ANALIZA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI SYSTEMÓW INFORMATYCZNYCH POD KĄTEM ZAGROŻEŃ I RYZYKA

zwana dalej:

ANALIZĄ ZAGROŻEŃ I RYZYKA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

§ 1

Administrator Danych ze względu na ciążące na nim obowiązki wynikające z ustawy o ochronie danych osobowych, a dokładnie art. 32 rozporządzenie parlamentu europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 4 maja 2016 r.) tej ustawy, zobowiązany jest do zastosowania środków technicznych i organizacyjnych, które mają zapewnić ochronę przetwarzanych danych osobowych, w świetle adekwatnych zagrożeń, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

§ 2

W związku z § 1 niniejszego dokumentu Administrator Danych wprowadza dokument „Analiza zagrożeń i ryzyka" w podmiocie o nazwie: **Urząd Gminy i Miasta Gryfów Śląski** w celu badania i obserwowania istniejącego środowiska przetwarzania danych osobowych.

Ilekroć w „Analizie zagrożeń i ryzyka przy przetwarzaniu danych osobowych” jest mowa o:

1. **ANALIZIE RYZYKA** – systematyczne wykorzystanie informacji do zidentyfikowania źródeł i oszacowania ryzyka;
2. **SZACOWANIU RYZYKA** – proces oceny i analizy ryzyka;
3. **OCENIE RYZYKA** – proces porównania oszacowanego ryzyka z określonymi kryteriami w celu określenia znaczenia ryzyka;
4. **POSTĘPOWANIU Z RYZYKIEM** – wdrażanie środków modyfikujących ryzyko;
5. **ZARZĄDZANIU RYZYKIEM** – działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka;
6. **RYZYKU SZCZĄTKOWYM** – ryzyko pozostające po procesie postępowania z ryzykiem;
7. **AKCEPTOWANIU RYZYKA** – decyzja, aby zaakceptować ryzyko;
8. **BEZPIECZEŃSTWIE INFORMACJI** – zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;
9. **ZDARZENIU ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – zdarzenie związane z bezpieczeństwem informacji, jako określonym stanem systemu, usługi lub sieci, który wskazuje na możliwe naruszenie Polityki Ochrony Danych, błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem;
10. **INCYDENCIE ZWIĄZANYM Z BEZPIECZEŃSTWEM INFORMACJI** – jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne zakłócenia zadań biznesowych i zagrażają bezpieczeństwu informacji;
11. **AKTYWACH** – wszystko, co ma wartość dla organizacji;
12. **ZAGROŻENIACH SYSTEMU** – to wszystkie niekorzystne czynniki mogące przyczynić się w trakcie pracy z danymi osobowymi do wystąpienia incydentu, mogącego mieć wpływ na ich ujawnienie bądź utratę;
13. **DOSTĘPNOŚCI** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego jest możliwy do wykorzystania na żądanie, w określonym czasie, przez podmiot uprawniony do pracy w systemie teleinformatycznym;
14. **INCYDENCIE BEZPIECZEŃSTWA TELEINFORMATYCZNEGO** — należy przez to rozumieć takie pojedyncze zdarzenie lub serię zdarzeń, związanych z bezpieczeństwem informacji niejawnych, które zagrażają ich poufności, dostępności lub integralności;
15. **INFORMATYCZNYM NOŚNIKU DANYCH** — należy przez to rozumieć materiał służący do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej;
16. **INTEGRALNOŚCI** — należy przez to rozumieć właściwość określającą, że zasób systemu teleinformatycznego nie został zmodyfikowany w sposób nieuprawniony;
17. **OPROGRAMOWANIU ZŁOŚLIWYM** — należy przez to rozumieć oprogramowanie, którego celem jest przeprowadzenie nieuprawnionych lub szkodliwych działań w systemie teleinformatycznym;
18. **PODATNOŚCI** — należy przez to rozumieć słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie;
19. **POŁĄCZENIU MIĘDZYSYSTEMOWYM** — należy przez to rozumieć techniczne albo organizacyjne połączenie dwóch lub więcej systemów teleinformatycznych, umożliwiające ich współpracę, a w szczególności wymianę danych;
20. **POUFNOŚCI** — należy przez to rozumieć właściwość określającą, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;
21. **PRZEKAZYWANIU INFORMACJI** — należy przez to rozumieć zarówno transmisję informacji, jak i przekazywanie informacji na informatycznych nośnikach danych, na których zostały utrwalone;
22. **TESTACH BEZPIECZEŃSTWA** — należy przez to rozumieć testy poprawności i skuteczności funkcjonowania zabezpieczeń w systemie teleinformatycznym;

23. **ZABEZPIECZENIU** — należy przez to rozumieć środki o charakterze fizycznym, technicznym lub organizacyjnym zmniejszające ryzyko;
24. **ZAGROŻENIU** — należy przez to rozumieć potencjalną przyczynę niepożądanego zdarzenia, które może wywołać szkodę w zasobach systemu teleinformatycznego;
25. **ZASOBACH SYSTEMU TELEINFORMATYCZNEGO** – należy przez to rozumieć informacje przetwarzane w systemie teleinformatycznym, jak również osoby, usługi, oprogramowanie, dane i sprzęt oraz inne elementy mające wpływ na bezpieczeństwo tych informacji;

§ 4

Skuteczność zastosowanych środków powinna podlegać cyklicznym badaniom. Przy stosowaniu zabezpieczeń powinno się też uwzględniać zmieniające się warunki oraz postęp techniczny (informatyczny), co może powodować konieczność zmiany czy modernizowania wprowadzonych wcześniej przez Administratora Danych systemów ochrony. Analiza zagrożeń i ryzyka, określa środki zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

§ 5

Wymogi ogólne bezpieczeństwa przetwarzanych danych osobowych, wprowadzone przez Administratora Danych określa załącznik nr 1.

§ 6

Możliwe zagrożenia występujące w systemach informatycznych, określa załącznik nr 2.

§ 7

Podatność systemu na zagrożenia, określa załącznik nr 3.

§ 8

Analizę zagrożeń i ryzyka, określa załącznik nr 4.

§ 9

Wnioski i działania naprawcze, określa załącznik nr 5.

§ 10

Wzór klauzuli poufności, określa załącznik nr 6.

§ 11

Przebieg przykładowej kontroli podatności systemu, określa załącznik nr 7.

§ 12

Rekomendacja odpowiedniej postawy upoważnionego do przetwarzania danych osobowych, określa załącznik nr 8.

§ 13

Tabela szacowania ryzyka została określona w załączniku nr 9.

.....

(Podpis Administratora Danych Osobowych)

WYMOGI OGÓLNE BEZPIECZEŃSTWA PRZETWARZANYCH DANYCH OSOBOWYCH, WPROWADZONE PRZEZ ADMINISTRATORA DANYCH W:

Urząd Gminy i Miasta Gryfów Śląski, Administrator Danych Osobowych – Burmistrz Gminy i Miasta Gryfów Śląski

§ 1

W czasie przetwarzania danych osobowych informacje mogą występować w postaci:

1. plików lub informacji przechowywanych na dysku twardym komputera;
2. plików lub informacji zapisanych na nośnikach komputerowych;
3. wersji roboczych lub gotowych dokumentów wydrukowanych na papierze.

§ 2

Bezpieczeństwo przetwarzanych lub przechowywanych informacji zawierające dane osobowe wymaga:

1. zapewnienia ochrony fizycznej pomieszczeń, stanowiska, jak i infrastruktury komputerowej przed nieuprawnionym dostępem;
2. ochrony nośników technicznych i wydruków dokumentów wytwarzanych przy pomocy sprzętu komputerowego, w tym określenia zasad postępowania z nimi przed nieuprawnionym dostępem;
3. zabezpieczenia przed nieupoważnionym dostępem do danych osobowych znajdujących się w zasobach systemu informatycznego;
4. zapewnienia dostępności do danych osobowych znajdujących się na technicznych nośnikach informacji oraz w pamięci systemu informatycznego dla upoważnionych użytkowników;
5. zapewnienia możliwości kontroli dostępu do zasobów systemu informatycznego oraz wykonywanych na nim czynności;
6. zapewnienia możliwości kontroli nośników, na których przetwarzano lub przechowywano dane osobowe.

.....

(Podpis Administratora Danych Osobowych)

ZAGROŻENIA ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH

§ 1

W myśl ustawy o ochronie danych osobowych, każdy Administrator Danych Osobowych powinien zapewnić takie warunki pracy w systemie, aby cechował się on poufnością, integralnością i rozliczalnością.

§ 2

Każde zauważone zagrożenie związane z poufnością, integralnością lub rozliczalnością, powinno być niezwłocznie zgłoszone Administratorowi Danych Osobowych bądź wyznaczonemu Inspektorowi Ochrony Danych.

§ 3

1. Poufność, to zapewnienie danym osobowym niemożności ich udostępniania nieupoważnionym osobom czy podmiotom.
2. Zapewnienie poufności danych osobowych wynika z obowiązku wypełnienia nakładanych na Administratora Danych Osobowych zadań, wynikających z ustaw, wraz z wszelkimi konsekwencjami organizacyjnymi i prawnymi.
3. Strategiczną częścią zabezpieczania danych osobowych przed utratą poufności jest odpowiednio prowadzony system szkoleń dla pracowników merytorycznych mających dostęp do informacji.
4. Na Inspektorze Ochrony Danych spoczywa obowiązek zapoznania osób upoważnionych do przetwarzania danych z przepisami o ochronie danych osobowych oraz konsekwencjami prawnymi z nich wynikającymi.
5. Utrata poufności informacji o zasadach funkcjonowania systemu ochrony danych osobowych jest niezwykle ważna oraz wymaga położenia nacisku na przestrzeganie procedur przez osoby sprawujące opiekę nad systemami i siecią.

§ 4

Zagrożenia, jakie można wyróżnić ze względu na utratę poufności przy przetwarzaniu danych osobowych:

1. nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe;
2. ujawnienie haseł dostępu do stanowiska komputerowego, na którym przetwarzane są dane osobowe;
3. nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik;
4. utrata nośnika zawierającego dane osobowe;
5. klęska żywiołowa, w wyniku której utracono poufność danych osobowych;
6. nieuprawnione wyniesienie danych osobowych zawartych na nośniku papierowym;
7. udostępnianie danych osobowych osobom nieupoważnionym;

8. wejście w posiadanie danych osobowych przez osobę nieuprawnioną;
9. pokonanie zabezpieczeń fizycznych lub programowych;
10. niekontrolowana obecność osób nieuprawnionych w obszarze przetwarzania danych osobowych;
11. niedyskrecja osób uprawnionych do przetwarzania danych osobowych;
12. nieuprawnione kopiowanie danych na nośniki informacji (CD, DVD, pendrive, itp.);
13. niekontrolowane wynoszenie poza obszar przetwarzania danych osobowych nośników informacji i komputerów przenośnych;
14. naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych;
15. podsłuch lub podgląd danych osobowych;
16. elektromagnetyczna emisja ujawniająca;
17. podsłuch akustyczny i podsłuch emisji ujawniającego promieniowania elektromagnetycznego;
18. stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników firmy;
19. zagubienie dokumentów lub utrata przetwarzanych informacji.

§ 5

Skala identyfikacji skutków utraty zasobów dla atrybutu poufności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Brak skutków utraty poufności
< 1 – 3 >	Niski skutek utraty poufności
< 4 – 7 >	Średni skutek utraty poufności
< 8 – 9 >	Wysoki skutek utraty poufności
< 9 – 10 >	Całkowita utrata poufności

§ 6

1. Integralność to zapewnienie, aby wszelkie modyfikacje wykonywane w dokumentacji papierowej stanowiącej część zbioru danych osobowych, w systemie informatycznym, w systemie jego katalogów oraz indywidualnych plikach posiadające w sobie dane osobowe były skutkiem rozważnych i zaplanowanych działań użytkowników systemu.
2. Integralność, to cecha zapewniająca, że dane nie zostały zmodyfikowane lub zniszczone w sposób nieautoryzowany.
3. Integralność danych dotyczy przede wszystkim wartości informacyjnych przetwarzanych w postaci elektronicznej. Dlatego tak ważne jest zachowanie integralności dla bezpieczeństwa systemu i sieci.

4. Administrator Danych powinien objąć procedurami weryfikacji i rozliczania pracowników sprawujących opiekę nad systemami i siecią oraz wprowadzić bieżącą, regularną detekcję prób ingerencji do systemu informatycznego oraz wszelkie próby naruszenia jego struktury, ponieważ skutkiem takich działań jest uszkodzenie bazy danych i w rezultacie naruszenie zapisów ustawy.

§ 7

Zagrożenia, jakie można wyróżnić ze względu na utratę integralności przy przetwarzaniu danych osobowych:

1. nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego;
2. błędy, pomyłki;
3. brak mechanizmów uniemożliwiających skasowanie lub zmianę logów przez administratora lub innego użytkownika;
4. wadliwe działanie systemu operacyjnego;
5. brak w wykorzystywanych aplikacjach mechanizmów zapewniających integralność danych.
6. uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych;
7. celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych,
8. działanie złośliwego oprogramowania (wirusy);
9. pożar, zalanie, ekstremalna temperatura, itp.;
10. zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny).

§ 8

Skala identyfikacji skutków utraty zasobów dla atrybutu integralności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Utrata integralności nie występuje
< 1 – 3 >	Niski skutek utraty integralności
< 4 – 7 >	Średni skutek utraty integralności
< 8 – 9 >	Wysoki skutek utraty integralności
< 10 >	Bezwzględny skutek utraty integralności

§ 9

Rozliczalność to cecha zapewniająca działanie podmiotu przetwarzającego dane osobowe, która może być przypisana w sposób jednoznaczny tylko temu, jednemu podmiotowi.

§ 10

Zagrożenia, jakie można wyróżnić ze względu na utratę rozliczalności systemu ochrony danych osobowych:

1. brak kontroli nad dokumentami wykorzystywanymi do bieżącej pracy w zakresie ich kopiowania i drukowania;
2. wyparcie się pracy na stanowisku, gdzie przetwarza się dane osobowe;
3. wprowadzenie zmian w treści dokumentu zawierającego dane osobowe;
4. błędy oprogramowania lub sprzętu;
5. nieprzydzielenie użytkownikom indywidualnych identyfikatorów;
6. niewłaściwa administracja systemem informatycznym;
7. niewłaściwa konfiguracja systemu informatycznego;
8. zniszczenie lub sfałszowanie logów systemowych;
9. brak rejestracji udostępnienia danych osobowych;
10. podszywanie się pod innego użytkownika;
11. niespełnienie przez system wymagań ustawowych.

§ 11

Skala identyfikacji skutków utraty zasobów dla atrybutu rozliczalności danych osobowych.

WARTOŚĆ	SKUTKI
< 0 >	Utrata rozliczalności nie występuje
< 1 – 3 >	Niski skutek utraty rozliczalności
< 4 – 6 >	Średni skutek utraty rozliczalności
< 7 – 8 >	Wysoki skutek utraty rozliczalności
< 9 >	Ekstremalny skutek utraty rozliczalności
< 10 >	Absolutny skutek utraty rozliczalności

§ 12

Dla ochrony danych osobowych szczególnie niebezpieczne są występujące zagrożenia miejsc, w których przetwarza się dane osobowe, które występują przeważnie ze względu na ingerencję:

1. **SIŁY NATURY** (to zdarzenia niewynikające z działalności człowieka), mogą to być:
   - **a)** uderzenie pioruna;
   - **b)** pożar będący konsekwencją ww. uderzenia pioruna;
   - **c)** starzenie się sprzętu;
   - **d)** starzenie się nośników pamięci;
   - **e)** smog, kurz;
   - **f)** katastrofy budowlane;
   - **g)** ulewny deszcz;

h) huragan;
i) ekstremalne temperatury, wilgotność;
j) epidemia.

2. **LUDZI** (mogą to być pracownicy lub osoby z zewnątrz, które działają w sposób celowy lub przypadkowy), mogą to być:

a) błędy i pomyłki użytkowników;
b) błędy i pomyłki administratorów;
c) błędy utrzymania systemu w poufności, integralności i rozliczalności;
d) zaniedbania użytkowników przy przesyłaniu, udostępnianiu i kopiowaniu;
e) zagubienie nośnika zawierającego dane osobowe;
f) niewłaściwe zniszczenie nośnika;
g) nielegalne użycie oprogramowania;
h) choroba ważnych osób i nieuprawnione zastępstwo;
i) epidemia kadry i brak osób upoważnionych do dostępu;
j) podpalenie obiektu;
k) zalanie wodą;
l) katastrofa budowlana będąca konsekwencją przypadkowego działania człowieka;
m) zakłócenia elektromagnetyczne, radiotechniczne;
n) podłożenie i wybuch bomby, ładunku wybuchowego;
o) użycie broni;
p) zmiany napięcia w sieci;
q) utrata prądu;
r) zbieranie się ładunków elektrostatycznych;
s) utrata kluczowych pracowników;
t) niedobór pracowników;
u) defekty oprogramowania;
v) szpiegostwo;
w) terroryzm;
x) wandalizm;
y) destrukcja zbiorów i programów impulsem elektromagnetycznym;
z) kradzież;
aa) włamanie do systemu;
bb) wyłudzenie, fałszowanie dokumentów;
cc) podszycie się pod uprawnionego użytkownika;
dd) podsłuch;
ee) użycie złośliwego oprogramowania;
ff) wykorzystanie promieniowania ujawniającego.

.....
(Podpis Administratora Danych Osobowych)

PODATNOŚĆ SYSTEMU NA ZAGROŻENIA

§ 1

Podatność systemu na zagrożenia stanowi pewnego rodzaju słabość. Obecnie, szczególnie trudno jest obronić się przed zagrożeniami w zakresie teleinformatycznym, co związane jest z coraz to bardziej wyrafinowaną cyberprzestępczością. Wraz z coraz to większą ilością dostępnych w środowisku internetowym usług, nasilają się działania przestępcze. Chroniąc placówkę przed takowym działaniem, należy wdrożyć odpowiednie procedury.

§ 2

Podatność systemu na zagrożenia może wynikać z:

1. **Dostępności systemu wynikającego np. z braku ochrony fizycznej budynku lub znacznej liczby personelu, mającego potencjalnie dostęp do systemu oraz wiedzę, jak obsługiwać system.**

   Fizyczna ochrona danych osobowych to jeden z podstawowych obszarów w zakresie przetwarzania danych osobowych. Osoba przetwarzająca dane osobowe bardzo często nie zdaje sobie sprawy, jak ważne jest przestrzeganie chociażby „zasady czystego biurka", która bardzo często jest marginalizowana i zwyczajnie nieprzestrzegana. Bardzo często nieświadomość pracowników w tej materii wiąże się z negatywnymi konsekwencjami dla placówki, np. kwestia złożenia skargi, której przedmiotem jest niedochowywanie należytej staranności w zakresie fizycznej ochrony danych osobowych. Proces wdrażania w placówce „kodeksu dobrych praktyk" w kontekście ochrony danych osobowych jest procesem długoletnim i dynamicznym, ale bezsprzecznie powinno się w pierwszej kolejności uwrażliwiać na fizyczną ochronę danych osobowych. Ponadto, tylko i wyłącznie osoby upoważnione do przetwarzania danych osobowych powinny posiadać wiedzę o tym, w jaki sposób obsługiwać system informatyczny, będący integralnym elementem placówki.

2. **Dostępności informacji znajdujących się w systemie za pośrednictwem połączeń zewnętrznych.**

   System informatyczny w placówce powinien być odpowiednio zabezpieczony, również jeśli dostęp do niego jest możliwy za pośrednictwem połączeń zewnętrznych. Niezależnie od zastosowanych rozwiązań teletransmisyjnych, system ten powinien być „szczelny", to znaczy wystarczająco odporny na wszelkiego rodzaju zewnętrzne zagrożenia.

3. **Możliwości celowego wprowadzania luk w sprzęcie i oprogramowaniu lub wprowadzania wirusów komputerowych.**

   Możność nieuprawnionego działania na sprzęcie, czy oprogramowaniu może być wynikiem zastosowanej manipulacji, podsłuchu czy podstawienia. Podsłuch polega na tym, że charakter poufności przekazywanych treści zostaje naruszony. Manipulacja z kolei, będzie działaniem, które ukierunkowane jest na uzyskanie dostępu do treści danych i nieuprawnioną ingerencję w nie. Natomiast podstawienie, polega między innymi na wprowadzeniu drugiej strony w błąd, co do swojej tożsamości, po to tylko, by uzyskać konkretne informacje. Kadra powinna być odpowiednio uwrażliwiona na otrzymywanie korespondencji mailowej, co do której zaistnieje podejrzenie, że została przesłana w celu wprowadzenia wirusa komputerowego.

4. **Możliwości awarii sprzętu lub oprogramowania ze względu na uszkodzenia, błędy projektowe lub umyślną interwencję.**

   Sprzęt informatyczny powinien być cyklicznie odpowiednio serwisowany, tak by wyeliminować zagrożenia. Należy zaznaczyć, iż z firmą informatyczną zewnętrzną, nie podpisujemy upoważnienia do przetwarzania danych osobowych, ale przynajmniej klauzulę poufności informacji w kontekście przetwarzanych danych osobowych. Wzór klauzuli poufności stanowi załącznik nr 7.

5. **Przesyłania informacji przez niezabezpieczone łącza telekomunikacyjne**.

   Brak zabezpieczeń kryptograficznych łącza telekomunikacyjnego czy nieefektywność fizycznych zabezpieczeń, również stanowi zagrożenie utraty poufności danych osobowych.

§ 3

1. Podatność systemu na zagrożenia została ograniczona poprzez:

   a) ochronę fizyczną obiektu, w tym stanowisk komputerowych;

   b) kontrolę dostępu do pomieszczeń, gdzie przetwarzane są dane osobowe;

   c) wydzielenie stref ochronnych;

   d) ograniczenie liczby personelu, mającego potencjalnie dostęp do pomieszczeń, w których znajdują się dane osobowe;

   e) zbudowanie stabilnej sieci zasilającej;

   f) przeglądy okresowe nośników;

   g) kontrolę zmian konfiguracji;

   h) testowanie oprogramowania;

   i) audyt;

   j) zabezpieczanie haseł;

   k) użycie oprogramowania antywirusowego;

   l) backupy.

2. By maksymalnie wyeliminować zagrożenie dla całego systemu ochrony danych osobowych, należy wdrożyć procedury kontrolne, które nie będą zorientowane tylko i wyłącznie na jeden obszar przetwarzania danych osobowych, np. środowisko komputerowe. Warunkiem wyeliminowania działań cyberprzestępców, jest pełne współdziałanie wszystkich obszarów przetwarzania danych osobowych:

   a) prowadzenie odpowiedniej dokumentacji;

   b) fizyczna ochrona danych osobowych;

   c) środowisko komputerowe;

   d) „kodeks dobrych praktyk” wdrożony przez Inspektora Ochrony Danych, o ile jest powołany lub Administratora Danych Osobowych.

3. Przebieg przykładowej kontroli tych obszarów stanowi załącznik nr 8.

§ 4

W celu wdrażania systemu ochrony danych osobowych w taki sposób, by uniemożliwić działanie nieuprawnione na danych osobowych, Administrator Danych Osobowych zobowiązuje pracowników podmiotu o nazwie **Urząd Gminy i Miasta Gryfów Śląski** do stosownego zachowania w trakcie przetwarzania danych osobowych, czego aprobatę wyraził w swojej rekomendacji, która stanowi załącznik nr 9.

§ 5

W celu oszacowania potencjalnych strat wynikających z utraty (ujawnienia) danych osobowych przetwarzanych w jednostce, wykonano analizę ryzyka na podstawie przewidywanych zagrożeń dla zasobów. Analiza ryzyka musi być wykonywana okresowo przez Inspektora Ochrony Danych i Administratora Systemu Informatycznego - raz do roku na tej podstawie aktualizowana jest tabela ryzyka znajdująca poniżej - § 6.

§ 6

Identyfikacja podatności systemu informatycznego na określone zagrożenia.

WARTOŚĆ	SKUTKI
< 0 >	Brak podatności
< 1 – 4 >	Niski poziom
< 5 – 7 >	Średni poziom
< 8 – 9 >	Wysoki poziom
< 10 >	Ekstremalny poziom

.....
(Podpis Administratora Danych Osobowych)

ANALIZA ZAGROŻEŃ I SZACOWANIE RYZYKA

§ 1

Administrator Danych Osobowych, aby poprawnie przeprowadzić analizę ryzyka, powinien określić:

1. **ZASOBY** - które będzie chronić:
   - **a)** sprzęt komputerowy przechowujący dane - dysk twardy,
   - **b)** dane osobowe przetwarzane w formie papierowej i elektronicznej,
   - **c)** aplikacje, w których przetwarzane są dane osobowe,
   - **d)** pomieszczenia, w których pracują osoby przetwarzające dane osobowe;
2. **ZAGROŻENIA** - czynnik, który może powodować wystąpienie incydentu;
3. **PODATNOŚĆ** - słabość zasobów, która może być wykorzystana przez potencjalne zagrożenie;
4. **SKUTKI** - jaki wpływ będzie miał zaistniały incydent na utratę danych osobowych.

§ 2

Administrator Danych Osobowych bądź Inspektor Ochrony Danych, aby dokonać skutecznego zarządzania bezpieczeństwem informacji w podmiocie, dokonuje dokładnej analizy zagrożeń w związku z reagowaniem na zmieniające się warunki otoczenia mające wpływ na ryzyko w organizacji. Tak stworzony efektywny system zarządzania daje możliwość podjęcia działań redukujących wartość ryzyka do akceptowanego poziomu.

§ 3

Poniższy schemat obrazuje prawidłowy tok szacowania i postępowania z ryzykiem, jakie podejmuje Administrator Danych Osobowych.

§ 4

1. Analiza ryzyka jest częścią szacowania ryzyka. Jest ona pojęciem węższym niż szacowanie ryzyka, nie zawiera bowiem oceny ryzyka.
2. Ocena ryzyka, czyli określenie, które ryzyka są akceptowalne poprzez porównanie wyznaczonych poziomów ryzyka z tymi, które można zaakceptować.
3. Szacowanie ryzyka obejmuje analizę ryzyka i ocenę ryzyka.

§ 5

1. Administrator Danych Osobowych szacuje wynik ryzyka. Poprzez określenie poziomu ryzyka akceptowalnego i kończy etap szacowania ryzyka.
2. Administrator Danych osobowych wyciąga wnioski oraz podejmuje działania naprawcze, mające na celu obniżenie wartości ryzyka akceptowalnego.
3. Tabela szacowania ryzyka stanowi załącznik nr 10.

§ 6

1. Administrator Danych Osobowych określa poziom ryzyka utraty bezpieczeństwa danych osobowych na poziomie średnim w podmiocie o nazwie **Urząd Gminy i Miasta Gryfów Śląski** przy uwzględnieniu ryzyka ogólnego przy wartości **31,6**

   RYZYKO = wartość skutków x podatność zasobów systemu

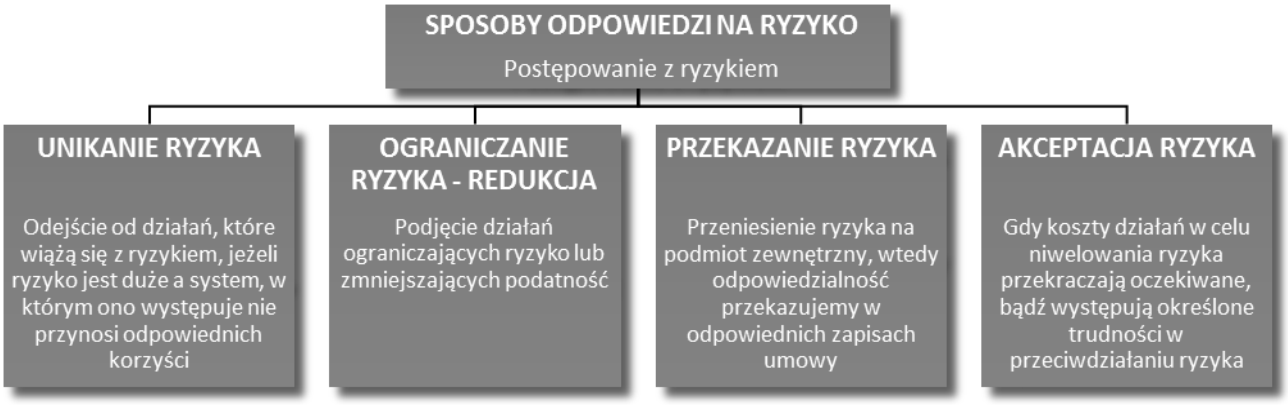
   (max. = 100)

WARTOŚĆ	POZIOM RYZYKA
<1-20>	**NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<21-60>	**ŚREDNI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<61-80>	**WYSOKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
<81-100>	**MAKSYMALNY** poziom ryzyka utraty bezpieczeństwa danych osobowych

2. Poziomy ryzyka utraty bezpieczeństwa danych osobowych:
   a) **NISKI** – niskie szkody w przypadku realizacji zagrożenia i niska możliwość jego wystąpienia;
   b) **ŚREDNI** – wysokie szkody w przypadku realizacji zagrożenia i niska możliwość jego realizacji bądź niskie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego realizacji;
   c) **WYSOKI** – wysokie szkody w przypadku realizacji zagrożenia i wysoka możliwość jego wystąpienia;
   d) **MAKSYMALNY** – wysokie szkody w przypadku realizacji zagrożenia oraz wysoka możliwość jego wystąpienia, skutkująca nie tylko na organizację, ale na podmioty trzecie.

§ 7

Administrator Danych Osobowych po oszacowaniu ryzyka przystępuje do etapu postępowania z ryzykiem. Koniecznym jest podjęcie działania, które będzie odpowiedzią podmiotu na oszacowany poziom występującego ryzyka. W ramach postępowania z ryzykiem możemy podjąć cztery różne działania.



§ 8

Proces zarządzania ryzykiem związany z bezpieczeństwem informacji zapewnia:

1. identyfikowanie zagrożeń dla przetwarzanych informacji;
2. oszacowanie ryzyka w kategoriach konsekwencji dla funkcjonowania biznesowego oraz prawdopodobieństwa wystąpienia zagrożeń;
3. odpowiednie przedstawienie oraz zrozumienie prawdopodobieństwa oraz konsekwencji materializacji ryzyka;
4. ustanowienie priorytetów dotyczących postępowania z ryzykiem;
5. wprowadzanie priorytetowych działań mających na celu redukcję ryzyka;
6. zaangażowanie kierownictwa podczas podejmowania decyzji związanych z zarządzaniem ryzykiem oraz bieżące informowanie go o postępach realizowanych działań minimalizujących;
7. monitorowanie i regularne przeglądanie ryzyka oraz procesu zarządzania nimi;
8. kształcenie pracowników w zakresie ryzyka oraz działań mających na celu obniżenie poziomu prawdopodobieństwa ich wystąpienia.

.....

(Podpis Administratora Danych Osobowych)

WNIOSKI I DZIAŁANIA NAPRAWCZE

W ZWIĄZKU Z PRZEPROWADZONĄ „ANALIZĄ RYZYKA I ZAGROŻEŃ

PRZY PRZETWARZANIU DANYCH OSOBOWYCH”

§ 1

1. Administrator Danych Osobowych w placówce o nazwie: **Urząd Gminy i Miasta Gryfów Śląski**, przeprowadził analizę dla wszystkich chronionych zasobów oraz wszystkich możliwych zagrożeń.
2. Administrator Danych Osobowych jest zobowiązany dostosować środki bezpieczeństwa, zarówno techniczne, jak i fizyczne oraz organizacyjne, do wyników, jakie oddała przeprowadzona analiza.
3. Zmiany związane z pkt 2 należy wprowadzić do aktualnej Polityki Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym.

§ 2

W wyniku przeprowadzonej analizy w placówce o nazwie: **Urząd Gminy i Miasta Gryfów Śląski**, Administrator Danych Osobowych wyróżnił potencjalnie najniebezpieczniejsze zagrożenia, a w szczególności są to:

- **ODCIĘCIE ZASILANIA,**
- **KRADZIEŻ,**
- **AWARIA SPRZĘTU,**

§ 3

W celu zmniejszenia zagrożeń, wymienionych w § 2 przez Administratora Danych Osobowych, należy zwrócić uwagę w szczególności na:

- **PRZEGLĄD BATERII W UPS-ach,**
- **ZABEZPIECZENIA PLACÓWKI W ZAKRESIE TECHNICZNYM,**
- **STAN TECHNICZNY SPRZĘTU,**

§ 4

Administrator Danych Osobowych w celu wyeliminowania zagrożeń, wynikłych w toku przeprowadzonej analizy, podejmuje działania naprawcze, polegające w szczególności na:

- **Kontakt z autoryzowanym serwisem celem modernizacja lub wymiany modułu zasilania,**
- **Zwiększenie kontroli doraźnych oraz interwału sporządzania raportu dziennego/miesięcznego,**
- **Starania w zakresie powiększenia gospodarki magazynowej z zakresu części zamiennych .**

.....

(Podpis Administratora Danych Osobowych)

WZÓR KLAUZULI POUFNOŚCI INFORMACJI [1]

§ 1

Strony umowy zobowiązują się wzajemnie do niewykorzystywania, nieujawniania oraz nieprzekazywania informacji, które stanowią tajemnicę przedsiębiorstwa drugiej strony niniejszej umowy.

§ 2

Strony powinny zachować poufność informacji, które zdobędą na każdym etapie jakiejkolwiek wzajemnej współpracy.

§ 3

Klauzula poufności danych obowiązuje strony przez okres trwania umowy, a także bezwzględnie po jej zakończeniu przez okres 2 lat.

§ 4

Strony odpowiadają za zachowanie powyższych informacji w tajemnicy przez osoby, którym wykonanie swoich obowiązków powierzyły.

§ 5

Strony umowy zobowiązują się do wykorzystywania przetwarzanych przez nie danych osobowych, w ramach realizacji niniejszej umowy, wyłącznie w celach określonych w umowie.

§ 6

Stronom umowy przysługuje w każdym czasie i bez ograniczenia - kontrola procesu przetwarzania i ochrony danych osobowych.

§ 7

Strony, dopełniając czynności wynikających z niniejszej umowy, zobowiązują się do przestrzegania przepisów 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.

§ 8

W przypadku niedochowania warunków umowy, strony zastrzegają sobie prawo rozwiązania niniejszej umowy w trybie natychmiastowym, w każdym czasie.

[1] **UWAGA:** Niniejszy dokument może być zastosowany:

- jako osobny (niezależny) dokument celem zobowiązania drugiej strony do zachowania poufności informacji,
- jako dodatkowe zapisy (paragrafy) do umowy lub innego dokumentu wiążącego strony wzajemną współpracą.

PRZEBIEG PRZYKŁADOWEJ KONTROLI PODATNOŚCI SYSTEMU

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI
1.	DOKUMENTACJA	Sprawdzenie, czy Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemem Informatycznym jest aktualna względem obowiązującego stanu prawnego oraz faktycznego.
2.	DOKUMENTACJA	Sprawdzenie, czy osoba ma upoważnienie do przetwarzania danych osobowych – upoważnienie powinno odzwierciedlać zakres obowiązków.
3.	DOKUMENTACJA	Sprawdzenie, czy osoby, które mają dostęp do danych osobowych, ale nie przetwarzają tych danych, posiadają zgody na przebywanie w obszarze przetwarzania.
4.	DOKUMENTACJA	Sprawdzenie, czy prowadzona jest aktualna ewidencja osób przetwarzających dane osobowe.
5.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Kontrolowanie osób przetwarzających dane osobowe - czy stosują się do „zasady czystego biurka”.
6.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajdują się szafy zamykane na klucz, w których przechowuje się dokumentację zawierającą dane osobowe podlegające ochronie (jeśli tak - można sporządzić dokumentację fotograficzną pomieszczeń, która stanowić będzie załącznik do poniższego sprawdzenia).
7.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajduje się niszczarka dokumentów (jeśli takie urządzanie nie znajduje się w pomieszczeniu, należy skontrolować pracownika, w jaki sposób niszczy zbędną dokumentację, która nie podlega archiwizacji). Szczególnie powinno się zwrócić uwagę, czy niepotrzebne dokumenty nie są przypadkiem wyrzucane do kosza na śmieci – dokumenty powinny być niszczone w sposób mechaniczny lub manualny, tak, by uniemożliwić ich odczytanie osobom postronnym.
8.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, mające na celu sprawdzenie, czy komputer jest zabezpieczony hasłem.
9.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy systemy komputerowe służące do przetwarzania danych osobowych zapamiętują wszelakie czynności, jakich dokonuje się przy przetwarzaniu danych osobowych.
10.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Monitorowanie, czy osoby przetwarzające dane osobowe w programie komputerowym bazodanowym (czyli dotyczącym baz danych) logują się za pomocą WŁASNEGO identyfikatora i hasła.
11.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie aktywności systemu antywirusowego, na komputerach, które m.in. służą do obsługi systemów przetwarzających dane osobowe.
12.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, czy pracownik korzysta z wygaszacza ekranu.

LP.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI
13.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy monitor komputera został usytuowany w sposób uniemożliwiający wgląd do danych - osobom postronnym.
14.	ZBIORY DANYCH OSOBOWYCH	Kontrolowanie, czy opracowano prawidłowy rejestr czynności przetwarzania danych, który jest na bieżąco uzupełniany.
15.	ZBIORY DANYCH OSOBOWYCH	Sprawdzenie, czy wszystkie zbiory, które prowadzi się w placówce, znajdują się w rejestrze czynności przetwarzania.
16.	ZBIORY DANYCH OSOBOWYCH	Przeprowadzenie wywiadu, którego celem jest ustalenie, czy pracownik przetwarza zbiór danych osobowych, który nie figuruje w rejestrze czynności przetwarzania (szczególnie ma się na względzie projekty prowadzone przez referaty).
17.	KONTROLA PRAKTYKI	Przeprowadzenie analizy pod kątem pracowników - jakie obecnie mają problemy w zakresie przetwarzania danych osobowych oraz czy ostatnio miały miejsce zdarzenia typu: • próby nieuprawnionego dostępu do danych osobowych; • działanie zewnętrznych aplikacji, wirusów czy złośliwego oprogramowania; • nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym; • próba nieuprawnionej interwencji przy sprzęcie komputerowym; • wynoszenie niezabezpieczonych pamięci z miejsca pracy; • udzielanie informacji osobom postronnym, pomijając formalny tryb administracyjny.

REKOMENDACJA ODPOWIEDNIEJ POSTAWY OSÓB POSIADAJĄCYCH UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1

Przepisy kodeksu pracy zobowiązują pracownika do sumiennego wykonywania swoich obowiązków. Pracownik powinien odpowiednio przestrzegać czasu pracy, co w konsekwencji oznacza, że nie powinien on w godzinach pracy zajmować się prywatnymi sprawami, chociażby prywatną korespondencją.

§ 2

Pracodawca wyposaża pracowników w konkretne narzędzia pracy, jak telefon czy komputer i nie musi godzić się na wykorzystywanie ich do prywatnych celów.

§ 3

Pracodawca może kontrolować pracownika w ramach stosownego wykorzystywania narzędzi, które powinny służyć tylko do celów służbowych. Za interesem pracodawcy przemawia fakt, że musi on chronić tajemnicę przedsiębiorstwa oraz zabezpieczać odpowiednio placówkę pod względem systemu ochrony danych osobowych.

§ 4

Należy przypomnieć niniejszym dokumentem, iż w placówce wdrożono postanowienia Polityki Ochrony Danych Osobowych oraz Instrukcji Zarządzania Systemem Informatycznym, co w konsekwencji oznacza, iż dobrych praktyk powinno się przestrzegać.

§ 5

Jeśli pracodawca podczas kontroli stwierdzi, iż zakaz nie jest respektowany, może wobec pracownika wyciągnąć konsekwencje służbowe.

§ 6

Pracodawca może ustalić, że na służbowych komputerach nie można instalować aplikacji oraz używania portali społecznościowych. Ponadto, pracodawca może zakazać wnoszenia prywatnych nośników danych tj. nośników: optycznych (płyty CD, DVD itp.), półprzewodnikowych (układy scalone), magnetycznych (w tym pamięci ferrytowe), magnetooptycznych, polimerowych (np. Millipede), papierowych (np. karty dziurkowane), z linią opóźniającą (np. pamięci rtęciowe).

§ 7

Pracodawca niniejszym dokumentem informuje pracowników, iż kontrola w danym zakresie będzie miała miejsce, a pracownicy przyjmują ten fakt do wiadomości.

.....

(Podpis Administratora Danych Osobowych)

TABELA SZACOWANIA RYZYKA

SZACOWANIE RYZYKA DLA BEZPIECZEŃSTWA INFORMACJI																			RYZYKO OGÓLNE [3]:
RYZYKO ŚREDNIE [2]:					29			35			33			29			32		31,6
ZAGROŻENIA																			
	INTEGRALNOŚĆ	AWARIA SPRZĘTU	5	5	25	8	5	40	8	5	40	8	4	32	8	5	40		
		ODCIĘCIE ZASILANIA	6	5	30	6	5	30	8	6	48	7	6	42	7	5	35		
		POŻAR	5	2	10	7	6	42	7	5	35	8	4	32	6	6	36		
		ATAK WIRUSA	6	3	18	7	5	30	8	5	40	5	5	25	5	4	20		
		KRADZIEŻ	8	4	32	8	6	48	6	5	30	7	4	28	6	4	24		
		NIEUPRAWNIONY DOSTĘP	8	5	40	5	4	20	7	6	42	7	5	35	6	5	30		
	ROZLICZALNOŚĆ	AWARIA SPRZĘTU	9	5	45	7	5	35	5	5	25	6	5	30	6	5	30		
		ODCIĘCIE ZASILANIA	7	5	35	6	6	36	7	5	35	8	6	48	9	5	45		
		POŻAR	8	4	32	7	4	28	5	4	20	7	4	28	6	5	30		
		ATAK WIRUSA	6	5	30	6	5	30	5	5	25	5	4	20	5	5	25		
		KRADZIEŻ	7	4	28	7	3	21	6	5	30	6	4	24	6	5	30		
		NIEUPRAWNIONY DOSTĘP	6	4	24	8	3	24	7	5	35	8	3	18	8	5	40		
	POUFNOŚĆ	AWARIA SPRZĘTU	5	4	20	8	5	40	4	4	16	5	4	20	7	6	42		
		ODCIĘCIE ZASILANIA	4	5	20	7	5	35	6	6	36	7	5	35	5	5	25		
		POŻAR	7	3	21	7	6	42	7	6	42	8	3	24	6	5	30		
		ATAK WIRUSA	6	5	30	7	5	35	7	5	35	5	4	20	6	5	30		
		KRADZIEŻ	8	6	48	8	5	40	7	4	28	8	4	32	5	5	25		
		NIEUPRAWNIONY DOSTĘP	7	5	35	8	6	48	7	5	35	7	4	28	7	4	28		
SZACOWANIE			SKUTKI	PODATNOŚĆ	RYZYKO [4]	SKUTKI	PODATNOŚĆ	RYZYKO [3]	SKUTKI	PODATNOŚĆ	RYZYKO [3]	SKUTKI	PODATNOŚĆ	RYZYKO [3]	SKUTKI	PODATNOŚĆ	RYZYKO [3]		
ZASOBY SZACOWANE			SPRZĘT			LUDZIE			APLIKACJA			POMIESZCZENIA			DODATKOWE ZABEZPIECZENIA				

Skala poziomu ryzyka:

[2] **RYZYKO ŚREDNIE** = suma ryzyka każdego z sześciu zakresów poufności, rozliczalności i integralności dzielona przez 18

[3] **RYZYKO OGÓLNE** = suma ryzyka średniego z zasobów: sprzęt, ludzie, aplikacja, pomieszczenia, zabezpieczenia dodatkowe, dzielona przez 5

[4] **RYZYKO** = wartość skutków x podatność zasobów systemu (max. = 100)

WARTOŚĆ	POZIOM RYZYKA
1-20	**NISKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
21-60	**ŚREDNI** poziom ryzyka utraty bezpieczeństwa danych osobowych
61-80	**WYSOKI** poziom ryzyka utraty bezpieczeństwa danych osobowych
81-100	**MAKSYMALNY** poziom ryzyka utraty bezpieczeństwa danych osobowych

PODSUMOWANIE

W podmiocie o nazwie: **Urząd Gminy i Miasta Gryfów Śląski** po przeprowadzeniu analizy poufności, integralności i rozliczalności systemów informatycznych pod kątem zagrożeń i ryzyka, zwanej dalej: analizą zagrożeń i ryzyka przy przetwarzaniu danych osobowych wartość i poziom ryzyka przedstawia się następująco:

Ryzyko ogólne wynosi: **31,6 / 100.**

Powyższa wartość ryzyka określa **Średnie** ryzyko utraty bezpieczeństwa danych osobowych.

.....

(Data i Podpis Administratora Danych Osobowych)