Załącznik nr 6 do Regulaminu Organizacyjnego Biura
Stowarzyszenia „Bursztynowy Pasaż”
”

POLITYKA BEZPIECZEŃSTWA I OCHRONY DANYCH OSOBOWYCH

Stowarzyszenia „Bursztynowy Pasaż” (LGD)

UL. Szkolna 3 84-250 Gniewino

opracowanie powstałe na potrzeby wdrożenia RODO
w Stowarzyszeniu „Bursztynowy Pasaż”

Zatwierdzam:

Luty 2024

I. Wstęp

Polityka bezpieczeństwa w Stowarzyszeniu „Bursztynowy Pasaż" określa zasady przetwarzania danych osobowych zapewniające poufność, integralność i rozliczalność tych danych. Najważniejszym celem realizacji poniższego opracowania jest zapewnienie wysokiego poziomu bezpieczeństwa przetwarzanych danych (zarówno w zbiorach manualnych jak i w systemach informatycznych).

II. Pojęcia

- **Administrator Danych Osobowych** – Zarząd Stowarzyszenia „Bursztynowy Pasaż"
- **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
- **Przetwarzanie danych** – jakiekolwiek operacje wykonane na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.
- **Zbiór danych** – uporządkowany zestaw danych osobowych dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest zcentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
- **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
- **Hasło** – ciąg znaków literowych, cyfrowych lub innych przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
- **Integralność danych** – funkcjonalność zapewniająca, że dane osobowe nie są udostępniane, zmienione lub zniszczone w sposób nieautoryzowany.
- **Poufność danych** – funkcjonalność zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
- **Aktywa** – to wszystko, co ma wartość dla organizacji, jak np. dane osobowe.
- **Aktywa podstawowe** – procesy, działania biznesowe oraz informacje związane z funkcjonowaniem organizacji (w tym dane osobowe).
- **Aktywa wspierające** – środki umożliwiające korzystanie z aktywów podstawowych np. sprzęt, oprogramowanie, sieć, pracownicy.
- **Identyfikowanie ryzyka** – czynność polegająca na określeniu, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i spowodować stratę.
- **Kryteria akceptacji ryzyka** – kryteria, które określają dopuszczalność danego ryzyka.
- **Kryteria oceny ryzyka** – kryteria, które określają poziomy odniesienia, względem których określa się ważność ryzyka.
- **Naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa danych prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych.

- **Ocena ryzyka** – czynność polegająca na porównaniu wyników uzyskanych podczas analizy ryzyka z kryteriami oceny ryzyka określonymi na etapie ustanawiania kontekstu działania organizacji.
- **Podatność** – słabość, która może być wykorzystana przez zagrożenie, powodując niekorzystne skutki np.. luka w systemie informatycznym.
- **Szacowanie ryzyka** – całościowy proces identyfikacji ryzyka, analizy oraz oceny ryzyka.
- **Właściciel aktywów** – osoba odpowiedzialna w danym momencie za konkretny proces przetwarzania danych i mająca prawo do podejmowania w tym zakresie decyzji np. dyrektor departamentu, kierownik określonej komórki organizacyjnej.
- **Zagrożenie** – źródło potencjalnej szkody.
- **Zabezpieczenie** – środek, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia lub też minimalizację potencjalnych strat związanych ze zrealizowanym zagrożeniem, np. program antywirusowy, drzwi antywłamaniowe, stosowane procedury bezpieczeństwa.

III. Postanowienia ogólne

1. Stowarzyszenie „Bursztynowy Pasaż" realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych stosuje odpowiednie środki oraz dokłada wszelkich starań aby należycie chronić interesy osób, których dane dotyczą.
2. Administratorem Danych Osobowych w Stowarzyszeniu „Bursztynowy Pasaż" jest Zarząd Stowarzyszenia.
3. Nadzór nad przetwarzaniem danych osobowych w Stowarzyszeniu pełni Administrator Danych Osobowych.
4. Osoby upoważnione do przetwarzania danych osobowych prowadzą rejestry udostępnionych danych zawierające w szczególności: datę udostępniania, podstawę prawną, zakres udostępnionych danych oraz osobę lub instytucję dla której dane udostępniono.

IV. Szacowanie ryzyka

Etap 1
Ustalenie kontekstu

1.1 Określenie informacji i uwarunkowań związanych z działaniem Stowarzyszenia „Bursztynowy Pasaż"

INFORMACJE ZEWNĘTRZNE

a) dot. środowiska polityczno – prawnego

LGD funkcjonuje na podstawie następujących regulacji prawnych:
- Ustawa z dnia 20 lutego 2015 o rozwoju lokalnym z udziałem lokalnej społeczności
- Ustawa z dnia 7 kwietnia 1989 Prawo o Stowarzyszeniach
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiające przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju

Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylające rozporządzenie Rady (WE) nr 1083/2006
- Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/1060 z dnia 24 czerwca 2021 ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej
- Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz.U. 1994 nr 121 poz. 591)
Na działalność Stowarzyszenia mają wpływ zmiany zachodzące w Rządzie RP (np. zmiana partii rządzącej), które przekładają się na aktualizacje ustaw oraz ich interpretacje.

b) o zasięgu terytorialnym działalności organizacji

Terenem działania Stowarzyszenia jest obszar Rzeczypospolitej Polskiej oraz poza jego granicami zgodnie z obowiązującym prawem.

c) dot. korzystania z usług lub zasobów podmiotów zewnętrznych

LGD współpracuje z firmami zewnętrznymi przy zakupie produktów i usług niezbędnych do prawidłowego funkcjonowania biura Stowarzyszenia oraz wywiązywania się z zapisów umowy zawartej z Urzędem Marszałkowskim.

Współpraca ta dotyczy m.in.:
- najmu pomieszczenia na biuro,
- zakupu usługi dostarczenia łącza internetowego i telefonicznego,
- zakupu usługi pocztowej,
- ubezpieczenia mienia biura,
- napraw i aktualizacji dot. sprzętu komputerowego biura oraz zarządzanych przez LGD stron internetowych,
- napraw posiadanego i wynajmowanego mienia biura (naprawa drzwi, montaż mebli biurowych itp.),
- zakupu materiałów promocyjnych,
- realizacji kampanii promocyjnych (ogłoszenia w prasie lokalnej, druk ulotek i plakatów, itp.).

Ponadto LGD ściśle współpracuje (w tym wymienia informacje dotyczące regulacji prawnych oraz codziennych aspektów związanych z działalnością biura) z:
- Departamentem Programów Rozwoju Obszarów Wiejskich Województwa Pomorskiego
- Pomorską Siecią LEADER
- Polską Siecią LGD
- urzędami gmin: Choczewo, Gniewino, Wejherowo, Cewice, Nowa Wieś Lęborska, Wicko i Łeba
- biurem: USŁUGI KSIĘGOWE WGT Weronika Głowienka-Treder w Gniewowie
- Agencją Restrukturyzacji i Modernizacji Rolnictwa
- z partnerami zewnętrznymi, z którymi realizujemy projekty współpracy (inne LGD) oraz okazjonalnie i w mniejszym zakresie wymiany danych z:
- innymi, zaprzyjaźnionymi LGD'ami
- Głównym Punktem Informacyjnym Funduszy Europejskich w Gdańsku

- Powiatowym Urzędem Pracy w Wejherowie i Lęborku
- jednostkami organizacyjnymi gmin: Choczewo, Gniewino, Wejherowo, Cewice, Nowa Wieś Lęborska, Wicko i Łeba (np. pomocą społeczną, centrami kultury)

Rynek odbiorców LGD stanowią:
- mikro i małe przedsiębiorstwa*
- osoby bezrobotne z zamiarem rozpoczęcia działalności gospodarczej*
- organizacje pozarządowe*
- urzędy gmin*
- jednostki organizacyjne gmin (np. pomoc społeczna)*
- organizacje niesformalizowane (sołectwa, KGW, OSP)*
- gminne centra kultury i pozostałe jednostki oraz spółki gminne*
- sołtysi, Rady Sołeckie i lokalni liderzy*
- miejscowi artyści*
- rolnicy*

* z obszaru działania LGD.

Wszystkie ww. organizacje i osoby mają możliwość przystąpienia do konkursów ogłaszanych przez Stowarzyszenie.

e) dot. środowiska społecznego

Obszar działania LGD stanowią gminy wiejskie powiatu wejherowskiego: Choczewo, Gniewino, Wejherowo oraz powiatu lęborskiego Cewice, Nowa Wieś Lęborska, Wicko i Łeba, wchodzącego w skład Województwa Pomorskiego. Powyższe gminy, ze względu na swoje położenie znacznie się od siebie różnią, w szczególności na następujących płaszczyznach:
- ilości mieszkańców (gminy zlokalizowane bezpośrednio przy miastach powiatowych są znacznie większe)
- posiadanej infrastruktury turystycznej, sportowej, rekreacyjnej i kulturalnej (przewaga gmin nadmorskich i gm. Gniewino)
- pozostałości po Państwowych Gospodarstwach Rolnych
- ilości i poziomu świadczonych usług
- wielkości sektora gospodarczego
- lokalizacji i braku bezpośredniego dostępu do morza przez większą część gmin członkowskich
- różny poziom zanieczyszczeń powietrza (większy przy miastach powiatowych)

Elementami łączącymi gminy członkowskie są:
- podobny (niski) poziom bezrobocia
- aktywność w pozyskiwaniu dofinansowania z funduszy zewnętrznych
- aktywna współpraca z lokalnym sektorem biznesu
- sytuacja społeczno – gospodarcza (np..: obserwuje się duży napływ mieszkańców z Trójmiasta i tzw. „Małego Trójmiasta Kaszubskiego" i Lęborka)
- uwarunkowania rozwojowe gmin
- warunki przyrodnicze
- odsetek gospodarstw rolnych bez działalności rolniczej
- wielokulturowość lokalnego społeczeństwa i ciągła potrzeba integracji

f) dot. środowiska międzynarodowego

LGD funkcjonuje m.in. na podstawie przepisów Unii Europejskiej w zakresie rozwoju mikro i małych przedsiębiorstw oraz rozwoju lokalnego kierowanego na społeczność i jest od tych przepisów zależne. Na działalność Stowarzyszenia mają wpływ zmiany zachodzące w polityce międzynarodowej RP.

INFORMACJE WEWNĘTRZNE

a) struktura i rozmiar organizacji

Członkami LGD są osoby fizyczne, przedsiębiorcy, przedstawiciele organizacji pozarządowych, osoby prawne oraz jednostki samorządu terytorialnego. Obecnie LGD posiada ponad 40 członków będących przedstawicielami sektora gospodarczego, społecznego i publicznego. Każdy członek ma bezpośrednią możliwość wpływania na funkcjonowanie i rozwój LGD poprzez zasiadanie w Zarządzie, Komisji Rewizyjnej czy Radzie

Organy LGD:
- **Walne Zebranie Członków**, które wg statutu obejmuje m.in.: uchwalanie i zmiany statutu, wybór Zarządu i jego odwoływanie, wybór członków Komisji Rewizyjnej, wybór Rady Walne Zebranie Członków podejmuje decyzje w formie uchwały większością głosów w głosowaniu jawnym, przy obecności przynajmniej 50% wszystkich członków. Wszyscy członkowie mają równą ilość i moc głosu.
- **Zarząd (organ wykonawczy)** do którego należy reprezentowanie Stowarzyszenia na zewnątrz, kierowanie i organizowanie bieżącej działalności Stowarzyszenia czy zaciąganie zobowiązań finansowych. Zarząd LGD, zgodnie ze statutem składa się od 3 do 6 osób, w tym Prezesa, Wiceprezesa i pozostałych członków Zarządu.
- **Komisja Rewizyjna (organ kontrolny)** składa się przynajmniej z trzech osób, w tym przewodniczącego, sekretarza i członka wybieranych przez Walne Zebranie Członków. Komisja Rewizyjna podejmuje decyzje drogą uchwał zwykłą większością głosów, przy co najmniej 50% składu Komisji. Zadaniem Komisji Rewizyjnej jest kontrolowanie działalności Stowarzyszenia przynajmniej raz do roku pod względem zgodności z przepisami prawa, statutem i uchwałami Walnego Zebrania Członków Stowarzyszenia, przedstawianie Walnemu Zebraniu Członków Stowarzyszenia ocen działalności Zarządu oraz stawianie wniosku o udzielenie Zarządowi absolutorium, sporządzanie corocznych ocen działalności Stowarzyszenia i podawanie ich do wiadomości członków.

Ponadto w strukturach Stowarzyszenia występuje **Rada.** Do zadań Rady należy ocena oraz wybór operacji, które będą dofinansowane w ramach przedsięwzięć zawartych w lokalnej strategii rozwoju. Ważną kompetencją Rady jest przyjmowanie i aktualizowanie LSR oraz lokalnych kryteriów wyboru operacji. Strukturę Rady i jej kompetencje określa Statut Stowarzyszenia a szczegółowe zasady funkcjonowania organu oraz wybór operacji do dofinansowania określa Regulamin Rady.

Obsługą Stowarzyszenia zajmuje się **Biuro LGD**, które prowadzi sprawy wszystkich organów Stowarzyszenia oraz wdraża LSR. Biuro LGD spełnia wszelkie warunki pozwalające na efektywne zarządzanie i pracę zatrudnionych tam osób. Wybrani zgodnie z procedurą rekrutacji pracownicy zatrudnieni są na podstawie umów o pracę.
Biuro LGD znajduje się w Gniewinie, przy ul. Szkolnej 3. Lokal jest użytkowany na podstawie umowy najmu zawartej z zarządzającym obiektem. W skład pomieszczeń

wchodzą lokale użytkowe na II kondygnacji, o łącznej powierzchni 53 m². Układ pomieszczeń zapewnia możliwość przyjmowania i obsługi interesantów chcących uzyskać informacje i fachowe doradztwo. Ponadto Biuro pozwala na archiwizowanie dokumentów oraz odpowiedni komfort pracy osobom zatrudnionym.
Biuro wyposażone jest w dostęp do internetu oraz sieci telefonicznej, posiada dostęp do wody bieżącej, a w zimę ogrzewane jest gazem. Pracownicy mają do dyspozycji pomieszczenia sanitarne oraz socjalne.
W biurze muszą być zatrudnione co najmniej 3 osoby na następujących stanowiskach:
- Dyrektor biura
- Specjalista ds. wdrażania Lokalnej Strategii Rozwoju i promocji
- Specjalista ds. wdrażania Lokalnej Strategii Rozwoju.
Wszystkie zatrudnione osoby posiadają bogate doświadczenie w zakresie wdrażania LSR. Osoby te były odpowiedzialne za realizację strategii w latach 2009 – 2015 i 2014 - 2023, poprawne funkcjonowanie biura pod kątem organizacyjnym i finansowym oraz działania organów Stowarzyszenia. Osoby zatrudnione w biurze mają doświadczenie i niezbędną wiedzę w zakresie wdrażania i aktualizacji strategii, rozliczania poniesionych kosztów w zakresie funkcjonowania LGD, wdrażania i rozliczania projektów współpracy oraz fachowego doradztwa na rzecz wnioskodawców i beneficjentów operacji dostępnych w ramach LSR. Dyrektor biura zatrudniony jest są w biurze LGD od 2012 roku, Specjalista ds. wdrażania Lokalnej Strategii Rozwoju i promocji od 2016 roku, natomiast Specjalista ds. wdrażania Lokalnej Strategii Rozwoju rozpocznie swoją pracę w 2024 r.

b) strategie i polityki stosowane w organizacji

Zasady funkcjonowania LGD reguluje **Statut Stowarzysze**nia oraz stosowne regulaminy:
- **Regulamin Zarządu**
- **Regulamin Rady**
- **Regulamin organizacyjny biura** Stowarzyszenia „Bursztynowy Pasaż"
Dodatkowym dokumentem mającym wpływ na pracę Stowarzyszenia jest Umowa o Warunkach i Sposobie Realizacji Strategii Rozwoju Lokalnego Kierowanego przez Społeczność nr 00006.UM11.6572.20001.2023 zawarta w dniu 24.01.2024 r. oraz odpowiednia Umowa o przyznaniu pomocy związana z Zarządzaniem LGD . LGD ma obowiązek stosowania się do wszystkich zawartych w umowach zapisów oraz pracy na podstawie dołączonych do umów harmonogramów i procedur.

c) potencjał ludzki w Zarządzie Stowarzyszenia oraz Radzie

Zarząd Stowarzyszenia składa się z osób o wieloletnim doświadczenie w kierowaniu organizacjami pozarządowymi oraz osobami fachowymi w dziedzinie funduszy europejskich, tworzenia i zarządzania procesami rozwoju na poziomie lokalnym oraz animowania i aktywizacji społeczności lokalnych.
Nie mniej niż trzech członków Zarządu, w tym Prezes lub Wiceprezes, posiada:
- przynajmniej dwuletnie doświadczenie w zakresie przygotowania i rozliczania projektów dofinansowanych ze środków Unii Europejskiej, w tym z Programu Rozwoju Obszarów Wiejskich na lata 2007 – 2013 i 2014-2020,
- przynajmniej dwuletnie doświadczenie w zarządzaniu organizacją pozarządową w randze członka, Wiceprezesa lub Prezesa Zarządu Stowarzyszenia lub Fundacji.
Nie mniej niż jeden członek Zarządu posiada przynajmniej dwuletnie doświadczenie w zakresie aktywizowania społeczności lokalnej poprzez działalność kulturalną, sportową lub rekreacyjną. Wymogi związane z doświadczeniem i kompetencjami członków Zarządu

uregulowane są w Regulaminie Zarządu Stowarzyszenia „Bursztynowy Pasaż" przyjętym przez Walne Zebranie Członków w dniu 14.06.2019 r.

Rada składa się z osób będących lokalnymi liderami i animatorami życia społecznego oraz mieszkańcami obszaru LGD. Stowarzyszenie „Bursztynowy Pasaż" stawia przed członkami ciała decyzyjnego konkretne zadania w związku z tym wymaga odpowiednich kwalifikacji i doświadczenia.
W składzie Rady:
a) wszyscy członkowie Rady posiadają udokumentowaną wiedzę z zakresu rozwoju obszarów wiejskich i Rozwoju Lokalnego Kierowanego przez Społeczność,
b) ponad połowę składu Rady stanowią osoby zameldowane na pobyt stały na obszarze objętym LSR przez okres co najmniej trzech lat,
c) co najmniej jedna osoba będąca członkiem Rady posiada udokumentowaną znajomość co najmniej jednego języka roboczego UE w stopniu umożliwiającym swobodne porozumiewanie się.
Stosowne wymogi dotyczące kompetencji i doświadczenia członków organu decyzyjnego zostały uregulowane regulaminie Rady, który określa zasady w sprawach związanych ze swoim wewnętrznym funkcjonowaniem w postaci uchwał, w tym planem szkoleń na dany okres programowania.

d) systemy obiegu informacji

Ręczny system obiegu informacji w LGD:
- urządzenie wejściowe: dokumenty w tradycyjnej formie
- procesor: kartki z poleceniami
- urządzenie do przechowywania danych: segregatory i szafy na dokumenty
- urządzenie wyjściowe: dokumenty sporządzane na komputerach i drukowane następnie na drukarkach oraz dokumenty wypełniane ręcznie (np. lista obecności, rejestr doradztw)
- system kontrolny: ręczne odszukiwanie, uzupełnianie, systematyzowanie i sprawdzanie posiadanych danych

System skomputeryzowany obiegu informacji w LGD:
- urządzenie wejściowe: skaner, klawiatura komputera, komputer
- procesor
- urządzenie do przechowywania danych: twarde dyski, płyty CD, DVD, pen drivy, dyski zewnętrzne
- urządzenie wyjściowe: wyświetlacze video, projektory, drukarki, inne komputery
- system kontrolny: programy wchodzące w skład pakietu Microsoft.

W Stowarzyszeniu „Bursztynowy Pasaż" występuje płaski (liniowy) system obiegu informacji, charakteryzujący się występowaniem niewielkiej liczba szczebli i małej ilości pracowników oraz członków organizacji. W związku z czym czas przepływu informacji w kierunku pionowym jest dość krótki oraz występuje mniejsze zniekształcenie przekazywanych informacji. Pracownicy biura otrzymują polecenia bezpośrednio od członków Zarządu oraz przewodniczących Rady oraz Komisji Rewizyjnej. Podjęte decyzje są następnie, za pośrednictwem odpowiednich kanałów komunikacji, przekazywane członkom Stowarzyszenia lub jego wnioskodawcom oraz przedsiębiorstwom tworzącym otoczenie zewnętrzne.

e) procesy podejmowania decyzji,

Podejmowanie decyzji to proces, którego celem jest dokonanie wyboru najlepszego rozwiązania. W Stowarzyszeniu „Bursztynowy Pasaż" został przyjęty następujący schemat podejmowania decyzji:

Etap w procesie podejmowania decyzji	Osoby odpowiedzialne za realizacje poszczególnych etapów
1. Analiza sytuacji - obejmuje zdefiniowanie problemu, ustalenie przyczyn problemu oraz określenie celów podjęcia decyzji)	Pracownicy biura LGD
2. Wyszukiwanie możliwych rozwiązań	Pracownicy biura LGD
Przekazanie zebranych materiałów Zarządowi LGD	
3. Ocena możliwych rozwiązań	Zarząd LGD
Ewentualna dyskusja z pracownikami biura LGD (szukanie dodatkowych rozwiązań, przeprowadzenie dodatkowych analiz itp…)	
4.Wybór najlepszego rozwiązania	Zarząd LGD
5. Wdrażanie podjętej decyzji	Pracownicy biura LGD
Rozpoczęcie procedury pozwalającej na wdrożenie podjętej decyzji w Stowarzyszeniu (w razie konieczności zwołanie zebrania Zarządu, Walnego Zebrania Członków lub Rady)	
6. Śledzenie skutków podjęcia decyzji	Pracownicy biura LGD

f) rola przywództwa w organizacji

Rolę przywództwa w LGD pełni Zarząd Stowarzyszenia. Biorąc pod uwagę fakt, iż członkowie Zarządu pracują równolegle w innych organizacjach, ich możliwość fizycznego, codziennego przebywania w biurze LGD jest ograniczona. Jednak przy wykorzystaniu elektronicznych kanałów komunikacji, kontakt pracowników biura z Zarządem jest ciągły i nie stanowi problemu w procesie podejmowania decyzji.

Warto zwrócić uwagę na fakt, że pracownicy biura również posiadają pewne cechy przywódcze (np. kreatywność, planowanie, organizacja pracy czy umiejętność przewodzenia przy realizacji projektów). Ale to Zarząd w pełni kontroluje procesy podejmowania decyzji i kierunki rozwoju Stowarzyszenia.

g) informacje dotyczące środowiska technologicznego i możliwości jego zmian (finansowych, technicznych, organizacyjnych)

Biuro Stowarzyszenia wyposażone jest w sprzęt komputerowy w pełni dostosowany do poziomu realizowanych w organizacji zadań oraz umożliwiający szybki kontakt pracowników biura zarówno z bezpośrednimi przełożonymi (Zarząd), członkami Stowarzyszenia jak i odbiorcami.

Nie ma żadnych przeciwskazań do rozwoju technologicznego LGD, jednak przy podejmowaniu decyzji o zakupie nowego sprzętu czy usługi o większych parametrach technicznych Stowarzyszenie kieruje się racjonalnością wydatku. Pracownicy biura wykazują się aktywnością w rozszerzaniu swojej wiedzy i pozyskiwaniu dodatkowych umiejętności, poprzez udział w szkoleniach i warsztatach tematycznych, dostosowując się tym samym do ciągłych zmian zachodzących w środowisku technologicznym otoczenia firmy.

h) normy i standardy przyjęte przez organizację (kultura organizacyjna)

Pracownicy Stowarzyszenia to ludzie wnoszący do firmy zaangażowanie, dynamikę i otwartości na zmiany. Cechują się oni zrozumieniem misji i strategii LGD oraz rozumieją główne cele funkcjonowania organizacji. Tym samym polepszenie sposobów działania i ewentualne przeformułowanie celów (o ile zajdzie taka potrzeba) nie stanowi większego problemu. Stosowanie jasnych zasad funkcjonowania oraz przejrzysta struktura organizacji umożliwia prowadzenie jednolitych sposobów pomiaru i kryteriów oceny efektów.

Pracownicy i członkowie Stowarzyszenia w porozumiewaniu się stosują wspólny aparat pojęciowy, co przyczynia się do unikania konfliktów oraz wyzwalania negatywnych emocji. Integracja członków organizacji odbywa się podczas codziennych kontaktów oraz zwoływanych zebrań. Pracownicy i członkowie nie wykazują potrzeby organizacji dodatkowych spotkań integracyjnych.

1.2 Szczegółowy opis przetwarzanych danych i ich klasyfikacja

AKTYWA:
I. PODSTAWOWE:

c) działania biznesowe (czynności związane z monitorowaniem i zarządzaniem procesami)

- działania monitorujące bieżącą działalność LGD:
    - monitorowanie pracy wykonywanej przez pracowników biurowych
    - monitorowanie poziomu realizacji LSR
    - monitorowanie zgodności wydatkowania środków pieniężnych z zatwierdzonym przez Walne
    - monitorowanie stanu i ilości posiadanych przez LGD środków majątkowych
    - monitorowanie poziomu wykonania harmonogramu szkoleń dla pracowników biura i członków Rady
    - monitorowanie poziomu realizacji harmonogramu ogłaszania konkursów
    - monitorowanie poziomu raportowania i rozliczania z Urzędem Marszałkowskim,
    - monitorowanie poziomu wykonywania harmonogramu realizacji projektów własnych
    - monitorowanie poziomu realizacji planu promocji i informacji
    - monitorowanie jakości usług świadczonych przez pracowników biura
    - monitorowanie legalności i prawomocności wdrażanych procedur decyzyjnych w LGD
- działania naprawcze eliminujące wynikłe na etapie monitorowania problemy (analiza przyczyn wystąpienia danego problemu, zaplanowanie działań mających na celu wyeliminowanie problemu oraz realizacja tych działań)
- działania monitorujące zmiany zachodzące na rynku funkcjonowania Stowarzyszenia występujące na płaszczyznach makro i mikrootoczenia LGD
- działania planujące, mające na celu wyznaczenie krótko i długofalowej polityki firmy

II. WSPIERAJĄCE:

L.p.	Kategoria aktywu	Aktywo	„Osoba odpowiedzialna za aktywo”
1	sprzęt	Urządzenia przetwarzające dane (3 zestawy komputerowe)	Pracownicy biura
2	sprzęt	Urządzenia przenośne (laptop, aparat fotograficzny, rzutnik, ekran)	Pracownicy biura
3	sprzęt	Urządzenia stacjonarne (drukarki, skanery, niszczarka do dokumentów, aparat telefoniczny, komputer stacjonarny)	Pracownicy biura
4	Sprzęt	Nośniki danych (pendrive’y, dysk przenośny, płyty CD i DVD)	Pracownicy biura
5	Sprzęt	Inne (szafki zamykane na klucz, szafki z „otwartymi pułkami”	Pracownicy biura
6	Sprzęt	Urządzenia: kontroler IDE ATA/ATAPI kontrolery uniwersalnej magistrali systemowej	Pracownicy biura
7	Sprzęt	Urządzenia: Porty (COM i LPT)	Pracownicy biura
8	Sprzęt	Stacja dysków CD-ROM / DVD	Pracownicy biura
9	Sprzęt	Nagrywarka CD / DVD	Pracownicy biura
10	Sprzęt	Urządzenie wejściowe Logitech	Pracownicy biura
11	Oprogramowanie	System operacyjny: Windows 7	Pracownicy biura
12	Oprogramowanie	Program antywirusowy	Pracownicy biura
13	Oprogramowanie	Narzędzia administracyjne	Pracownicy biura
14	Oprogramowanie	Zapora sieci Windows MC Afee	Pracownicy biura
15	Oprogramowanie	Microsoft, Acrobat, Adobe, GG, Google Chrome, Internet Explorer, Mozilla, Opera, 7-Zip, Adobe Photoshop CS6, LibreOffice, a) „Płatnik” (program ZUS), b) system księgowo-kadrowo-płacowy LEFTHAND, przelewy bankowe i międzybankowe – strony internetowe banków	Pracownicy biura
16	Sieć	Urządzenia (router do Wi-Fi)	Pracownicy biura + monitoring Wynajmującego + 1 laptop Wynajmującego
17	Sieć	Ruter brzegowy (brama sieciowa)	Pracownicy biura
18	Sieć	Usługi sieciowe (LAN lokalna sieć komputerowa + podłączenie kablem USB)	Pracownicy biura
19	Sieć	AP Wi-Fi	Pracownicy biura + monitoring Wynajmującego + 1 laptop

			Wynajmującego
20	Sieć	Interfejsy HID	Pracownicy biura
21	Personel	Kierownictwo	Zarząd – 3 osoby
22	Personel	Pracownicy	3 osoby
23	Personel	Administratorzy	(okazjonalnie, w przypadku wystąpienia potrzeby np. informatyk, instruktor BHP)
24	Siedziba	W budynku Hali Widowiskowo – Sportowej w Gniewinie (I piętro, osobne wejście, lokalizacja w centrum miejscowości)	Pracownicy biura

AKTYWA PODSTAWOWE					
L.p.	**Dane osobowe (kogo dotyczą)**	**Informacje**	**Proces**	**Osoby odpowiedzialne**	**Koszty utraty aktywów***
1	dane Stowarzyszenia „Bursztynowy Pasaż”	- informacje o zasobach i środkach LGD, słabe i mocne strony przedsiębiorstwa (w tym NIP, REGON, KRS, sprawozdania, podsumowania, raporty, umowy) - informacje na temat przepływu środków finansowych (dowody księgowe, wyciągi z konta, listy płac, potwierdzenia przelewu, bilanse, rachunki zysków i strat, plany finansowe itp.) - informacje na temat posiadanych środków majątkowych Stowarzyszenia (dokumentacja z inwentaryzacji) - informacje o przebiegu wdrażania Lokalnej Strategii Rozwoju oraz trudnościach i punktach krytycznych (raporty, sprawozdania, zdjęcia, dane finansowe i merytoryczne, itp.)	- realizacja Lokalnej Strategii Rozwoju - przetwarzanie danych o zasobach i środkach LGD (analiza danych, sporządzanie i prezentacja sprawozdań i raportów, przygotowywanie planów finansowych) - podejmowanie decyzji strategicznych dla Stowarzyszenia - procesy księgowe i skarbowe związane z działalnością Stowarzyszenia - inwentaryzowanie posiadanych przez LGD środków majątkowych	Zarząd Stowarzyszenia przy pomocy pracowników biura LGD	Odtworzenie aktywów - niskie Utrata reputacji organizacji - średnie Utrata poufności - średnie Możliwość nałożenia kary przez organ nadzorczy – nie występuje
2	pracowników biura	- dane osobowe pozyskane w procesie rekrutacji pracownika (CV, kserokopia dowodu, kserokopie dokumentów potwierdzających posiadane kwalifikacje, kserokopie świadectw pracy i listów motywacyjnych, itp.) - informacje na temat podnoszenia kwalifikacji przez pracowników biura LGD (np. certyfikaty, dyplomy, świadectwa itp.) - informacje pozyskane podczas wykonywania obowiązków służbowych (lista obecności, wnioski urlopowe, delegacje, dane finansowe dot. wynagrodzeń, itp.)	- podnoszenie wiedzy przez pracowników LGD (realizacja harmonogramu szkoleń) - przetwarzanie danych osobowych pracowników na cele działalności LGD - inwentaryzowanie posiadanych przez LGD środków majątkowych	Pracownicy biura	Odtworzenie aktywów - niskie Utrata reputacji organizacji – bardzo wysokie Utrata poufności – bardzo wysokie Możliwość nałożenia kary przez organ nadzorczy - niskie
3	- członków Zarządu, Rady	- informacje na temat podejmowanych decyzji przez organy decyzyjne Stowarzyszenia (uchwały Zarządu, uchwały Rady, zarządzenia Prezesa, protokoły, listy obecności, nr. kont bankowych, informacje o wykonywanej pracy (zajmowanych stanowiskach) oraz aktywności społecznej, itp.)	- przetwarzanie danych w celach realizacji zadań przypisanych do zajmowanego stanowiska	Pracownicy biura	Odtworzenie aktywów - niskie Utrata reputacji organizacji - średnie Utrata poufności - średnie Możliwość nałożenia kary przez organ nadzorczy - niskie
4	- członków	- informacje na temat podejmowanych decyzji (uchwały	- przetwarzanie danych kontaktowych	Pracownicy biura	Odtworzenie aktywów -

	zwyczajnych Stowarzyszenia	Walnego Zebrania Członków, uchwały Komisji Rewizyjnej, protokoły, listy obecności, dane osobowe zgromadzone podczas procesu rekrutacji: imię i nazwisko, adres, adres e-mail, nr tel. oraz (od członków pełniących funkcje zarządcze) kserokopia dowodu osobistego itp.	członków w celu realizacji zadań LGD		niskie Utrata reputacji organizacji - wysokie Utrata poufności - wysokie Możliwość nałożenia kary przez organ nadzorczy - niskie
5	- wnioskodawców w konkursach ogłaszanych w ramach naborów	- informacje na temat wnioskodawców i składanych projektów (na etapach: oceny przez Radę, oceny przez Urząd Marszałkowski, podpisania i realizacji umowy z Urzędem Marszałkowskim, kontroli oraz podsumowania realizacji projektu zarówno przez LGD jak i wnioskodawcę) np. imię i nazwisko, adres, adres e-mail, nr tel., kserokopia dowodu osobistego, ksera dokumentów wewnętrznych firm, nr konta bankowego, dane finansowe na temat projektu, przynależność do grupy defaworyzowanej, itp.	- przeprowadzanie konkursów w ramach naborów LGD	Pracownicy biura	Odtworzenie aktywów - średnie Utrata reputacji organizacji – bardzo wysokie Utrata poufności – bardzo wysokie Możliwość nałożenia kary przez organ nadzorczy - niskie
6	- uczestników konkursów, na które LGD pozyskało środki z zewnątrz	- informacje na temat projektów realizowanych w ramach konkursów, na które LGD pozyskało środki z zewnątrz (na wszystkich etapach) np. imię i nazwisko, adres, adres e-mail, nr tel., dane finansowe na temat projektu itp.	- przeprowadzenie konkursów, na które LGD pozyskało środki z zewnątrz	Pracownicy biura	Odtworzenie aktywów - średnie Utrata reputacji organizacji - wysokie Utrata poufności - średnie Możliwość nałożenia kary przez organ nadzorczy - niskie
7	- uczestników konkursów finansowanych ze środków własnych LGD	- informacje na temat projektów realizowanych w ramach konkursów, realizowanych przez LGD ze środków własnych (na wszystkich etapach) np. imię i nazwisko, adres, adres e-mail, nr tel., dane finansowe na temat projektu, zdjęcia, itp.)	- przeprowadzenie konkursów, które LGD realizuje ze środków własnych	Pracownicy biura	Odtworzenie aktywów - średnie Utrata reputacji organizacji - wysokie Utrata poufności - średnie

					Możliwość nałożenia kary przez organ nadzorczy - niskie
8	- sponsorów	- informacje na temat współpracy ze sponsorami np. nazwa i adres firmy, dane osób reprezentujących firmę, nr tel. adres e-mail, dane finansowe dot. współpracy, NIP, REGON, nr KRS, nr konta bankowego itp.)	- realizacja projektów współfinansowanych przez sponsorów	Zarząd Stowarzyszenia przy pomocy pracowników biura LGD	Odtworzenie aktywów - niskie Utrata reputacji organizacji – bardzo wysokie Utrata poufności - wysokie Możliwość nałożenia kary przez organ nadzorczy - niskie
9	- partnerów, z którymi LGD realizuje projekty współpracy	- informacje na temat przebiegu współpracy z partnerami przy realizacji projektów współpracy np. nazwa i adres partnera, dane osób reprezentujących firmę, nr tel. adres e-mail, dane finansowe, NIP, REGON, nr KRS, nr konta bankowego, upoważnienia, kserokopie dowodów osobistych, zdjęcia, itp.	- realizacja projektów współpracy	Zarząd Stowarzyszenia przy pomocy pracowników biura LGD	Odtworzenie aktywów - niskie Utrata reputacji organizacji - wysokie Utrata poufności - średnie Możliwość nałożenia kary przez organ nadzorczy - niskie
10	- przedsiębiorstwa, od których zakupuje produkty i usługi niezbędne do funkcjonowania biura i realizacji celów statutowych	- informacje na temat zamawianych produktów i usług (zapytania ofertowe, umowy, zlecenia, protokoły odbiorów itp.) np. nazwa i adres firmy, dane osób reprezentujących firmę, nr tel. adres e-mail, dane finansowe, NIP, REGON, nr KRS, nr konta bankowego itp.	- zakup produktów i usług niezbędnych do bieżącego funkcjonowania biura oraz realizacji Umowy Ramowej	Pracownicy biura	Odtworzenie aktywów - niskie Utrata reputacji organizacji - średnie Utrata poufności - niskie Możliwość nałożenia kary przez organ nadzorczy – nie występuje
11	- osoby prywatne i przedsiębiorstwa,	- informacje pozyskane od osób „doradzanych” takie jak imię i nazwisko, adres e-mail, nr tel., miejsce zamieszkania,	- udzielanie informacji na temat świadczonych w LGD usług osobom	Pracownicy biura	Odtworzenie aktywów - niskie Utrata reputacji

	którym LGD świadczy usługi doradcze (na podstawie karty doradztw)	przynależność do grupy defaworyzowanej, (karta doradztw), itp.	zainteresowanym		organizacji - niskie Utrata poufności - niskie Możliwość nałożenia kary przez organ nadzorczy – nie występuje
12	- uczestników szkoleń i spotkań informacyjnych organizowanych przez LGD	- informacje pozyskane od osób uczestniczących w szkoleniach i spotkaniach informacyjnych organizowanych przez LGD (np. ankiety, listy obecności, zdjęcia, przynależność do grupy defaworyzowanej)	- organizacja szkoleń i spotkań informacyjnych skierowanych do rynku odbiorców LGD	Pracownicy biura	Odtworzenie aktywów - średnie Utrata reputacji organizacji - średnie Utrata poufności - niskie Możliwość nałożenia kary przez organ nadzorczy - nie występuje

* Skala kosztów utraty aktywów (wyjaśnienie):
a) koszty związane z odtworzeniem aktywów (bardzo niskie, niskie, średnie, wysokie, bardzo wysokie)
b) koszty utraty reputacji organizacji (bardzo niskie, niskie, średnie, wysokie, bardzo wysokie)
c) koszty związane z utratą dostępności danych (bardzo niskie, niskie, średnie, wysokie, bardzo wysokie)
d) koszty związane z utratą poufności (bardzo niskie, niskie, średnie, wysokie, bardzo wysokie)
e) możliwość nałożenia kary przez organ nadzorczy (UM) (bardzo niskie, niskie, średnie, wysokie, bardzo wysokie)

1.3 Szczegółowy opis stosowanych zabezpieczeń i innych ograniczeń w LGD
oraz kreślenie kryteriów akceptacji ryzyka wraz z przypisaniem poziomu podatności danych zasobów na opisane zagrożenia.

Podatność zasobów (aktywów wyszczególnionych w 1.2 niniejszego opracowania) na wystąpienie określonych zagrożeń określa łatwość wyrządzenia szkody dla wskazanego zasobu w kontekście utraty poufności, integralności i dostępności. Oszacowanie poziomów podatności na podstawie przeprowadzonego poniżej rozpoznania środowiskowego i analizy „czarnych scenariuszy", dokonano w skali 0-8 wg następujących wytycznych:

Poziomy podatności zasobów na zagrożenia		
L.p.	Poziom podatności	Zakres wartości
1	Brak	0

2	Niski	1-2
3	Średni	3-4
4	Wysoki	5-6
5	Bardzo wysoki	7-8

Podział zabezpieczeń z uwzględnieniem poszczególnych rodzajów zagrożeń:

Zagrożenie	Opis stosowanego zabezpieczenia	Poziom podatności na wystąpienie zagrożenia
ZAGROŻENIA ORGANIZACYJNE		
nieuprawniony dostęp do pomieszczenia, w którym przechowywane są dane osobowe, przez pracowników podmiotu, od którego LGD wynajmuje pomieszczenia biurowe	przetrzymywanie ważnych dokumentów LGD w szafkach i szufladach zamykanych na klucz	2
brak kontroli nad dokumentami na stanowisku pracy	wytyczne zawarte w zakresie obowiązków pracownika	2
brak mechanizmów uniemożliwiających skasowanie lub zmianę haseł dostępu przez administratora lub innego użytkownika	wytyczne zawarte w zakresie obowiązków pracownika	4
zła organizacja pracy	wytyczne zawarte w zakresie obowiązków pracownika oraz Regulaminie Organizacyjnym Stowarzyszenia	2
choroba ważnych w firmie osób i nieuprawnione zastępstwo	procedury zawarte w Statucie i Regulaminie Organizacyjnym Stowarzyszenia	2
epidemia kadry i brak kompetentnych i zaufanych osób upoważnionych do dostępu do danych osobowych	procedury zawarte w Statucie i Regulaminie Organizacyjnym Stowarzyszenia	4
utrata kluczowych pracowników	procedury zawarte w Statucie i Regulaminie Organizacyjnym Stowarzyszenia	4
niedobór pracowników	procedury zawarte w Statucie i Regulaminie Organizacyjnym Stowarzyszenia	2
brak możliwości rozliczania działań użytkowników – brak kontroli nad dostępem do przetwarzania danych	wytyczne zawarte w zakresie obowiązków pracownika oraz Regulaminie Organizacyjnym Stowarzyszenia	2
niestosowanie się do instrukcji bezpiecznej eksploatacji programów i urządzeń	procedury zawarte w Regulaminie Organizacyjnym Stowarzyszenia	2
ZAGROŻENIA PERSONALNE		
ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura	wytyczne zawarte w zakresie obowiązków pracownika oraz	2
nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik przez pracowników biura	wytyczne zawarte w zakresie obowiązków pracownika oraz w umowie o pracę	2
utrata / zagubienie nośnika zawierającego dane osobowe	wytyczne zawarte w zakresie obowiązków pracownika oraz w umowie o pracę	2
nieuprawnione wyniesienie danych osobowych	wytyczne zawarte w zakresie	2

zawartych na nośniku elektronicznym	obowiązków pracownika oraz w umowie o pracę	
błędy i pomyłki użytkowników	wytyczne zawarte w zakresie obowiązków pracownika oraz w umowie o pracę	4
błędy i pomyłki administratorów	wytyczne zawarte w zakresie obowiązków pracownika oraz w umowie o pracę	4
zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych	wytyczne zawarte w zakresie obowiązków pracownika oraz w umowie o pracę	4
wyłudzenie danych	Kodeks Karny	1
podszycie się pod uprawnionego pracownika	Kodeks Karny	1
stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od pracowników firmy	Kodeks Karny	0
dostęp nieuprawnionych użytkowników do informacji prezentowanej na ekranie stanowiska komputerowego	odpowiednie ustawienie ekranu względem osób wchodzących do biura, zastosowanie wygaszaczy ekranu zabezpieczonych hasłem dostępu	1
zaniedbania ze strony personelu obsługującego proces przetwarzania danych	wytyczne zawarte w zakresie obowiązków pracownika oraz w umowie o pracę	2
utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych i pogwarancyjnych sprzętu oraz czynności konserwujących	brak wytycznych	6
odczytanie informacji z nośników przewidzianych do naprawy	brak wytycznych	6
zapisywanie informacji niejawnych na prywatne nośniki pracownika	wytyczne zawarte w zakresie obowiązków pracownika oraz w umowie o pracę	0
przypadkowa zmiana ustawień konfiguracyjnych	brak wytycznych	3
wykorzystanie błędów w obiegu dokumentów w firmie	wytyczne zawarte w zakresie obowiązków pracownika oraz Regulaminie Organizacyjnym Stowarzyszenia	1
wykorzystanie zużytych materiałów – wydruków lub dyskietek zamiast ich niszczenia	brak wytycznych	0
ZAGROŻENIA TECHNICZNE		
błędy oprogramowania lub sprzętu	wytyczne zawarte w zakresie obowiązków pracownika oraz Regulaminie Organizacyjnym Stowarzyszenia	3
wadliwe działanie systemu operacyjnego		3
wirus		4
nielegalne użycie oprogramowania	brak wytycznych	1
uszkodzenie sprzętu i oprogramowania podczas wykonywania naprawy i konserwacji	brak wytycznych	3

przez niewyszkolonych pracowników		
wykorzystanie pozostawionych niedokończonych fragmentów tworzonych dokumentów w pamięci RAM	brak wytycznych	2
podglądanie ekranu monitora przez użytkowników z innych komputerów	brak wytycznych	3
ZAGROŻENIA FIZYCZNE		
klęska żywiołowa, w wyniku której utracono poufność danych osobowych (np. pożar)	brak szczegółowych wytycznych (usuwanie skutków w porozumieniu z wynajmującym)	2
włamanie, w wyniku którego utracono dane osobowe	brak szczegółowych wytycznych (usuwanie skutków w porozumieniu z wynajmującym i policją)	2
włamanie z wandalizmem, w wyniku którego utracono poufność danych osobowych	brak szczegółowych wytycznych (usuwanie skutków w porozumieniu z wynajmującym i policją)	4
starzenie się sprzętu w wyniku którego zostają utracone dane osobowe	brak wytycznych	5
awaria systemu wodociągowego i kanalizacyjnego (zalanie pomieszczeń biurowych wodą)	brak szczegółowych wytycznych (usuwanie awarii w porozumieniu z wynajmującym)	2
zmiany napięcia w sieci oraz przerwa w dostarczaniu prądu	brak wytycznych	2
brak systemu alarmowego w budynku	instalacja systemu monitoringowego na zewnątrz budynku przez wynajmującego	4

Etap 2
Mechanizmy kontrolne

Ta część opracowania ma na celu opisanie i identyfikację zastosowanych w Stowarzyszeniu „Bursztynowy Pasaż" środków bezpieczeństwa i mechanizmów kontrolnych przyczyniających się do spełnienia wymagań biznesowych, prawnych i innych ograniczeń dla procesów przetwarzania danych, w tym danych osobowych.

2.1 Identyfikacja wymagań dla procesów przetwarzania danych w kontekście konkretnych celów działalności Stowarzyszenia „Bursztynowy Pasaż"

Głównym celem tego etapu jest sprawdzenie, czy w każdym procesie przetwarzania danych, dane osobowe są przetwarzane zgodnie z zasadami opisanymi w art. 5 RODO, na podstawie jednej z przesłanek wskazanych w art. 6 RODO oraz przy zapewnieniu osobom, których dane dotyczą, możliwości realizowania ich praw wskazanych w art. 12-22 RODO.

Fragment** **ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. do którego będzie się bezpośrednio odnosił etap 2 niniejszego opracowania.

Artykuł 5
Zasady dotyczące przetwarzania danych osobowych

1.Dane osobowe muszą być:
a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność”).

2.Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

Artykuł 6 Zgodność przetwarzania z prawem

1.Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:
a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

(…)

Artykuł 7
Warunki wyrażenia zgody

1.Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
2.Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.
3.Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
4.Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

L.p.	Dane osobowe (kogo dotyczą)	Proces	Cel przetwarzania danych wraz z odpowiednią do tego celu podstawą prawną przetwarzania danych	Wymagania dot. przejrzystości informacji udzielanych osobom, których dane dotyczą, na temat ułatwiania wykonywania ich praw	Zakres danych niezbędny do realizacji celu	Częstotliwość zbierania danych	Źródła i sposób pozyskiwania danych	Jakość przetwarzania danych (weryfikacja tej jakości)	Czas przetwarzania danych osobowych	Sposób postępowania z danymi / usunięcia danych po osiągnięciu celu
1	dane Stowarzyszenia „Bursztynowy Pasaż”	1.1 przetwarzanie danych o zasobach i środkach LGD (analiza danych, sporządzanie i prezentacja sprawozdań oraz raportów, przygotowywanie planów finansowych)	- realizacja założeń Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. a), b), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- podpisanie oświadczeń dot. przetwarzania danych osobowych przez strony podejmujące współprace - zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	NIP, REGON, KRS, adres zameldowania lub siedziby firmy, imię i nazwisko (nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy), nr tel., adres e-mail; od osób reprezentujących podmiot (nr i seria dowodu tożsamości); sprawozdania, podsumowania, raporty, umowy, zdjęcia, dane finansowe i merytoryczne, itp. zarówno LGD jak i podmiotów współpracujących (wartości netto i brutto, ceny netto i brutto, wartości rabatów i upustów, nazwy banków i nr kont bankowych, forma i termin płatności, kwoty zadłużenia, daty rozpoczęcia i zakończenia współpracy, wartości dofinansowania)	- jednorazowo na początku podejmowania współpracy - ewentualna aktualizacja danych przy przedłużaniu współpracy lub na specjalne żądanie podmiotu	Bezpośrednio od podmiotu (dane dostarczone w wersji papierowej lub elektronicznej za pośrednictwem poczty elektronicznej)	- bieżąca aktualizacja danych osobowych podmiotu , - zgodność z art. 5 pkt. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania umowy / współpracy / działalności firmy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]
		1.2 podejmowanie decyzji strategicznych dla Stowarzyszenia	- realizacja założeń Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. a), b), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	j.w.	- jednorazowo na początku podejmowania współpracy - w razie potrzeby np. na prośbę Zarządu przez Walnym Spotkaniem Członków Stowarzyszenia	- bezpośrednio od podmiotu - ze źródeł ogólnodostępnych (np. internet) (dane dostarczone w wersji papierowej lub elektronicznej za pośrednictwem poczty elektronicznej)	- bieżąca aktualizacja danych osobowych podmiotu , - zgodność z art. 5 pkt. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania umowy / współpracy lub do momentu dezaktualizacji danych z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]
		1.3 procesy księgowe i skarbowe związane z działalnością Stowarzyszenia	- realizacja założeń Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. b), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	-dowody księgowe, wyciągi z konta, listy płac, potwierdzenia przelewu, bilanse, rachunki zysków i strat, plany finansowe itp. - wartości netto i brutto, ceny netto i brutto, wartości rabatów i upustów, nazwy banków i nr kont bankowych, forma i termin płatności, kwoty zadłużenia, daty rozpoczęcia i zakończenia współpracy, wartości dofinansowania, NIP, PESEL, adres zameldowania lub prowadzenia działalności	- w okresach rozliczeniowych określonych przepisami prawa - w razie potrzeby np. na prośbę Zarządu przez Walnym Spotkaniem Członków Stowarzyszenia	- bezpośrednio od podmiotu lub z dokumentów finansowych LGD	- bieżąca aktualizacja danych osobowych podmiotu , - zgodność z art. 5 pkt. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania umowy / współpracy lub do momentu dezaktualizacji danych z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]
		1.4 inwentaryzowanie posiadanych przez LGD środków majątkowych	- realizacja założeń Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- informacje na temat posiadanych środków majątkowych Stowarzyszenia (dokumentacja z inwentaryzacji) wraz z wglądem do całej dokumentacji finansowej i merytorycznej LGD (dane j.w.)	- w okresach rozliczeniowych określonych przepisami prawa - w razie potrzeby np. na prośbę Zarządu	- bezpośrednio od podmiotu lub z dokumentów finansowych i merytorycznych LGD	- bieżąca aktualizacja danych osobowych podmiotu , - zgodność z	- do końca trwania umowy / współpracy lub do momentu dezaktualizacji danych z	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]

			przetwarzania danych: - art. 6 pkt. b), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.					art. 5 pkt. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	przedłużeniem o okres archiwizacji	
2	dane pracowników biura	2.1 rekrutacja pracowników	- realizacja wszystkich założeń Statutu LGD[1],LSR[2] będącej załącznikiem do Umowy Ramowej[3] oraz Regulaminu Biura LGD[4] - zgodnie z załącznikiem nr 1 Regulaminu Biura LGD[4] - art. 6 pkt. a) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- podpisanie oświadczeń dot. przetwarzania danych osobowych - zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- dane osobowe pozyskane w procesie rekrutacji pracownika: CV, kserokopia dowodu, kserokopie dokumentów potwierdzających posiadane kwalifikacje, kserokopie świadectw pracy i listów motywacyjnych, itp. (imię, nazwisko, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, nr tel., adres e-mail; nr i seria dowodu tożsamości, zdjęcie z wizerunkiem pracownika, NIP, PESEL, płeć)	- jednorazowo przy składaniu dokumentacji aplikacyjnej	- bezpośrednio od aplikanta	- bieżąca aktualizacja danych osobowych podmiotu , - zgodność z art. 5 pkt. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca prowadzenia procesu rekrutacyjnego - dla osób zatrudnionych w wyniku prowadzonej rekrutacji: do końca trwania umowy / współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3] - wg Kodeksu pracy (archiwizacja przez 50 lat)
		2.2 przetwarzanie danych osobowych na cele działalności statutowej LGD	- realizacja wszystkich założeń Statutu LGD[1],LSR[2] będącej załącznikiem do Umowy Ramowej[3] oraz Regulaminu Biura LGD[4] Podstawa prawna przetwarzania danych: - art. 6 pkt. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- podpisanie oświadczeń dot. przetwarzania danych osobowych przez strony podejmujące współpracę, - zawarcie umowy o pracę - zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	imię, nazwisko, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, nr tel., adres e-mail; nr i seria dowodu tożsamości, zdjęcie z wizerunkiem pracownika, NIP, PESEL, wartości netto i brutto wynagrodzeń, nagród i premii, płeć	- jednorazowo na początku podejmowania współpracy - ewentualna aktualizacja danych przy przedłużaniu współpracy lub na specjalne żądanie pracownika	- bezpośrednio od pracownika	- bieżąca aktualizacja danych osobowych podmiotu , - zgodność z art. 5 pkt. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania umowy / współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3] - wg Kodeksu pracy (archiwizacja przez 50 lat)
		2.3 podnoszenie wiedzy przez pracowników LGD (realizacja harmonogramu szkoleń)	- realizacja założeń §13 Regulaminu Biura LGD[4] - art. 6 pkt. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- informacje na temat podnoszenia kwalifikacji przez pracowników biura LGD np. certyfikaty, dyplomy, świadectwa itp. (imię i nazwisko, nazwa zajmowanego stanowiska, płeć)	- jednorazowo na początku podejmowania współpracy - ewentualna aktualizacja danych przy przedłużaniu współpracy lub na specjalne żądanie pracownika	- bezpośrednio od pracowników	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania umowy / współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3] - wg Kodeksu pracy (archiwizacja przez 50 lat)
		2.4 wykonywanie obowiązków służbowych przez pracowników biura	- realizacja założeń Regulaminu Biura LGD[4] oraz 21-31 Statutu LGD[1] - art. 6 pkt. b) Rozporządzenia	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27	lista obecności, delegacje, dane finansowe dot. wynagrodzeń, premii, nagród itp. (imię i nazwisko, nazwa zajmowanego stanowiska, wartości netto i brutto wynagrodzeń, nagród i premii)	- jednorazowo na początku podejmowania współpracy - ewentualna	- bezpośrednio od pracowników	- bieżąca aktualizacja danych osobowych , - zgodność z	- do końca trwania umowy / współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w

			Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	kwietnia 2016 r.		aktualizacja danych przy przedłużaniu współpracy lub na specjalne żądanie pracownika		art. 5 pkt. d) Rozporządzeni a Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.		Umowie Ramowej[3] - wg Kodeksu pracy (archiwizacja przez 50 lat)
		2.5 przerwy w wykonywaniu obowiązków służbowych pracowników	- realizacja założeń §20-21 Regulaminu Biura LGD[4] - art. 6 pkt. a), b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	zwolnienia i zaświadczenia lekarskie, wnioski urlopowe itp. (imię, nazwisko, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, nr i seria dowodu tożsamości, NIP, PESEL, wartości netto i brutto wynagrodzeń, powód przerwy w wykonywaniu obowiązków służbowych)	- każdorazowo w chwili wystąpienia potrzeby przerwy w wykonywaniu obowiązków służbowych Pracownika (kilka razy w miesiącu)	- bezpośrednio od pracowników	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzeni a Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania umowy / współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3] - wg Kodeksu pracy (archiwizacja przez 50 lat)
		2.6 zakończenie współpracy	- realizacja założeń Regulaminu Biura LGD[4] oraz §21-31 Statutu LGD[1] zgodnie z poszczególnymi umowami o pracę - art. 6 pkt. b) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	dokumenty podające przyczynę ustania stosunku pracy np. wypowiedzenie; świadectwa pracy (imię i nazwisko, imiona rodziców, data i miejsce urodzenia, PESEL, okres zatrudnienia, przyczyna ustania stosunku pracy)	- jednorazowo w chwili ustania stosunku pracy	- bezpośrednio od pracowników z dokumentów aplikacyjnych posiadanych w firmie	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzeni a Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania umowy / współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3] - wg Kodeksu pracy (archiwizacja przez 50 lat)
3	dane członków Zarządu, Rady, członków Komisji Rewizyjnej	3.1 przetwarzanie danych w celach realizacji zadań przypisanych do zajmowanego stanowiska oraz przestrzeganie wytycznych Umowy Ramowej[3]	- realizacja założeń Regulaminu Biura LGD[4] oraz §21-36 Statutu LGD[1] - art. 6 pkt. a), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	imię, nazwisko, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, nr i seria dowodu tożsamości, NIP, PESEL, REGON, nr KRS, wartości netto i brutto wynagrodzeń, nazwy banków i nr kont bankowych, nr tel., e-mail	- każdorazowo w przypadku zaistnienia potrzeby (od kilku do kilkunastu razy w miesiącu)	- bezpośrednio od podmiotu	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzeni a Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania umowy / współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3] - wg Kodeksu pracy (archiwizacja przez 50 lat)

4	dane członków zwyczajnych Stowarzyszenia	4.1 przetwarzanie danych członków w celu realizacji zadań statutowych Stowarzyszenia	- realizacja założeń §11-20 Statutu LGD[1] - art. 6 pkt. a), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- dane osobowe zebrane w chwili przystąpienia do Stowarzyszenia (imię, nazwisko, nazwa firmy, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, nr i seria dowodu tożsamości, nr tel., e-mail,) - dodatkowe dane osobowe niezbędne do pełnienia dodatkowych funkcji w Stowarzyszeniu (nazwa pracodawcy, nazwa stanowiska, nazwa banku i nr konta bankowego, NIP, PESEL, kwoty netto i brutto wynagrodzeń)	- jednorazowo w przypadku przystąpienia do LGD - jednorazowo w przypadku objęcia stanowiska - bieżąca aktualizacja danych w chwili zaistnienia potrzeby (1-3 razy w miesiącu)	- bezpośrednio od członka Stowarzyszenia	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania umowy / współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]
5	dane wnioskodawców w konkursach ogłaszanych w ramach naborów LGD	5.1 przeprowadzanie konkursów w ramach naborów LGD	- realizacja założeń Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. a), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- informacje na temat wnioskodawców i składanych projektów na etapach: oceny przez, oceny przez Urząd Marszałkowski, podpisania i realizacji umowy z Urzędem Marszałkowskim, kontroli oraz podsumowania realizacji projektu zarówno przez LGD jak i wnioskodawcę (imię i nazwisko, nazwa firmy, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, nr i seria dowodu tożsamości, adres e-mail, nr tel., kserokopia dowodu osobistego, seria i nr dowodu lub innego dokumentu potwierdzającego tożsamość, NIP, PESEL, REGON, nr KRS, nazwa banku i nr konta bankowego, przynależność do grupy defaworyzowanej, przychód i dochód firmy, data i miejsce urodzenia, kwota netto i brutto dofinansowania, wartość projektu)	- jednorazowo w przypadku złożenia wniosku o dofinansowanie projektu - bieżąca aktualizacja danych w chwili zaistnienia potrzeby (1-2 razy w miesiącu)	- bezpośrednio od wnioskodawców	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]
6	dane uczestników konkursów, na które LGD pozyskało środki z zewnątrz	6.1 przeprowadzenie konkursów, na które LGD pozyskało środki z zewnątrz	- realizacja założeń §7-10 Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. a), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	informacje na temat projektów realizowanych w ramach konkursów, na które LGD pozyskało środki z zewnątrz (na wszystkich etapach) (imię i nazwisko, nazwa firmy, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, nr i seria dowodu tożsamości, adres e-mail, nr tel., seria i nr dowodu lub innego dokumentu potwierdzającego tożsamość, NIP, PESEL, REGON, nr KRS, nazwa banku i nr konta bankowego, przynależność do grupy defaworyzowanej, przychód i dochód firmy, data i miejsce urodzenia, kwota netto i brutto dofinansowania, wartość projektu	- jednorazowo w przypadku złożenia deklaracji udziału w konkursie - bieżąca aktualizacja danych w chwili zaistnienia potrzeby (1-2 razy w miesiącu)	- bezpośrednio od uczestników konkursu	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]

7	dane uczestników konkursów finansowanych ze środków własnych LGD	7.1 przeprowadzenie konkursów, które LGD realizuje ze środków własnych	- realizacja założeń §7-10 Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. a), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	informacje na temat projektów realizowanych w ramach konkursów na wszystkich jego etapach) (imię i nazwisko, nazwa firmy, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, nr i seria dowodu tożsamości, adres e-mail, nr te..l, seria i nr dowodu lub innego dokumentu potwierdzającego tożsamość, NIP, PESEL, REGON, nr KRS, nazwa banku i nr konta bankowego, przynależność do grupy defaworyzowanej, przychód i dochód firmy, data i miejsce urodzenia, kwota netto i brutto dofinansowania, wartość projektu	- jednorazowo w przypadku złożenia deklaracji udziału w konkursie - bieżąca aktualizacja danych w chwili zaistnienia potrzeby (1-2 razy w miesiącu)	- bezpośrednio od uczestników konkursu	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzeni a Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]
8	dane sponsorów	8.1 realizacja projektów współfinansowanych przez sponsorów	- realizacja założeń §7-10 Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. a), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- informacje na temat współpracy ze sponsorami np. imię i nazwisko, nazwa firmy, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, nr i seria dowodu tożsamości, adres e-mail, nr tel., seria i nr dowodu lub innego dokumentu potwierdzającego tożsamość, NIP, PESEL, REGON, nr KRS, nazwa banku i nr konta bankowego	- jednorazowo w przypadku podjęcia współpracy - bieżąca aktualizacja danych w chwili zaistnienia potrzeby (1-2 razy w roku)	- bezpośrednio od sponsorów	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzeni a Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]
9	dane partnerów, z którymi LGD realizuje projekty współpracy	9.1 realizacja projektów współpracy	- realizacja założeń §7-10 Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. a), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- informacje na temat przebiegu współpracy z partnerami przy realizacji projektów współpracy imię i nazwisko, nazwa firmy, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, nr i seria dowodu tożsamości, adres e-mail, nr tel., seria i nr dowodu lub innego dokumentu potwierdzającego tożsamość, NIP, PESEL, REGON, nr KRS, nazwa banku i nr konta bankowego, kserokopia dowodu osobistego, wizerunek,	- jednorazowo w przypadku podjęcia współpracy - bieżąca aktualizacja danych w chwili zaistnienia potrzeby (1-2 razy w roku)	- bezpośrednio od partnerów	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzeni a Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]
10	dane przedsiębiorstw, od których LGD zakupuje produkty i usługi niezbędne do funkcjonowania biura i realizacji celów statutowych	10.1 zakup produktów i usług niezbędnych do bieżącego funkcjonowania biura oraz realizacji Umowy Ramowej [3]	- realizacja założeń §7-10 Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. a), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	informacje na temat zamawianych produktów i usług: zapytania ofertowe, umowy, zlecenia, protokoły odbiorów itp. (nazwa firmy, imię i nazwisko, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, adres e-mail, nr tel., NIP, REGON, nr KRS, nazwa banku i nr konta bankowego, wartość netto i brutto ofert handlowej, nr i seria dowodu tożsamości)	- jednorazowo w przypadku podjęcia współpracy - bieżąca aktualizacja danych w chwili zaistnienia potrzeby (1-2 razy w roku)	- bezpośrednio od partnerów	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzeni a Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania współpracy z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]

11	dane osób prywatny i przedsiębiorstw, którym LGD świadczy usługi doradcze (na podstawie karty doradztw)	11.1 udzielanie informacji na temat usług świadczonych w LGD podmiotom zainteresowanym	- realizacja założeń §7-10 Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. a), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- informacje pozyskane od osób „doradzanych” nazwa firmy, imię i nazwisko, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, adres e-mail, nr tel., przynależność do grupy defaworyzowanej,	- jednorazowo w chwili udzielania doradztwa	- bezpośrednio od osób, którym świadczone jest doradztwo	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzeni a Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania współpracy / projektu, z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]
12	dane uczestników szkoleń i spotkań informacyjnych organizowanych przez LGD	12.1 organizacja szkoleń i spotkań informacyjnych skierowanych do rynku odbiorców LGD	- realizacja założeń §7-10 Statutu LGD[1] oraz LSR[2] będącej załącznikiem do Umowy Ramowej[3] Podstawa prawna przetwarzania danych: - art. 6 pkt. a), c) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- zgodność z art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- informacje pozyskane od osób uczestniczących w szkoleniach i spotkaniach informacyjnych organizowanych przez LGD nazwa firmy, imię i nazwisko, nazwa miasta i ulicy, nr domu, klatki, mieszkania, kod pocztowy, adres e-mail, nr tel., przynależność do grupy defaworyzowanej,	- jednorazowo w chwili udziału szkolenia	- bezpośrednio od uczestników szkolenia	- bieżąca aktualizacja danych osobowych , - zgodność z art. 5 pkt. d) Rozporządzeni a Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.	- do końca trwania współpracy / projektu, z przedłużeniem o okres archiwizacji	- dane zostają zarchiwizowane, a następnie usunięte / zniszczone po okresie wskazanym w Umowie Ramowej[3]

1. LSR – dokładna nazwa: Lokalna Strategia Rozwoju na lata 2016-2023 Stowarzyszenia „Bursztynowy Pasaż” Lokalna Grupa Działania
2. Statut LGD – dokładna nazwa dokumentu: Statut Stowarzyszenia "Bursztynowy Pasaż" z dnia 15.05.2023r.
3. Umowa Ramowa – dokładna nazwa dokumentu: Umowa o warunkach i sposobie realizacji Strategii Rozwoju Lokalnego Kierowanego Przez Społeczność nr. 00006.UM11.6572.20001.2023 zawarta w dniu 24.01.2024 r. w Gdańsku
4. Regulamin organizacyjny biura Stowarzyszenia „Bursztynowy Pasaż

2.2 Wymagania dotyczące zastosowania środków kontroli i bezpieczeństwa oraz stopień ich wypełnienia

Rozdział dotyczy wymagań w zakresie kontroli przetwarzania poszczególnych danych osobowych wraz z oszacowaniem poziomu podatności tych zasobów na wystąpienie zagrożenia w postaci niedozwolonego lub niezgodnego z prawem przetwarzania oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

Zasoby / dane osobowe	Poziom podatności zasobów na zagrożenia	Potrzeba przeprowadzenia oceny skutków dla ochrony danych (w przypadku naruszenia ich integralności)
dane Stowarzyszenia „Bursztynowy Pasaż”	1	nie występuje
dane pracowników biura	1	nie występuje
dane członków Zarządu, Rady, członków Komisji Rewizyjnej	2	nie występuje
dane członków zwyczajnych Stowarzyszenia	0	nie występuje
dane wnioskodawców w konkursach ogłaszanych w ramach naborów LGD	4	nie występuje
dane uczestników konkursów, na które LGD pozyskało środki z zewnątrz	2	nie występuje
dane uczestników konkursów finansowanych ze środków własnych LGD	2	nie występuje
dane sponsorów	1	nie występuje
dane partnerów, z którymi LGD realizuje projekty współpracy	0	nie występuje
dane przedsiębiorstw, od których LGD zakupuje produkty i usługi niezbędne do funkcjonowania biura i realizacji celów statutowych	0	nie występuje
dane osób prywatny i przedsiębiorstw, którym LGD świadczy usługi doradcze (na podstawie karty doradztw)	0	nie występuje
dane uczestników szkoleń i spotkań informacyjnych organizowanych przez LGD	0	nie występuje

Poziomy podatności zasobów na zagrożenia		
L.p.	Poziom podatności	Zakres wartości
1	Brak	0
2	Niski	1-2
3	Średni	3-4
4	Wysoki	5-6
5	Bardzo wysoki	7-8

Z powyższych analiz wynika, że ryzyko podatności zasobów danych osobowych przetwarzanych w Stowarzyszeniu „Bursztynowy Pasaż” występuje na poziomie niskim

lub średnim (w 1 przypadku). Dlatego nie ma potrzeby przeprowadzania oceny skutków dla ochrony danych oraz przeprowadzania konsultacji z organem nadzorczym, o których mowa w art. 35 RODO.

Etap 3 i 4
Szacowanie ryzyka oraz postępowanie z ryzykiem - decyzja

Szacowanie ryzyka ma na celu określenie, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i jak dotkliwe straty mogą powstać.
Przeprowadzając ewaluację ryzyka w Stowarzyszeniu „Bursztynowy Pasaż" zastosowano metodę burzy mózgów.

Przy szacowaniu podatności na urzeczywistnienie się określonych zagrożeń wzięto pod uwagę następujące czynniki:
- atrakcyjność aktywu (danych osobowych)
- czynniki środowiskowe
- istniejące zabezpieczenia
- rodzaj podatności
- statystyki dotyczące występowania takich samych lub podobnych zdarzeń w przeszłości.

Skutki urzeczywistnienia się danego zagrożenia mogą mieć dwojaki charakter: materialny (np. koszty odtworzenia danego aktywu) oraz niematerialny (utrata dobrego wizerunku firmy, wpływ ujawnienia danych na pozycję społeczną osoby, której dotyczą).
W poniższym opracowaniu przyjęto następującą skalę opisującą poziom (wielkość) skutków urzeczywistnienia się danego zagrożenia:
- **poziom 1** – **bardzo niski** skutek (brak wpływu na reputację, niewielkie straty finansowe / materialne – poniżej 500 zł)
- **poziom 2** – **niski** skutek (negatywne opinie o LGD ale o zasięgu lokalnym i bez udziału mediów, straty finansowe / materialne – w zakresie 500 – 1000 zł)
-- **poziom 3** – **średni** skutek (negatywne opinie o LGD o zasięgu lokalnym, ale bez udziału mediów lokalnych, wszczęcie procedury kontrolnej przez organ nadzorczy (UM), straty finansowe / materialne – w zakresie 1000 – 5000 zł)
- **poziom 4** – **wysoki** skutek (negatywne opinie o LGD o zasięgu regionalnym z udziałem mediów lokalnych, wszczęcie procedury kontrolnej przez organ nadzorczy (UM), straty finansowe / materialne – w zakresie 5000 – 10 000 zł)
- **poziom 5** – **bardzo wysoki** skutek (negatywne opinie o LGD z udziałem mediów o zasięgu lokalnym, wszczęcie procedury kontrolnej przez organ nadzorczy (UM), straty finansowe / materialne – powyżej 10 000 zł)

Prawdopodobieństwo wystąpienia danego zdarzenia (scenariusza) dotyczącego poszczególnych zagrożeń zostało scharakteryzowane wg następującej skali:
- **prawie pewne –** zdarzenie występuje co najmniej raz w tygodniu
- **prawdopodobne** – zdarzenie występuje co najmniej raz w tygodniu
- **możliwe** – zdarzenie występuje co najmniej raz na kwartał
- **mało prawdopodobne** – zdarzenie występuje co najmniej raz w roku
- **rzadkie** – zdarzenie nie występuje lub występuje rzadziej niż raz w roku

Przy przeprowadzaniu identyfikacji poziomu ryzyka zastosowano macierz ryzyka (iloczyn prawdopodobieństwa i skutków wystąpienia danego incydentu (scenariusza)).

		SKUTEK				
		bardzo niski	niski	średni	wysoki	bardzo wysoki
PRAWDOPODOBIEŃSTWO	Prawie pewne	Ś	W	K	K	K
	Prawdopodobne	Ś	W	W	K	K
	Możliwe	N	Ś	W	W	K
	Mało prawdopodobne	N	Ś	Ś	W	W
	Rzadkie	N	N	Ś	W	W

N – niski poziom ryzyka – poziom ryzyka akceptowany; działania podejmowane w zależności od wymaganych nakładów
Ś – średni poziom ryzyka – poziom ryzyka nieakceptowany; działanie może zostać przesunięte w czasie, ale wymaga okresowego monitoringu
W – wysoki poziom ryzyka – poziom ryzyka nieakceptowany; działanie może zostać przesunięte w czasie, ale wymaga stałego monitorowania
K – wysoki poziom ryzyka – poziom ryzyka nietolerowany; wymaga natychmiastowego działania

Natomiast **postępowanie z ryzykiem ma na celu podjęcie decyzji dotyczącej ryzyk poszczególnych operacji przetwarzania.** W niniejszym opracowaniu zostały wyróżnione następujące rodzaje postępowań (w oparciu o normę ISO/IEC 27005):
- modyfikowanie (redukcja) ryzyka polegająca na obniżeniu poziomu ryzyka
- zachowanie (akceptacja) ryzyka – świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji
- unikanie ryzyka – polega na unikaniu przez firmę działań, które powodują powstanie określonych typów ryzyka
- dzielenie (przeniesienie) ryzyka – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta.

Zagrożenie (źródło potencjalnej szkody)	Przyczyna występowania zagrożenia	Identyfikacja występujących podatności	Skutki urzeczywistnienia się danego zagrożenia	Prawdopodobieństwo wystąpienia incydentu	Poziom ryzyka
nieuprawniony dostęp do pomieszczenia, w którym przechowywane są dane osobowe, przez pracowników podmiotu (lub ich zleceniobiorców), od którego LGD wynajmuje pomieszczenia biurowe	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak stałego nadzoru odpowiedniego rangą pracownika podmiotu, od którego LGD wynajmuje biuro, nad zleceniodawcami podczas wykonywania zleconych im prac na terenie budynku	Bardzo niski	Rzadkie	**Niski**
	SCENARIUSZ 2 Działanie umyślne człowieka	Brak stałego nadzoru odpowiedniego rangą pracownika podmiotu, od którego LGD wynajmuje biuro, nad zleceniodawcami podczas wykonywania zleconych im prac na terenie budynku	Niskie	Rzadkie	**Niski**
brak kontroli nad dokumentami na stanowisku pracy	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Niestosowanie się pracownika do procedur dot. pracy w biurze wynikające np. z nawału pracy	Bardzo niskie	Rzadkie	**Niski**
	SCENARIUSZ 2 Działanie umyślne człowieka	Świadome niestosowanie się pracownika do procedur dot. pracy w biurze	Niskie	Rzadkie	**Niski**
brak mechanizmów uniemożliwiających skasowanie lub zmianę haseł dostępu przez administratora lub innego użytkownika	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak wiedzy lub doświadczenia administratora lub innego użytkownika	Niskie	Rzadkie	**Niski**
	SCENARIUSZ 2 Działanie umyślne człowieka	Predyspozycja pracowników do celowego działania na szkodę firmy	Bardzo niskie	Rzadkie	**Niski**
zła organizacja pracy	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak procedur i wytycznych mających na celu zwiększenie efektywności firmy, wynikających z braku wiedzy lub doświadczenia Zarządu	Niskie	Rzadkie	**Niski**
choroba ważnych w firmie osób i nieuprawnione zastępstwo	*SCENARIUSZ 1* Sytuacja losowa	Brak procedur i wytycznych uporządkowujących pracę w firmie pod nieobecność Zarządu	Bardzo niskie	Rzadkie	**Niski**
epidemia kadry i brak kompetentnych i zaufanych	*SCENARIUSZ 1* Sytuacja losowa	Mała ilość pracowników firmy, brak możliwości opracowania skutecznego systemu zastępstw	Niskie	Rzadkie	**Niski**

osób upoważnionych do dostępu do danych osobowych					
utrata kluczowych pracowników	*SCENARIUSZ 1* Działanie wewnętrzne	Małe zadowolenie pracowników z wykonywanej pracy prowadzące do podjęcia przez nich decyzji o zmianie pracy (odejście pracowników na własne żądanie)	Niskie	Rzadkie	**Niski**
	SCENARIUSZ 2 Działanie zewnętrzne	Małe zadowolenie pracowników z wykonywanej pracy prowadzące do niskiej lojalności względem firmy, co z kolei przekłada się na podatność na przyjęcie lepszej oferty pracy od konkurencji	Niskie	Rzadkie	**Niski**
niedobór pracowników	*SCENARIUSZ 1* Działanie wewnętrzne	Zatrudnianie zbyt małej ilości pracowników, nieadekwatnej do ilości pracy w firmie	Średnie	Rzadkie	**Średni**
brak możliwości rozliczania działań użytkowników – niekontrolowany dostęp do danych osobowych w firmie	*SCENARIUSZ 1* Działanie wewnętrzne	Brak procedur dotyczących przetwarzania danych osobowych oraz brak szczegółowych zakresów obowiązków pracowników	Niskie	Rzadkie	**Niski**
Niestosowanie się do instrukcji bezpiecznej eksploatacji programów i urządzeń	*SCENARIUSZ 1* Działanie wewnętrzne	Niskie kwalifikacje lub doświadczenie kadry przekładające się na niezrozumienie dostępnych instrukcji	Średnie	Rzadkie	**Średni**
ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak procedur dotyczących ochrony danych osobowych lub „luźna" atmosfera w pracy przekładająca się na zmniejszenie przestrzegania wytycznych	Niskie	Rzadkie	**Niski**
	SCENARIUSZ 2 Działanie umyślne człowieka	Predyspozycja pracowników do celowego działania na szkodę firmy	Średnie	Rzadkie	**Średni**
nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik przez pracowników biura	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak procedur dotyczących ochrony danych osobowych lub „luźna" atmosfera w pracy przekładająca się na zmniejszenie przestrzegania wytycznych	Niskie	Rzadkie	**Niski**
	SCENARIUSZ 2 Działanie umyślne człowieka	Predyspozycja pracowników do celowego działania na szkodę firmy	Średnie	Rzadkie	**Średni**
utrata / zagubienie nośnika zawierającego dane osobowe	*SCENARIUSZ 1* Działanie	Brak procedur dotyczących przechowywania i przenoszenia danych osobowych lub roztargnienie pracownika	Średnie	Rzadkie	**Średni**

	przypadkowe człowieka				
nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak procedur dotyczących przechowywania i przenoszenia danych osobowych lub roztargnienie pracownika	Niskie	Rzadkie	**Niski**
	SCENARIUSZ 2 Działanie umyślne człowieka	Predyspozycja pracowników do celowego działania na szkodę firmy	Średnie	Rzadkie	**Średni**
błędy i pomyłki użytkowników	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Niskie kwalifikacje lub doświadczenie użytkowników	Średnie	Rzadkie	**Średni**
błędy i pomyłki administratorów	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Niskie kwalifikacje lub doświadczenie administratorów	Średnie	Rzadkie	**Średni**
zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Niskie kwalifikacje lub doświadczenie użytkowników lub brak odpowiednich procedur	Niskie	Rzadkie	**Niski**
wyłudzenie danych	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Niekompetencja pracowników	Wysokie	Rzadkie	**Wysoki**
	SCENARIUSZ 2 Działanie umyślne człowieka (zewnętrzne)	Podatność pracowników na wpływy innych (przekupstwo)	Wysoki	Rzadkie	**Wysoki**
podszycie się pod uprawnionego pracownika	*SCENARIUSZ 1* Działanie umyślne człowieka	Niekompetencja pracowników i niestosowanie się do procedur bezpieczeństwa	Średnie	Rzadkie	**Średni**
	SCENARIUSZ 2Działanie umyślne człowieka (zewnętrzne)	Brak mechanizmów uwierzytelniania	Średnie	Rzadkie	**Średni**

stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od pracowników firmy	*SCENARIUSZ 1* Działanie zewnętrzne	Brak wytycznych dotyczących postępowania w sytuacjach kryzysowych	Wysokie	Rzadkie	**Wysoki**
dostęp nieuprawnionych użytkowników do informacji prezentowanej na ekranie stanowiska komputerowego	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak procedur bezpieczeństwa przetwarzania danych osobowych	Niskie	Rzadkie	**Niski**
zaniedbania ze strony personelu obsługującego proces przetwarzania danych	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Niekompetencja pracowników i niestosowanie się do procedur	Średnie	Rzadkie	**Średni**
utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych i pogwarancyjnych sprzętu oraz czynności konserwujących	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak procedur bezpieczeństwa przetwarzania danych osobowych	Średnie	Mało prawdopodobne	**Średni**
odczytanie informacji z nośników przewidzianych do naprawy	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Niekompetencja pracowników i niestosowanie się do procedur	Średnie	Rzadkie	**Średni**
zapisywanie informacji niejawnych na prywatne nośniki pracownika	*SCENARIUSZ 1* Działanie umyślne człowieka	Predyspozycja pracowników do celowego działania na szkodę firmy	Średnie	Rzadkie	**Średni**
przypadkowa zmiana ustawień konfiguracyjnych	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Niekompetencja pracowników	Niskie	Rzadkie	**Niski**
wykorzystanie błędów w obiegu dokumentów w firmie	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Niekompetencja pracowników i niestosowanie się do procedur	Średnie	Rzadkie	**Średni**
wykorzystanie zużytych materiałów – wydruków lub dyskietek zamiast ich	*SCENARIUSZ 1* Działanie przypadkowe	Niekompetencja pracowników i niestosowanie się do procedur	Niskie	Rzadkie	**Niski**

niszczenia	człowieka				
błędy oprogramowania lub sprzętu	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak aktualnych poprawek bezpieczeństwa oraz brak stałego nadzoru informatyka	Bardzo niskie	Możliwe	**Niski**
wadliwe działanie systemu operacyjnego	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak aktualnych poprawek bezpieczeństwa oraz brak stałego nadzoru informatyka	Bardzo niskie	Możliwe	**Niski**
wirus	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak aktualnych poprawek bezpieczeństwa oraz brak stałego nadzoru informatyka	Bardzo niskie	Rzadkie	**Niski**
nielegalne użycie oprogramowania	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Niekompetencja pracowników i niestosowanie się do procedur	Bardzo niskie	Rzadkie	**Niski**
uszkodzenie sprzętu i oprogramowania podczas wykonywania naprawy i konserwacji przez niewyszkolonych pracowników	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak stałego nadzoru informatyka	Niskie	Rzadkie	**Niski**
wykorzystanie pozostawionych niedokończonych fragmentów tworzonych dokumentów w pamięci RAM	*SCENARIUSZ 1* Działanie przypadkowe człowieka	Brak stałego nadzoru informatyka oraz niekompetencja pracowników w zakresie wiedzy informatycznej	Niskie	Rzadkie	**Niski**
podglądanie ekranu monitora przez użytkowników z innych komputerów	*SCENARIUSZ 1* Działanie umyślne człowieka	Brak aktualnych poprawek bezpieczeństwa	Niskie	Rzadkie	**Niski**
klęska żywiołowa, w wyniku której utracono poufność danych osobowych (np. pożar)	*SCENARIUSZ 1* Działanie przypadkowe człowieka lub sytuacja losowa	Brak fizycznej ochrony budynków i systemu alarmowego (oddymiającego / gaszącego)	Wysokie	Rzadkie	**Wysoki**

	SCENARIUSZ 2 Działanie umyślne człowieka (np. wandalizm)	Brak fizycznej ochrony budynków, systemu alarmowego (oddymiającego / gaszącego) oraz lokalizacja w nie do końca zabudowanej części miejscowości	Wysokie	Rzadkie	**Wysoki**
włamanie, w wyniku którego utracono dane osobowe	*SCENARIUSZ 1* Działanie umyślne człowieka	Brak fizycznej ochrony budynków, systemu alarmowego oraz lokalizacja w nie do końca zabudowanej części miejscowości	Wysokie	Rzadkie	**Wysoki**
włamanie z wandalizmem, w wyniku którego utracono poufność danych osobowych	*SCENARIUSZ 1* Działanie umyślne człowieka	Brak fizycznej ochrony budynków, systemu alarmowego oraz lokalizacja w nie do końca zabudowanej części miejscowości	Średnie	Rzadkie	**Średnie**
starzenie się sprzętu w wyniku którego zostają utracone dane osobowe	*SCENARIUSZ 1* Sytuacja losowa	Brak stałego nadzoru informatyka oraz niekompetencja pracowników w zakresie wiedzy informatycznej	Niskie	Rzadkie	**Niski**
awaria systemu wodociągowego i kanalizacyjnego (zalanie pomieszczeń biurowych wodą)	*SCENARIUSZ 1* Sytuacja losowa	Wrażliwość sprzętu na wilgoć	Bardzo niskie	Rzadkie	**Niski**
zmiany napięcia w sieci oraz przerwa w dostarczaniu prądu	*SCENARIUSZ 1* Sytuacja losowa	Wrażliwość sprzętu na zmianę napięcia w sieci	Bardzo niskie	Rzadkie	**Niski**
brak systemu alarmowego w budynku	*SCENARIUSZ 1* Sytuacja losowa	Niedostateczny poziom ochrony budynków	Niskie	Rzadkie	**Niski**

W wyniku przeprowadzonej powyżej analizy stwierdza się, że dla większości zagrożeń (rozpatrywanych w kontekście realizacji poszczególnych scenariuszy zdarzeń) poziom ryzyka jest niski lub średni. Jedynie w 6 przypadkach odnotowano wysoki poziom ryzyka, co wymaga stałego monitorowania zagrożenia.

Proces / rodzaj operacji przetwarzania danych	Zidentyfikowane ryzyka	Poziom ryzyka	Decyzja	Uzasadnienie akceptacji wyliczonego poziomu ryzyka	Postępowanie z ryzykiem - decyzja
1.1 Przetwarzanie danych o zasobach i środkach LGD (analiza danych, sporządzanie i prezentacja sprawozdań oraz raportów, przygotowywanie planów finansowych)	Nieuprawniony dostęp do pomieszczenia, w którym przechowywane są dane osobowe, przez pracowników podmiotu (lub ich zleceniobiorców), od którego LGD wynajmuje pomieszczenia biurowe (działanie przypadkowe człowieka)	Niski	Zwiększyć czujność względem pracowników i wykonawców wynajmującego.	Akceptacja poziomu ryzyka. Zastosowane dodatkowe (fizyczne) systemy ochrony danych w postaci np. monitoringu na zewnątrz budynku czy przechowywaniu dokumentów w zamkniętych szafkach, są wystarczające.	Akceptacja ryzyka
	Epidemia kadry i brak kompetentnych i zaufanych osób upoważnionych do dostępu do danych osobowych	Niski	Stałe monitorowanie lokalnego rynku pracy na wypadek konieczności zatrudnienia pracownika na zastępstwo.	Akceptacja poziomu ryzyka. Małe prawdopodobieństwo wystąpienia epidemii w firmie.	Akceptacja ryzyka
	Utrata kluczowych pracowników	Niski	Stałe monitorowanie lokalnego rynku pracy na wypadek konieczności zatrudnienia pracownika na zastępstwo.	Akceptacja poziomu ryzyka. Systematyczne badanie lokalnego rynku pracy pozwala przypuszczać, że problem z zatrudnieniem osoby na zastępstwo nie będzie miał miejsca.	Akceptacja ryzyka
	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)	Niski	Wdrożenie dodatkowych procedur związanych z ochroną oraz częstotliwością zmian haseł dostępu do stanowisk komputerowych.	Brak akceptacji poziomu ryzyka. Na stanowiskach komputerowych w firmie przechowywane są dane wrażliwe. Udostępnienie ich osobom niepowołanym może negatywnie wpłynąć na wizerunek firmy oraz przynieść konsekwencje prawne.	Modyfikacja (redukcja) ryzyka
	Utrata / zagubienie nośnika zawierającego dane osobowe (działanie przypadkowe człowieka)	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników,	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone	Akceptacja ryzyka

			dostosowujących się do procedur panujących w firmie	określone procedury i wytyczne przy przetwarzaniu danych osobowych, co jest szczególnie ważne w związku z koniecznością dostarczania dokumentacji konkursowej (PROW) do siedziby Urzędu Marszałkowskiego.	
	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych i pogwarancyjnych sprzętu oraz czynności konserwujących	Średni	Wprowadzenie procedur ochrony danych osobowych podczas przeprowadzanych w firmie napraw i przeglądów gwarancyjnych oraz korzystanie z usług tylko znanych i sprawdzonych firm informatycznych.	Brak akceptacji poziomu ryzyka. Niekontrolowany dostęp osób nieuprawnionych do odczytania danych osobowych może przynieść negatywne skutki zarówno prawne jak i finansowe, dlatego pracownicy zobligowani są do bezwzględnego przestrzegania wprowadzonych procedur.	Modyfikowanie (redukcja) ryzyka
	Błędy oprogramowania lub sprzętu	Niski	Systematyczne poddawanie sprzętu i systemu informatycznego badaniom technicznym i serwisowym, bezwzględne korzystania z legalnego oprogramowania oraz posiadanie programów antywirusowych.	Akceptacja poziomu ryzyka. Stowarzyszenie systematycznie poddaje sprzęt serwisowaniu oraz korzysta z legalnego oprogramowania i posiada właściwą ochronę antywirusową.	Akceptacja ryzyka
	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy	Akceptacja poziomu ryzyka. Koszty wprowadzenia	Akceptacja ryzyka

			ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	
	Włamanie z wandalizmem, w wyniku którego utracono poufność danych osobowych	Średni	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	Akceptacja ryzyka
1.2 podejmowanie decyzji strategicznych dla Stowarzyszenia	Zła organizacja pracy	Niski	Zatrudnianie w firmie kompetentnych i wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Choroba ważnych w firmie osób i nieuprawnione zastępstwo.	Niski	Wprowadzenie w firmie procedur i wytycznych uporządkowujących pracę pod nieobecność kluczowych pracowników (członków Zarządu)	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące pracę w firmie pod nieobecność kluczowych pracowników.	Akceptacja ryzyka
	Brak możliwości rozliczania działań pracowników – niekontrolowany dostęp do danych osobowych w firmie	Niski	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie dostępu do danych oraz zasady ich przetwarzania.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie dostępu do danych i zasady ich przetwarzania. Poza tym firma zatrudnia małą ilość pracowników, co przekłada się na łatwość w śledzeniu przepływu danych.	Akceptacja ryzyka

	Nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym spowodowane predyspozycją pracowników do celowego działania na szkodę firmy.	Średni	Wprowadzenie szczegółowych wytycznych przy rekrutacji pracowników (sprawdzanie opinii o potencjalnym pracowniku na podstawie rozmów z poprzednimi pracodawcami).	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie rekrutacji pracowników oraz zbiera opinię o potencjalnych pracownikach na podstawie rozmów z wcześniejszymi pracodawcami.	Akceptacja ryzyka
	Wykorzystanie błędów w obiegu dokumentów w firmie	Średni	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie obiegu dokumentów.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie obiegu dokumentów oraz zatrudnia wykwalifikowanych i kompetentnych pracowników.	Akceptacja ryzyka
1.3 procesy księgowe i skarbowe związane z działalnością Stowarzyszenia	Brak mechanizmów uniemożliwiających skasowanie lub zmianę haseł dostępu przez administratora lub innego użytkownika (zarówno działanie przypadkowe jak i celowe użytkowników)	Niski	Zatrudnianie tylko kompetentnych i wykwalifikowanych pracowników.	Akceptacja poziomu ryzyka. Stowarzyszenie zatrudniania kompetentnych i wykwalifikowanych pracowników.	Akceptacja ryzyka
	Choroba ważnych w firmie osób i nieuprawnione zastępstwo.	Niski	Wprowadzenie w firmie procedur i wytycznych uporządkowujących pracę pod nieobecność kluczowych pracowników (członków Zarządu)	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące pracę w firmie pod nieobecność kluczowych pracowników.	Akceptacja ryzyka
	Błędy i pomyłki użytkowników.	Średni	Zatrudnianie tylko kompetentnych i wykwalifikowanych pracowników.	Akceptacja poziomu ryzyka. Stowarzyszenie zatrudniania kompetentnych i wykwalifikowanych pracowników.	Akceptacja ryzyka
	Wadliwe działanie systemu operacyjnego.	Niski	Stały nadzór informatyka i systematyczne serwisowanie sprzętu.	Akceptacja poziomu ryzyka. Stowarzyszenie systematycznie serwisuje posiadany sprzęt wraz z oprogramowaniem.	Akceptacja ryzyka
1.4 inwentaryzowanie	Zaniedbania użytkowników przy	Niski	Zatrudnianie	Akceptacja poziomu ryzyka.	Akceptacja ryzyka

posiadanych przez LGD środków majątkowych	przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)		wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	
	Wykorzystanie błędów w obiegu dokumentów w firmie	Średni	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie obiegu dokumentów.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie obiegu dokumentów oraz zatrudnia wykwalifikowanych i kompetentnych pracowników.	Akceptacja ryzyka
	Błędy i pomyłki użytkowników.	Średni	Zatrudnianie tylko kompetentnych i wykwalifikowanych pracowników.	Akceptacja poziomu ryzyka. Stowarzyszenie zatrudniania kompetentnych i wykwalifikowanych pracowników.	Akceptacja ryzyka
2.1 rekrutacja pracowników	Nieuprawniony dostęp do pomieszczenia, w którym przechowywane są dane osobowe, przez pracowników podmiotu (lub ich zleceniobiorców), od którego LGD wynajmuje pomieszczenia biurowe (działanie przypadkowe człowieka)	Niski	Zwiększyć czujność względem pracowników i wykonawców wynajmującego.	Akceptacja poziomu ryzyka. Zastosowane dodatkowe (fizyczne) systemy ochrony danych w postaci np. monitoringu na zewnątrz budynku czy przechowywaniu dokumentów w zamkniętych szafkach, są wystarczające.	Akceptacja ryzyka
	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)	Niski	Wdrożenie dodatkowych procedur związanych z ochroną oraz częstotliwością zmian haseł dostępu do stanowisk komputerowych.	Brak akceptacji poziomu ryzyka. Na stanowiskach komputerowych w firmie przechowywane są dane wrażliwe. Udostępnienie ich osobom niepowołanym może negatywnie wpłynąć na wizerunek firmy oraz przynieść konsekwencje prawne.	Modyfikacja (redukcja) ryzyka
	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże,	Akceptacja ryzyka

			budynku.	dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	
	Włamanie z wandalizmem, w wyniku którego utracono poufność danych osobowych	Średni	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	Akceptacja ryzyka
	Wykorzystanie błędów w obiegu dokumentów w firmie	Średni	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie obiegu dokumentów.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie obiegu dokumentów oraz zatrudnia wykwalifikowanych i kompetentnych pracowników.	Akceptacja ryzyka
	Brak kontroli nad dokumentami na stanowisku pracy	Niski	Zastosowanie wytycznych i konkretnych procedur dotyczących pracy w biurze.	Akceptacja poziomu ryzyka. Pracownicy Stowarzyszenia stosują wytyczne i procedury dotyczące pracy w biurze.	Akceptacja ryzyka
	Dostęp nieuprawnionych użytkowników do informacji prezentowanej na ekranie komputera	Niski	Zastosowanie odpowiedniego ustawienia stanowisk komputerowych w biurze.	Akceptacja poziomu ryzyka. Pracownicy Stowarzyszenia mają odpowiednio ustawione stanowiska komputerowe, tak aby petenci nie widzieli ekranu komputerów bezpośrednio po wejściu do pomieszczenia.	Akceptacja ryzyka
2.2 przetwarzanie danych osobowych na cele działalności statutowej LGD	Nieuprawniony dostęp do pomieszczenia, w którym przechowywane są dane osobowe, przez pracowników podmiotu (lub ich zleceniobiorców), od którego LGD wynajmuje pomieszczenia biurowe (działanie przypadkowe człowieka)	Niski	Zwiększyć czujność względem pracowników i wykonawców wynajmującego.	Akceptacja poziomu ryzyka. Zastosowane dodatkowe (fizyczne) systemy ochrony danych w postaci np. monitoringu na zewnątrz budynku czy przechowywaniu dokumentów w zamkniętych szafkach, są wystarczające.	Akceptacja ryzyka
	Starzenie się sprzętu, w wyniku którego	Niski	Stały nadzór informatyka	Akceptacja poziomu ryzyka.	Akceptacja ryzyka

	zostają utracone dane osobowe		nad sprzętem komputerowym firmy oraz systematyczna, dostosowana do potrzeb firmy, wymiana starego sprzętu lub jego części na nowy.	Firma jest objęta stałym nadzorem informatyka oraz systematycznie wymienia stary sprzęt na nowy.	
	Epidemia kadry i brak kompetentnych i zaufanych osób upoważnionych do dostępu do danych osobowych	Niski	Stałe monitorowanie lokalnego rynku pracy na wypadek konieczności zatrudnienia pracownika na zastępstwo.	Akceptacja poziomu ryzyka. Małe prawdopodobieństwo wystąpienia epidemii w firmie.	Akceptacja ryzyka
	Przypadkowa zmiana ustawień konfiguracyjnych	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie.	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne.	Akceptacja ryzyka
	Utrata kluczowych pracowników	Niski	Stałe monitorowanie lokalnego rynku pracy na wypadek konieczności zatrudnienia pracownika na zastępstwo.	Akceptacja poziomu ryzyka. Systematyczne badanie lokalnego rynku pracy pozwala przypuszczać, że problem z zatrudnieniem osoby na zastępstwo nie będzie miał miejsca.	Akceptacja ryzyka
	Odczytanie informacji z nośników przewidzianych do naprawy	Średni	Stosowanie odpowiednich procedur dotyczących naprawy sprzętu komputerowego.	Akceptacja poziomu ryzyka. Stowarzyszenie korzysta z usług zaufanych firm komputerowych.	Akceptacja ryzyka
	Utrata / zagubienie nośnika zawierającego dane osobowe (działanie przypadkowe człowieka)	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych, co jest szczególnie	Akceptacja ryzyka

				ważne w związku z koniecznością dostarczania dokumentacji konkursowej (PROW) do siedziby Urzędu Marszałkowskiego.	
	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	Akceptacja ryzyka
	Wykorzystanie błędów w obiegu dokumentów w firmie	Średni	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie obiegu dokumentów.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie obiegu dokumentów oraz zatrudnia wykwalifikowanych i kompetentnych pracowników.	Akceptacja ryzyka
	Awaria systemu wodociągowego i kanalizacyjnego (zalanie pomieszczeń biurowych wodą)	Niski	Wynajem pomieszczenia biurowego zlokalizowanego w nowym budownictwie.	Akceptacja poziomu ryzyka. Stowarzyszenie wynajmuje pomieszczenie biurowe w nowym budynku, co znacznie minimalizuje prawdopodobieństwo wystąpienia awarii.	Akceptacja ryzyka
	Zmiany napięcia w sieci oraz przerwa w dostarczaniu prądu.	Niski	Stosowanie urządzeń magazynujących prąd (UPS).	Akceptacja poziomu ryzyka. Stowarzyszenie posiada urządzenia dostarczające energię do wybranych stanowisk komputerowych.	Akceptacja ryzyka

	Brak systemu alarmowego budynku.	Niski	Zakup i montaż systemu alarmowego.	Akceptacja poziomu ryzyka. Koszty instalacji systemu alarmowego jest zbyt wysokie i nie racjonalny w odniesieniu do prawdopodobieństwa wystąpienia celowego włamania do biura.	Akceptacja ryzyka
	Klęska żywiołowa, w wyniku której utracono poufność danych (np. pożar)	Wysokie	Instalacja systemu przeciwpożarowego oraz zatrudnienie ochrony budynku.	Akceptacja poziomu ryzyka. Koszty instalacji systemu przeciwpożarowego oraz zatrudnienia ochrony są zbyt wysokie.	Unikanie ryzyka
2.3 podnoszenie wiedzy przez pracowników LGD (realizacja harmonogramu szkoleń)	Utrata / zagubienie nośnika zawierającego dane osobowe (działanie przypadkowe człowieka)	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych, co jest szczególnie ważne w związku z koniecznością dostarczania dokumentacji konkursowej (PROW) do siedziby Urzędu Marszałkowskiego.	Akceptacja ryzyka
	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie	Akceptacja ryzyka

				zdecydowali się na ich poniesienie.	
	Wirus	Niski	Stosowanie legalnego i aktualnego programu antywirusowego.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada legalny i aktualny program antywirusowy.	Akceptacja ryzyka
	Zaniedbania ze strony personelu odpowiadającego za przetwarzanie danych osobowych.	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
2.4 wykonywanie obowiązków służbowych przez pracowników biura	Utrata kluczowych pracowników	Niski	Stałe monitorowanie lokalnego rynku pracy na wypadek konieczności zatrudnienia pracownika na zastępstwo.	Akceptacja poziomu ryzyka. Systematyczne badanie lokalnego rynku pracy pozwala przypuszczać, że problem z zatrudnieniem osoby na zastępstwo nie będzie miał miejsca.	Akceptacja ryzyka
	Użycie nielegalnego oprogramowania	Niski	Używanie legalnego oprogramowania komputerowego.	Akceptacja poziomu ryzyka. Firma używa legalnego oprogramowania komputerowego.	Akceptacja ryzyka
	Uszkodzenie sprzętu i oprogramowania podczas wykonywania naprawy i konserwacji przez niewyszkolonych pracowników	Niski	Stały nadzór informatyka nad sprzętem komputerowym firmy.	Akceptacja poziomu ryzyka. Firma jest objęta stałym nadzorem informatyka.	Akceptacja ryzyka
	Wykorzystanie pozostawionych niedokończonych fragmentów tworzonych dokumentów w pamięci RAM	Niski	Stały nadzór informatyka nad sprzętem komputerowym firmy.	Akceptacja poziomu ryzyka. Firma jest objęta stałym nadzorem informatyka.	Akceptacja ryzyka
	Utrata / zagubienie nośnika zawierającego dane osobowe (działanie przypadkowe człowieka)	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych, co jest szczególnie ważne w związku z koniecznością	Akceptacja ryzyka

				dostarczania dokumentacji konkursowej (PROW) do siedziby Urzędu Marszałkowskiego.	
	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	Akceptacja ryzyka
	Wykorzystanie błędów w obiegu dokumentów w firmie	Średni	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie obiegu dokumentów.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie obiegu dokumentów oraz zatrudnia wykwalifikowanych i kompetentnych pracowników.	Akceptacja ryzyka
	Zapisywanie informacji niejawnych na prywatne nośniki pracownika	Średni	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie pracy biurowej.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie pracy biurowej oraz zatrudnia wykwalifikowanych i kompetentnych pracowników.	Akceptacja ryzyka
2.5 przerwy w wykonywaniu obowiązków służbowych pracowników	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych	Akceptacja ryzyka

			firmie .	osobowych.	
	Wykorzystanie błędów w obiegu dokumentów w firmie	Średni	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie obiegu dokumentów.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie obiegu dokumentów oraz zatrudnia wykwalifikowanych i kompetentnych pracowników.	Akceptacja ryzyka
2.6 zakończenie współpracy	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	Akceptacja ryzyka
	Zaniedbania ze strony personelu odpowiadającego za przetwarzanie danych osobowych.	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Błędy i pomyłki użytkowników.	Średni	Zatrudnianie tylko kompetentnych i wykwalifikowanych pracowników.	Akceptacja poziomu ryzyka. Stowarzyszenie zatrudniania kompetentnych i wykwalifikowanych pracowników.	Akceptacja ryzyka
3.1 przetwarzanie danych w celach realizacji zadań przypisanych do zajmowanego stanowiska oraz przestrzeganie wytycznych Umowy Ramowej[3]	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)	Niski	Wdrożenie dodatkowych procedur związanych z ochroną oraz częstotliwością zmian haseł dostępu do stanowisk komputerowych.	Brak akceptacji poziomu ryzyka. Na stanowiskach komputerowych w firmie przechowywane są dane wrażliwe. Udostępnienie ich osobom niepowołanym może negatywnie wpłynąć na wizerunek firmy oraz przynieść konsekwencje prawne.	Modyfikacja (redukcja) ryzyka
	Stosowanie korupcji oraz szantażu w	Wysoki	Zatrudnianie	Akceptacja poziomu ryzyka.	Akceptacja ryzyka

	celu wydobycia określonych informacji od pracowników firmy		odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie.	Firma zatrudnia tylko zaufany personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych oraz wystąpieniu sytuacji kryzysowych.	
	Utrata / zagubienie nośnika zawierającego dane osobowe (działanie przypadkowe człowieka)	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie.	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych, co jest szczególnie ważne w związku z koniecznością dostarczania dokumentacji konkursowej (PROW) do siedziby Urzędu Marszałkowskiego.	Akceptacja ryzyka
	Wyłudzenie danych	Wysoki	Zatrudnianie wykwalifikowanych i zaufanych pracowników, dostosowujących się do procedur panujących w firmie .	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Podszycie się pod uprawnionego pracownika	Średni	Zatrudnianie wykwalifikowanych i zaufanych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne	Akceptacja ryzyka

			procedur panujących w firmie	przy przetwarzaniu danych osobowych.	
	Zła organizacja pracy	Niski	Zatrudnianie w firmie kompetentnych i wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Brak możliwości rozliczania działań pracowników – niekontrolowany dostęp do danych osobowych w firmie	Niski	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie dostępu do danych oraz zasady ich przetwarzania.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie dostępu do danych i zasady ich przetwarzania. Poza tym firma zatrudnia małą ilość pracowników, co przekłada się na łatwość w śledzeniu przepływu danych.	Akceptacja ryzyka
	Nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym spowodowane predyspozycją pracowników do celowego działania na szkodę firmy.	Średni	Wprowadzenie szczegółowych wytycznych przy rekrutacji pracowników (sprawdzanie opinii o potencjalnym pracowniku na podstawie rozmów z poprzednimi pracodawcami).	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie rekrutacji pracowników oraz zbiera opinię o potencjalnych pracownikach na podstawie rozmów z wcześniejszymi pracodawcami.	Akceptacja ryzyka
	Wykorzystanie błędów w obiegu dokumentów w firmie	Średni	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie obiegu dokumentów.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie obiegu dokumentów oraz zatrudnia wykwalifikowanych i kompetentnych pracowników.	Akceptacja ryzyka
	Błędy i pomyłki administratorów	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny	Akceptacja ryzyka

			pracowników, dostosowujących się do procedur panujących w firmie.	personel.	
	Wykorzystanie zużytych materiałów – wydruków lub dyskietek zamiast ich niszczenia	Niski	Wprowadzenie w firmie zasad dotyczących niszczenia dokumentów oraz innych nośników danych.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury dotyczące zasad niszczenia dokumentów oraz innych nośników danych.	Akceptacja ryzyka
	Przypadkowa zmiana ustawień konfiguracyjnych	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie.	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel.	Akceptacja ryzyka
4.1 przetwarzanie danych członków w celu realizacji zadań statutowych Stowarzyszenia	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Zła organizacja pracy	Niski	Zatrudnianie w firmie kompetentnych i wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Brak możliwości rozliczania działań pracowników – niekontrolowany dostęp do danych osobowych w firmie	Niski	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie dostępu do danych oraz zasady ich	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie dostępu do danych i zasady ich przetwarzania. Poza tym firma	Akceptacja ryzyka

			przetwarzania.	zatrudnia małą ilość pracowników, co przekłada się na łatwość w śledzeniu przepływu danych.	
	Wykorzystanie błędów w obiegu dokumentów w firmie	Średni	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie obiegu dokumentów.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie obiegu dokumentów oraz zatrudnia wykwalifikowanych i kompetentnych pracowników.	Akceptacja ryzyka
5.1 przeprowadzanie konkursów w ramach naborów LGD	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)	Niski	Wdrożenie dodatkowych procedur związanych z ochroną oraz częstotliwością zmian haseł dostępu do stanowisk komputerowych.	Brak akceptacji poziomu ryzyka. Na stanowiskach komputerowych w firmie przechowywane są dane wrażliwe. Udostępnienie ich osobom niepowołanym może negatywnie wpłynąć na wizerunek firmy oraz przynieść konsekwencje prawne.	Modyfikacja (redukcja) ryzyka
	Utrata / zagubienie nośnika zawierającego dane osobowe (działanie przypadkowe człowieka)	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych, co jest szczególnie ważne w związku z koniecznością dostarczania dokumentacji konkursowej (PROW) do siedziby Urzędu Marszałkowskiego.	Akceptacja ryzyka
	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Zła organizacja pracy	Niski	Zatrudnianie w firmie	Akceptacja poziomu ryzyka.	Akceptacja ryzyka

			kompetentnych i wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	
	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	Akceptacja ryzyka
	Wirus	Niski	Stosowanie legalnego i aktualnego programu antywirusowego.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada legalny i aktualny program antywirusowy.	Akceptacja ryzyka
6.1 przeprowadzenie konkursów, na które LGD pozyskało środki z zewnątrz	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)	Niski	Wdrożenie dodatkowych procedur związanych z ochroną oraz częstotliwością zmian haseł dostępu do stanowisk komputerowych.	Brak akceptacji poziomu ryzyka. Na stanowiskach komputerowych w firmie przechowywane są dane wrażliwe. Udostępnienie ich osobom niepowołanym może negatywnie wpłynąć na wizerunek firmy oraz przynieść konsekwencje prawne.	Modyfikacja (redukcja) ryzyka
	Utrata / zagubienie nośnika zawierającego dane osobowe (działanie przypadkowe człowieka)	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych, co jest szczególnie ważne w związku z koniecznością dostarczania dokumentacji konkursowej (PROW) do siedziby	Akceptacja ryzyka

				Urzędu Marszałkowskiego.	
	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych i pogwarancyjnych sprzętu oraz czynności konserwujących	Średni	Wprowadzenie procedur ochrony danych osobowych podczas przeprowadzanych w firmie napraw i przeglądów gwarancyjnych oraz korzystanie z usług tylko znanych i sprawdzonych firm informatycznych.	Brak akceptacji poziomu ryzyka. Niekontrolowany dostęp osób nieuprawnionych do odczytania danych osobowych może przynieść negatywne skutki zarówno prawne jak i finansowe, dlatego pracownicy zobligowani są do bezwzględnego przestrzegania wprowadzonych procedur.	Modyfikacja (redukcja) ryzyka
	Zła organizacja pracy	Niski	Zatrudnianie w firmie kompetentnych i wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	Akceptacja ryzyka
7.1 przeprowadzenie konkursów, które LGD	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym	Niski	Wdrożenie dodatkowych procedur związanych z	Brak akceptacji poziomu ryzyka. Na stanowiskach komputerowych	Modyfikacja (redukcja) ryzyka

realizuje ze środków własnych	przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)		ochroną oraz częstotliwością zmian haseł dostępu do stanowisk komputerowych.	w firmie przechowywane są dane wrażliwe. Udostępnienie ich osobom niepowołanym może negatywnie wpłynąć na wizerunek firmy oraz przynieść konsekwencje prawne.	
	Utrata / zagubienie nośnika zawierającego dane osobowe (działanie przypadkowe człowieka)	Średni	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych, co jest szczególnie ważne w związku z koniecznością dostarczania dokumentacji konkursowej (PROW) do siedziby Urzędu Marszałkowskiego.	Akceptacja ryzyka
	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych i pogwarancyjnych sprzętu oraz czynności konserwujących	Średni	Wprowadzenie procedur ochrony danych osobowych podczas przeprowadzanych w firmie napraw i przeglądów gwarancyjnych oraz korzystanie z usług tylko znanych i sprawdzonych firm informatycznych.	Brak akceptacji poziomu ryzyka. Niekontrolowany dostęp osób nieuprawnionych do odczytania danych osobowych może przynieść negatywne skutki zarówno prawne jak i finansowe, dlatego pracownicy zobligowani są do bezwzględnego przestrzegania wprowadzonych procedur.	Modyfikacja (redukcja) ryzyka
	Zła organizacja pracy	Niski	Zatrudnianie w firmie kompetentnych i	Akceptacja poziomu ryzyka. Firma zatrudnia tylko	Akceptacja ryzyka

			wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	
	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	Akceptacja ryzyka
8.1 realizacja projektów współfinansowanych przez sponsorów	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Zła organizacja pracy	Niski	Zatrudnianie w firmie kompetentnych i wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
9.1 realizacja projektów współpracy	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka

	Zła organizacja pracy	Niski	Zatrudnianie w firmie kompetentnych i wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
10.1 zakup produktów i usług niezbędnych do bieżącego funkcjonowania biura oraz realizacji Umowy Ramowej [3]	Zaniedbania użytkowników przy przesyłaniu, kopiowaniu i udostępnianiu danych (działanie przypadkowe człowieka)	Niski	Zatrudnianie wykwalifikowanych i odpowiedzialnych pracowników, dostosowujących się do procedur panujących w firmie	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Zła organizacja pracy	Niski	Zatrudnianie w firmie kompetentnych i wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
11.1 udzielanie informacji na temat usług świadczonych w LGD podmiotom zainteresowanym	Zła organizacja pracy	Niski	Zatrudnianie w firmie kompetentnych i wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże,	Akceptacja ryzyka

			budynku.	dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	
	Brak kontroli nad dokumentami na stanowisku pracy	Niski	Zastosowanie wytycznych i konkretnych procedur dotyczących pracy w biurze.	Akceptacja poziomu ryzyka. Pracownicy Stowarzyszenia stosują wytyczne i procedury dotyczące pracy w biurze.	Akceptacja ryzyka
12.1 organizacja szkoleń i spotkań informacyjnych skierowanych do rynku odbiorców LGD	Zła organizacja pracy	Niski	Zatrudnianie w firmie kompetentnych i wykwalifikowanych pracowników oraz stosowanie określonych procedur i wytycznych przy przetwarzaniu danych osobowych	Akceptacja poziomu ryzyka. Firma zatrudnia tylko wykwalifikowany i kompetentny personel oraz ma wprowadzone określone procedury i wytyczne przy przetwarzaniu danych osobowych.	Akceptacja ryzyka
	Włamanie, w wyniku którego utracono dane osobowe	Wysoki	Zastosowane dodatkowego systemy ochrony w postaci zainstalowania monitoringu na zewnątrz budynku.	Akceptacja poziomu ryzyka. Koszty wprowadzenia dodatkowych systemów ochrony budynku np. poprzez zatrudnienie firmy ochroniarskiej są zbyt duże, dlatego zarówno właściciel budynku, jak i wynajmujący nie zdecydowali się na ich poniesienie.	Akceptacja ryzyka
	Wykorzystanie błędów w obiegu dokumentów w firmie	Średni	Wprowadzenie w firmie procedur i wytycznych uporządkowujących kwestie obiegu dokumentów.	Akceptacja poziomu ryzyka. Stowarzyszenie posiada procedury i wytyczne uporządkowujące kwestie obiegu dokumentów oraz zatrudnia wykwalifikowanych i kompetentnych pracowników.	Akceptacja ryzyka
	Brak kontroli nad dokumentami na stanowisku pracy	Niski	Zastosowanie wytycznych i konkretnych procedur dotyczących pracy w biurze.	Akceptacja poziomu ryzyka. Pracownicy Stowarzyszenia stosują wytyczne i procedury dotyczące pracy w biurze.	
	Nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik przez pracowników biura	Średni	Zastosowanie wytycznych i konkretnych procedur dotyczących pracy w	Akceptacja poziomu ryzyka. Pracownicy Stowarzyszenia stosują wytyczne i procedury dotyczące	Akceptacja ryzyka

			biurze oraz zatrudnianie kompetentnych i wykwalifikowanych pracowników.	pracy w biurze.	

Poniżej zaprezentowane zostały procedury wprowadzone do realizacji, dotyczące tych procesów przetwarzania danych, w których została podjęta decyzja o modyfikacji (redukcji) poziomu ryzyka.

Proces / rodzaj operacji przetwarzania danych	Zidentyfikowane ryzyka	Poziom ryzyka	Procedura zmniejszająca szansę wystąpienia danego ryzyka
1.1 Przetwarzanie danych o zasobach i środkach LGD (analiza danych, sporządzanie i prezentacja sprawozdań oraz raportów, przygotowywanie planów finansowych)	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)	Niski	**Zmiana haseł dostępu do stanowisk komputerowych w biurze powinna mieć miejsce nie rzadziej niż raz na 6 miesięcy. Zabrania się przechowywania haseł dostępu do stanowisk komputerowych w papierowej dokumentacji biurowej.**
	Utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych i pogwarancyjnych sprzętu oraz czynności konserwujących	Średni	**Zmiana haseł dostępu do stanowisk komputerowych w biurze powinna mieć miejsce nie rzadziej niż raz na 6 miesięcy. Rekomenduje się również natychmiastową zmianę haseł każdorazowo po serwisowaniu lub naprawie sprzętu komputerowego oraz korzystanie z usług jedynie zaufanych (sprawdzonych) firm informatycznych.**
2.1 rekrutacja pracowników	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)	Niski	**Zmiana haseł dostępu do stanowisk komputerowych w biurze powinna mieć miejsce nie rzadziej niż raz na 6 miesięcy. Zabrania się przechowywania haseł dostępu do stanowisk komputerowych w papierowej dokumentacji biurowej.**
3.1 przetwarzanie danych w celach realizacji zadań przypisanych do zajmowanego stanowiska oraz przestrzeganie wytycznych Umowy Ramowej[3]	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)	Niski	**Zmiana haseł dostępu do stanowisk komputerowych w biurze powinna mieć miejsce nie rzadziej niż raz na 6 miesięcy. Zabrania się przechowywania haseł dostępu do stanowisk komputerowych w papierowej dokumentacji biurowej.**
5.1 przeprowadzanie konkursów w ramach naborów LGD	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez	Niski	**Zmiana haseł dostępu do stanowisk komputerowych w biurze powinna mieć miejsce nie rzadziej niż raz na 6 miesięcy. Zabrania się przechowywania haseł dostępu do stanowisk komputerowych w papierowej dokumentacji biurowej.**

	pracowników biura (działanie przypadkowe człowieka)		
6.1 przeprowadzenie konkursów, na które LGD pozyskało środki z zewnątrz	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)	Niski	**Zmiana haseł dostępu do stanowisk komputerowych w biurze powinna mieć miejsce nie rzadziej niż raz na 6 miesięcy. Zabrania się przechowywania haseł dostępu do stanowisk komputerowych w papierowej dokumentacji biurowej.**
	Utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych i pogwarancyjnych sprzętu oraz czynności konserwujących	Średni	**Zmiana haseł dostępu do stanowisk komputerowych w biurze powinna mieć miejsce nie rzadziej niż raz na 6 miesięcy. Rekomenduje się również natychmiastową zmianę haseł każdorazowo po serwisowaniu lub naprawie sprzętu komputerowego oraz korzystanie z usług jedynie zaufanych (sprawdzonych) firm informatycznych.**
7.1 przeprowadzenie konkursów, które LGD realizuje ze środków własnych	Ujawnienie haseł dostępu do stanowiska komputerowego, na którym przechowywane są dane osobowe przez pracowników biura (działanie przypadkowe człowieka)	Niski	**Zmiana haseł dostępu do stanowisk komputerowych w biurze powinna mieć miejsce nie rzadziej niż raz na 6 miesięcy. Zabrania się przechowywania haseł dostępu do stanowisk komputerowych w papierowej dokumentacji biurowej.**
	Utrata lub odczytanie informacji przez osoby nieuprawnione podczas napraw gwarancyjnych i pogwarancyjnych sprzętu oraz czynności konserwujących	Średni	**Zmiana haseł dostępu do stanowisk komputerowych w biurze powinna mieć miejsce nie rzadziej niż raz na 6 miesięcy. Rekomenduje się również natychmiastową zmianę haseł każdorazowo po serwisowaniu lub naprawie sprzętu komputerowego oraz korzystanie z usług jedynie zaufanych (sprawdzonych) firm informatycznych.**

Etap 5.
Ogólna ocena ryzyka a ocena skutków dla ochrony danych

Na podstawie powyższych analiz oraz wytycznych zawartych w przepisie prawa (art. 35 ust. 3 RODO) wnioskujemy, że nie ma konieczności przeprowadzenia oceny skutków dla ochrony danych oraz nie ma potrzeby zasięgania opinii ekspertów i osób, których dane dotyczą lub ich przedstawicieli.

Biorąc pod uwagę specyfikę działalności LGD, Stowarzyszenie na bieżąco dostosowuje procedury ochrony danych osobowych do wytycznych Urzędu Marszałkowskiego Województwa Pomorskiego oraz na bieżąco konsultuje z pracownikami UM wątpliwości dotyczące powyższego zagadnienia. Pracownicy biura LGD uczestniczą również we wszystkich szkoleniach i spotkaniach informacyjnych dot. RODO organizowanych przez Urząd Marszałkowski WP.

V. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

Środki ochrony fizycznej:

1. Pomieszczenia, w którym znajduje się biuro Stowarzyszenia są zamykane na klucz każdorazowo po opuszczeniu przestrzeni przez wszystkich pracowników.
2. Dokumenty papierowe zawierające dane osobowe, upoważnione osoby przechowują w obszarze przetwarzania danych w szafkach zamykanych na klucz.
3. Stanowiska komputerowe zlokalizowane są w pomieszczeniach, w których mogą przebywać osoby trzecie, dlatego są umieszczone w sposób, który uniemożliwia takim osobom wgląd do przetwarzanych danych osobowych.
4. W przypadku dłuższej bezczynności sprzętu komputerowego samoistnie uruchamia się tzw. wygaszacz ekranu, który może być wyłączony jedynie po podaniu prawidłowego hasła użytkownika. Czas niezbędny do uruchomienia wygaszacz nie może być dłuższy niż 15 minut.
5. Wydruki dokumentów zawierają dane osobowe powinny znajdować się w miejscu, które uniemożliwi dostęp osobom postronnym.

Środki sprzętowe oraz informatyczne.

1. Każdy dokument w wersji papierowej przeznaczony do wyrzucenia powinien być uprzednio zniszczony w sposób uniemożliwiający jego odczytanie (przy pomocy niszczarki do dokumentów).
2. Sieć powinna być podłączona do internetu za pomocą Firewall'a (zapory ogniowej).
3. Przynajmniej raz na 2 miesiące należy wykonać kopie zapasowe elektronicznych danych, które będą przechowywane na dysku zewnętrznym.
4. Na wszystkich stanowiskach komputerowych musi być zainstalowane aktualne programy antywirusowe.

Środki ochrony w ramach oprogramowania systemu:

1. Dostęp do elektronicznej bazy danych zarezerwowany jest wyłącznie dla pracowników biura.
2. Dostęp do każdego stanowiska komputerowego został opatrzony hasłem.

3. Z powodu ograniczonej ilości pracowników biura (3 osoby), nie ma konieczności stosowania odrębnych identyfikatorów dla każdego użytkownika systemu.

Środki organizacyjne:

1. Osoby zajmujące się przetwarzaniem danych w Stowarzyszeniu muszą posiadać pisemne upoważnienie do przetwarzania danych osobowych nadane przez Administratora Danych Osobowych.
2. Osoby upoważnione do przetwarzania danych osobowych są przed dopuszczeniem do pracy szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych. Przeprowadzenie ww. szkolenia zlecane jest firmie zewnętrznej lub prowadzone jest przez Administratora Danych Osobowych.
3. Administrator Danych Osobowych w przypadku zatrudnienia nowych pracowników oraz w przypadku wygaśnięcia stosunku pracy aktualizuje ewidencję osób upoważnionych do przetwarzania danych osobowych w Stowarzyszeniu.
4. Zlecenie podmiotowi zewnętrznemu przetwarzania danych osobowych całości lub części posiadanych przez Stowarzyszenie danych może nastąpić wyłącznie na podstawie określonych procedur / przepisów prawa (umowa powierzenia przetwarzania danych osobowych, Umowa Ramowa, procedury, wytyczne itp.)

V. Procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

1. Sytuacje, w których zostają naruszone lub występuje podejrzenie naruszenia przetwarzanych danych osobowych:

- losowego lub nieprzewidzianego oddziaływania czynników zewnętrznych (m.in. pożar, zalanie pomieszczeń),
- występowanie niewłaściwych parametrów środowiska tj. nadmierna wilgotność lub wysoka temperatura prowadzące do uszkodzenia sprzętu elektronicznego,
- umyślne uszkodzenie sprzętu lub oprogramowania,
- pojawienie się odpowiedniego komunikatu alarmowego emitowanego przez urządzenia elektroniczne,
- podejrzenie nieuprawnionej modyfikacji danych w systemie lub inne odstępstwa od stanu oczekiwanego,
- naruszenie lub próby naruszenia integralności systemu lub zawartych w nim baz danych,
- dopuszczenie do pracy osób, które formalnie nie powinny mieć dostępu do bazy danych osobowych w firmie,
- ujawnienie nieautoryzowanych kont dostępu do systemu elektronicznego,
- naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (np. niewylogowanie się z systemu po zakończonej pracy, pozostawienie dokumentów zawierających dane osobowe na widoku osób trzecich, niezabezpieczenie drzwi wejściowych do biura po zakończeniu pracy,
- nienadzorowane otwarte szafy, biurka, szuflady, itp.,
- niezabezpieczone urządzenia archiwizujące dokumenty,
- pozostawienie niezniszczonych lub niewłaściwe niszczenie dokumentów zawierających dane osobowe,
- wynoszenie dokumentacji z danymi osobowymi poza biuro w sytuacjach tego niewymagających,

W przypadku stwierdzenia wystąpienia zdarzeń mających wpływ na naruszenie przetwarzanych w Stowarzyszeniu danych osobowych, pracownicy biura są zobowiązani do niezwłocznego powiadomienia o tym fakcie Administratora Danych Osobowych.

Pracownicy biura LGD dokumentują zaistniałe przypadki naruszenia danych osobowych prowadząc rejestr zgłaszanych naruszeń (będący załącznikiem nr 1) oraz niezwłocznie przedstawiają Administratorowi Danych Osobowych raport (zgodnie z załącznikiem nr 2 do niniejszego dokumentu). Nie ma potrzeby zgłaszania Administratorowi Danych Osobowych tych zdarzeń, w których występuje małe prawdopodobieństwo, by dane naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób trzecich.

Etap 6.
INSTRUKCJE ZARZĄDZANIA SYSTEMAMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH

I. Instrukcja zarządzania systemem informatycznym

a) procedury nadawania uprawnień do przetwarzania danych:
- do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczony jedynie pracownik biura LGD, na podstawie „polecenia przetwarzania danych osobowych" wydanego przez Administratora Danych Osobowych.
- Polecenia przetwarzania danych osobowych przechowuje się w dokumentacji „Polityki bezpieczeństwa informacji" oraz prowadzony jest ich rejestr.
- Dostęp do danych osobowych przetwarzanych w systemie informatycznym może mieć miejsce wyłącznie po podaniu odpowiedniego hasła.
- Dla każdego urządzenia, na którym są przechowywane dane osobowe przypisane jest osobne hasło bezpieczeństwa.
- Zmiana haseł bezpieczeństwa musi nastąpić każdorazowo po zakończeniu stosunku pracy przez jakiegokolwiek pracownika biura LGD.

b) stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem:
- Dane osobowe przetwarzane są z użyciem dedykowanych serwerów, komputerów stacjonarnych.
- Hasło bezpieczeństwa powinno mieć minimum 8 znaków i być zmieniane minimum co 6 miesięcy.
- Hasło powinno być tak zbudowane, aby nie można go było kojarzyć z użytkownikiem danego komputera.
- Hasło użytkownika należy utrzymać w tajemnicy również po upływie jego ważności.
- Hasło nie może znajdować się w miejscu widocznym oraz nie mogą mieć do niego dostęp osoby nieupoważnione. Użytkownikowi nie wolno udostępniać swojego hasła, jak również dopuszczać osoby nieuprawnione do stanowiska roboczego po uwierzytelnieniu w systemie.

c)procedury rozpoczęcia, zawieszenia i zakończenia pracy:
- W celu uruchomienia komputera , użytkownik musi podać odpowiednie hasło.
- System jest tak skonfigurowany, aby po okresie 10 minut bezczynności uruchamiany był wygaszacz ekranu. Do ponownego wznowienia pracy konieczne jest ponowne zalogowanie się przy użyciu hasła.

- Po zakończeniu pracy użytkownik zobowiązany jest do wyłączenia komputera.
- Przebywanie osób nieuprawnionych w pomieszczeniach, w których są przetwarzane dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania.
- Pomieszczenia, w których przetwarzane są dane osobowe, należy zamknąć, na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.

d) procedury tworzenia i przechowywania kopii zapasowych zbiorów danych:
- za sporządzanie i bezpieczeństwo kopii zapasowych odpowiedzialny jest Specjalista ds. promocji i współpracy.
- W wyznaczonym terminie osoba odpowiedzialna wykonuje kopię pełną.
- Wykonane kopie zapasowe zapisywane są w pamięci przenośnej (dysk zewnętrzny) oraz przechowywane w miejscu wiadomym tylko pracownikom biura LGD.
- Sprzęt komputerowy, na którego dyskach twardych zawarte są dane osobowe, przechowywany jest w zabezpieczonych pomieszczeniach.

e) sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego:
- Stosowanie specjalistycznego programu antywirusowego.
- Wprowadzenie dla pracowników biura zakazu otwierania plików pochodzących z niewiadomego źródła.

f) udostępnianie danych osobowych:
- Udostępnianie danych instytucjom może odbywać się wyłącznie zgodnie z przepisami prawa.
- Osoby wyznaczone przez Administratora Danych Osobowych prowadzą rejestr udostępniania danych osobowych, zgodnie z załącznikiem nr 3 do Polityki Bezpieczeństwa i Ochrony Danych Osobowych.

g) wykonywanie napraw, przeglądów i konserwacji:
- przeglądy i konserwacje sprzętu, na którym znajdują się dane osobowe, wykonywane są przez pracowników firm informatycznych, zatrudnianych na podstawie odpowiednich dokumentów (umów, zleceń itp.). Prowadzony jest rejestr napraw, przeglądów i konserwacji sprzęty informatycznego Stowarzyszenia, zgodnie z załącznikiem nr 4 do Polityki Bezpieczeństwa i Ochrony Danych Osobowych .
- Usługi dotyczące instalacji, napraw i konserwacji sprzętu informatycznego należy zlecać podmiotom, które gwarantują prawidłowe wykonanie usług.
- Naprawa sprzętu, na którym znajdują się dane osobowe, powinna odbywać się pod nadzorem pracowników biura LGD w miejscu jego użytkowania.
- W przypadku konieczności naprawy w serwisie, sprzęt komputerowy przed oddaniem do serwisu powinien być odpowiednio przygotowany. Dane należy zarchiwizować na nośnik zewnętrzny, a dyski twarde bezwzględnie wymontować na czas naprawy lub trwale usunąć z nich dane.

II. Instrukcja postępowania z kluczami oraz zabezpieczenie pomieszczeń

a) Główne wejście do biura Stowarzyszenia „Bursztynowy Pasaż" polega ochronie polegającej na całodobowym monitoringu, zainstalowanym przez właściciela budynku.

b) W przypadku zaistnienia sytuacji niepożądanej (takiej jak np. uszkodzenia drzwi, będące potwierdzeniem wandalizmu lub włamania), pracownik LGD, który pierwszy znajdzie się na miejscu zdarzenia niezwłocznie powiadamia bezpośredniego przełożonego oraz wyznaczonego do kontaktu pracownika Centrum Sportowo – Konferencyjnego Sp. z o.o.

c) Wymienione w punkcie b) osoby wspólnie podejmują działania w celu usunięcia zaistniałej sytuacji oraz znalezienia winnych.

d) Pracownicy biura Stowarzyszenia zobowiązani są w godzinach pracy do:
- zwracania uwagi na zachowanie osób wchodzących i wychodzących z budynku,
- reagowania na wejście do budynku osób będących pod wpływem działania środków odurzających,
- reagowania na próby zniszczenia, wynoszenia lub wywożenia mienia z budynku,
- reagowania na próby wnoszenia do budynku przedmiotów podejrzanych lub niebezpiecznych,
- natychmiastowego reagowania poprzez zawiadomienie odpowiednich służb o zaobserwowanych próbach stworzenia zagrożenia dla życia i zdrowia oraz utraty lub zniszczenia mienia.

e) Zabezpieczenie pomieszczeń biura i procedura postępowania z kluczami:
- biuro Stowarzyszenia otwierają i zamykają wyznaczone osoby (pracownicy biura),
- każdy pracownik biura posiada osobny zestaw kluczy, z który ponosi pełna odpowiedzialność,
- w przypadku zgubienia kluczy należy niezwłocznie poinformować o zaistniałej sytuacji bezpośredniego przełożonego oraz wyznaczonego do kontaktów pracownika podmiotu Wynajmującego
- przed otwarciem zamków, wyznaczone osoby sprawdzają od strony wizualnej stan drzwi wejściowych,
- po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, pracownicy biura sprawdzają stan zachowanych zabezpieczeń sprzętu biurowego i komputerowego, dokumentacji i innego wyposażenia,
- w przypadku stwierdzenia jakichkolwiek nieprawidłowości pracownicy biura natychmiast zawiadamiają o zaistniałej sytuacji bezpośredniego przełożonego oraz wyznaczonego do kontaktów pracownika podmiotu Wynajmującego i stosują się do ich decyzji,
- po zakończeniu pracy pracownicy zobowiązani są do uporządkowania swoich stanowisk pracy oraz wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych polegających na: zabezpieczeniu dokumentacji, komputerów i nośników pamięci, wyłączeniu wszystkich urządzeń energetycznych zasilanych energią elektryczną (czajniki, wentylatory itp.) zgodnie z zasadami bhp, zamknięciu okien i drzwi.

f) Klucze od biurek stanowiskowych i szaf biurowych znajdują się w posiadaniu pracowników biura, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.

g) Przebywanie pracowników poza godzinami pracy w budynku możliwy jest wyłącznie za wiedzą bezpośredniego przełożonego.

- Otwarcie budynku w dni wolne od pracy, przez pracowników biura, możliwe jest wyłącznie za wiedzą bezpośredniego przełożonego.

III. Instrukcja dot. kasacji i utylizacji sprzętu komputerowego, elementów eksploatacyjnych i nośników danych

a) Zarząd Stowarzyszenia musi być każdorazowo poinformowany o sprzęcie wycofanym z eksploatacji, trwale uszkodzonym lub wyeksploatowanym.

b) W przypadku nośników danych typu płyty DVD, CD-R czy dyskietki proces kasacji zostaje przeprowadzony przez pracowników biura, w taki sposób, aby stało się niemożliwe odzyskanie z nich jakichkolwiek danych (np. za pomocą niszczarki).

c) Przed oddaniem sprzętu komputerowego do kasacji należy pozbawić go nośników danych lub trwale pozbawić ich możliwości odczytania z nich danych.

d) Pracownik odpowiedzialny za prowadzenie ewidencji środków trwałych ma obowiązek sporządzenia dokumentacji dot. zgody na kasację sprzętu będącego w wykazie środków trwałych Stowarzyszenia.

e) W przypadku otrzymania od bezpośrednich przełożonych zgody na kasację, sprzęt o którym mowa, zostaje zdjęty z ewidencji środków trwałych i przekazany do utylizacji.

f) W przypadku gdy na miejsce uszkodzonego sprzętu komputerowego lub materiałów eksploatacyjnych dokonuje się zakupu sprzętu zastępczego proces utylizacji dokonuje firma, która sprzedała nowy sprzęt lub materiały eksploatacyjne.

V. Postanowienia końcowe (wytyczne dla pracowników biura)

1. W przypadku zbierania danych osobowych od osoby, której te dane dotyczą, Administrator Danych Osobowych (lub osoba przez niego upoważniona) zobowiązany jest poinformować tę osobę o:
- nazwie, siedzibie i danych kontaktowych LGD,
- celach przetwarzania pozyskanych danych osobowych,
- podstawie prawnej przetwarzania,
- odbiorcach danych osobowych lub o kategoriach odbiorców,
- okresie przetwarzania pozyskanych danych osobowych , a gdy nie jest to możliwe o kryteriach ustalania tego czasu,
- prawie do żądania od administratora dostępu do swoich danych osobowych, ich sprostowania, usunięcia, ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie przenoszenia danych osobowych,
- prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
- o prawie wniesienia skargi do organu nadzorczego,
- informowanie, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem koniecznym do zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
- zautomatyzowanym systemie podejmowania decyzji w firmie, w tym profilowaniu, jeżeli taki proces jest prowadzony przez LGD.

2. W przypadku pozyskania danych osobowych w sposób inny niż od osoby, której te dane dotyczą, Administrator Danych Osobowych (lub osoba przez niego upoważniona) jest również zobowiązany do poinformowania tej osoby o:
- kategorii pozyskanych danych osobowych,
- źródle pochodzenia danych osobowych oraz czy pochodzą one ze źródeł publicznie dostępnych.

3. Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością karną wynikającą z rozdziału VIII – środki ochrony prawnej, odpowiedzialność i sankcje, rozporządzenia unijnego.

4. W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 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.

Administrator Danych Osobowych

……
/pieczęć i podpis/

Załącznik nr 1
do Polityki Bezpieczeństwa i Ochrony Danych Osobowych
Stowarzyszenia „Bursztynowy Pasaż" (LGD)

REJESTR NARUSZEŃ

danych osobowych przetwarzanych w Stowarzyszeniu „Bursztynowy Pasaż" z siedzibą w Gniewinie przy ul. Szkolnej 3.

L.p.	Administrator / Współadministratorzy / Podmiot przetwarzający	Data i godzina wystąpienia incydentu prowadzącego do naruszenia	Data i godzina stwierdzenia naruszenia	Miejsce incydentu prowadzącego do naruszenia	Nośniki danych osobowych których dotyczy naruszenie	Charakter naruszenia danych osobowych (opis naruszenia danych)	Kategorie osób, których danych osobowych dotyczy naruszenie	Przybliżona liczba osób których danych osobowych dotyczy naruszenie
1	2	3	4	5	6	7	8	9
1.								
2.								
...								

Kategorie danych osobowych, których dotyczy naruszenie	Przybliżona liczba wpisów (rekordów) danych osobowych, których dotyczy naruszenie	Skutki naruszenia, w tym możliwe konsekwencje naruszenia dla osób fizycznych	Środki zastosowane w celu zaradzenia naruszeniu ochrony danych, w tym w celu zminimalizowania jego ewentualnych negatywnych skutków	Ocena ryzyka naruszenia praw i wolności osób fizycznych, wynikającego z naruszenia danych osobowych	Informacja, czy naruszenie zostało zgłoszone organowi nadzorczemu, data i godzina zgłoszenia (potwierdzenie zgłoszenia: kopia pisma, maila itp.)	W przypadku zgłoszenia po upływie 72 godzinnego terminu – wyjaśnienie przyczyn opóźnienia	W przypadku braku zgłoszenia – wyjaśnienie powodów braku zgłoszenia naruszenia organowi nadzorczemu
10	11	12	13	14	15	16	17

Informacja czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu ochrony danych, sposób i data wysłania zawiadomienia (potwierdzenie zawiadomienia: kopia pisma, maila itp.)	W przypadku braku zawiadomienia – wyjaśnienie powodów braku zawiadomienia osób, których dane dotyczą	W przypadku wydania publicznego komunikatu zamiast zawiadamiania osób, których dane dotyczą, wyjaśnienie powodów wydania komunikatu oraz potwierdzenie wydania (link do strony www, screen, nr umowy na publikację artykułu w prasie itp.)
18	19	20

Załącznik nr 2
do Polityki Bezpieczeństwa i Ochrony Danych Osobowych
Stowarzyszenia „Bursztynowy Pasaż" (LGD)

RAPORT

z naruszenia bezpieczeństwa danych osobowych przetwarzanych w Stowarzyszeniu „Bursztynowy Pasaż" z siedzibą w Gniewinie przy ul. Szkolnej 3

1. Data i godzina naruszenia ……
2. Osoba powiadamiająca o naruszeniu: ……
……
(imię i nazwisko, stanowisko służbowe)
3. Lokalizacja zdarzenia: ……..
……
(adres, nazwa pomieszczenia)
4. Rodzaj naruszenia oraz okoliczności towarzyszące:
……
……
……
……
……
……
5. Podjęte działania:
……
……
……
……
……
6. Przyczyny wystąpienia zdarzenia:
……
……
……
……
……
7. Postepowanie wyjaśniające:
……
……
……
……
……

……
(data i podpis osoby sporządzającej raport)

Załącznik nr 3
do Polityki Bezpieczeństwa i Ochrony Danych Osobowych
Stowarzyszenia „Bursztynowy Pasaż" (LGD)

REJESTR UDOSTĘPNIEŃ DANYCH OSOBOWYCH INNYM PODMIOTOM

w Stowarzyszeniu „Bursztynowy Pasaż" z siedzibą w Gniewinie przy ul. Szkolnej 3

L.p.	**Imię i nazwisko / Nazwa zbioru** *(możliwie najlepszy opis osoby , której dane dotyczą lub całego zbioru danych)*	**Data udostępnienia**	**Nazwa podmiotu, któremu udostępniono dane** *(np. upoważniony organ, instytucja lub inny, który wykazał uprawnienie do udostępniania mu danych)*	**Cel udostępniania** *(podstawa prawna, nr umowy, itp.)*	**Zakres udostępnianych danych** *(jakie dane zostały udostępnione)*	**Rodzaj zbioru / zasobu i jego lokalizacja** *(np. papierowy wydruk, dane w formie elektronicznej)*
1	2	3	4	5	6	7
1						
2						
3						
4						
5						
6						
7						
8						
9						
...						

Załącznik nr 4
do Polityki Bezpieczeństwa i Ochrony Danych Osobowych
Stowarzyszenia „Bursztynowy Pasaż" (LGD)

REJESTR NAPRAW, PRZEGLĄDÓW I KONSERWACJI

sprzętu informatycznego w Stowarzyszeniu „Bursztynowy Pasaż" z siedzibą w Gniewinie przy ul. Szkolnej 3

L.p.	Imię i nazwisko i/lub nazwa firmy przeprowadzającej naprawę, przegląd lub konserwację	Data wystąpienia zdarzenia	Powód realizacji usługi / nazwa urządzenia podlegającego usłudze	Czy usługa realizowana jest w siedzibie LGD?	Czy wystąpiła konieczność wyniesienia sprzętu poza siedzibę LGD?	Nazwa firmy, adres i dane kontaktowe firmy, do której został przekazany sprzęt informatyczny	Data powierzenia oraz powrotu sprzętu do siedziby LGD	Rodzaj dokonywanych czynności (naprawa, instalacja oprogramowania itp.)	Podpis osoby odpowiedzialnej za realizację usługi
1	2	3	4	5	6	7	8	9	10
1									
2									
3									
4									
5									
6									
7									
8									
9									
…									