Przedsiębiorstwo ***harvest*** Sp. z o.o.
ul. Wrzesińska 56, 62-020 Swarzędz
tel./fax +48 (0) 61 817-20-20, 651-10-10, 651-10-11

POLITYKA OCHRONY DANYCH OSOBOWYCH

ADMINISTRATOR: PRZEDSIĘBIORSTWO HARVEST SP. Z O.O.

ADRES: UL. WRZESIŃSKA 56, 62-020 SWARZĘDZ

Data i miejsce sporządzenia dokumentu:	22 /05/2018
Ilość stron:	

Przedsiębiorstwo ***harvest*** Sp. z o.o.
ul. Wrzesińska 56, 62-020 Swarzędz
tel./fax +48 (0) 61 817-20-20, 651-10-10, 651-10-11

SPIS TREŚCI

Przedsiębiorstwo ***harvest*** Sp. z o.o.
ul. Wrzesińska 56, 62-020 Swarzędz
tel./fax +48 (0) 61 817-20-20, 651-10-10, 651-10-11

1. WSTĘP

1.1. INFORMACJE OGÓLNE

1. Administratorem Danych jest Przedsiębiorstwo Harvest Sp. z o.o. z siedzibą w Swarzędzu przy ulicy Wrzesińskiej 56.

2. Polityka Bezpieczeństwa została wprowadzona w celu ochrony Danych osobowych.

1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.

2. Zakres przedmiotowy Polityki Bezpieczeństwa wraz z elementami wymaganymi przepisami prawa.

Przedsiębiorstwo Harvest Sp. z o.o. mieści się w Swarzędzu 62-020 przy ul. Wrzesińskiej 56.
W Budynku głównym tj. biurowiec znajduje się Biuro Zarządu, Biuro Techniczne, Sekretariat, Magazyn, Archiwum a także pomieszczenia socjalne (szatnie, toalety, kuchnie).
W skład całego Zakładu wchodzi dodatkowo Warsztat mechaniczny, Wiata magazynowa.

W skład zbiorów danych przetwarzanych w Przedsiębiorstwie Harvest Sp. z o.o. wchodzi:
-lista kontrahentów
-lista pracowników
-lista klientów

1.3. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENCIE POLITYKI BEZPIECZEŃSTWA

Polityka Bezpieczeństwa posługuje się wieloma specjalistycznymi terminami z zakresu ochrony danych osobowych, które mogą być niewłaściwie rozumiane przez pracowników Administratora Danych – osoby obowiązane do przetwarzanie danych osobowych zgodnie z wymogami ustawowymi.

1. **Administrator danych** – organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3 Ustawy o ochronie danych osobowych, decydująca o celach i środkach przetwarzania danych osobowych,
2. **ABI** – Administrator Bezpieczeństwa Informacji,
3. **ASI** – Administrator Systemów Informatycznych,
4. **ustawa** – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r., poz. 922 ze zm.),
5. **rozporządzenie** – Rozporządzenie 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. z 2004 r. Nr 100, poz. 1024 ze. zm.),
6. **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
7. **przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

1. Punkt ten wskazuje osoby odpowiedzialne za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami Ustawy, Rozporządzenia, Polityki Bezpieczeństwa oraz Instrukcji zarządzania systemami informatycznymi.

2.2. ADMINISTRATOR DANYCH

1. Administratorem Danych jest Przedsiębiorstwo Harvest Sp. z o.o. ul. Wrzesińska 56, 62-020 Swarzędz, REGON 008406598.

2. Obowiązki należące do Administratora Danych w zakresie ochrony danych osobowych:

   1. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:

      a) przetwarzane zgodnie z prawem,

      b) zbierane dla oznaczonych, zgodnych z prawem celów,

      c) merytorycznie poprawne i adekwatne w stosunku do celów.

   2. Wyznacza osobę, zwaną dalej Administratorem Bezpieczeństwa Informacji, odpowiedzialnym za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń.

   3. Opracowuje instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych, przeznaczoną dla osób zatrudnionych przy przetwarzaniu tych danych.

   4. Określa budynki, pomieszczenia lub części pomieszczeń, tworzące obszar, w którym przetwarzane są dane osobowe z użyciem stacjonarnego sprzętu komputerowego.

5. Opracowuje instrukcję, określającą sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji.

6. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.

2.3. ADMINISTRATOR BEZPIECZEŃSTWA INFORMACJI

1. Powołanie Administratora Bezpieczeństwa Informacji jest fakultatywne (wzór powołania: Załącznik nr 1 do Polityki Bezpieczeństwa).

2. Zakres uprawnień i obowiązków Administratora Bezpieczeństwa Informacji

    1. Nadzór nad przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym.

    2. Nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe.

    3. Nadzór nad wykorzystywanym oprogramowaniem oraz jego legalnością.

    4. Przeciwdziałanie dostępowi osób niepowołanych do systemu, w których przetwarzane są dane osobowe.

    5. Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych.

    6. Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych.

    7. Podejmowanie decyzji o instalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych.

    8. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.

    9. Definiowanie użytkowników i haseł dostępu.

10. Aktualizowanie oprogramowania antywirusowego i innego, chyba że aktualizacje te wykonywane są automatycznie.

11. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.

12. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.

13. Sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

2.4. ADMINISTRATOR SYSTEMÓW INFORMATYCZNYCH

1. Wyznaczenie Administratora Systemów Informatycznych jest fakultatywne (wzór wyznaczenia: Załącznik nr 3 do Polityki Bezpieczeństwa).

2. Katalog uprawnień i obowiązków Administratora Systemów Informatycznych:

-nadawanie / nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych,

-nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,

-podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,

identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych i tradycyjnych,

-sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi

2.5. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych zobowiązana jest do ich ochrony w sposób zgodny z przepisami Ustawy, Rozporządzenia oraz Polityki Bezpieczeństwa.

2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.

3. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Nadawaniem upoważnień do przetwarzania danych osobowych osobom, które w ramach swoich obowiązków służbowych przetwarzają dane osobowe Administratora Danych zajmuje się Administrator Bezpieczeństwa Informacji zgodnie ze wzorem Upoważnienia (załącznik nr 4a i 4b do Polityki bezpieczeństwa).

   Administrator Bezpieczeństwa Informacji zajmuje się również ewidencją nadanych upoważnień (ewidencja osób upoważnionych do przetwarzania danych Załącznik nr 7 do Polityki Bezpieczeństwa).

4. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Zgodnie z Ustawą o ochronie danych osobowych istnieje możliwość powierzenia przetwarzania danych osobowych przez Administratora Danych zewnętrznym podmiotom. Odbywa się to wyłącznie na drodze umowy powierzenia, w której jest określony zbiór, który zostanie przekazany, cel tego przekazania oraz zakres planowanego przetwarzania danych przez inny podmiot.

2. Za zawieranie umów powierzenia oraz ich dalsze rejestrowanie odpowiedzialny jest Administrator Bezpieczeństwa informacji

Przedsiębiorstwo ***harvest*** Sp. z o.o.
ul. Wrzesińska 56, 62-020 Swarzędz
tel./fax +48 (0) 61 817-20-20, 651-10-10, 651-10-11

5. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Wprowadzenie odpowiednich ze względu na charakter organizacji pracy Administratora Danych ogólnych zasad bezpieczeństwa przetwarzania danych - zgodnie z wymaganiami przepisów prawnych z zakresu ochrony danych osobowych – pozwoli na prawidłowe przetwarzanie danych.

2. Odpowiedzialność za bezpieczeństwo przetwarzania danych – dotyczy to co do zasady wszystkich pracowników pracujących ze zbiorami danych.

- Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze, indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
- Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych.
- W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. „czystego biurka”. Zasada ta oznacza nie pozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników.
- Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek.
- Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.
- Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem.

- Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

6. INSTRUKCJA POSTĘPOWNIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Procedury postępowania przypadku stwierdzenia naruszenia ochrony danych osobowych pozwalają na wypracowanie generalnych reguł dotyczących zachowania się pracowników Administratora Danych w przypadku wystąpienia naruszenia zasad ochrony danych osobowych.

2. Instrukcja postępowania w sytuacji naruszenia danych osobowych:

- Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Administratorowi Bezpieczeństwa Informacji i/lub Administratorowi Systemów Informatycznych (w odniesieniu do danych przetwarzanych w systemach informatycznych).
- Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Administratora Bezpieczeństwa Informacji i/lub Administratora Systemów Informatycznych lub upoważnionej przez nich osoby, osoba powiadamiająca powinna:
  - niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
  - zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
  - udokumentować wstępnie zaistniałe naruszenie,
  - nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia.

- Po przybyciu na miejsce naruszenia ochrony danych osobowych, Administrator Bezpieczeństwa Informacji lub Administrator Systemów Informatycznych lub osoba ich zastępująca:
  - zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania
  - wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem,
- Administrator Bezpieczeństwa Informacji i/lub Administrator Systemów Informatycznych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport.

Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, Administrator Bezpieczeństwa Informacji i/lub Administrator Systemów Informatycznych, zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

7. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Powyższy rozdział reguluje system kontroli przetwarzania i stanu zabezpieczenia danych osobowych, kto jest odpowiedzialny za ich przeprowadzenie i jak często należy badać stan zabezpieczeń.

Postanowienia dotyczące kontroli przetwarzania i stanu zabezpieczenia danych osobowych:

1. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Przedsiębiorstwie Harvest Sp. z o.o. ul. Wrzesińska 56, 62-020 Swarzędz sprawuje Administrator Bezpieczeństwa Informacji oraz Administrator Systemów Informatycznych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
2. Administrator Bezpieczeństwa Informacji dokonuje czynności kontrolnych w ramach sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, zgodnie z art. 36 ust. 2 pkt 1 ppkt a) Ustawy o ochronie danych osobowych.

3. Sprawdzenie dokonywane jest przez Administratora Bezpieczeństwa Informacji dla Administratora Danych, bądź dla Generalnego Inspektora Ochrony Danych Osobowych, gdy ten na podstawie przysługujących mu kompetencji zwróci się o to do Administrator Bezpieczeństwa Informacji.
4. ABI przeprowadza sprawdzenie w trybie:

1.1. sprawdzenia planowego

1.2. sprawdzenia doraźnego - w przypadku nieprzewidzianym w planie sprawdzeń, w sytuacji powzięcia wiadomości o naruszeniu ochrony danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego naruszenia, niezwłocznie po powzięciu przez ABI takich informacji;

1.3. sprawdzenia w przypadku zwrócenia się o to przez Generalnego Inspektora Ochrony Danych Osobowych.

2. Administrator Bezpieczeństwa Informacji opracowuje plan sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.
3. W toku sprawdzenia Administrator Bezpieczeństwa Informacji dokonuje i dokumentuje czynności, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.
4. Po zakończeniu sprawdzenia, Administrator Bezpieczeństwa Informacji przygotowuje dla Administratora Danych, sprawozdanie w tym zakresie. Sprawozdanie sporządzane jest w postaci elektronicznej albo w postaci papierowej.
5. Administrator Bezpieczeństwa Informacji ma prawo do kontroli podmiotów, którym powierzono przetwarzanie danych osobowych w trybie określonym w Polityce Bezpieczeństwa, o ile w umowie o powierzeniu przetwarzania danych osobowych istnieją stosowne zapisy w tym zakresie.
6. Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych stanowi Załącznik nr 10 do Polityki Bezpieczeństwa

Wzór protokołu z kontroli lub czynności sprawdzających, o których mowa w pkt 8 stanowi Załącznik nr 11 do Polityki Bezpieczeństwa

8. OPIS STRUKTURY ZBIORÓW DANYCH

Dla każdego zidentyfikowanego zbioru danych powinien być wskazany opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze.

Opisy poszczególnych pól informacyjnych gromadzonych w strukturze zbioru danych powinny jednoznacznie wskazywać jakie kategorie danych są w nich przechowywane.

Opis pola danych w przypadkach, gdy możliwa jest jednoznaczna interpretacja jego zawartości, powinien wskazywać nie tylko kategorie danych, ale również format zapisu.

Załącznik nr 6 do Polityki Bezpieczeństwa.

9. SPOSÓB PRZEPŁYWU DANYCH OSOBOWYCH POMIĘDZY SYSTEMAMI

1.Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.

2.Przesyłanie danych pomiędzy systemami i programami wskazanymi może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. CD, DVD, dysk wymienny, dysk przenośny Pen Drive, itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu/importu danych za pomocą teletransmisji (np. poprzez przesłanie danych w tworząc dokument w formacie PDF i wysłanie go na adres e-mail)

3.Przesyłanie danych może odbywać się zarówno w siedzibie firmy, jak i na zewnątrz (do klientów, kontrahentów, pracowników firmy).

Przedsiębiorstwo ***harvest*** Sp. z o.o.
ul. Wrzesińska 56, 62-020 Swarzędz
tel./fax +48 (0) 61 817-20-20, 651-10-10, 651-10-11

10. OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Wykaz podmiotów, którym dane zostały powierzone, wraz ze wskazaniem obszaru przetwarzania danych znajduje się w Załączniku nr 8 do Polityki Bezpieczeństwa.

11. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘDNE DLA ZAPEWNIENIA POUFNOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

1. Wykaz środków technicznych i organizacyjnych, które zostały zastosowane przez Administratora Danych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania danych, a także dla zagwarantowania poufności, integralności i rozliczalności przetwarzanych danych osobowych przedstawiono w Załączniku nr 9 do Polityki Bezpieczeństwa.

Przedsiębiorstwo ***harvest*** Sp. z o.o.
ul. Wrzesińska 56, 62-020 Swarzędz
tel./fax +48 (0) 61 817-20-20, 651-10-10, 651-10-11

12. ZAŁĄCZNIKI

Załącznik nr 1 – Powołanie Administratora Bezpieczeństwa Informacji

Załącznik nr 2 – Upoważnienie Administratora Bezpieczeństwa Informacji do nadawania upoważnień

Załącznik nr 3 – Wyznaczenie Administratora Systemów Informatycznych

Załącznik nr 4a – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę

Załącznik nr 4b – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie innej umowy niż umowa o pracę

Załącznik nr 5 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności

Załącznik nr 6 – Opis struktury zbiorów danych

Załącznik nr 7 – Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

Załącznik nr 8 – Wykaz podmiotów, którym Administrator Danych powierzył przetwarzanie danych osobowych

Załącznik nr 9 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

Załącznik nr 10 –Wzór sprawozdania ze sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych

Załącznik nr 11 – Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzający.

Załącznik nr 12 – Lista osób przeszkolonych w zakresie wdrożonej polityki ochrony danych osobowych w przedsiębiorstwie Harvest Sp. z o.o..

Dokument sporządzono:	**Pełen podpis Administratora Danych:**	**Pieczęć**
Data: 22/05/2018 Miejsce: Swarzędz		