Polityka Bezpieczeństwa Danych Osobowych

w

Grupie LUMEN POLSKA

ul. Długosza 42-46; 51-162 Wrocław

NIP: 5482318564

REGON: 072694908

Pieczęć firmowa:	Podpis Administratora Danych Osobowych:	Data:
LUMEN Polska sp. z o.o. 51-162 Wroclaw, ul. Długosza 42-46 NIP 548-231-85-64 REG. 072694908 tel 071-320-90-00, fax 071-320-90-20	LUMEN® POLSKA SP. Z O.O. PREZES *Petr Novák*	25 maja 2018

WSTĘP

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ww. rozporządzenia oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następujący zestaw procedur.

1. SŁOWNICZEK I WYKAZ SKRÓTÓW

1.1. Słowniczek

Administrator Danych Osobowych (ADO)	Administratorem danych osobowych są wspólnie spółki Grupy LUMEN POLSKA, związane porozumieniem o Współadministracji, zwane dalej również jako Współadministratorzy
Inspektor Ochrony Danych Osobowych (IODO)	osoba wyznaczona przez Współadministratorów do nadzorowania oraz wdrażania zasad ochrony danych osobowych
Administratorzy Systemów Informatycznych (ASI)	osoby odpowiedzialne za nadzór i bezpieczeństwo nad infrastrukturą IT i systemami informatycznymi Grupy LUMEN POLSKA
Biuro Długosza	Biuro LUMEN POLSKA (siedziba Spółki) przy ul. Długosza 42-46; 51-162 Wrocław Biuro PAL Sp. z o.o. (siedziba Spółki) przy ul. Długosza 42-46; 51-162 Wrocław Biuro PAL 1 Sp. z o.o. (siedziba Spółki) przy ul. Długosza 42-46; 51-162 Wrocław Biuro PRIME MANAGEMENT Sp. z o.o. (siedziba Spółki) przy ul. Długosza 42-46; 51-162 Wrocław Biuro SIDE Sp. z o.o. (siedziba Spółki) przy ul. Długosza 42-46; 51-162 Wrocław
Biuro Prosta	Biuro DNG Sp. z o.o. (siedziba Spółki) przy ul. Prosta 36, 50-508 Wrocław Biuro Remote MANAGEMENT Sp. z o.o. (siedziba Spółki) przy ul. Prosta 36, 50-508 Wrocław
Dane osobowe	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, przetwarzane przez Współadministratorów zarówno w systemach informatycznych jak i tradycyjnie (wersja papierowa)
Hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie Użytkownikowi
Grupa LUMEN POLSKA	Spółki tworzące Grupę LUMEN POLSKA: LUMEN POLSKA Sp. z o.o. ul. Długosza 42-46; 51-162 Wrocław, DNG Sp. z o.o. ul. Prosta 36, 50-508 Wrocław, PAL Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, PAL 1 Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, PRIME MANAGEMENT Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, SIDE Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, Remote MANAGEMENT Sp. z o.o. ul. Prosta 36, 50-508 Wrocław.
Identyfikator (login)	ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną (Użytkownika) do przetwarzania danych osobowych w systemie informatycznym
Instrukcja Zarządzania	instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych obowiązująca u

	Współadministratorów, opracowana na podstawie Rozporządzenia
Integralność danych	właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany
Nośniki danych	wszelkie nośniki, na których informacje zapisane są w postaci elektronicznej, w szczególności dyski, dyskietki, dyski CD-ROM, karty magnetyczne lub pamięci przenośne. Na potrzeby niniejszej Polityki Bezpieczeństwa za nośnik danych uważa się również dokument (dokumenty) papierowy zawierający dane osobowe
Odbiorca danych	każdy, komu udostępnia się dane osobowe, z wyłączeniem: osoby, której dane dotyczą; osoby upoważnionej do przetwarzania danych; podmiotu, któremu powierzono przetwarzanie danych; organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem
Opiekunowie Zbiorów	Użytkownik pełniący funkcję kierownika lub dyrektora, który został przypisany do danego zbioru lub zbiorów jako osoba odpowiedzialna za zarządzanie nim
Przetwarzanie danych osobowych	jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie danych osobowych, w szczególności w systemach informatycznych
Procesor	podmiot, któremu Współadministratorzy powierzyli dane osobowe w oparciu o pisemną umowę lub upoważnienie
Poufność danych	właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom
Polityka Bezpieczeństwa Danych Osobowych	niniejszy dokument
Przepisy szczególne	powszechnie obowiązujące akty prawne regulujące tematykę ochrony danych osobowych, będące przepisami szczególnymi w stosunku do Ustawy oraz Rozporządzenie ogólne, w tym m.in.
	ustawa z dnia 26 czerwca 1974 r. Kodeks pracy.
Rozporządzenie ogólne	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,
Rozliczalność	właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi
System informatyczny	zespół urządzeń, sprzętu komputerowego, oprogramowania oraz baz danych przetwarzających dane osobowe
Użytkownik	osoba upoważniona przez Współadministratorów do przetwarzania danych osobowych bez względu na formę w jakiej te dane są przetwarzane (elektronicznie, tradycyjnie)
Usuwanie danych	zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą
Ustawa z 2018 r.	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2016.922)
Współadministratorzy	Oznaczają współadministratorów w rozumieniu art. 26 Rozporządzenia, tj. dwóch lub więcej administratorów wspólnie ustalających cele i sposoby przetwarzania. Współadministratorami danych w niniejszej Polityki Bezpieczeństwa są: LUMEN POLSKA Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, DNG Sp. z o.o. ul. Prosta 36, 50-508 Wrocław, PAL Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, PAL 1 Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, PRIME Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, SIDE Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, Remote MANAGEMENT Sp. z o.o. ul. Prosta 36, 50-508 Wrocław. Współadministratorzy wspólnie ustalili, iż podmiotem odpowiedzialnym za realizację

	obowiązków wynikających z Rozporządzenia względem osób, których dane są przetwarzane, jest LUMEN POLSKA Sp. z o.o. z siedzibą we Wrocławiu.
Zakres zbierania danych osobowych	kategorie danych osobowych, które podlegają przetwarzaniu przez Współadministratorów
Zbiór danych osobowych	każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie

1.2. **Stosowane skróty**

UODO	Urząd Ochrony Danych Osobowych
ADO	Administrator Danych Osobowych
IODO	Inspektor Ochrony Danych Osobowych

2. DEFINICJA, CELE I ZAKRES ZASTOSOWANIA POLITYKI BEZPIECZEŃSTWA

2.1. Definicja Polityki Bezpieczeństwa	2.1.1. Polityka Bezpieczeństwa Danych Osobowych to dokument opisujący całokształt działań zmierzających do uzyskania i utrzymania wymaganego poziomu bezpieczeństwa danych osobowych, na każdym etapie ich przetwarzania. 2.1.2. Polityka Bezpieczeństwa Danych Osobowych to w szczególności zbiór zasad dotyczących bezpieczeństwa danych osobowych ustalonych w oparciu o: • wymagania wynikające z przepisów prawa mających zastosowanie do działalności Grupy LUMEN POLSKA, • szacowanie ryzyka w związku z prowadzeniem działalności gospodarczej przez Grupę LUMEN POLSKA, • wewnętrzne wymogi i uwarunkowania lokalowe Grypy LUMEN POLSKA.
2.2. Cel Polityki Bezpieczeństwa	2.2.1. Wdrożenie Polityki Bezpieczeństwa Danych Osobowych w Grupie LUMEN POLSKA ma na celu zabezpieczenie przetwarzanych przez Współadministratorów danych osobowych, bez względu na formę (elektroniczną bądź tradycyjną) w jakiej to przetwarzanie następuje. 2.2.2. Celem Polityki Bezpieczeństwa Danych Osobowych jest w szczególności: • dopełnienie wymogów wynikających z obowiązujących przepisów w zakresie ochrony danych osobowych (Rozporządzenie ogólne, Ustawa, Rozporządzenie, przepisy szczególne), • zabezpieczenie zasobów systemów informatycznych, infrastruktury technicznej, sprzętu i osprzętu przed kradzieżą, zniszczeniem lub uszkodzeniem

	• uniemożliwienie dostępu do informacji stanowiących dane osobowe, zawartych w systemach informatycznych zarządzanych przez Współadministratorów osobom do tego nieupoważnionym, • uniemożliwienie zniszczenia lub nieuprawnionej zmiany danych osobowych przetwarzanych w sposób tradycyjny (papierowy) oraz elektroniczny, • zabezpieczenie dokumentacji papierowej zawierającej dane osobowe przed ich kradzieżą lub kopiowaniem, • ochrona wizerunku Grupy LUMEN POLSKA jako podmiotu przetwarzającego dane osobowe, • zapewnienie odpowiedniego poziomu wiedzy wśród Użytkowników, • zapewnienie zgodności z prawem, rzetelności i przejrzystości, minimalizacji, prawidłowości, ograniczenia przechowywania, integralności i poufności, oraz rozliczalności przetwarzanych przez Grupę LUMEN POLSKA, • zapewnienie gotowości podejmowania działań w sytuacji otrzymania żądania od osoby, której dane dotyczą dostępu do danych osobowych jej dotyczących, usunięcia danych, sprostowania, ograniczenia przetwarzania, wycofania zgody na przetwarzanie danych • zapewnienie gotowości do podejmowania działań w sytuacjach kryzysowych (np. wycieku danych osobowych), zgłoszenia sprzeciwu przez osobę, której dane dotyczą wobec przetwarzania, wniesieniu skargi do GIODO, które umożliwią działalność Współadministratorów.
2.3. Zakres stosowania	2.3.1. Polityka Bezpieczeństwa Danych Osobowych dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny (papierowo), jak również w systemach informatycznych. 2.3.2. Procedury i zasady wskazane w Polityce Bezpieczeństwa Danych Osobowych stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych jak i innych (np. świadczących czynności na podstawie umów cywilnoprawnych, stażystów, praktykantów etc.).

3. WSPÓŁADMINISTRACJA

3.1. Do dnia 24 maja 2018 r. każda ze spółek wchodzących w skład Grupy LUMEN POLSKA samodzielnie administrowała danymi osobowymi swoich pracowników, klientów i kontrahentów, jak również dbała o ich bezpieczeństwo. W związku ze zmianą przepisów oraz wejściem w życie RODO postanowiły one jednak połączyć swoje siły i stworzyć wspólne zasady ochrony i przetwarzania danych osobowych. A wszystko po to, aby ujednolicić zasady przetwarzania danych osobowych, jak również zwiększyć ich bezpieczeństwo.

3.2. W dniu 25 maja 2018 r. spółki wchodzące w skład Grupy LUMEN POLSKA (wykaz Współadministratorów został opisany w art. 1. SŁOWNICZEK I WYKAZ SKRÓTÓW) zawarły porozumienie, w którym postanowiły wspólnie określić cele i sposoby przetwarzania danych osobowych znajdujących się w ich posiadaniu. Tym samym stały się one Współadministratorami zbieranych i przetwarzanych przez każdą ze spółek danych osobowych.

3.3. Zasadniczym celem przedmiotowego porozumienia było uregulowanie w sposób wyczerpujący i kompleksowy obowiązków Współadministratorów zarówno w sferze wewnętrznej – względem siebie, jak i w stosunkach zewnętrznych – w relacji do osób, których dane są przetwarzane oraz organów nadzoru. Dzięki temu niniejsza Polityka Bezpieczeństwa Ochrony Danych Osobowych Grupy LUMEN POLSKA może stać się jeszcze bardziej transparentna oraz efektywna.

3.4. Współadministratorzy danych realizują obowiązki informacyjne wynikające z RODO, w sposób ciągły w bezpośrednim kontakcie z osobami, których dane dotyczą.

4. OBOWIĄZKI ZWIĄZANE Z PRZETWARZANIEM DANYCH OSOBOWYCH

4.1. Zasady ogólne

4.1.1. Organizacja przetwarzania danych osobowych w Grupie LUMEN POLSKA opiera się na wyodrębnieniu następujących kategorii osób:

- organu zarządzającego Współadministratorów (członkowie Zarządu Spółek),
- Użytkowników (osoby upoważnione do przetwarzania danych osobowych przez Współadministratorów, w tym Opiekunowie Zbiorów),
- Personelu pomocniczego.

4.1.2. Dostęp do danych osobowych posiadają osoby tworzące organ zarządzający Współadministratorzy oraz Użytkownicy (w tym Opiekunowie Zbiorów). Personel pomocniczy nie przetwarza danych osobowych, może natomiast przebywać w obszarze przetwarzania danych na podstawie zgody wydanej przez Współadministratora. Zgoda, o której tu mowa stanowi **załącznik nr 6** do niniejszej Polityki Bezpieczeństwa.

4.1.3. Wszystkie osoby, których rodzaj wykonywanej pracy będzie wiązał się z dostępem do danych osobowych, przed przystąpieniem do pracy, mają obowiązek:

- zapoznać się (i podpisać stosowne oświadczenie potwierdzające ww. czynność) z obowiązującymi zasadami ochrony danych osobowych określonymi w Polityce Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania (**załącznik nr 1** do Polityki Bezpieczeństwa Danych Osobowych),podpisać oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczenia (np. hasła dostępowe) w tajemnicy (**załącznik nr 2** do Polityki Bezpieczeństwa Danych Osobowych).

4.2. Obowiązki Współadministratorów

Administratorem danych osobowych są wspólnie spółki Grupy LUMEN POLSKA, związane porozumieniem o współadministracji, a cechą wyróżniającą jest to, że wspólnie decydują o celach i środkach przetwarzania danych osobowych. Z uwagi na bezosobowy charakter tej definicji należy przyjąć, że organem zarządzającym Współadministratorów są członkowie Zarządu Spółek Grupy LUMEN POLSKA. W ramach swych obowiązków Współadministrator jest odpowiedzialny za:

4.2.1. Nadzorowanie, aby będące w jego posiadaniu dane osobowe były przetwarzane zgodnie z prawem.

4.2.2. Wyodrębnienie zbiorów przetwarzanych danych osobowych, a także ich aktualizowanie.

4.2.3. Zapewnienie środków technicznych i organizacyjnych do ochrony przetwarzanych danych osobowych, odpowiednich do zagrożeń oraz kategorii danych objętych ochroną.

4.2.4. Prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych: Polityka Bezpieczeństwa Danych Osobowych i Instrukcja Zarządzania oraz dokumenty z nimi związane.

4.2.5. Wyznaczenie osoby pełniącej funkcję IODO w przypadku gdy wyznaczenie IODO będzie obowiązkowe mając na uwadze przepisy prawa, lub Współadministrator podejmie decyzję o konieczności takiego wyznaczenia.

4.2.6. Prowadzenie rejestru czynności przetwarzania w przypadku gdy prowadzenie takiego rejestru będzie dla Współadministratora obowiązkowe, mając na uwadze przepisy prawa, lub Współadministrator podejmie decyzję o jego prowadzeniu.

4.2.7. Upoważnianie do przetwarzania danych Użytkowników (upoważnienia w imieniu Współadministratora nadaje, na podstawie pełnomocnictwa IODO jeśli został wyznaczony).

4.2.8. Wydawanie upoważnień na przebywanie w obszarze przetwarzania danych osobowych dla Personelu pomocniczego.

4.2.9. Niezwłoczne sprostowanie danych osobowych w przypadku otrzymania takiego żądania od osoby której dane dotyczą lub ich uzupełnienie w przypadku kiedy dane są niekompletne, a także ograniczenie przetwarzania.

4.2.10. Niezwłoczne usunięcie danych osobowych na żądanie osoby, której dane dotyczą w przypadkach wskazanych w Rozporządzeniu ogólnym tj. jeśli osoba której dane dotyczą cofnęła zgodę na której opiera się ich przetwarzanie, dane nie są już niezbędne do celów w których zostały zebrane, osoba wniosła sprzeciw wobec przetwarzania.

4.2.11. Informowanie procesorów przetwarzających dane o żądaniach osoby której dane dotyczą co do usunięcia danych osobowych.

4.2.12. Udostępnianie osobom, których dane dotyczą na ich żądanie dane ich dotyczące w

ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego.

4.2.13. Stosuje zatwierdzone kodeksy postępowania lub zatwierdzony mechanizm certyfikacji.

4.2.14. Wdraża odpowiednie środki techniczne i organizacyjne tj. pseudonimizacja, zaprojektowanie w celu skutecznej realizacji zasad ochrony danych tj. minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń w celu zapewnienia ochrony zgodniej z przepisami prawa i w celu ochrony praw osób, których dane dotyczą, a także w celu przetwarzania wyłącznie tych danych osobowych, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.

4.3. **Obowiązki Inspektora Ochrony Danych Osobowych**

4.3.1. Aktualizacja Polityki Bezpieczeństwa Danych Osobowych, a także nadzorowanie przestrzegania określonych w niej zasad.

4.3.2. Aktualizacja Instrukcji Zarządzania i czuwanie nad jej przestrzeganiem.

4.3.3. Konsultowanie kwestii związanych z udostępnianiem danych osobowych do organów i urzędów państwowych i samorządowych oraz innym administratorom danych, a także osobom fizycznym.

4.3.4. Zatwierdzanie wzorów dokumentów (odpowiednich klauzul w dokumentach) dotyczących danych osobowych np. formularze na stronach www, regulaminach pracy, oświadczeniach.

4.3.5. Opiniowanie umów, których przedmiotem – bezpośrednio lub pośrednio – są dane osobowe, w tym sporządzanie umów powierzenia przetwarzania danych, o których mowa w art. 31 Ustawy.

4.3.6. Wspieranie poszczególnych działów Spółek w Grupie LUMEN POLSKA oraz jej Zarządu w obszarach powiązanych z ochroną danych osobowych (opinie, analizy etc.)

4.3.7. Prowadzenie, przynajmniej raz do roku, szkoleń dla Użytkowników z zakresu ochrony danych osobowych. Szkolenia dotyczące zagadnień technicznych przetwarzania danych (zabezpieczenia logiczne, postępowanie z hasłami, etc.).

4.3.8. Analizowanie sytuacji oraz przyczyn, które doprowadziły do naruszenia zasad bezpieczeństwa, a także zabezpieczania wykrytych dowodów i śladów naruszenia bezpieczeństwa danych osobowych przetwarzanych w sposób tradycyjny (kartoteki papierowe) jak i elektronicznie (w tym ostatnim przypadku we współpracy z ASI).

4.3.9. Prowadzenie i koordynacja wewnętrznych audytów przestrzegania przepisów o ochronie danych osobowych, o których mowa w Rozdziale 11 niniejszej Polityki Bezpieczeństwa Danych Osobowych oraz przedstawiania raportów z ich wykonania do organu zarządzającego Współadministratorów.

4.3.10. Formułowanie pisemnych (papierowo lub elektronicznie) zaleceń oraz monitów w zakresie ochrony danych osobowych do Opiekunów Zbioru, Osób pracujących na zbiorze oraz pozostałych Użytkowników.

4.3.11. Pełnienie funkcji punktu kontaktowego dla (GIODO) UODO w kwestiach związanych z przetwarzaniem.

4.3.12. Wykonywanie innych zadań określonych w niniejszej Polityce Bezpieczeństwa Danych Osobowych oraz Instrukcji Zarządzania.

4.3.13. Zapewnienie prawidłowej eksploatacji systemu informatycznego, zgodnej z celami przetwarzania danych osobowych.

4.3.14. Nadzorowanie wykonywania kopii zapasowych oraz okresowe sprawdzanie pod kątem ich dalszej przydatności do odtwarzania danych osobowych w przypadku awarii systemu informatycznego.

4.3.15. Wyjaśnianie wszystkich zgłoszonych nieprawidłowości i incydentów mających lub mogących mieć wpływ na bezpieczeństwo systemu informatycznego.

4.3.16. Wykonywanie przeglądu, konserwacji oraz uaktualnienia systemu informatycznego służącego do przetwarzania danych.

4.3.17. Kontrola stanu bezpieczeństwa systemu informatycznego służącego do przetwarzania danych osobowych.

4.3.18. Uwierzytelnianie Użytkowników, w szczególności poprzez nadawanie, zmianę lub pozbawienie uprawnień dostępu do systemu informatycznego (szczegółowa procedura opisująca ww. czynności znajduje się w Instrukcji Zarządzania).

4.3.19. Monitorowanie uprawnień Użytkowników systemu informatycznego służącego do przetwarzania danych.

4.3.20. Wykonywanie polityki ochrony antywirusowej.

4.3.21. Wykonywanie innych zadań i prac wiążących się z dbaniem o bezpieczeństwo danych

osobowych przetwarzanych w systemach informatycznych wskazanych w Polityce Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania.

4.4. **Obowiązki Opiekunów Zbiorów**

4.4.1. Zawiadamianie Współadministratora o zamiarze utworzenia, likwidacji, modyfikacji struktury lub zmiany lokalizacji zbioru.

4.4.2. Zawiadamianie Współadministratora o zamiarze powierzenia przetwarzania danych zawartych w zbiorze, przy czym zawiadomienie to musi nastąpić zanim Spółki Grupy LUMEN POLSKA powierzy dane osobowe.

4.4.3. Zawiadamianie Współadministratora o zamiarze rozpoczęcia pracy na danych osobowych ze zbioru zewnętrznego (zakup bazy danych).

4.4.4. Współdziałanie z Współadministratorami w zakresie przestrzegania zasad ochrony danych osobowych opisanych w Polityce Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania.

4.4.5. Wykonywanie innych obowiązków wskazanych w pkt. 3.6.

4.5. **Obowiązki Użytkowników**

4.5.1. Przestrzeganie zasad ochrony danych osobowych określonych w Polityce Bezpieczeństwa Danych Osobowych i Instrukcji Zarządzania. Każdy Użytkownik zobowiązany jest zapoznać się, przed dopuszczeniem do przetwarzania danych, z wyżej wymienionymi dokumentami oraz złożyć stosowne oświadczenie, potwierdzające znajomość ich treści (**załącznik nr 1** do Polityki).

4.5.2. Uczestnictwo w szkoleniach z zakresu ochrony danych osobowych.

4.5.3. Przetwarzanie danych osobowych zgodnie z celami przetwarzania. Zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych w celu ochrony interesów osób, których te dane dotyczą.

4.5.4. Informowanie Współadministratora o wszelkich zauważonych nieprawidłowościach skutkujących obniżeniem poziomu ochrony danych osobowych.

4.5.5. Współpraca z Współadministratorem w zakresie wprowadzania zasad bezpiecznego przetwarzania danych osobowych oraz reagowania na wszelkie zdarzenia mogące mieć wpływ na obniżenia poziomu tego bezpieczeństwa.

4.5.6. Współpraca z Współadministratorem w zakresie wymiany informacji na tematy związane z ochroną danych osobowych.

4.5.7. Zapewnienie poufności danych osobowych, do których uzyskują dostęp.

4.5.8. W odniesieniu do sprzętu komputerowego i urządzeń teleinformatycznych, a także w związku z korzystaniem z zasobów systemów informatycznych służących do przetwarzania danych Użytkownik jest zobowiązany do:

- dbania o bezpieczną eksploatację systemu informatycznego; w przypadku wykrycia zagrożenia Użytkownik ma obowiązek poinformować o tym fakcie Współadministratora,
- dbania o bezpieczeństwo użytkowanego komputera, w tym celu Użytkownik ma obowiązek regularnie zmieniać hasła dostępowe do systemu operacyjnego oraz aplikacji służących do przetwarzania danych osobowych (obowiązek ten ma charakter bezwzględny jeśli istnieje podejrzenie, że hasło mogło zostać poznane przez osobę nieupoważnioną); hasła nie mogą być zapisywane i pozostawiane w łatwo dostępnych miejscach,
- wykazywania ostrożności przy odbieraniu poczty elektronicznej przychodzącej od nieznanych adresatów lub o podejrzanym tytule e-maila,

4.5.9. Dbanie o to, by dokumenty były przechowywane w zamkniętych szafach lub szufladach. Dostęp do kluczy mogą mieć tylko osoby upoważnione do przetwarzania danych.

4.6. **Obowiązki Personelu pomocniczego**

4.6.1. Zakaz przetwarzania danych osobowych (np. kserowania dokumentów, wynoszenia ich, wpuszczania do pomieszczeń osób postronnych etc.), do których otrzymują dostęp poprzez obecność w obszarach przetwarzania danych osobowych.

4.6.2. Przebywanie w obszarze przetwarzania danych tylko na podstawie zgody udzielonej przez Współadministratora. Zgoda, o której tu mowa stanowi **załącznik nr 6** do niniejszej Polityki Bezpieczeństwa.

4.6.3. Zachowanie w tajemnicy wszelkich danych osobowych, do których Personel pomocniczy uzyskał dostęp poprzez wykonywanie swoich czynności służbowych.

5. ZASADY UDOSTĘPNIANIA DANYCH OSOBOWYCH

5.1. Biorąc pod uwagę, że udostępnianie danych jest jedną z form ich przetwarzania, jest ono dopuszczalne wtedy, gdy spełniony jest jeden z warunków, o którym mowa w art. 6 Rozporządzenia ogólnego (artykuł określa warunki, które uzasadniają udostępnianie danych „zwykłych") bądź w art. 9 Rozporządzenia ogólnego (artykuł wylicza sytuacje, które uzasadniają udostępnienie danych szczególnych kategorii tzw. danych wrażliwych np. informacji o stanie zdrowia).

5.2. Udostępnienie danych „zwykłych" jest możliwe pod warunkiem ziszczenia się jednej z poniższych przesłanek (podmiot zwracający się o udostępnienie danych będzie w stanie wykazać, że przesłanka taka zachodzi):

- osoba, której dane dotyczą, wyrazi zgodę na udostępnienie danych osobowych,
- udostępnienie danych jest konieczne do wykonania umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- udostępnienie danych jest niezbędne dla wypełnienia obowiązku prawnego ciążącego na administratorze,
- udostępnienie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej,
- udostępnienie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Współadministratorowi (konieczność wskazania ogólnej podstawy prawnej),
- udostępnienie danych jest niezbędne dla wypełnienia prawnie uzasadnionych interesów realizowanych przez Współadministratora danych albo stronę trzecią.

5.3. Udostępnianie danych wrażliwych jest możliwe pod warunkiem ziszczenia się jednej z poniższych przesłanek (podmiot zwracający się o udostępnienie danych będzie w stanie wykazać, że przesłanka taka zachodzi):

- osoba, której dane dotyczą, wyrazi zgodę na piśmie na udostępnienie danych w jednym lub kilku konkretnych celach,
- przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Współadministratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą,
- udostępnienie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, nie jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
- udostępnienia dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą,
- udostępnienia dokonuje się w zakresie danych dotyczących osoby, która upubliczniła je w sposób oczywisty,
- udostępnienie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,
- udostępnienie danych jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą,
- udostępnienie danych jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i

usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia,

- udostępnienie danych jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego tj. ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową,
- udostępnienie danych jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, proporcjonalnych do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą,

5.4. Użytkownicy, których zadania służbowe wiążą się z udostępnianiem danych osobowych mają obowiązek prowadzić (w formie pisemnej lub elektronicznie) ewidencję danych, które są udostępniane (określającą wnioskodawcę, podstawę udostępnienia, zakres danych oraz datę ich udostępnienia). Wzór ewidencji stanowi **załącznik nr 4** do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

5.5. W razie wątpliwości czy dane osobowe mogą zostać udostępnione, Użytkownik zobowiązany jest zasięgnąć opinii Współadministratora.

6. ZASADY POWIERZANIA PRZETWARZANIA DANYCH OSOBOWYCH

6.1. Powierzenie przetwarzania danych osobowych Procesorom następuje w drodze umowy, o której mowa w art. 28 Rozporządzenia ogólnego. Zalecany wzór umowy powierzenia przetwarzania danych stanowi **załącznik nr 3** do Polityki Bezpieczeństwa Danych Osobowych.

6.2. Za przygotowanie właściwej umowy powierzenia przetwarzania danych odpowiedzialny jest Współadministrator. Przy przygotowaniu ww. umowy Współadministrator współpracuje z Opiekunem Zbioru, który inicjuje bądź jest bezpośrednio zaangażowany we współpracę z Procesorem.

6.3. Przekazanie zbiorów Procesorowi w celu ich przetwarzania nie powoduje zmiany właściwego administratora danych osobowych.

6.4. Procesor, któremu powierzono przetwarzanie danych obowiązany jest wykorzystywać powierzone mu dane wyłącznie w celach i w zakresie, które zostały wskazane w zawartej z nim umowie.

6.5. Procesor, któremu powierzono przetwarzanie danych obowiązany jest w szczególności do:

- stosowania odpowiednich środków ochrony danych osobowych, w tym do zapewnienia fizycznej ochrony pomieszczeń w których przetwarzane są dane, zapewnienia adekwatnych do zagrożeń środków organizacyjnych oraz informatycznych, zgodnie z przepisami prawa,
- niezwłocznego powiadomienia ADO o przypadkach naruszenia przetwarzania powierzonych danych osobowych oraz do dokumentowania wszelkich informacji, które mogą pomóc w ustaleniu okoliczności tego naruszenia,
- tworzenia kopii bezpieczeństwa systemów informatycznych, w których przetwarzane są powierzone dane osobowe, jeżeli jest to niezbędne do prawidłowej realizacji przedmiotu umowy,
- zapewnienia aby każdy pracownik i/lub współpracownik Procesora przetwarzający powierzone dane osobowe posiadał upoważnienie do przetwarzania tych danych osobowych,
- zniszczenia lub zwrotu przekazanych danych stosownie do zapisów umowy powierzenia przetwarzania danych.

6.6. Lista firm, którym Spółki Grypy LUMEN POLSKA powierzają dane osobowe do przetwarzania stanowi **załącznik nr 5** do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

7. WYKAZ OBSZARÓW, W KTÓRYCH PRZETWARZANE SĄ POSZCZEGÓLNE ZBIORY DANYCH OSOBOWYCH

7.1. **Zbiory w stosunku do których Spółki Grupy LUMEN POLSKA są Współadministratorami**

Nazwa zbioru danych	Adres miejsca przechowywania danych ze zbioru	Wykaz pomieszczeń (numer pokoju)
6.1.1. Zbiór „Pracownicy i współpracownicy"	• Biuro Długosza	• Serwerownia w Biurze Długosza (akta osobowe w formie elektronicznej) • Akta osobowe papierowe – szafa metalowa zamykana, Biuro Długosza
		• Agencja Finansowo-Księgowa „Raport" Sp. z o.o ul. Klecińska 182, 54-412 Wrocław
6.1.2. Zbiór „Kandydaci do pracy"	• Biuro Długosza	• Serwerownia w Biurze Długosza (aplikacje w formie elektronicznej)
6.1.3. Zbiór „Dane klientów biznesowych"	• Biuro Długosza	• Serwerownia w Biurze Długosza oraz Serwer plików QNAP w Biurze Długosza (plik w formie elektronicznej)
6.1.4. Zbiór „Baza danych marketingowa"	• Biuro Długosza	• Serwerownia w Biurze Długosza oraz Serwer plików QNAP w Biurze Długosza (plik w formie elektronicznej)
6.1.5. Zbiór „Baza danych relacji zewnętrznych"	• Biuro Długosza	• Serwerownia w Biurze Długosza oraz Serwer plików QNAP w Biurze Długosza (plik w formie elektronicznej)
6.1.6. Zbiór „Baza danych sprzedażowa"	• Biuro Długosza	• Serwerownia w Biurze Długosza oraz Serwer plików QNAP w Biurze Długosza (plik w formie elektronicznej)
		• Agencja Finansowo-Księgowa „Raport" Sp. z o.o ul. Klecińska 182, 54-412 Wrocław
6.1.7. Zbiór „Baza danych dostawców oraz danych zakupowych"	• Biuro Długosza	• Serwerownia w Biurze Długosza oraz Serwer plików QNAP w Biurze Długosza (plik w formie elektronicznej)

		• Agencja Finansowo-Księgowa „Raport" Sp. z o.o ul. Klecińska 182, 54-412 Wrocław
6.1.8. Zbiór „Ewidencja korespondencji przychodzącej/wychodzącej oraz proces archiwizacji"	• Biuro Długosza	• Recepcje każdego z biur Grupy LUMEN POLSKA
6.1.9. Zbiór „Baza zasobów finansowych"	• Biuro Długosza	• Serwerownia w Biurze Długosza oraz Serwer plików QNAP w Biurze Długosza (plik w formie elektronicznej)

Dane z opisanych wyżej zbiorów mogą być przetwarzane także w innych obszarach, ponieważ w firmie dopuszczalna jest praca zdalna (połączenie szyfrowane VPN) albo praca przy pomocy komputerów przenośnych.

8. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO ICH PRZETWARZANIA

8.1.1. Zbiór „Pracownicy i współpracownicy oraz zasoby ludzkie"

Zbiór danych osobowych o nazwie „Pracownicy i współpracownicy oraz zasoby ludzkie" przetwarzany jest w formie kartotek papierowych oraz w systemie informatycznym przy wykorzystaniu aplikacji:

- Sage Symfonia ERP
- Teczka personalna

8.1.2. Zbiór „Kandydaci do pracy"

Zbiór danych osobowych o nazwie „Kandydaci do pracy oraz zasoby ludzie" przetwarzany jest w formie papierowej oraz w systemie informatycznym przy wykorzystaniu aplikacji. Po zakończeniu rekrutacji aplikacje osobowe kandydatów do pracy są niszczone za pomocą niszczarki.

- Program pocztowy/ webmail

8.1.3. Zbiór „Dane klientów biznesowych"

Zbiór danych osobowych o nazwie „Klienci biznesowi" znajduje się na serwerze webowym i przetwarzany jest w systemie informatycznym przy wykorzystaniu aplikacji.

- Program pocztowy/ webmail
- Excel
- InsERT Subiekt nexo
- Sage Symfonia ERP
- ITCube CRM

8.1.4. Zbiór „Baza danych marketingowa"

Zbiór danych osobowych o nazwie „Marketing" znajduje się na serwerze webowym i przetwarzany jest w systemie informatycznym przy wykorzystaniu aplikacji.

- Program pocztowy/ webmail
- Excel
- ITCube CRM

8.1.5. Zbiór „Baza danych relacji zewnętrznych"

Zbiór danych osobowych o nazwie „Relacje zewnętrzne" znajduje się na serwerze webowym i przetwarzany jest w systemie informatycznym przy wykorzystaniu aplikacji.

- Program pocztowy/ webmail
- Excel
- ITCube CRM

8.1.6. Zbiór „Baza danych sprzedażowa"

Zbiór danych osobowych o nazwie „Baza sprzedażowa" znajduje się serwerze webowym i przetwarzany jest w formie papierowej oraz w systemie informatycznym przy wykorzystaniu aplikacji.

- ☐ Excel
- ☐ Sage Symfonia ERP
- ☐ InsERT Subiekt nexo
- ☐ Program pocztowy/webmail

8.1.7. Zbiór „Baza danych dostawców oraz danych zakupowych"

Zbiór danych osobowych o nazwie „Baza danych dostawców oraz danych zakupowych" przetwarzany jest w systemie informatycznym przy wykorzystaniu aplikacji.

- ☐ Excel
- ☐ Sage Symfonia ERP
- ☐ InsERT Subiekt nexo
- ☐ Program pocztowy/webmail

8.1.8. Ewidencja korespondencji przychodzącej/wychodzącej oraz proces archiwizacji"

Zbiór danych osobowych o nazwie „Ewidencja korespondencji przychodzącej/wychodzącej oraz proces archiwizacji Baza danych dostawców" przetwarzany jest w systemie informatycznym przy wykorzystaniu aplikacji.

- ☐ Excel
- ☐ Program pocztowy/webmail

8.1.9. Zbiór „Baza zasobów finansowych"

Zbiór danych osobowych o nazwie „Zasoby finansowe" przetwarzany jest w systemie informatycznym przy wykorzystaniu aplikacji.

- ☐ Excel
- ☐ Sage Symfonia ERP
- ☐ InsERT Subiekt nexo

9. OPIS STRUKTURY ZBIORÓW DANYCH WSKAZUJĄCY ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

8.1.1. Zbiór „Pracownicy i współpracownicy oraz zasoby ludzkie"

Lp.	System informatyczny	Zawartość pól informacyjnych
1.	Teczka personalna (papierowa) Sage Symfonia ERP (teczka elektroniczna) Płatnik	Imiona i nazwisko, imiona rodziców, nazwisko rodowe, data urodzenia, obywatelstwo, PESEL, NIP, miejsce zameldowania, adres zamieszkania, adres do korespondencji, informacja o stopniu niepełnosprawności, wykształcenie, zawód, przebieg dotychczasowego zatrudnienia, dodatkowe uprawnienia, zainteresowania, stan rodziny (imiona i nazwiska oraz daty urodzenia dzieci), osoba, którą należy powiadomić w razie wypadku (imię, nazwisko, adres i telefon), nr i seria dowodu osobistego, dane osoby ubezpieczonej (PESEL, NIP, nr i seria dowodu osobistego, imię i nazwisko, data urodzenia, stopień pokrewieństwa, informacja o stopniu niepełnosprawności, adres zamieszkania), nr rachunku bankowego

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. c) Rozporządzenia ogólnego.
Opiekun Zbioru (Opiekunowie Zbioru): Małgorzata Lubowicka-Sas, Członkowie Zarządu
Opis zbioru: Dane z opisywanego zbioru obejmują informacje o byłych i aktualnych pracownikach etatowych Spółki, a także osobach, które wykonują na jej rzecz czynności na podstawie umów cywilnoprawnych (umowy zlecenia, umowy o dzieło, umowy o świadczenie usług). Czynności związane z prowadzeniem dokumentacji pracowników prowadzone są przez Małgorzatę Lubowicką-Sas oraz Członków Zarządu.

Czynności związane z prowadzeniem dokumentacji pracowników prowadzone są także przez agencje Finansowo-Księgową „Raport" Sp. z o.o z siedzibą we Wrocławiu (Procesor) dla Spółek Grupy LUMEN POLSKA tj. PAL Sp. z o.o., PAL 1 Sp. z o.o. oraz SIDE Sp. z o.o.

Współadministratorzy przetwarzają dane osobowe ze zbioru „**Pracownicy i współpracownicy oraz zasoby ludzkie"** tylko i wyłącznie na podstawie prawa i w celu realizacji obowiązków nałożonych na Współadministratorów przepisami prawa, w związku z:
a) wypełnianiem obowiązków i uprawnień wynikających ze stosunku pracy, w tym obowiązków związanych z ubezpieczeniem społecznym, poprzez:
i. przetwarzanie danych osobowych Pracownika w procesie płacowym (m.in. wypłata wynagrodzeń i innych świadczeń wraz z potrąceniami);
ii. przetwarzanie danych osobowych Pracownika w procesie kadrowym (m.in. zawarcie umowy o pracę, aktualizacja danych osobowych pracownika, skierowanie na badania zdolności do pracy, prowadzenie i archiwizacja akt osobowych pracownika, doskonalenie zawodowe, kontrola czasu pracy, procedura na wypadek dyskryminacji i mobbingu, odpowiedzialność za powierzone pracownikowi mienie, realizacja wniosków o urlopy okolicznościowe i innych uprawnień/obowiązków wynikających ze stosunku pracy);
iii. przetwarzanie danych osobowych Pracownika dla realizacji zasad i procedur bezpieczeństwa i higieny pracy (np. w związku z wypadkiem przy pracy, chorobą zawodową, przeprowadzenie szkoleń z zakresu BHP);
iv. przetwarzanie danych Pracownika dla świadczeń z ubezpieczeń społecznych (m.in. rejestracja uprawnionego w ZUS, realizacja wniosków o urlopy macierzyńskie, urlopy ojcowskie, urlopy rodzicielskie i innych uprawnień wynikających z prawa ubezpieczeń społecznych);
b) zapewnieniem wypełnienia obowiązku wychowania w trzeźwości i przeciwdziałania alkoholizmowi (np. kontrola trzeźwości pracowników);
c) rozliczeniem podatku dochodowego od osób fizycznych (deklaracje podatkowe PIT), w tym prowadzeniem indywidualnych kart przychodów Pracownika;
d) wypełnianiem obowiązków wobec organów/urzędów państwowych/samorządowych (np. kontrole Państwowej Inspekcji Pracy, kontrole ZUS, kontrole Urzędu Skarbowego, żądania policji i innych organów ścigania, sporządzanie odpowiedzi na pisma/ żądania podmiotów uprawnionych ustawowo do udostępniania danych osobowych);
e) wypełnianiem obowiązków związanych z księgowaniem i sprawozdawczością finansową.

8.1.2. Zbiór „Kandydaci do pracy"

Lp.	System informatyczny	Zawartość pól informacyjnych
1.	Program pocztowy / webmail	Imiona i nazwisko, data urodzenia, adres zamieszkania, adres do korespondencji, wykształcenie, zawód, przebieg dotychczasowego zatrudnienia, dodatkowe uprawnienia, zainteresowania, wizerunek, adres IP

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. a) Rozporządzenia ogólnego.
Opiekun Zbioru (Opiekunowie Zbioru): Członkowie Zarządu, Petr Novak
Opis zbioru: Dane zbierane w celu prowadzenia procesu rekrutacji. Dane pozyskiwane są z różnych źródeł – są to dane pozyskiwane za pośrednictwem stron internetowych firm zajmujących się pozyskiwaniem pracowników, jak również aktualnych pracowników polecających swoich znajomych na dane stanowisko, na które prowadzona jest rekrutacja. Dane te trafiają do dyrektorów/kierowników poszczególnych działów Spółek Grupy LUMEN POLSKA prowadzącego rekrutację.

8.1.3. Zbiór „Dane klientów biznesowych"

Lp.	System informatyczny	Zawartość pól informacyjnych
1.	Program pocztowy / webmail; Excel; ITCube CRM; Sage Symfonia ERP; InsERT Subiekt nexo	Imię i nazwisko, adres e-mail, firma, telefon, kod pocztowy, miasto, adres IP

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. b) Rozporządzenia ogólnego.
Opiekun Zbioru (Opiekunowie Zbioru): Przemysław Śliwka, Petr Novak, Krzystof Jakacki.
Opis zbioru: Dane zbierane w ramach zawartej umowy, w celu realizacji bieżącego kontaktu, współpracy zawodowej, przyjmowania i składania ofert oraz prowadzenia korespondencji drogą

elektroniczną w procesach biznesowych i administracyjnych związanych z przedmiotem działalności Współadministratorów. Bez wykorzystania tego kanału komunikacji działalność Współadministratorów nie mogłaby sprostać rozwojowi technologicznemu, a kontakt z klientem mógłby okazać się znacznie utrudniony, a nawet niemożliwy. Baza danych jest obsługiwana przez Przemysława Śliwkę, Petra Novaka i Krzysztofa Jakackiego.

8.1.4. Zbiór „Baza marketingowa"

Lp.	System informatyczny	Zawartość pól informacyjnych
1.	Program pocztowy / webmail; Excel; ITCube CRM	Imię i nazwisko, adres e-mail, adres IP

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. a) Rozporządzenia ogólnego.
Opiekun Zbioru (Opiekunowie Zbioru): Marek Miszczuk
Opis zbioru: Dane zbierane w celach marketingowych, trafiają do opisywanego zbioru z różnych źródeł – są to dane pozyskiwane poprzez Spółki Grupy LUMEN POLSKA. Generalnie dane te trafiają do jednej bazy danych dedykowanej działaniom marketingowym dotyczącym działalności Spółek Grupy LUMEN POLSKA. Baza danych jest obsługiwana przez Marka Miszczuka.

Współadministratorzy przetwarzają dane osobowe tylko i wyłącznie na podstawie prawa i w ściśle określonych celach, tj. w celach marketingowych Współadministratorów. W tym w szczególności w celu promowania usług i towarów Współadministratorów, wydarzeń promocyjnych oraz marketingowych organizowanych przez Współadministratorów i innych wydarzeń zorganizowanych przez Współadministratorów w związku przedmiotem działalności, a także wydarzeń, w których Współadministratorzy są uczestnikami.

8.1.5. Zbiór „Baza danych relacji zewnętrznych"

Lp.	System informatyczny	Zawartość pól informacyjnych
1.	Program pocztowy / webmail; Excel; ITCube CRM .	Imię i nazwisko, adres e-mail, płeć, telefon, kod pocztowy, miasto, adres IP

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. a) Rozporządzenia ogólnego.
Opiekun Zbioru (Opiekunowie Zbioru): Przemysław Śliwka, Petr Novak, Krzystof Jakacki.
Opis zbioru: Dane zbierane w celach promowania Spółki. Baza danych jest obsługiwana przez Przemysława Śliwkę, Petra Novaka i Krzysztofa Jakackiego.

Dane osobowe, w tym m.in. adres poczty elektronicznej, są przetwarzane w celu realizacji bieżącego kontaktu, współpracy zawodowej, przyjmowania i składania ofert oraz prowadzenia korespondencji drogą elektroniczną w procesach biznesowych i administracyjnych związanych z przedmiotem działalności Współadministratorów. Bez wykorzystania tego kanału komunikacji działalność Współadministratorów nie mogłaby sprostać rozwojowi technologicznemu, a kontakt mógłby okazać się znacznie utrudniony, a nawet niemożliwy.

8.1.6. Zbiór „Baza danych sprzedażowa"

Lp.	System informatyczny	Zawartość pól informacyjnych
1.	Program pocztowy / webmail; Excel; Sage Symfonia ERP; InsERT Subiekt nexo	Imię i nazwisko, adres e-mail, płeć, telefon, kod pocztowy, miasto, dane firmy, adres IP

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. b) Rozporządzenia ogólnego.
Opiekun Zbioru (Opiekunowie Zbioru): Przemysław Śliwka, Petr Novak, Krzystof Jakacki.
Opis zbioru: Dane zbierane w celach sprzedażowych. Baza danych jest obsługiwana przez Przemysława Śliwkę, Petra Novaka i Krzysztofa Jakackiego.
Czynności związane z prowadzeniem procesów księgowo-rachunkowych prowadzone są także przez agencje Finansowo-Księgową „Raport" Sp. z o.o z siedzibą we Wrocławiu (Procesor) dla Spółek Grupy LUMEN POLSKA tj. PAL Sp. z o.o., PAL 1 Sp. z o.o. oraz SIDE Sp. z o.o.

8.1.7. Zbiór „Baza danych dostawców oraz danych zakupowych"

Lp.	System informatyczny	Zawartość pól informacyjnych
1.	Program pocztowy / webmail; Excel; Sage Symfonia ERP; InsERT Subiekt nexo	Imię i nazwisko, stanowisko służbowe, adres, adres mailowy, numer telefonu, nr rachunku bankowego, numer NIP

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. b) Rozporządzenia ogólnego.
Opiekun Zbioru (Opiekunowie Zbioru): Małgorzata Ziemecka, Petr Novak, Krzysztof Jakacki
Opis zbioru: Na opisywany zbiór składają się nazwy firm, dane kontaktowe osób z różnych firm, numery rachunków bankowych. Są to dane niezbędne do wykonywania codziennych obowiązków służbowych.

Czynności związane z prowadzeniem procesów księgowo-rachunkowych prowadzone są także przez agencje Finansowo-Księgową „Raport" Sp. z o.o z siedzibą we Wrocławiu (Procesor) dla Spółek Grupy LUMEN POLSKA tj. PAL Sp. z o.o., PAL 1 Sp. z o.o. oraz SIDE Sp. z o.o.

8.1.8. Zbiór „Ewidencja korespondencji wychodzącej/przychodzącej oraz archiwizacji"

Lp.	System informatyczny	Zawartość pól informacyjnych
1.	Program pocztowy / webmail; (Poczta Polska etc.)	Imię i nazwisko, stanowisko służbowe, adres, miejsce pracy

W tym zbiorze zbierane są dane w następującym zakresie:

- Imię i nazwisko
- Miejsce pracy
- Stanowisko służbowe
- Adres korespondencyjny

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. f) Rozporządzenia ogólnego.
Opiekun Zbioru (Opiekunowie Zbioru): Dagmara Kwiecień, Gabriela Kozłowska, Petr Novak i Krzysztof Jakacki.
Opis: W zbiorze tym znajdują się dane osobowe osób, do których i od których przychodzi korespondencja.

8.1.9. Zbiór „Baza zasobów finansowych"

Lp.	System informatyczny	Zawartość pól informacyjnych
1.	Excel; Sage Symfonia ERP; InsERT Subiekt nexo	Imię i nazwisko, stanowisko służbowe, adres, adres mailowy, numer telefonu

Podstawa prawna przetwarzania danych: art. 6 ust. 1 lit. b) Rozporządzenia ogólnego.
Opiekun Zbioru (Opiekunowie Zbioru): Gabriela Kozłowska, Petr Novak, Krzysztof Jakacki.
Opis zbioru: Na opisywany zbiór składają się nazwy firm, dane kontaktowe osób z różnych firm. Są to dane niezbędne do wykonywania codziennych obowiązków służbowych.

9 ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DO ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI DANYCH OSOBOWYCH

9.1. Środki ochrony fizycznej (budynki)	9.1.1. Żeby dostać się do każdego z biur Spółek Grypy LUMEN POLSKA niezbędne jest przejście przez recepcję budynku. Pracownicy uzyskują dostęp do budynków, pomieszczeń, dokumentów za pomocą kodu PIN, karty lub identyfikatora zbliżeniowego. 9.1.2. Biuro zabezpieczone przed pożarem poprzez system ppoż. 9.1.3. Budynki, w których znajdują się biura są nadzorowane przez ochronę. 9.1.4. Monitoring przy wejściach/wyjściach z biur. 9.1.5. Niepotrzebne dokumenty zawierające dane osobowe są niszczone przy pomocy niszczarek.
9.2. Środki ochrony fizycznej (serwerownia)	9.2.1 Serwerownia stanowi wydzielone pomieszczenie z limitowanym dostępem dla upoważnionych osób. Serwerownia główna znajduje się we Wrocławiu. 9.2.4. Serwerownia jest klimatyzowana w celu zapewnienia odpowiedniej temperatury dla urządzeń. 9.2.5. Serwery podpięte są do UPS'ów. Wejście do serwerowni zabezpieczone jest systemem alarmowym. Administracja budynku prowadzi rejestr osób pobierających i oddających klucze do pomieszczenia.
9.3. Środki ochrony logicznej serwerów	9.3.1 Serwery zabezpieczone są poprzez system. 9.3.2 Filtrowany jest ruch przychodzący i wychodzący na routerach. 9.3.3 Serwery pocztowe zabezpieczone są systemem antywirusowym i antyspamowym firmy Microsoft oraz antywirus ESET. 9.3.4 Serwery pracują pod kontrolą na bieżąco aktualizowanych systemów. 9.3.5 Logowanie do systemów spoza Spółek Grupy LUMEN POLSKA odbywa się za pośrednictwem szyfrowanych połączeń VPN.
9.4. Środki ochrony w ramach oprogramowania systemów oraz narzędzi i programów służących do przetwarzania danych osobowych	9.4.1. W Spółkach Grupy LUMEN POLSKA stosowane jest Active Directory umożliwiające nadawanie różnych poziomów uprawnień w oparciu o grupy. Logowanie do Active Directory wymaga uwierzytelnienia poprzez podanie loginu i hasła składającego się z minimum 8 znakowym będących kombinacją trzech z pośród czterech grup znakowych: wielkich i małych liter, znaków specjalnych i cyfr. 9.4.3. Hasło domenowe musi być zmieniane nie rzadziej niż co 42 dni (system wymusza zmianę automatycznie). 9.4.4. Jeśli dany system informatyczny nie jest

	logowany przez Active Directory to wymagane jest wówczas osobne uwierzytelnienie poprzez podanie indywidualnie nadanego loginu i wpisania hasła. 9.4.5. Na komputerach zainstalowane są wygaszacze ekranów aktywujące się po 5 minutach braku aktywności. 9.4.6. Wszystkie komputery zostały wyposażone w program antywirusowy (zarządzany centralnie). 9.4.7. Zablokowano strony www uznane za niebezpieczne. 9.4.8. Na zewnętrz widocznych jest 5 adresów IP. 9.4.9. Dla wszystkich systemów informatycznych służących do przetwarzania danych osobowych wykonywane są kopie zapasowe. 9.4.10. Kopie zapasowe przechowywane są w innej lokacji niż serwerownia główna. 9.4.2. Wszystkie systemy informatyczne są na bieżąco serwisowane, a nadzorowane przez firmę świadczącą usługi informatyczne.
	pośród czterech grup znakowych: wielkich i małych liter, znaków specjalnych i cyfr. 9.4.11. Hasło domenowe musi być zmieniane nie rzadziej niż co 42 dni (system wymusza zmianę automatycznie). 9.4.12. Jeśli dany system informatyczny nie jest logowany przez Active Directory to wymagane jest wówczas osobne uwierzytelnienie poprzez podanie indywidualnie nadanego loginu i wpisania hasła. 9.4.13. Na komputerach zainstalowane są wygaszacze ekranów aktywujące się po 5 minutach braku aktywności. 9.4.14. Wszystkie komputery zostały wyposażone w program antywirusowy (zarządzany centralnie). 9.4.15. Zablokowano strony www uznane za niebezpieczne. 9.4.16. Na zewnętrz widocznych jest 5 adresów IP. 9.4.17. Dla wszystkich systemów informatycznych służących do przetwarzania danych osobowych wykonywane są kopie zapasowe. 9.4.18. Kopie zapasowe przechowywane są w innej lokacji niż serwerownia główna. 9.4.19. Wszystkie systemy informatyczne są na bieżąco serwisowane, a nadzorowane przez firmę świadczącą usługi informatyczne.

9.5. Środki organizacyjne stosowane przez Grupę LUMEN POLSKA w celu ochrony danych osobowych	9.5.1. Każda osoba mająca dostęp do danych została zapoznana z zasadami bezpiecznego przetwarzania danych wynikającymi z niniejszej Polityki oraz Instrukcji Zarządzania. 9.5.2. Dostęp do pomieszczeń, w których są przetwarzane dane osobowe posiadają tylko osoby upoważnione. Prowadzona jest kontrola dostępu z dziennikiem zdarzeń. 9.5.3. Dostęp do komputerów na których są przetwarzane dane osobowe posiadają tylko osoby upoważnione. 9.5.4. Osoby mające dostęp do danych osobowych zobowiązane są, na mocy niniejszej Polityki, do zachowania danych osobowych oraz informacji o sposobach ich zabezpieczenia w tajemnicy. 9.5.5. Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych. 9.5.6. Prowadzona jest ewidencja incydentów naruszenia zasad ochrony danych osobowych. 9.5.7. Prowadzona jest ewidencja nadawanych uprawnień. 9.5.8. Prowadzona jest ewidencja przekazywania sprzętu.
	9.5.9. Prowadzona jest dokumentacja obejmująca Politykę Bezpieczeństwa oraz Instrukcję Zarządzania.

10. POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

10.1. W przypadku stwierdzenia naruszenia ochrony danych osobowych, osoba stwierdzająca naruszenie jest zobowiązana do natychmiastowego zgłoszenia tego naruszenia Współadministratorowi (lub IODO jeśli został powołany).

10.2. Zgłoszenie, o którym mowa w pkt. 10.1.powyżej musi opisywać charakter naruszenia, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie, jak również opisywać możliwe konsekwencje naruszenia ochrony danych osobowych.

10.3. Po otrzymaniu zgłoszenia, Współadministrator dokonuje oszacowania konsekwencji jakie mogą nastąpić wskutek naruszenia, jak również stosuje wszelkie środki jakie mogą zaradzić naruszeniu i zminimalizować jego ewentualne negatywne skutki.

10.4. Współadministrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu. Raport o sytuacji naruszenia bezpieczeństwa danych osobowych stanowi **Załącznik nr 7**.

10.5. Obowiązek zgłaszania naruszeń, o których mowa w pkt. 10 ciąży na każdym Użytkowniku.

10.6. Współadministrator podejmuje decyzję o ewentualnym zgłoszeniu danego naruszenia do właściwego organu nadzorczego w trybie Artykułu 33 Rozporządzenia ogólnego tj. Współadministrator dokonuje zgłoszenia organowi nadzorczemu bez zbędnej zwłoki, w terminie 72 godzin po stwierdzeniu naruszenia, chyba że jest mało prawdopodobne by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

10.7. Współadministrator podejmuje decyzję o zawiadomieniu osoby, której dane dotyczą o naruszeniu, takie zawiadomienie jest obowiązkowe jeżeli naruszenie danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osoby fizycznej. W zawiadomieniu Współadministrator podaje osobie, której dane dotyczą informacje i środki, o których mowa w

pkt. 10.2 powyżej.

11. PRZEGLĄDY POLITYKI BEZPIECZEŃSTWA I AUDYTY

11.1 Aktualizacja

11.1.1. Aktualizacji niniejszej Polityki Bezpieczeństwa Danych Osobowych dokonuje Współadministratorzy.

11.1.2. Opiekunowie Zbiorów mają obowiązek współpracować z Współadministratorami, zwłaszcza w odniesieniu do aktualności informacji dotyczących systemów informatycznych, zakresów danych, Procesorów, etc. Informacje mające wpływ na aktualność Polityki Bezpieczeństwa Danych Osobowych powinny być przekazywane do Współadministratorów (drogą mailową) najdalej w ciągu 7 dni od okoliczności uzasadniających dokonanie zmiany, z zastrzeżeniem, że umowy powierzenia powinny być przedstawiane do zaopiniowania/stworzenia przed rozpoczęciem współpracy z potencjalnym Procesorem.

11.1.3. Niniejsza Polityka Bezpieczeństwa Danych Osobowych powinna być poddawana przeglądowi przynajmniej raz w roku. W razie istotnych zmian dotyczących przetwarzania danych osobowych Współadministratorzy mogą zarządzić przegląd Polityki Bezpieczeństwa stosownie do występujących sytuacji i zdarzeń.

11.1.4. Współadministratorzy analizują, czy Polityka Bezpieczeństwa Danych Osobowych i Instrukcja Zarządzania oraz inne dokumenty, powiązane z nimi są adekwatne do:

- zmian w budowie systemu informatycznego,
- zmian organizacyjnych Współadministratorów,
- zmian w obowiązującym prawie,
- innych zmian, które mogą mieć wpływ na bezpieczeństwo danych.

11.2. Audyty

11.2.1. Raz do roku Współadministratorzy przeprowadzają audyt wewnętrzny, mający na celu ustalenie stopnia zgodności działalności Grupy LUMEN POLSKA z Rozporządzeniem ogólnym, Ustawą, Rozporządzeniem i Przepisami szczególnymi.

11.2.2. Oprócz audytu, o którym mowa w pkt. 10.2.1., Współadministratorzy mogą zarządzić audyt *ad hoc* np. po zaistnieniu incydentu mającego wpływ na bezpieczeństwo danych osobowych.

12. POSTANOWIENIA KOŃCOWE

12.1. Z treścią niniejszej Polityki Bezpieczeństwa Danych Osobowych i jej załącznikami powinni zapoznać się wszyscy Użytkownicy (w tym Opiekunowie Zbiorów), których obowiązki służbowe wiążą się z koniecznością dostępu do danych osobowych i ich przetwarzaniem.

12.2. Naruszenie postanowień niniejszej Polityki Bezpieczeństwa Danych Osobowych przez osoby zatrudnione w Grupie LUMEN POLSKA (bez względu na formę umowy) może skutkować koniecznością rozwiązania stosownej umowy (w przypadku pracowników etatowych naruszenie jej postanowień może zostać uznane za ciężkie naruszenie obowiązków pracowniczych w rozumieniu przepisów kodeksu pracy).

12.3. Niniejszą Politykę Bezpieczeństwa Danych Osobowych i jej załączniki można przedstawiać partnerom lub innym podmiotom współpracującym z Grupą LUMEN POLSKA na podstawie pisemnej zgody udzielonej przez Współadministratorów.

12.4. Niniejsza Polityka Bezpieczeństwa Danych Osobowych wchodzi w życie z dniem jej podpisania.

13. WYKAZ ZAŁĄCZNIKÓW

Załącznik nr 1 – Oświadczenie o zapoznaniu się z systemem ochrony danych osobowych
Załącznik nr 2 – Oświadczenie o zachowaniu danych osobowych i sposobów ich zabezpieczenia w tajemnicy
Załącznik nr 3 - Wzór umowy powierzenia przetwarzania danych osobowych
Załącznik nr 4 – Ewidencja udostępnionych danych osobowych
Załącznik nr 5 – Lista firm, którym Spółka powierza przetwarzanie danych osobowych
Załącznik nr 6 – Wzór zgody na przebywanie w obszarze przetwarzania danych osobowych
Załącznik nr 7 – Wzór raportu o sytuacji naruszenia bezpieczeństwa danych osobowych

OŚWIADCZENIE
O ZAPOZNANIU SIĘ Z SYSTEMEM OCHRONY DANYCH OSOBOWYCH

Ja, niżej podpisana(y) .....,

oświadczam, że zostałam(em):

1. poinstruowana(y) w zakresie bezpiecznego przetwarzania danych osobowych w świetle przepisów prawa, w szczególności:
   - ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (tekst jednolity: Dz.U.2018.1000),
   - rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),
   - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (GDPR - General Data Protection Regulation),
2. zapoznana(y) z obowiązującymi w Grupie LUMEN POLSKA dokumentami: polityką bezpieczeństwa danych osobowych oraz instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

_____
(data i podpis składającego oświadczenie)

Wrocław, dnia .....

OŚWIADCZENIE
O ZACHOWANIU DANYCH OSOBOWYCH W TAJEMNICY

Ja, niżej podpisany(a) .....,
oświadczam, że:
Współpracuję z ---------- z siedzibą -------- (**Grupa LUMEN POLSKA**) na podstawie umowy ..... (Umowa) oraz:

1. Zobowiązuję się do zachowania w tajemnicy wszelkich danych osobowych przekazanych mi przez Grupę LUMEN POLSKA bądź uzyskanych przeze mnie ustnie, pisemnie lub w jakiejkolwiek innej formie, jakąkolwiek drogą na podstawie zawartej Umowy oraz wykorzystywanie ich jedynie w celach związanych z wykonywaniem powierzonych zadań. Powyższy obowiązek rozciąga się również na okres po zakończeniu współpracy z Grupą LUMEN POLSKA. Przez dane osobowe rozumie się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
2. Niniejsze oświadczenie obejmuje również obowiązek zachowania w tajemnicy wszelkich informacji na temat sposobów zabezpieczeń danych osobowych przetwarzanych w Grupie LUMEN POLSKA. Powyższy obowiązek rozciąga się również na okres po zakończeniu współpracy z Grupą LUMEN POLSKA.
3. Jednocześnie oświadczam, że są mi znane przepisy dotyczące odpowiedzialności karnej za przetwarzanie danych osobowych, których przetwarzanie jest zabronione oraz za przetwarzanie danych osobowych przez osoby nieuprawnione.
4. Po rozwiązaniu lub wygaśnięciu Umowy, jak również na każde żądanie Grupy LUMEN POLSKA zobowiązuję się niezwłocznie do natychmiastowego zwrotu wszelkich materiałów i dokumentów zawierających dane osobowe, jakie znajdą się w moim posiadaniu lub jakie otrzymam w związku z Umową.
5. Jednocześnie przyjmuję do wiadomości, iż naruszenie powyższych obowiązków będzie powodowało pociągnięcie do odpowiedzialności karnej i cywilnej oraz może skutkować rozwiązaniem Umowy w trybie natychmiastowym.

_____
(podpis składającego oświadczenie)

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu .../.../... w ..... pomiędzy:

Spółką [x] z siedzibą w [x], przy ulicy [x], wpisaną do rejestru przedsiębiorców pod numerem [x], posiadającą numer [x], numer REGON [x], reprezentowaną przez:

1. ...
2. ...

zwaną dalej „**Administratorem**"

Niezależnie od kategorii osób, których dane, Administratorem Danych Osobowych wszystkich danych osobowych w rozumieniu RODO są wspólnie spółki Grupy LUMEN POLSKA, związane porozumieniem o współadministracji dalej: Współadministratorzy.

a

Spółką [x] z siedzibą w [x], przy ulicy [x], wpisaną do rejestru przedsiębiorców pod numerem [x], posiadającą numer [x], numer REGON [x], reprezentowaną przez:

---

zwaną dalej „**Procesorem**",

dalej łącznie zwanymi „**Stronami**" lub pojedynczo „**Stroną**".

§1

Definicje

Ilekroć w niniejszej umowie powierzenia przetwarzania danych osobowych mowa o:

1. **„Administratorze danych"** – wspólnie spółki Grupy LUMEN POLSKA, związane porozumieniem o współadministracji, które to wspólnie z innymi ustalają cele i sposoby przetwarzania danych osobowych, dalej także: **Współadministratorzy**,
2. **„Danych osobowych"** – rozumie się przez to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"),
3. **„Przetwarzaniu danych"** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,

4. **„Systemie informatycznym"** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych,

5. **„Umowie"** – rozumie się przez to niniejszą umowę powierzenia przetwarzania danych osobowych,

6. **„RODO"** – rozumie się przez to Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych uchylenia dyrektywy 95/46/WE,

7. „**Współadministratorzy**" – oznaczają współadministratorów w rozumieniu art. 26 Rozporządzenia, tj. dwóch lub więcej administratorów wspólnie ustalających cele i sposoby przetwarzania. Współadministratorami danych w niniejszej Polityki Bezpieczeństwa są: DNG Sp. z o.o. ul. Prosta 36, 50-508 Wrocław, PAL Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, PAL 1 Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, PRIME Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, SIDE Sp. z o.o. ul. Długosza 42-46, 51-162 Wrocław, Remote MANAGEMENT Sp. z o.o. ul. Prosta 36, 50-508 Wrocław. Współadministratorzy wspólnie ustalili, iż podmiotem odpowiedzialnym za realizację obowiązków wynikających z Rozporządzenia względem osób, których dane są przetwarzane, jest LUMEN POLSKA Sp. z o.o. z siedzibą we Wrocławiu.

§2

Przedmiot Umowy

1. Przedmiotem Umowy jest powierzenie Procesorowi przez Administratora, przetwarzania danych osobowych w związku z prowadzeniem współpracy w zakresie świadczenia przez Procesora na rzecz Administratora następujących usług:

   a) ----------

   b) ----------.

2. Administrator oświadcza, że jest administratorem danych, o których mowa w § 3 ust. 1 Umowy.

3. Administrator powierza Procesorowi przetwarzanie danych osobowych, a Procesor zobowiązuje się do ich przetwarzania zgodnego z prawem i Umową.

4. Procesor będzie przetwarzać dane osobowe wyłącznie w zakresie, celu i okresie przewidzianym w Umowie.

§3

Powierzenie przetwarzania danych osobowych

1. Administrator powierza Procesorowi przetwarzanie danych osobowych:

   - ----------

- ----------

- ----------

2. Zakres powierzonych do przetwarzania danych osobowych obejmuje: ----------
----------.

3. Celem powierzenia przetwarzania danych osobowych jest prawidłowe wykonanie przez Procesora usług określonych w § 2 ust. 1 Umowy.

4. Procesor, w zakresie realizacji celu określonego w ust. 3 powyżej, jest uprawniony do wykonywania następujących operacji na danych: zbieranie, utrwalanie, organizowanie, porządkowanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, przechowywanie, opracowywanie, ograniczanie, usuwanie lub niszczenie.

§4

Obowiązki Procesora

1. Procesor będzie przetwarzał powierzone mu dane osobowe na warunkach i zgodnie z treścią obowiązujących w tym zakresie przepisów prawa. W szczególności przetwarzanie powierzonych danych odbywało się będzie w zgodzie z postanowieniami: RODO, Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100 poz. 1024 z późn. zm.) oraz innych właściwych w zakresie przetwarzania danych osobowych przepisów prawa, w tym polskiej ustawy o ochronie danych osobowych.

2. W związku z powierzeniem przetwarzania danych osobowych Procesor zobowiązuje się do:

   2.1. przetwarzania danych osobowych wyłącznie na udokumentowane polecenie Administratora,

   2.2. zapewnienia by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,

   2.3. podjęcia wszelkich środków gwarantujących bezpieczeństwo powierzonych do przetwarzania danych osobowych, w tym m.in. do wdrożenia, przy uwzględnieniu stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, odpowiednich środków technicznych i organizacyjnych, w celu zapewnienia stopnia bezpieczeństwa odpowiadającemu temu ryzyku, w tym między innymi w stosownym przypadku:

      2.3.1. pseudonimizacji i szyfrowania danych osobowych,

2.3.2. zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,

2.3.3. zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,

2.3.4. regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2.4. przestrzegania określonych w § 6 Umowy warunków podpowierzenia przetwarzania danych osobowych innemu podmiotowi,

2.5. aktywnej współpracy z Administratorem przez cały okres trwania powierzenia przetwarzania danych osobowych, która w szczególności polega na tym, iż Procesor biorąc pod uwagę charakter przetwarzania, poprzez odpowiednie środki techniczne i organizacyjne, w miarę możliwości będzie pomagał Administratorowi wywiązywać się z obowiązków względem osób, których dane dotyczą oraz, uwzględniając charakter przetwarzania oraz dostępne mu informacje, będzie pomagał Administratorowi wywiązywać się z obowiązków w zakresie zagwarantowania bezpieczeństwa danych osobowych, w szczególności w zakresie usunięcia na żądanie osoby której dane dotyczą przekazane mu przez Administratora wszelkich łącz do danych osobowych, kopi tych danych lub ich replikacji.

3. Procesor zobowiązuje się niezwłocznie zawiadomić Administratora:

3.1. każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia Administratora wynika z przepisów prawa, a w szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienie poufności wszczętego dochodzenia,

3.2. każdym nieupoważnionym dostępie do danych osobowych,

3.3. każdym żądaniu otrzymanym bezpośrednio od osoby, której dane przetwarza, w zakresie przetwarzania dotyczącej jej danych osobowych, powstrzymując się jednocześnie od odpowiedzi na żądanie, chyba, że zostanie do tego upoważniony przez Administratora.

4. Procesor, na każdy pisemny wniosek Administratora, zobowiązany jest do udzielenia kompleksowej, pisemnej odpowiedzi, na skierowane przez Administratora pytania dotyczące kwestii związanych z przetwarzaniem powierzonych danych osobowych.

5. Odpowiedzi, o której mowa w ust. 4 powyżej, Procesor udzieli niezwłocznie, nie później niż w terminie 7 dni roboczych od dnia otrzymania wniosku Administratora.

§5

Prawo kontroli

1. Administrator ma prawo do kontroli przetwarzania przez Procesora powierzonych mu danych osobowych z punktu widzenia zgodności tego przetwarzania z przepisami prawa oraz

postanowieniami Umowy w postaci audytu realizowanego przez Administratora lub audytora upoważnionego przez Administratora.

2. Informacja o terminie i zakresie audytu, o którym mowa w ust. 1 powyżej, będzie przekazana Procesorowi z co najmniej 24-godzinnym wyprzedzeniem.

3. Procesor umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora, przeprowadzanie audytu, o którym mowa w ust. 1 i zobowiązuje się ściśle współpracować w celu jego prawidłowego przeprowadzenia. W szczególności, Procesor zobowiązany jest udostępnić wgląd do wszystkich materiałów oraz systemów, w których realizowane jest przetwarzanie danych Administratora oraz umożliwić kontakt z osobami zaangażowanymi w ich przetwarzanie.

4. Administrator lub audytor upoważniony przez Administratora, przed rozpoczęciem czynności audytowych podpisze zobowiązanie o zachowaniu w poufności wszelkich informacji uzyskanych podczas realizacji audytu, w tym danych osobowych, których administratorem danych jest Procesor.

§6

Podpowierzenie

1. Procesor ma prawo podpowierzania danych osobowych, o których mowa w § 3 ust. 1 Umowy, w zakresie i celu niezbędnym do realizacji celu powierzenia przetwarzania danych osobowych określonego w § 3 ust. 3 Umowy (ogólna zgoda Administratora na podpowierzenie przetwarzania danych osobowych).

2. Procesor jest zobowiązany do poinformowania Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

3. Jeżeli do wykonania w imieniu Administratora konkretnych czynności przetwarzania Procesor korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający, w drodze zawartej pomiędzy tym podmiotem a Procesorem umowy, nałożone zostaną te same obowiązki ochrony danych jak w § 4 Umowy, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych ochrony danych.

4. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na Procesorze.

§7

Odpowiedzialność Procesora

1. Procesor jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową oraz obowiązującymi w tym zakresie przepisami prawa.

2. W przypadku ujawnienia okoliczności stanowiących uchybienia w zakresie wykonywania zapisów Umowy lub obowiązujących w tym zakresie przepisów prawa z winy Procesora, Procesor zobowiązuje się do ich usunięcia w wyznaczonym przez Administratora rozsądnym terminie. W przypadkach naruszeń podstawowych zasad przetwarzania danych osobowych Administrator ma prawo wezwać Procesora do natychmiastowego usunięcia naruszenia. W razie niezastosowania się przez Procesora do wydanych przez Administratora wytycznych, Administrator jest uprawniony do żądania zapłaty kary umownej w wysokości 1 000 zł (słownie: tysiąc złotych) za każdy przypadek stwierdzonej nieprawidłowości.

3. Jeżeli podobne nieprawidłowości zostaną ujawnione ponownie, Administrator jest uprawniony do żądania zapłaty kary umownej bez wyznaczania terminu do ich usunięcia.

4. W przypadku naruszenia postanowień Umowy lub obowiązujących w tym zakresie przepisów prawa z przyczyn leżących po stronie Procesora, w następstwie, czego Administrator, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Procesor zobowiązuje się do zapłaty Administratorowi równowartości roszczeń osób trzecich, kar oraz równowartości kosztów postępowania sądowego, które będą wynikiem nieprawidłowego działania Procesora i zostaną stwierdzone ostatecznym wyrokiem sądowym lub decyzją administracyjną.

5. Administratorowi przysługuje względem Procesora prawo do dochodzenia odszkodowania przewyższającego zastrzeżoną karę umowę – do pełnej wysokości poniesionej szkody.

§8

Usunięcie lub zwrot danych osobowych

1. Zależnie od decyzji Administratora w tym zakresie, w terminie do 14 dni roboczych od dnia zakończenia Umowy, Procesor jest zobowiązany do usunięcia lub zwrotu wszelkich powierzonych mu danych osobowych oraz usunięcia wszelkich ich istniejących kopii, chyba, że obowiązujące przepisy prawa nakazują przechowywanie tych danych osobowych.

2. Powierzenie przetwarzania danych osobowych trwa do upływu wyżej wskazanego terminu.

§9

Czas trwania i wypowiedzenie Umowy

1. Umowa zawarta jest na czas nieokreślony.

2. Każda ze Stron ma prawo złożenia drugiej Stronie oświadczenia o wypowiedzeniu Umowy z zachowaniem 2 (dwu) tygodniowego okresu wypowiedzenia.

2. Administrator ma prawo wypowiedzieć Umowę w trybie natychmiastowym, gdy Procesor:

   2.1. wykorzystał dane osobowe w sposób niezgodny z Umową,

   2.2. wykonuje Umowę niezgodnie z obowiązującymi w tym zakresie przepisami prawa,

2.3. nie zaprzestał niewłaściwego przetwarzania danych osobowych,

2.4. zawiadomił o swojej niezdolności do wypełnienia Umowy, a w szczególności wymagań określonych w § 4 Umowy.

3. Jeżeli jedna ze Stron rażąco narusza zobowiązania wynikające z Umowy, druga Strona może wypowiedzieć Umowę ze skutkiem natychmiastowym oraz żądać naprawienia szkody poniesionej na skutek takiego naruszenia.

4. Oświadczenie o wypowiedzeniu Umowy wymaga formy pisemnej pod rygorem nieważności.

§10

Pozostałe postanowienia

1. Wszystkie dane osobowe przetwarzane przez Procesora są własnością Administratora.

2. Przetwarzanie danych dozwolone jest wyłącznie w celu określonym w § 3 ust. 3 Umowy.

3. Wykorzystanie przez Procesora danych Administratora w celach innych niż określone Umową wymaga każdorazowo pisemnej zgody Administratora.

§11

Postanowienia końcowe

1. W sprawach nieuregulowanych postanowieniami Umowy zastosowanie będą mieć właściwe w tym zakresie przepisy prawa polskiego.

2. Wszelkie zmiany, uzupełnienia lub rozwiązanie Umowy wymagają zachowania formy pisemnej takie samej w jakiej niniejsza Umowa została zawarta pod rygorem nieważności.

3. Strony zgodnie oświadczają, iż w przypadku sporów powstałych na tle realizacji Umowy dążyć będą do polubownego ich załatwienia. W przypadku, gdy nie dojdzie do załatwienia sporu w powyższy sposób, właściwym do jego rozstrzygnięcia będzie sąd powszechny właściwy miejscowo według właściwości ogólnej.

4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Administrator: **Procesor:**

_____ _____

... ...

Ewidencja udostępniania danych osobowych organom uprawnionym i podmiotom trzecim

Lp.	Podmiot, który zwrócił się z prośbą o udostępnienie danych	Nazwa zbioru danych osobowych	Cel udostępnienia danych/podstawa prawna	Zakres udostępnionych danych	Data udostępnienia

LISTA FIRM, KTÓRYM GRUPA LUMEN POLSKA POWIERZA PRZETWARZANIE DANYCH OSOBOWYCH

Lista firm:

Lp.	Nazwa firmy/instytucji	Siedziba
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		

UPOWAŻNIENIE NR .....
DO PRZEBYWANIA W OBSZARZE PRZETWARZANIA DANYCH OSOBOWYCH

Upoważniam Panią/a.....
będącą/będącym pracownikiem firmy

.....
współpracującej z ---------- (dalej „**Grupa LUMEN POLSKA**") w zakresie .....
do przebywania w godz. ..... w biurze Grupy LUMEN POLSKA przy ul. ----------.

Upoważniający informuje, że ww. lokalizacja stanowi obszar, w którym przetwarzane są dane osobowe. Niniejsze upoważnienie jest ważne na czas trwania Pana/Pani współpracy z firmą ..... i wykonywania na rzecz Grupy LUMEN POLSKA usług wskazanych w umowie między ww. firmą a Grupą LUMEN POLSKA.

Pouczenie:

1. Osoba upoważniona zobowiązuje się do nieprzetwarzania danych osobowych znajdujących się w obszarach, o których mowa wyżej, w tym w szczególności do wynoszenia dokumentów, robienia ich kserokopii, utrwalania w innej postaci (np. cyfrowej).
2. Osoba upoważniona zobowiązuje się do zachowania w tajemnicy wszelkich informacji na temat sposobów zabezpieczeń danych osobowych przetwarzanych w Grupie LUMEN POLSKA.
3. Osoba upoważniona oświadcza, że są jej znane przepisy dotyczące odpowiedzialności karnej za przetwarzanie danych osobowych, których przetwarzanie jest zabronione oraz za przetwarzanie danych osobowych przez osoby nieuprawnione.

.....
(data i podpis ADO)

.....
(podpis osoby upoważnianej)

Załącznik nr 7 wzór raportu o naruszeniu bezpieczeństwa danych osobowych

RAPORT
z naruszenia bezpieczeństwa danych osobowych

1. Data: ..... Godzina: .....
2. Osoba powiadamiająca o zaistniałym zdarzeniu: ..... (imię, nazwisko, stanowisko, nazwa użytkownika - jeśli występuje)
3. Lokalizacja zdarzenia: ..... (np. nr pokoju, nazwa pomieszczenia)
4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące: ....
5. Przyczyny wystąpienia zdarzenia: ....
6. Podjęte działania: ....
7. Postępowanie wyjaśniające: ....

.....
(data, podpis ADO)