Lumiko Sp. z o.o.
ul. Międzyrzecka 81
21-400 Łuków, Poland
tel. +48 25 798 20 26

NIP: 8252030306 | KRS: 0000243924

OCHRONA DANYCH OSOBOWYCH W LUMIKO SP. Z O.O.

§ 1
Postanowienia ogólne

1. Niniejszy dokument zatytułowany: „Ochrona danych osobowych w Lumiko Sp. z o.o.” ma za zadanie w sposób skondensowany wskazać zasady i regulacje ochrony danych osobowych w Lumiko Sp z o.o.
2. Realizacji obowiązków wynikających z art. 24 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 (Dz.Urz.UE.L Nr 119, str. 1 L w Lumiko Sp. z o.o. służy szereg dokumentów i działań wdrożonych w dniu 25.05.2018r. takich jak: „ Polityką Bezpieczeństwa w Lumiko Sp. z o.o., Instrukcja zarządzania systemem informatycznym.

§ 2
Definicje

Ilekroć w procedurze jest mowa o:

1) **LUMIKO lub pracodawcy** – rozumie się przez to LUMIKO Sp. z o.o. z siedzibą w Łukowie, ul. Międzyrzecka 81; 21-400 Łuków, wpisaną do Rejestru Przedsiębiorców przez Sąd Rejonowy Lublin – Wschód w Lublinie z siedzibą w Świdniku VI Wydział Krajowego Rejestru Sądowego pod numerem KRS: 0000243924, REGON: 060064542, NIP: 8252030306; kapitał zakładowy 2 500 000 zł;
2) **Administratorze danych (lub „ADO”)** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, które decydują o celach i środkach przetwarzania danych osobowych. Administratorem danych jest zatem : LUMIKO Sp. z o.o. z siedzibą w Łukowie, ul. Międzyrzecka 81; 21-400 Łuków;
3) **Prezes Urzędu Ochrony danych Osobowych (PUODO) –** organ właściwy do spraw ochrony danych osobowych na terytorium Polski.
4) **Dane osobowe lub dane** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
5) **Dane osobowe wrażliwe –** należy przez to rozumieć dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej oraz dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

6) **Zbiór danych osobowych** – należy przez to rozumieć uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
7) **Przetwarzanie danych osobowych** – należy przez to rozumieć między innymi operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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

§ 3
Administrator Danych Osobowych

1. Najwyższe kierownictwo Lumiko Sp. z o.o. jest zaangażowane w zapewnienie bezpieczeństwa ochrony danych osobowych. Do obowiązków ADO należy:
   1) podejmowanie odpowiednich i niezbędnych działań mających na celu zapewnienie prawidłowej ochrony danych osobowych, w szczególności poprzez sporządzanie i wdrażanie właściwych warunków organizacyjnych i technicznych,;
   2) w przypadku naruszenia ochrony danych osobowy ADO bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je PUODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Zasady postepowania określa Procedura postępowania w przypadku naruszenia ochrony danych osobowych
   3) śledzenie osiągnięć w dziedzinie bezpieczeństwa danych osobowych;
   4) wdraża nowe narzędzia i metody pracy mające na celu zwiększenie ochrony danych osobowych;
   5) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez: organizację i nadzorowanie przestrzegania zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej i elektronicznej;
   6) prowadzenie dokumentacji opisującej zastosowaną politykę bezpieczeństwa przetwarzania danych osobowych;

7) dokonuje bieżącej aktualizacji wewnętrznych procedur działania w przypadku zmiany przepisów prawa lub zmiany stanu faktycznego;
8) prowadzi ewidencję sprzętu oraz dokonuje inwentaryzację sprzętu i oprogramowania służącego do przetwarzania informacji;
9) podejmuje działania mające na celu zapewnienie, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne wiedzę i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
10) nadawanie i uchylanie uprawnień do przetwarzania danych osobowych;
11) prowadzenie rejestru osób Upoważnionych do przetwarzania danych, zawierającego imię i nazwisko Upoważnionego, datę nadania i ustania, zakres Upoważnienia do przetwarzania danych osobowych, identyfikator w przypadku gdy Upoważniony został zarejestrowany w systemie informatycznym, służącym do przetwarzania danych osobowych;
12) zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzanych danych osobowych w sposób zautomatyzowany, polegającego w szczególności na:
    a) dbałości o aktualizację oprogramowania,
    b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
    c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
    d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
    e) zapewnieniu bezpieczeństwa plików systemowych,
    f) redukcji ryzyka wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
    g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
    h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa.

§ 4
Przetwarzanie danych osobowych

1. Za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Przy rozstrzyganiu czy określona informacja lub informacje stanowią dane osobowe, Podmiot dokonuje zindywidualizowanej oceny, przy uwzględnieniu konkretnych okoliczności oraz rodzaju środków czy metod potrzebnych w określonej sytuacji do identyfikacji osoby.
2. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Danymi osobowymi będą zarówno takie dane, które pozwalają na określenie tożsamości konkretnej osoby, jak i takie, które nie pozwalają na jej natychmiastową identyfikację, ale są, przy pewnym nakładzie kosztów, czasu i działań, wystarczające do jej ustalenia;
3. Przetwarzanie danych osobowych jest dopuszczalne tylko wtedy gdy:
    1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych;
    2) 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;
    3) przetwarzanie danych jest niezbędne do wypełniania obowiązku prawnego, któremu podlega administrator;
    4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
    5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
    6) 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.
4. Przetwarzając dane osobowe Administrator Danych Osobowych realizuje następujące zasady:

1) Minimalizacji danych; Przetwarzane są jedynie dane niezbędne do osiągnięcia określonego celu przetwarzania.
2) Celu; Dane osobowe zbierane są w konkretnym, wyraźnym i prawnie uzasadnionym celu i nieprzetwarzane dalej w sposób niezgodny z tymi celami.
3) Zgodności z prawem, rzetelności i przejrzystości; Przetwarzanie zgodnie z prawem danych osobowych z jednoczesnym realizowaniem obowiązku informacyjnego względem osoby, której dane są przetwarzane.
4) Prawidłowości; Dane osobowe powinny być prawidłowe i w razie potrzeby uaktualniane a te które są nieprawidłowe w świetle celów ich przetwarzania, powinny zostać usunięte.
5) Ograniczenie przechowywania; Dane powinny być przechowywane w formie umożliwiającej identyfikację osoby, przez okres nie dłuższy niż jest to konieczne do realizacji celu przetwarzania.
6) Integralności i poufności; Dane przetwarzane powinny być w sposób zapewniający bezpieczeństwo danych.
7) Rozliczalności. Administrator jest odpowiedzialny za przestrzeganie przepisów o ochronie danych osobowych i musi być w stanie wykazać ich przestrzeganie.

5. Zgoda osoby, od której dane maja być przetwarzane jest dobrowolna, konkretna, świadoma i jednoznaczna, i sformułowana jasnym i prostym językiem w formie pisemnego oświadczenia.
6. Jeżeli przetwarzanie danych osobowych służy różnym celom zgoda jest udzielona na wszystkie te cele. Obowiązuje zasada jeden cel – jedna zgoda.
7. Zgoda na przetwarzanie danych osobowych zawiera:
   1) podstawę prawną;
   2) zakres danych osobowych, które będą przetwarzane;
   3) cel przetwarzania danych osobowych;
   4) dane administratora danych osobowych;
   5) oświadczenie o możliwości wycofania zgody na przetwarzanie danych osobowych;
   6) podpis osoby, która wyraża zgodę na przetwarzanie danych osobowych.
8. Administrator danych osobowych przed odebraniem zgody informuje osobę, od której dane będą przetwarzane o możliwości wycofania zgody na przetwarzanie danych osobowych w każdym momencie.
9. Wycofanie zgody wyrażone jest w formie pisemnej, jasnym i prostym językiem.

10. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem;

11. W momencie wycofania zgody przez osobę, której dane są przetwarzane Administrator Danych Osobowych niezwłocznie zaprzestaje przetwarzania tych danych;

12. Dane osobowe mogą być udostępniane osobom lub podmiotom uprawnionym do ich otrzymania na mocy przepisów prawa;

13. Administrator Danych Osobowych zachowuje szczególną staranność i nadzór w zakresie udostępniania danych osobowych;

14. Udostępnienie danych nie może naruszać praw i wolności osób, których one dotyczą;

15. Jeżeli w udostępnianych dokumentach zawarte są dane osobowe niemające bezpośredniego związku z celem udostępniania, dokonuje się ich anonimizacji;

16. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi w drodze pisemnej umowy;

17. Podmiot przetwarzający, któremu powierzono przetwarzanie danych osobowych może przetwarzać te dane wyłącznie w zakresie i celu przewidzianym w umowie;

18. Podmiot przetwarzający przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora danych osobowych;

19. Osoby, których dane są przetwarzane mają prawo do:

1) Dostępu do danych osobowych;
2) Sprostowania;
3) Usunięcia danych („prawo do bycia zapomniany”);
4) Sprzeciwu;
5) Ograniczenia przetwarzania;
6) Przenoszenia;

§ 5
Obowiązek informacyjny

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą Administrator Danych Osobowych spełnia obowiązek informacyjny, informuje tę osobę o:

1) nazwie Administratora Danych Osobowych i jego danych kontaktowych;

2) podstawę prawną przetwarzania;

3) celach przetwarzania danych;

4) kategoriach danych osobowych;

5) odbiorcach danych osobowych lub kategoriach odbiorców;

6) prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

7) jeżeli przetwarzanie odbywa się na podstawie zgody podmiotu danych – informacje o prawie do cofnięcia zgody w dowolnym momencie;

8) uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią, jeżeli na tej podstawie odbywa się przetwarzanie;

9) okresie przechowywania danych lub w braku możliwości – kryteria ustalania tego okresu.

2. Obowiązek informacyjny wypełniany jest w chwili zbierania danych.
3. Administrator Danych Osobowych posiada pisemne potwierdzenia spełnienia obowiązku informacyjnego.
4. W przypadku zbierania danych osobowych nie od osoby, której one dotyczą Administrator Danych Osobowych informuje tę osobę o:

1) nazwie Administratora Danych Osobowych i jego danych kontaktowych;
2) źródle danych osobowych;
3) celach przetwarzania danych;
4) kategoriach danych osobowych;
5) odbiorcach danych osobowych lub kategoriach odbiorców;
6) prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
7) jeżeli przetwarzanie odbywa się na podstawie zgody podmiotu danych – informacje o prawie do cofnięcia zgody w dowolnym momencie;
8) podstawie prawnej przetwarzania;
9) uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią, jeżeli na tej podstawie odbywa się przetwarzanie;

10) okresie przechowywania danych lub w braku możliwości – kryteria ustalania tego okresu.

5. Obowiązek informacyjny wypełniany jest w ciągu miesiąca od pozyskania zebranych danych poprzez wysłanie informacji za pośrednictwem poczty tradycyjnej bądź wiadomości mailowej osobie, której dane są przetwarzane.

6. Jeżeli dane osobowe można zgodnie z prawem ujawnić innemu odbiorcy, Administrator Danych osobowych informuje o tym osobę, której dane dotyczą w momencie pierwszorazowego ujawnienia danych temu odbiorcy.

7. Udzielenie informacji nie jest konieczne, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami, utrwalenie lub ujawnienie danych jest wyraźnie przewidziane prawem albo jeżeli poinformowanie osoby, której dane dotyczą, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.

§ 6
Bezpieczeństwo

1. Spółka zapewnia stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw i wolności osób fizycznych w skutek przetwarzania danych osobowych.

2. Spółka przeprowadza i dokumentuje analizy ryzyka, dokonuje oceny skutków procesów przetwarzania danych osobowych.

3. Po dokonaniu identyfikacji i analizy ryzyka, ADO stosuje środki bezpieczeństwa w celu zminimalizowania ryzyka naruszenia praw i wolności do określonego poziomu w szczególności:

1) pseudoanimizację i szyfrowanie danych osobowych;

2) zarządzanie systemem w sposób zapewniający zachowanie ciągłości, poufności, integralności i dostępności przetwarzania informacji;

3) zarządzanie systemem w sposób zapewniający zdolność do szybkiego przywrócenia dostępu do danych osobowych w razie wystąpienia incydentu fizycznego lub technicznego;

4) regularne testowanie, mierzenie, ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;

5) wszelki inne środki, których zastosowanie minimalizowałoby ryzyko lub je całkowicie eliminowało;

4. Naruszenie ochrony danych to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub przetwarzanych w inny sposób.

1. Za naruszenie ochrony danych osobowych uważa się w szczególności:
    1) nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;
    2) wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (np. zmian zawartości danych, utrata bądź przejęcie całości lub części danych);
    3) naruszenie lub próby naruszenia integralności systemu;
    4) zmianę lub utratę danych zapisanych na kopiach zapasowych;
    5) naruszenie lub próby naruszenia poufności danych lub ich części;
    6) nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);
    7) udostępnienie osobom nieupoważnionym danych osobowych lub ich części;
    8) zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji zmierzające do zakłócenia działania bądź pozyskania w sposób niedozwolony (lub w celach niezgodnych z przeznaczeniem) danych przetwarzanych w sposób zautomatyzowany lub niezautomatyzowany;
    9) inny stan sprzętu komputerowego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy.
    10) Za naruszenie ochrony danych osobowych uważa się również włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

5. W przypadku wystąpienia naruszenia ochrony danych osobowych pracownik jednostki zobowiązany jest do niezwłocznego poinformowania Administratora Danych Osobowych

6. Dalsze postępowania odbywa się z godnie z Procedurą postępowania w przypadku naruszenia danych osobowych

§ 7

Postanowienia końcowe

1. Ochrona Danych osobowych stanowi ważny i integralny element prowadzonej przez Spółkę działalności. Odzwierciedleniem czego jest stworzona w 2018r. Polityka Bezpieczeństwa w Lumiko Sp. z o.o., Instrukcja zarządzania systemem informatycznym a także inne procedury i wewnętrzne regulacje.
2. Lumiko Sp. z o.o. z siedzibą w Łukowie, ul. Międzyrzecka 81; 21-400 Łuków czyni wszelkie starania by jej pracownicy , klienci i kontrahenci byli zaznajomieni z zasadami ochrony danych osobowych