja	1	3	**3**	akceptacja
	nieuprawniona modyfikacja / usunięcie	1	3	**3**	akceptacja	1	3	**3**	akceptacja	1	3	**3**	akceptacja
	nieuprawnione kopiowanie danych	1	3	**3**	akceptacja	1	3	**3**	akceptacja	1	3	**3**	akceptacja
	kradzież danych lub nośników	1	3	**3**	obniżenie	1	3	**3**	akceptacja	1	3	**3**	akceptacja
	utrata / kradzież danych dostępowych (hasła, klucze, certyfikaty)	0	0	**0**	brak	1	3	**3**	akceptacja	1	3	**3**	akceptacja
	błąd / awaria oprogramowania	0	0	**0**	brak	1	3	**3**	akceptacja	1	3	**3**	akceptacja
	brak / błędy w wykonywaniu kopii bezpieczeństwa	0	0	**0**	brak	1	3	**3**	akceptacja	1	3	**3**	akceptacja
	udostępnienie danych osobom nieupoważnionym	1	3	**3**	akceptacja	2	3	**6**	obniżenie	1	3	**3**	akceptacja
	fałszowanie danych	0	0	**0**	brak	1	3	**3**	akceptacja	1	3	**3**	akceptacja
	nieprawidłowe / brak procedur niszczenia nośników z danymi	0	0	**0**	brak	1	3	**3**	akceptacja	0	0	**0**	brak
	nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	0	0	**0**	brak	2	3	**6**	akceptacja	0	0	**0**	brak
BŁĘDY LUDZKIE	nieprzestrzeganie procedur	2	3	**6**	obniżenie	2	3	**6**	obniżenie	2	3	**6**	obniżenie
	pomyłki	3	2	**6**	obniżenie	3	2	**6**	obniżenie	3	2	**6**	obniżenie
	brak świadomości / wiedzy	2	2	**4**	akceptacja	3	2	**6**	obniżenie	3	2	**6**	obniżenie
	błędy projektowe / konfiguracyjne	0	0	**0**	brak	1	1	**1**	akceptacja	1	1	**1**	akceptacja
ZAGROŻENIA CIĄGŁOŚCI DZIAŁANIA	brak aktualnej dokumentacji	0	0	**0**	brak	0	0	**0**	brak	0	0	**0**	brak
	nieprawidłowe / brak umowy o współpracy	0	0	**0**	brak	0	0	**0**	brak	0	0	**0**	brak
	nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	0	0	**0**	brak	0	0	**0**	brak	1	1	**1**	akceptacja
	upadek firmy outsourcingowej lub dostawczej	0	0	**0**	brak	0	0	**0**	brak	0	0	**0**	brak
	awaria łączy telekomunikacyjnych	0	0	**0**	brak	0	0	**0**	brak	2	2	**4**	akceptacja

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	SKALA
brak zagrożenia	0
zagrożenie niskie	1
zagrożenie średnie	2
zagrożenie wysokie	3

SKUTKI WYSTĄPIENIA ZAGROŻENIA	SKALA
brak skutków	0
małe (do 5000 PLN, incydent prasowy lokalny)	1
średnie (5000-20000 PLN, incydent prasowy ogólnopolski)	2
duże (od 20000 PLN lub naruszenie prawa)	3

POZIOM RYZYKA	R=P*S
brak ryzyka	0
ryzyko pomijalne i akceptowalne (akceptacja)	1-2
ryzyko jest opcjonalne (akceptacja lub obniżenie)	3-6
ryzyko jest nieakceptowalne (konieczne obniżenie)	7-9

REDUKACJA/MINIMALIZACJA RYZYKA - zastosowanie zabezpieczeń w celu obniżenia ryzyka
UNIKANIE RYZYKA - unikanie i eliminacja działań powodujących ryzyko
PRZENIESIENIE RYZYKA - przekazanie/ przerzucenie ryzyka na inny podmiot

Data aktualizacji:
przez:

ZAGROŻENIE	OPIS	RODZAJ ZAGROŻENIA
PHISHING	Mail z prośbą o zalogowanie się do „podróbki" strony, np. bankowej, lub pseudo konta gmail i w rezultacie przejęcie hasła.	Ataki socjotechniczne
CYBERSQUATTING	Zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www. Zamiast logować się do www.mbank.pl logowanie byłoby w www.rnbank.pl	
	Maile od „przełożonych" do księgowego z dyspozycją wykonania przelewu.	
	Faxy, w których intruz podszywa się pod dostawcę i informuje o zmianie numeru konta bankowego.	
	Maile lub rozmowy tel., w których intruz podaje się np. za pracownika firmy dostarczającej oprogramowanie i prosi o hasło w celu „przetestowania uprawnień".	
WYŁUDZANIE INFORMACJI	Maile, które zachęcają lub „zmuszają" do otwarcia załączników lub kliknięcia na hiperilnk, wpisywanie komend.	
PODRZUCONE NOŚNIKI DANYCH	Pen drive pozostawiony w biurze.	
ATAKI TELEFONICZNE	Intruz przedstawia się jako pracownik dostawcy łącza naprawiający usterkę i prosi o uruchomienie określonej strony internetowej.	
	Intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację" lub prosi o udostępnienie pulpitu	
ŁAMANIE I POZYSKIWANIE HASEŁ	Łamanie metodami słownikowymi i siłowymi	Ataki na infrastrukturę
	Ujawnianie haseł	
	Nieprawidłowe przechowywanie (karteczki, pliki)	
	Odgadywanie zbyt słabych, najpopularniejszych haseł	
	Stosowanie domyślnych haseł producenta	
	Stosowanie słownikowych haseł (np. 8 znaków z 3 grup: „Grażynka1")	
	Stosowanie jednego hasła do wielu (często wszystkich) systemów	
ATAKI NA SPRZĘT	Włamania do urządzeń nieaktualizowanych - urządzenia sieciowe (routery, access pointy, firewalle) oraz inne np. macierze, dyski NAS działają dzięki umieszczonemu na nich oprogramowaniu. To oprogramowanie, jak każde inne podlega testom bezpieczeństwa i znajdowane są w nim dziury. Brak aktualizacji tego oprogramowania skutkuje podatnością na włamania, kradzież danych, zakłócanie pracy...	
	Włamania do urządzeń nieodpowiednio skonfigurowanych - błędy konfiguracyjne popełniane przez administratorów mogą ułatwiać hackerom włamanie się do sieci lub urządzenia. Powodem jest najczęściej brak profesjonalnej wiedzy u osób konfigurujących urządzenia. Przykładem może być pozostawienie domyślnych haseł lub dostępu do strony konfiguracyjnej z poziomu Internetu.	
	Włamania z użyciem niezabezpieczonych interfejsów lokalnych - urządzenia takie jak routery, switche, firewalle posiadają często porty konfiguracyjne (USB, Ethernet lub COM - szeregowe), które podłącza się do komputera aby skonfigurować urządzenie. Dostęp do tych portów powinien być odpowiednio zabezpieczonych hasłem, aby przypadkowa osoba, która podłączy do nich swój komputer nie mogła zmienić konfiguracji. Administratorzy często jednak pozostawiają te porty niezabezpieczone.	
	Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze) - urządzenia sieciowe posiadają często włączone wszystkie możliwe usługi sieciowe (DHCP, DNS, SSH, HTTP, telnet, FTP), mimo iż nie wszystkie z nich są potrzebne w danym środowisku. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy. Wyłączenie niepotrzebnych serwisów ogranicza ilość dziur i możliwość przechwycenia / podsłuchania ruchu lub haseł. Włączone powinny być tylko te usługi, które są niezbędne do działania danego środowiska.	
ATAKI NA OPROGRAMOWANIE	Wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu - w każdym oprogramowaniu (przeglądarki, pakiety biurowe, systemy operacyjne, systemy serwerowe...) prędzej czy później znajdowane są błędy pozwalające na przełamania zabezpieczeń i uzyskanie zdalnego dostępu lub zdalne wykonanie kodu. Informacje o tych błędach są upubliczniane po tym, jak producent oprogramowania przygotuje odpowiednią łatę lub aktualizację. Jeżeli nie zainstalujemy tych aktualizacji, narażamy się na ryzyko, że ktoś wykorzysta ogólnodostępne informacje o znanych błędach aby włamać się, wykraść dane, lub w inny sposób nam zaszkodzić (np. nieaktualizowany Windows 7).	
	Włamania z wykorzystaniem luk typu zero day - Zero-day to błędy w oprogramowaniu, o których informacje zostają upublicznione zanim jeszcze autor oprogramowania zdąży wypuścić aktualizację. Często pojawiają się narzędzia umożliwiające wykorzystanie tych błędów (exploity) i przełamanie zabezpieczeń skutkujące włamaniem, kradzieżą danych itp. Innymi słowy - Zero day – podatność sprzętu lub oprogramowania znana wąskiej grupie osób i pozwalająca na przełamanie zabezpieczeń, na którą producent nie dostarczył jeszcze odpowiedniej aktualizacji.	
	Włamania z wykorzystaniem domyślnych haseł - włamania będące wynikiem tego, że administrator po uruchomieniu oprogramowania lub urządzenia nie zmienił domyślnego hasła. Intruz, któremu uda się rozpoznać model urządzenia w pierwszej kolejności próbuje się do niego zalogować hasłem podanym w instrukcji obsługi przez producenta. Często się to niestety udaje.	
	Włamania z wykorzystaniem najczęstszych błędów - programiści pisząc oprogramowanie często popełniają te same znane błędy. Istnieje zestawienie takich błędów, np. dla aplikacji webowych - OWASP TOP 10. Wiele programów i stron internetowych pada ofiarą ataków właśnie za pośrednictwem tych najczęstszych błędów.	
	Włamania z wykorzystaniem API (interfejsów programistycznych) - niektóre aplikacje, systemy ale też serwisy internetowe (np. Allegro) posiadają specjalne interfejsy, dzięki którym programiści używając odpowiednich bibliotek mogą odwoływać się do nich z poziomu oprogramowania, Możliwe jest np. wystawienie aukcji na allegro bez konieczności logowania się na swoje konto przeglądarką internetową. Błędy w tych bibliotekach powodowały często, że programista mógł np. uzyskać szerszy dostęp do bazy danych i wyciągnąć dane wszystkich klientów.	

	Namierzanie wersji testowych (np. strona www) - niektóre portale lub aplikacje webowe posiadają swoje kopie utrzymywane do celów testowych lub rozwojowych. Programiści zamieszczają na nich zmiany w kodzie zanim trafią one na główne serwery. Strony te są często gorzej zabezpieczone i łatwiej jest się do nich włamać, a mogą zawierać również krytyczne dane. Często udaje się je namierzyć wpisując np. zamiast adresu www.strona.pl adres test.strona.pl .	
SKANOWANIE SIECI I USŁUG	Atakujący poznaje wersję systemu operacyjnego lub wersję serwera www a przez to potem może dobrać skuteczny atak.	
PODSŁUCHIWANIE TRANSMISJI (okablowanie, wifi, telefonia, internet)	Łatwo dostępne gniazdka sieciowe, gdzie atakujący może się podłączyć np. z własnym urządzeniem i za jego pomocą podsłuchiwać naszą sieć (możliwość podpięcia się pod drukarkę na korytarzu lub do gniazdka w salce konferencyjnej).	
ATAKI MAN-IN-THE-MIDDLE	Przejęcie komputera w firmie w celu podsłuchiwania w sieci firmowej (w rezultacie możliwość podsłuchu haseł).	
ESKALACJA UPRAWNIEŃ	Zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych.	
	Przejęcie uprawnień użytkownika zaawansowanego.	
	Przejęcie uprawnień administratora.	
	Przejęcie uprawnień systemowych.	
	Przejęcie innych poświadczeń (certyfikaty elektroniczne, pliki cookies z identyfikatorami sesji).	
DOS	Zmasowany atak pojedynczego atakującego na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować".	
DDOS	Zmasowany atak komputerów-zombie na zlecenie atakującego na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować".	
WIRUSY I TROJANY	Trojany – instalują się często z nielegalnym oprogramowaniem. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika.	Złośliwe oprogramowanie
BACKDOORY	Instalują się z maili lub z linków w mailach. Po uruchomieniu umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad komputerem. Taki komputer-zombie może być użyty do wszelkich zachcianek intruza.	
KEYLOGGERY	Programy przechwytujące hasła wpisywane na klawiaturze przez użytkownika i oddające je intruzowi.	
RANSOMEWARE	Program do szyfrowania plików. Odszyfrowanie wymaga zapłaty 500 USD. Bardzo groźny.	
EXPLOITY/ EXPLOITPAKI	Oprogramowanie wykorzystujące znane luki w systemach. Uruchomiony pozwala na przejęcie systemu przez intruza.	
WŁAMANIE DO OBIEKTÓW	Może skutkować zainstalowaniem nieautoryzowanych urządzeń, np. keyloggerów, podsłuchów.	Zagrożenia dla sprzętu
KRADZIEŻ/ ZNISZCZENIE SPRZĘTU	Kradzież komputerów w organizacji i laptopów poza nią, uszkodzenie sprzętu na skutek przepięcia czy upadku.	
POŻAR/ EKSPLOZJA	Pożar serwerowni, wybuch gazów technicznych.	
ZALANIE	Powódź, pęknięta rura kanalizacyjna, zalanie kawą.	
PRZEGRZANIE	Wysoka temperatura w serwerowni.	
AWARIA ZASILANIA	Skoki napięcia, przerwy w dostawie.	
AWARIA SPRZĘTU	Awaria dysków, modułów, płyty głównej, sterowników, routerów.	
NIEUPRAWNIONY DOSTĘP	Nadane zbyt wysokie uprawnienia użytkownikom lub brak kontroli nad dostępem do plików, baz, komputerów.	Zagrożenia dla danych
KRADZIEŻ TOŻSAMOŚCI	Przejęcie poczty, np. gmailowej, pozyskanie danych z dowodu osobistego i w rezultacie np. założenie firmy „słupa", wzięcie kredytu, zakup na allegro na cudze konto.	
NIEUPRAWNIONA MODYFIKACJA/ USUNIĘCIE	Może mieć również charakter niezamierzony lub być efektem pomyłki.	
	Sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji.	
NIEUPRAWNIONE KOPIOWANIE DANYCH	Kopiowanie danych z katalogów, dysków, baz, programów, kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą.	
KRADZIEŻ DANYCH LUB NOŚNIKÓW	Na zewnątrz i wewnątrz organizacji.	
UTRATA/ KRADZIEŻ DANYCH DOSTĘPOWYCH	Utrata/ kradzież haseł, kluczy, certyfikatów.	
BŁĄD/ AWARIA OPROGRAMOWANIA	Uszkodzenie bazy danych, programu kadrowo-płacowego.	
BRAK/ BŁĘDY W WYKONYWANIU KOPII BEZPIECZEŃSTWA	Doraźne lub za rzadkie wykonywanie kopii, błędy podczas procesu wykonywania kopii, kopie dostępne w sieci bez zabezpieczeń.	
UDOSTEPNIANIE DANYCH OSOBOM NIEUPOWAŻNIONYM	Upublicznienie danych w przestrzeni publicznej, dostęp przez internet, przesłanie lub wydawanie informacji osobie nieupoważnionej, wyrzucanie na śmietnik, wynoszenie na wolne powietrze.	
NIEPRAWIDŁOWE/ BRAK PROCEDUR NISZCZENIA NOSNIKÓW Z DANYMI	Wyrzucenie uszkodzonych nośników bez ich zniszczenia, wyrzucenie niezniszczonych pendrive, CD, DVD.	
NIEPRAWIDŁOWE/ BRAK PROCEDUR NAPRAWY W SERWISACH ZEWNĘTRZNYCH	Naprawa sprzętu z nośnikami w serwisie bez standardu bezpiecznej naprawy i bez umowy bezpieczeństwa.	
NIEPRZESTRZEGANIE PROCEDUR	Świadome naruszenie pisemnych lub ustnych procedur, np. niewylogowywanie się z systemu, przekazywanie haseł koledze.	Błędy ludzkie
POMYŁKI ADMINISTRATORÓW, UŻYTKOWNIKÓW	Pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia.	
BRAK ŚWIADOMOŚCI/ WIEDZY	Braki w inteligencji, nieprzeszkolony personel.	
BŁĘDY PROJEKTOWE/ KONFIGURACYJNE	Błędy programistów prowadzące do niewłaściwego przetwarzania danych, niezabezpieczenie danych w bazie www przed indeksacją robotów google.	
BRAK AKTUALNEJ DOKUMENTACJI	Brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania utrudnia przywracanie środowiska i zarządzanie nim gdy np. odejdzie pracownik IT.	
NIEPRAWIDŁOWE/ BRAK UMOWY O WSPÓŁPRACY	Brak odpowiedzialności stwarza ryzyko braku staranności.	

NIEPRAWIDŁOWE/ BRAK UMOWY GWARANCYJNEJ LUB WSPARCIA SERWISOWEGO	Umowy wymagają przedłużania, czas reakcji nie oznacza czasu naprawy.	**Zagrożenia ciągłości działania**
UPADEK FIRMY OUTSOURCINGOWEJ LUB DOSTAWCZEJ	Ryzyko braku zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji.	
AWARIA ŁĄCZY TELEKOMUNIKACYJNYCH	Krytyczna w przypadku usług chmurowych oraz platform SaaS.	

Załącznik nr 5	**LISTA POTENCJALNYCH ZABEZPIECZEŃ**	Nr	
		Wydanie	01
		Data wydania:	
		Strona	1 z 2

ZABEZPIECZENIE	OPIS	RODZAJ ZABEZPIECZENIA
Regulamin ODO dla pracowników i współpracowników	Zabezpieczenia: Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy, Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych i podpisują stosowne Oświadczenie poufności	Zabezpieczenia organizacyjne
Szkolenia personelu	Zabezpieczenia: Szkolenia wewnętrzne, elearning	
Audyty	Procedury: Procedura audytu	
Testy penetracyjne	Zabezpieczenia: testy penetracyjne	
Procedury przywracania w razie incydentu	Procedury: Plan ciągłości działania	
Polityka kluczy / polityka kontroli dostępu	Procedury: Polityka kluczy, Polityka kontroli dostępu, Zabezpieczenia: kontrola kluczy zapasowych, zakaz wstępu osobom nieupoważnionym, kontrola wydawania kluczy, kontrola składowania kluczy	Zabezpieczenia fizyczne
Dostęp do pomieszczeń i sprzętu	Zabezpieczenia: ograniczenie dostępu do pomieszczeń, komputerów, drukarek, xero osobom nieupoważnionym, chyba że w obecności osoby upoważnionej	
Zabezpieczenie dostępu do pomieszczeń (w tym biurowych)	Zabezpieczenia: drzwi zamykane na klucz, drzwi ognioodporne, drzwi antywłamaniowe, drzwi zamykane siłownikami	
Zabezpieczenie dostępu do serwerowni	Zabezpieczenia: drzwi zamykane na klucz, wejście kodowane, czytnik biometryczny	
Zabezpieczenie dostępu do archiwum	Zabezpieczenia: drzwi zamykane na klucz	
Zabezpieczenie dokumentacji w pomieszczeniach	Zabezpieczenia: zamknięte niemetalowe szafy, zamknięte metalowe szafy, sejf, sejf ogniotrwały, skrytki na klucze	
Systemy alarmowe / zabezpieczenia antywłamaniowe	Zabezpieczenia: system alarmowy, kraty, rolety	
Ochrona fizyczna obiektu / pomieszczeń	Zabezpieczenia: ochrona własna, firma ochroniarska	
Strefy dostępu	Zabezpieczenia: Organizacja stref ograniczonego dostępu	
System kontroli dostępu	Zabezpieczenia: System kart wejściowych, system biometryczny, portiernia	Zabezpieczenia techniczne
System ppoż	Zabezpieczenia: system w obiekcie, system gaszenia serwerowni, gaśnice	
Mnitoring środowiskowy	Zabezpieczenia: w archiwum - czujniki wilgotności, w serwerowni - czujnik temperaturowy, powiadamianie mailem o alertach	
Klimatyzacja	Zabezpieczenia: klimatyzacja w serwerowni	
Monitoring wizyjny	Zabezpieczenia: monitoring wizyjny w obrębie obiektu i otoczeniu	
Systemy UPS / agregaty prądotwórcze	Zabezpieczenia: Zastosowano UPS podtrzymujący zasilanie serwera, UPS na kluczowych elementów systemu IT	
Systemy antywirusowy i antyspamowy	Zabezpieczenia: wersja stanowiskowa, serwerowa, licencjonowany, aktualizowany online, skanowanie poczty, skanowanie portów USB, wersja na komputery, smartfony, tablety	
Sewery proxy i bramki filtrujące	Zabezpieczenia: skan niebezpiecznej zawartości, blokada ruchu na podstawie bazy reputacji, blokada dostępu do określonych stron	
Systemy firewall, NG firewall, UTM	Zabezpieczenia: Firewall / NG Firewall / UTM do ochrony dostępu do sieci komputerowej, firewall sprzętowy, firewall programowy	
Sondy IDS / IPS	Zabezpieczenia: system IDS/IPS do ochrony dostępu do sieci komputerowej	
Monitorowanie zużycia	Zabezpieczenia: Systemy monitorujące stan usług i zasobów krytycznych, serwerów, baz danych i urządzeń sieciowych	
SIEM - Security Information and Event Managment	Zabezpieczenia: Analityczny system do wykrywania zagrożeń	
Skanery podatności	Zabezpieczenia: System wykrywania słabości i zagrożeń	
Systemy do inwentaryzacji	Zabezpieczenia: System do inwentaryzacji sprzętu, zarządzania licencjami, monitoring użytkowników, kontrola smartfonów	
Szyfrowanie	Zabezpieczenia: Szyfrowanie poczty (SSL), szyfrowanie połączeń internetowych SSL/VPN, szyfrowanie Pendrive, szyfrowanie dysków komputerów przenośnych (bitlocker), szyfrowanie plików (7zip), szyfrowanie baz danych, szyfrowanie sieci WIFI	

Hardening	Włączenie szyfrowania, Zmiana domyślnych haseł, Wyłączenie niepotrzebnych funkcji i usług, Bazuje na dobrych praktykach lub standardach , dodatki noscript i adblocker do przeglądarek	Zabezpieczenia informatyczne
Redundancja krytycznych zasobów	Zabezpieczenia: macierz dyskowa RAID 3, redundancja łącz	
Aktualizacje systemu	Zabezpieczenia: zarządzanie aktualizacjami systemu operacyjnego, aplikacji, przeglądarek internetowych	
Backupy i archiwizacja	Procedury: Procedura tworzenia kopii zapasowych, Zabezpieczenia: Backup serwerów, aplikacji, plików, konfiguracji, licencji, haseł, zabezpieczenie przed ransomeware, kopie poza serwerownią, niszczenie/czyszczenie nośników przed utylizacją	
Rozliczalnosć operacji	Zabezpieczenie: program / aplikacja posiada mechanizm odnotowywania wykonywania operacji na danych osobowych. Odnotowane i logowane są: tworzenie rekordu, zmiana, usunięcie, wgląd w dane, użytkownik dokonujący zmian, każdy użytkownik posiada swój indywidualny login	
Postępowanie z nośnikami	Procedury: Procedura postępowania z nośnikami i sprzętem poza organizacją, Regulamin korzystania z komputerów przenośnych, Zabezpieczenia: ograniczono możliwość kopiowania danych na pendrive, zastosowano blokadę portów USB do korzystania z pendrive, wymuszono użycie szyfrowanych firmowych pendirve	
Zabezpieczenie pracy użytkowników	Procedury: Procedura korzystania z internetu, Procedura korzystania z poczty elektronicznej, Zabezpieczenia: zahasłowane wygaszacze ekranu aktywowane w przypadku nieaktywności użytkownika, poufne ustawienie monitorów, filtry polaryzacyjne, terminacja sesji	
Wirtualizacja	Zabezpieczenia: wirtualizacja	
Niszczenie nośników	Procedury: Procedura niszczenia nośników, Zabezpieczenia: niszczarki paskowe, niszczarki o podwyższonym standardzie, niszczenie/czyszczenie nośników przed utylizacją, firma niszcząca dokumenty	
Zarządzanie uprawnieniami	Procedury: Procedura zarządzania uprawnieniami, Zabezpieczenia: minimalizacja uprawnień, separacja obowiązków, zarządzanie uprawnieniami, konta firmowe + prywatne	
Uwierzytelnianie	Procedury: Polityka haseł, Zabezpieczenia: długość hasła, częstotliwość zmiany, wymuszenie zmiany, uwierzytelnianie za pomocą kodu PIN, uwierzytelnianie biometryczne, hasło na BIOS. Uwierzytelnianie do aplikacji, stacji roboczej, smartfona, dysku sieciowego, sieci, poczty,	
Umowy serwisowe	Procedury: Umowy powierzenia, SLA, kary umowne	Zabezpieczenia zewnętrzne
Procedury napraw w serwisach zewnętrznych	Procedury: Procedury napraw w serwisach zewnętrznych	
Outsourcing	Zabezpieczenia: korzystanie z ISP, hostingu, cloud	

Załącznik nr 5	PLAN POSTĘPOWANIA Z RYZYKIEM	Nr załącznika	
		Wydanie	01
		Data wydania:	
		Strona	1 z 1

Zagrożenie do obniżenia		Grupa aktywów	Poziom ryzyka	Zabezpieczenie do wdrożenia	Przewidywany termin wdrożenia	Osoba odpowiedzialna	Data wdrożenia	Ocena wykonania
ATAKI SOCJOTECHNICZNE	phishing	SI	6	szkolenia personelu,	31.12.2018			
	cybersquatting	SI	6	szkolenia personelu,	31.12.2018			
	wyłudzanie informacji	SI	6	szkolenia personelu,	31.12.2018			
	nakłanianie do wykonania czynności	DE	6	szkolenia personelu,				
		SI	6	szkolenia personelu,				
	podrzucanie nośników danych	DE	6	szkolenia personelu,	31.12.2018			
		SI	6	szkolenia personelu,				
	ataki telefoniczne	-	-	-	-	-	-	-
ATAKI NA INFRASTRUKTURĘ	łamanie haseł (słownikowe, siłowe)	DE	6	szkolenia personelu z zakresu tworzenia, przechowywania i zmiany haseł,	31.12.2018			
		SI	6	szkolenia personelu z zakresu tworzenia, przechowywania i zmiany haseł,	31.12.2018			
	ataki na sprzęt	-	-	-	-	-	-	-
	skanowanie sieci i usług	-	-	-	-		-	-
	podsłuchiwanie transmisji (okablowanie, wifi, telefonia, internet)	SI	6	zabezpieczenie dostępu do pomieszczeń i infrastruktury informatycznej	31.12.2018			
	ataki man-in-the-middle	-	-	-	-	-	-	-
	eskalacja uprawnień	-	-	-	-	-	-	-
	DOS	-	-	-	-	-	-	-
	DDOS	-	-	-	-	-	-	-
ZŁOŚLIWE OPROGRAMOWANIE	wirusy / trojany	DE	6	szkolenia personelu, aktualizacja zabezpieczeń informatycznych	31.12.2018			
		SI	6					
	backdoory	DE	6					
		SI	6					
	keyloggery	DE	6					
		SI	6					
	ransomeware	DE	6					
		SI	6					
	exploity / exploitpacki	DE	6					
		SI	6					
ZAGROŻENIA DLA SPRZĘTU	kradzież / zniszczenie sprzętu	DE	6	zabezpieczenie dostępu do pomieszczeń	31.12.2018			
		SI	6					
		AW	6					
	pożar / eksplozja	-	-	-	-		-	-
	zalanie	-	-	-	-		-	-
	przegrzanie	-	-	-	-		-	-
	awaria zasilania	-	-	-	-		-	-
	awaria sprzętu	-	-	-	-		-	-
ZAGROŻENIA DLA DANYCH	nieuprawniony dostęp	SI	6	szkolenie personelu, silne hasła, zmiany hasła				
	kradzież tożsamości	-	-	-	-		-	-
	nieuprawniona modyfikacja / usunięcie	-	-	-	-		-	-
	nieuprawnione kopiowanie danych	-	-	-	-	-	-	-
	kradzież danych lub nośników	-	-	-	-	-	-	-
	utrata / kradzież danych dostępowych (hasła, klucze, certyfikaty)	-	-	-	-		-	-
	błąd / awaria oprogramowania	-	-	-	-		-	-
	brak / błędy w wykonywaniu kopii bezpieczeństwa	-	-	-	-		-	-
	udostępnienie danych osobom nieupoważnionym	DE	6	zabezpieczenie dokumentacji w pomieszczeniach (szafy zamykane na klucz), szkolenia personelu, stały monitoring wydanych upoważnień	31.12.2018			
	fałszowanie danych	DT	6					
		DE	6					
	nieprawidłowe / brak procedur niszczenia nośników z danymi	-	-	-	-		-	-
	nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	-	-	-	-		-	-
BŁĘDY LUDZKIE	nieprzestrzeganie procedur	DT	6	szkolenia personelu	31.12.2018			
		DE	6					
		SI	6					
	pomyłki	DT	6	szkolenia personelu	31.12.2018			
		DE	6					
		SI	6					
	brak świadomości / wiedzy	DE	6	szkolenia personelu	31.12.2018			
		SI	6					
	błędy projektowe / konfiguracyjne	-	-	-	-		-	-
ZAGROŻENIA CIĄGŁOŚCI DZIAŁANIA	brak aktualnej dokumentacji	-	-	-	-		-	-
	nieprawidłowe / brak umowy o współpracy	-	-	-	-		-	-
	nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	-	-	-	-		-	-
	upadek firmy outsourcingowej lub dostawczej	-	-	-	-		-	-
	awaria łączy telekomunikacyjnych	DE	6	outsourcing	31.12.2018			
		SI	6					

Zaktualizowano dnia: przez

Protokół zdawczo-odbiorczy

Dnia ..... roku w siedzibie firmy

Potwierdza się, że przekazano:

1. Klucze do biura:

   ☐ 1 komplet

2. Telefon komórkowy wraz z kartą SIM - .....
3. Komputer przenośny .....

Osoba zdająca: .....

Osoba odbierająca: ..... - pracownik

zdający odbierający

data i podpis data i podpis

UWAGA

Zasady użytkowania kluczy:

Samowolne dorabianie dodatkowych kluczy do pomieszczeń firmy jest zabronione. W przypadku uzasadnionej konieczności dorobienia dodatkowego klucza do pomieszczenia czynności tej dokonuje wyznaczony pracownik na wyraźne polecenie przełożonego.

W przypadku utraty klucza, fakt ten należy niezwłocznie zgłosić przełożonemu (zgłoszenie incydentu).

Zasady użytkowania komputerów przenośnych:

1. Komputer może być wykorzystywany tylko do celów służbowych.
2. Dodatkowe oprogramowanie może być instalowane tylko za pisemną zgodą Administratora
3. Zabrania się dokonywania samodzielnych napraw i zmian w konfiguracji komputera.
4. Przynajmniej raz w tygodniu należy aktualizować zainstalowane oprogramowanie antywirusowe.
5. W czasie pracy komputer powinien mieć zapewniony dopływ powietrza do otworów wentylacyjnych znajdujących się pod spodem i wokół obudowy (najlepsze jest płaskie twarde podłoże).
6. Trzymać urządzenie z dala od źródeł wysokich temperatur (grzejniki, bezpośrednie nasłonecznienie).
7. Unikać mocnych wstrząśnień notebooka.
8. Chronić komputer przed zalaniem.
9. Do czyszczenia używać tylko miękkich szmatek i środków przeznaczonych do tego typu urządzeń.
10. W przypadku uszkodzenia komputera lub awarii systemu może nastąpić utrata przechowywanych na dysku plików. W związku z tym należy okresowo wykonywać kopie dokumentów na dysku sieciowym.

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH (PDO)

NUMER UPOWAŻNIENIA: .....

Na podstawie art. 29 oraz art. 32 ust. 4 RODO upoważniam Panią / Pana ..... do przetwarzania danych osobowych w Urzędzie Gminy w Golubiu-Dobrzyniu w okresie od ..... do.....:

w zakresie:

- pobierania opłat za gospodarowanie odpadami komunalnymi TAK/NIE*
- pobieranie podatków i opłat lokalnych TAK/NIE*

**niepotrzebne skreślić*

ZATWIERDZAM UPOWAŻNIENIE:	ODBIERAM UPOWAŻNIENIE:
.....	.....
Data i Podpis AD	Data i Podpis AD

ZOBOWIĄZANIE OSOBY UPOWAŻNIONEJ

Oświadczam, że znane mi są przepisy dotyczące przetwarzania i ochrony danych osobowych, w szczególności: ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w zakresie niezbędnym do wykonywania czynności służbowych.
Ustawa o ochronie danych osobowych z dnia 10 maja 2018 roku (Dz.U. z 2018 r. poz. 1000)

Zobowiązuje się do zachowania w tajemnicy przetwarzanych danych osobowych i sposobów ich zabezpieczeń, również po ustaniu stosunku pracy/ zakończeniu pełnienia funkcji.

.....
Data i czytelny Podpis osoby upoważnionej