**POLITYKA BEZPIECZEŃSTWA**
**DANYCH OSOBOWYCH**
**w Wielkopolskiej Giełdzie Odzieżowej Spółce z o.o.**
**(dalej zwanym Podmiotem)**

Wielkopolska Giełda Odzieżowa Spółka z o.o. z siedzibą w Poznaniu (KRS nr 0000128092), tj. Podmiot, świadomy wagi problemów związanych z ochroną prawa do prywatności, w tym w szczególności prawa osób fizycznych powierzających swoje dane osobowe do właściwej i skutecznej ochrony tych danych, a także regulacji prawnych wynikających z wejścia w życie 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, deklaruje:

- zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych;
- zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Podmiocie w zakresie problematyki bezpieczeństwa tych danych;
- zamiar traktowania obowiązków osób zatrudnionych przy przetwarzaniu danych osobowych jako należących do kategorii podstawowych obowiązków pracowniczych oraz stanowczego egzekwowania ich wykonania przez zatrudnione osoby;
- zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.

## ROZDZIAŁ I
## Postanowienia ogólne
### § 1

- Polityka bezpieczeństwa danych osobowych (zwana dalej „Polityką"), określa środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Ponadto Polityka określa także sposób przepływu danych pomiędzy poszczególnymi systemami, zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych lub w formie tradycyjnej, albo w sytuacji powzięcia podejrzenia o takim naruszeniu.
- Polityka jest zintegrowanym zbiorem ogólnych zasad, procedur, praw wewnętrznych i praktycznych doświadczeń regulujących sposób zarządzania, ochrony, użytkowania i przechowywania danych osobowych gromadzonych przez Administratora Danych w Podmiocie w postaci elektronicznej oraz w dokumentach w wersji papierowej.
- Integralną częścią Polityki oraz jej uszczegółowieniem jest „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania Danych Osobowych w Podmiocie (zwana dalej „Instrukcją"), która zawiera wytyczne dotyczące bezpiecznego przetwarzania danych osobowych przy użyciu systemów informatycznych, stanowiąca Załącznik do Polityki.
- Polityka obowiązująca w Podmiocie ma charakter obligatoryjny i dotyczy wszystkich osób, które przetwarzają dane osobowe w ramach współpracy z Podmiotem, tj. pracowników,

współpracowników współdziałających na podstawie umowy cywilnoprawnej, konsultantów i innych osób mających dostęp do danych osobowych.

- Administrator Danych realizując niniejszą Politykę dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczące, w szczególności zapewnia, aby te dane były:
    - przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
    - zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
    - adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
    - prawidłowe i w razie potrzeby uaktualniane, należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
    - przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane;
    - przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.
- Polityka została opracowana zgodnie z wymogami określonymi prawem powszechnie obowiązującym. Polityka w szczególności realizuje normy prawne wynikające z 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 mającego zastosowanie do dnia 25 maja 2018 r.
- Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.

## § 2
## Definicje

1. Na użytek Polityki:

- dane osobowe – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna, to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
- zbiór danych – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
- przetwarzanie danych - oznacza 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;

- system informatyczny – oznacza zespół współpracujących ze sobą urządzeń, programów, procedur, przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
- identyfikator użytkownika (login) – oznacza ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
- hasło – oznacza ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
- uwierzytelnienie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
- Administrator Danych – rozumie się przez to Podmiot, tj. Wielkopolska Giełda Odzieżowa Spółka z o.o.;
- użytkownik – rozumie się przez to osobę wyznaczoną przez Administratora Danych lub osobę przez niego upoważnioną, uprawnioną do bezpośredniego dostępu do danych osobowych przetwarzanych zarówno w formie tradycyjnej jak i elektronicznej;
- organ nadzorczy – oznacza organ publiczny odpowiedzialny za monitorowanie stosowania przepisów prawa powszechnie obowiązującego dotyczącego ochrony podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem oraz ułatwiania swobodnego przepływu danych osobowych w Unii Europejskiej;
- pomieszczenia – rozumie się przez to budynki, pomieszczenia lub części pomieszczeń określone przez Administratora Danych, tworzące obszar, w którym przetwarzane są dane osobowe zarówno w formie tradycyjnej i elektronicznej;
- dostępność – oznacza gwarancję dostępu do danych osobowych tylko przez osoby uprawnione
- integralność danych – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
- poufność danych – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom;
- rozliczalność – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
- integralność systemu – rozumie się przez to nienaruszalność systemu, niemożność jakiejkolwiek manipulacji
- podmiot przetwarzający – rozumie się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora, na podstawie pisemnej umowy zawartej z Administratorem.

## § 3
## Cele Polityki

- Polityka została opracowana i wdrożona dla stworzenia i utrzymania wysokiego poziomu bezpieczeństwa zbioru danych osobowych w celu zapewnienia poufności danych, integralności danych i dostępności zasobów oraz zapewnienia rozliczalności podejmowanych działań.
- Celem opracowania i wdrożenia Polityki jest:
    - maksymalne ograniczenie ryzyka związanego z nieuprawnionym przetwarzaniem lub utratą danych osobowych;

    - zagwarantowanie pełnej ochrony danych osobowych posiadanych przez Administratora Danych zbiorów bez względu na formę w jakiej zbiór jest przetwarzany;
    - opracowanie zasad postępowania w sytuacjach kryzysowych;
    - wdrożenie reguł, praw i procedur zapewniających odpowiedni poziom bezpieczeństwa zarządzania danymi osobowymi będącymi w posiadaniu Administratora Danych.
- W celu zwiększenia efektywności ochrony danych osobowych dokonano połączenia różnych zabezpieczeń w sposób umożliwiający stworzenie kilku warstw ochronnych. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników. Ponadto cele realizowane są poprzez:
    - stałe doskonalenie oraz rozwijanie organizacyjnych i technicznych środków ochrony danych osobowych przetwarzanych zarówno w formie tradycyjnej jak i elektronicznej;
    - podejmowanie wszelkich, dozwolonych prawem działań niezbędnych dla ochrony praw jednostki związanych z bezpieczeństwem ich danych osobowych;
    - staranny dobór, ocenę i kwalifikację dostawców usług;
    - stosowanie odpowiednich urządzeń i oprogramowania wykorzystywanych do przetwarzania i zabezpieczania danych osobowych.
- Zastosowane zabezpieczenia gwarantują:
    - poufność danych;
    - integralność danych;
    - rozliczalność;
    - integralność systemu;
    - uwierzytelnienie.

**§ 4**

**Zakres zastosowania Polityki**

- Polityka odnosi się do wszystkich danych osobowych przetwarzanych zarówno w sposób tradycyjny jak i w systemach informatycznych. Ochronie podlegają wszystkie dane osobowe przetwarzane przez Administratora Danych, również te, które Administrator Danych powierza do przetwarzania innym podmiotom.
- Realizację celów określonych w § 3 Polityki, powinny zagwarantować następujące założenia:
    - wdrożenie procedur określających postępowanie osób zatrudnionych przy przetwarzaniu danych osobowych oraz ich odpowiedzialność za bezpieczeństwo tych danych;
    - przeszkolenie użytkowników w zakresie bezpieczeństwa i ochrony danych osobowych;
    - przypisanie użytkownikom określonych atrybutów pozwalających na ich identyfikację (hasła, identyfikatory), zapewniających im dostęp do różnych poziomów baz danych osobowych – stosownie do indywidualnego zakresu upoważnienia;
    - okresowe sprawdzanie przestrzegania przez użytkowników wdrożonych metod postępowania przy przetwarzaniu danych osobowych;
    - opracowanie procedur odtwarzania systemu w przypadku wystąpienia awarii;
    - śledzenie osiągnięć w dziedzinie bezpieczeństwa systemów informatycznych i – w miarę możliwości organizacyjnych i techniczno-finansowych – wdrażanie nowych narzędzi i metod pracy oraz sposobów zarządzania systemami informatycznymi, które będą służyły wzmocnieniu bezpieczeństwa danych osobowych.

**ROZDZIAŁ II**

**Przedsięwzięcia zabezpieczające przez naruszeniem bezpieczeństwa danych osobowych**

**§ 5**

Za naruszenie bezpieczeństwa danych osobowych uważa się w szczególności:

- nieuprawniony dostęp lub próbę dostępu do danych osobowych lub pomieszczeń, w których się one znajdują;
- wszelkie modyfikacje danych osobowych lub próby ich dokonania przez osoby nieuprawnione (np. zmiany zawartości danych, utrata całości lub części danych);
- naruszenie lub próby naruszenia integralności systemu;
- zmianę lub utratę danych zapisanych na kopiach zapasowych;
- naruszenie lub próby naruszenia poufności danych lub ich części;
- nieuprawniony dostęp (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu);
- udostępnienie osobom nieupoważnionym danych osobowych lub ich części;
- zniszczenie, uszkodzenie lub wszelkie próby nieuprawnionej ingerencji w systemy informatyczne zmierzające do zakłócenia ich działania bądź pozyskania;
- inny stan systemu informatycznego lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu pracy;
- włamanie do budynku lub pomieszczeń, w których przetwarzane są dane osobowe lub próby takich działań.

**§ 6**

- Każdy nowy pracownik lub użytkownik – przed uzyskaniem dostępu do danych osobowych przetwarzanych w Podmiocie – podlega przeszkoleniu w zakresie przepisów o ochronie danych osobowych oraz wynikających z nich zadań oraz obowiązków.
- Wszyscy użytkownicy podlegają szkoleniom, stosownie do potrzeb wynikających ze zmian systemie informatycznym (wymiana sprzętu na nowszej generacji, zmiana oprogramowania) oraz w związku ze zmianą przepisów o ochronie danych osobowych lub zmian wewnętrznych regulacji.
- Za organizacje szkoleń odpowiedzialny jest Administrator Danych.

**§ 7**

- Każdy użytkownik zobowiązany jest do utrzymania właściwego poziomu bezpieczeństwa w zakresie swoich obowiązków i uprawnień.
- Każdy użytkownik składa oświadczenie zgodnie ze wzorem określonym w Załączniku nr 1 do Polityki, w którym potwierdza zapoznanie się z aktami prawnymi powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, Polityką oraz Instrukcją. Ponadto użytkownik zobowiązuje się do zapewnienia ochrony przetwarzanych przez niego danych osobowych. Oświadczenie to jest przechowywane przez Administratora Danych w aktach osobowych użytkownika przez okres 5 lat licząc od daty zakończenia współpracy z użytkownikiem (np. od daty rozwiązania umowy o pracę).
- Każdy użytkownik, zarówno w trakcie, jak i po ustaniu współpracy z Podmiotem ma obowiązek ochrony wszelkich informacji dotyczących funkcjonowania systemów lub urządzeń służących do przetwarzania danych osobowych oraz sposobów zabezpieczenia danych.
- Niedozwolone jest przetwarzanie danych osobowych w sposób inny niż opisany w niniejszej Polityce lub Instrukcji.
- Użytkownicy zobowiązani są:

- przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych;
- informować Administratora Danych lub pracowników ochrony o wszelkich nietypowych zajściach mogących mieć wpływ na bezpieczeństwo przetwarzania danych:
- przestrzegać zasad i procedur ochrony danych osobowych, w czasie pracy a także po jej zakończeniu.

**§ 8**

Do podstawowych zabezpieczeń przez naruszeniem ochrony danych osobowych należą:

- zabezpieczenie obiektu, w którym znajdują się pomieszczenia;
- wydzielenie pomieszczeń;
- wyposażenie pomieszczeń w specjalne szafy do przechowywania danych w formie tradycyjnej;
- zabezpieczenie wejść do pomieszczeń odpowiednimi zamkami.

**§ 9**

- Klucze i karty dostępu do pomieszczeń wydawane są wyłącznie osobom do tego uprawnionym.
- Dokumenty zawierające dane osobowe przechowywane są w przeznaczonych do tego szafach, do których dostęp mają wyłącznie użytkownicy.

**§ 10**

- Do obowiązków Administratora Danych należy:
  - zapewnienie środków organizacyjnych i technicznych zapewniających zabezpieczenie danych osobowych przed dostępem osób nieupoważnionych;
  - nadawanie, zmiana, odbieranie uprawnień użytkowników do przetwarzania danych osobowych;
  - wystawianie upoważnień do przetwarzania danych osobowych;
  - weryfikacja zakresu przetwarzania danych pod kątem adekwatności;
  - przechowywanie imiennych upoważnień do przetwarzania danych osobowych;
  - prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
  - prowadzenie i aktualizacja dokumentacji opisującej sposób przetwarzania danych osobowych;
  - nadzór i akceptacja treści podpisanych umów powierzenia przetwarzania danych osobowych innym podmiotom;
  - nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe;
  - nadzór nad prawidłowym archiwizowaniem dokumentów zawierających dane osobowe oraz zapewnienie nadzoru nad właściwym usuwaniem bądź niszczeniem dokumentów zawierających dane osobowe;
  - informowanie organów uprawnionych do ścigania przestępstw w przypadku celowego naruszenia bezpieczeństwa przetwarzanych danych osobowych;
  - zapewnienie właściwej konfiguracji systemu informatycznego zapewniającej bezpieczeństwo i ograniczenie dostępu do danych osobowych osób nieupoważnionych.

- Administrator Danych kierując się kryterium posiadania odpowiednich kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych, może wyznaczyć w Podmiocie Inspektora Ochrony Danych, do zadań którego należało będzie:
    - informowanie Administratora Danych, podmiotu przetwarzającego oraz pracowników (w tym użytkowników), którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów powszechnie obowiązujących dotyczących ochrony danych osobowych i doradzanie im w tej sprawie;
    - monitorowanie przestrzegania prawa powszechnie obowiązującego dotyczącego ochrony danych osobowych, Polityki i Instrukcji, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
    - współpraca z organem nadzorczym;
    - pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.
- Inspektor Ochrony Danych w przypadku powołania będzie również upoważniony i odpowiedzialny w Podmiocie za prawidłowe funkcjonowanie sprzętu komputerowego, oprogramowania i jego konserwację w szczególności za:
    - nadawanie, zmianę i blokowanie uprawnień użytkowników do systemu informatycznego;
    - właściwą konfigurację systemu informatycznego zapewniającą bezpieczeństwo i ograniczenie dostępu do danych osobowych osób nieupoważnionych;
    - monitorowanie funkcjonowania zabezpieczeń wdrożonych w celu ochrony danych osobowych;
    - nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, które zawierają dane osobowe;
    - okresowe wykonywanie kopii bezpieczeństwa danych oraz nadzór nad ich zabezpieczeniem;
    - podejmowanie działań w przypadku wykrycia naruszenia zabezpieczeń w systemie informatycznym lub podejrzenia takiego naruszenia (np. pojawienie się wirusa w systemie). Inspektor Ochrony Danych, w takich sytuacjach, w szczególności zobowiązany jest do:
        - fizycznego odłączenia urządzeń, które umożliwiają nieautoryzowany dostęp do zbioru danych osobowych;
        - wylogowania użytkownika, który zgłosił podejrzenie lub naruszenie integralności zbioru danych osobowych;
        - podjęcie działań uniemożliwiających dalsze nielegalne przetwarzanie danych osobowych;
        - usunięcia skutków incydentu;
        - przywrócenie normalnego działania systemu (np. odtworzenie bazy danych z ostatniej kopii);
        - zmiany hasła użytkownika, który zgłosił naruszenie systemu informatycznego;
        - poinformowania o incydencie Administratora Danych, w tym sporządzenia notatki dotyczącej opisu, przyczyn i znanych skutków incydentu;
        - wyjaśnienia przyczyn wystąpienia incydentu i podjęcia działań zmierzających do ograniczenia ryzyka wystąpienia ponownego incydentu w przyszłości;
        - wydania zgody na ponowne rozpoczęcie przetwarzania danych osobowych;

        - przedstawienia Administratorowi Danych propozycji poprawy bezpieczeństwa przetwarzania danych osobowych;
        - w przypadku, gdy incydent wywołany był świadomie przez użytkownika – zabezpieczenia niezbędnych dowodów;
    - okresowa analiza przyczyn i skutków sytuacji, które naruszały bezpieczeństwo danych oraz informowanie Administratora Danych o wynikach analizy;
    - zabezpieczenie komputerów przenośnych poprzez:
        - ustawienie automatycznego wymuszenia zmiany hasła co 30 dni;
        - ustawienie wymogu dotyczącego haseł zgodnie z wytycznymi Ustawy (odpowiednia ilość i rodzaj znaków);
        - instalację oprogramowania antywirusowego;
        - stosowanie środków ochrony kryptograficznej wobec przetwarzanych danych osobowych na komputerach przenośnych;
    - ograniczenie możliwości instalowania oprogramowania na stacjach roboczych przez osoby nieupoważnione.

## ROZDZIAŁ III
## Przetwarzanie danych osobowych
### § 11

- Przetwarzanie danych osobowych, bez względu na formę w jakiej są one przetwarzane, odbywa się wyłącznie na obszarze przetwarzania danych osobowych wyznaczonym przez Administratora Danych.
- Przetwarzanie danych osobowych za pomocą urządzeń przenośnych może odbywać się poza pomieszczeniami, o których mowa w § 11 ust. 3 Polityki, wyłącznie za zgodą Administratora Danych.
- Szczegółowy wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe określa Załącznik nr 4 do Polityki.

### § 12

- W celu ograniczenia dostępu osób postronnych do pomieszczeń należy zapewnić, aby:
    - drzwi wejściowe były zabezpieczone tak, aby otwarcie z zewnątrz mogło nastąpić wyłącznie przez uprawnione osoby;
    - pomieszczenia, w których znajdują się serwery były wyposażone w sprawne systemy klimatyzacji, ochrony przeciwpożarowej i przeciwwłamaniowej;
    - przebywanie osób trzecich w pomieszczeniach może odbywać się wyłącznie w obecności użytkowników lub za zgodą Administratora Danych.
- Stały dostęp do pomieszczeń, w których przetwarzane są dane osobowe, mają tylko użytkownicy.
- W trakcie prac technicznych wykonywanych przez osoby trzecie w pomieszczeniach, przetwarzanie danych jest zabronione.
- W przypadku, gdy przebywanie w obszarze przetwarzania danych osób nieupoważnionych jest konieczne, są one zobowiązane do podpisania oświadczenia o zachowaniu poufności informacji pozyskanych w trakcie wykonywania prac oraz sposób ich zabezpieczenia. Wzór oświadczenia stanowi Załącznik nr 5 do Polityki.

### § 13

Administrator Danych jest odpowiedzialny za całość zagadnień dotyczących ochrony i bezpieczeństwa danych osobowych.

**§ 14**

- Przetwarzanie jest dopuszczalne wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim spełniony jest co najmniej jeden z poniższych warunków:
    - osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
    - 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;
    - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze Danych;
    - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
    - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora Danych 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.
- Jeżeli przetwarzanie odbywa się na podstawie zgody, Administrator Danych musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
- Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.
- Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
- Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

**§ 15**

- Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, Administrator Danych podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:
    - swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
    - dane kontaktowe Inspektora Ochrony Danych w przypadku jego ustanowienia;
    - informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją.

- Poza informacjami, o których mowa w § 15 ust. 1 Polityki, podczas pozyskiwania danych osobowych Administrator Danych podaje osobie, której dane dotyczą, następujące inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
    - okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
    - informacje o 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;
    - informacje o prawie wniesienia skargi do organu nadzorczego;
    - informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązania do ich podania i jakie są ewentualne konsekwencje niepodania danych.
- Osoba, której dane dotyczą, jest uprawniona do uzyskiwania od Administratora Danych potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:
    - cele przetwarzania;
    - kategorie odnośnych danych osobowych;
    - informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione;
    - w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
    - informacje o prawie do żądania od Administratora Danych sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
    - informacje o prawie wniesienia skargi do organu nadzorczego;
    - jeśli dane osobowe nie zostały zebrane od osoby, której dotyczą – wszelkie dostępne informacje o ich źródle.
- Osoba, której dane dotyczą, ma prawo żądania od Administratora Danych niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
- Osoba, której dane dotyczą, ma prawo żądania od Administratora Danych niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
    - dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
    - osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
    - osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
    - dane osobowe były przetwarzane niezgodnie z prawem;
    - dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie powszechnie obowiązującym.

**§ 16**

Szczegółowy wykaz zbiorów danych osobowych wraz ze specyfikacją dot. m.in. opisu ich struktury, zakresu gromadzonych danych, celu przetwarzania, osób upoważnionych, a także ze wskazaniem programów zastosowanych do ich przetwarzania określa Załącznik do Polityki.

## ROZDZIAŁ IV
## Kontrola przestrzegania zasad bezpieczeństwa ochrony danych osobowych
### § 17

- Potencjalne zagrożenia dla bezpieczeństwa przetwarzania danych osobowych w Podmiocie:
    - połączenie systemu informatycznego, w którym przetwarzane są dane osobowe z ogólnodostępną siecią Internet – oprogramowanie szpiegujące czy monitorujące pracę komputera (wirusy komputerowe, konie trojańskie, rookity, keylogger, phishing itp.);
    - zamierzone działania ludzkie mające na celu nieautoryzowane przetwarzanie danych osobowych:
        - ujawnienie hasła i loginu;
        - podszycie się pod użytkownika;
        - użycie złośliwego oprogramowania;
        - włamania do systemu;
        - kradzież danych;
        - uszkodzenie zabezpieczeń fizycznych np. włamanie;
    - działania użytkownika, które w sposób przypadkowy mogą doprowadzić do nieautoryzowanego przetwarzania danych osobowych (m.in. błędy ludzkie):
        - udostępnienie stanowisk pracy osobom nieuprawnionym;
        - niewłaściwa konstrukcja haseł;
        - nieautoryzowane kopiowanie danych osobowych;
        - utrata nośnika zawierającego dane osobowe;
        - nieodpowiednie niszczenie nośników danych (np. kartki papieru, dyski);
        - pozostawienie zewnętrznych nośników danych w komputerze, np. pendrive;
        - używanie nośników danych udostępnionych przez osoby postronne;
        - samowolne instalowanie przez użytkowników oprogramowania nieznanego pochodzenia;
        - niewłaściwe ustawienie monitora komputerowego, umożliwiające osobom nieupoważnionym wgląd w przetwarzane dane osobowe;
        - pozostawienie dokumentów zawierających dane osobowe w miejscu ogólnodostępnym np. w drukarce, w kserokopiarce itp.;
        - pozostawienie kluczy w drzwiach do pomieszczeń stanowiących obszar przetwarzania danych osobowych lub w szafkach, gdzie znajdują się dane osobowe;
    - inne czynniki techniczne:
        - stosowanie bezprzewodowych kanałów komunikacyjnych np. wifi;
        - korzystanie z punktów typu HotSpot;
        - wahania napięcia;
    - zdarzenia losowe (np. pożar, włamanie, powódź, zalanie, kradzież, awaria oprogramowania).
- Do przypadków naruszenia bezpieczeństwa systemu informatycznego można m.in. zaliczyć:
    - brak możliwości uruchomienia przez użytkownika aplikacji pozwalającej na dostęp do danych osobowych;

- ograniczone w stosunku do normalnej sytuacji, uprawnienia użytkownika w aplikacji (np. brak możliwości wykonania pewnych operacji normalnie dostępnych użytkownikowi) lub uprawnienia poszerzone w stosunku do normalnej sytuacji;
- zidentyfikowanie w systemie wirusa lub innego programu mogącego uszkodzić, skasować lub skopiować dane osobowe;
- stwierdzenie próby lub podejrzenie nieautoryzowanego przetwarzania danych osobowych (np. zmieniona zawartość zbioru danych, zmiana kolejności ułożenia dokumentów, otwarte drzwi, nieautoryzowane zniszczenie zawartości zbioru danych);
- naruszenie technicznego stanu urządzeń;
- naruszenie zawartości zbioru danych osobowych;
- nieskuteczne zniszczenie nośników zawierających dane osobowe (np. nieprawidłowe zniszczenie dokumentów w wersji papierowej, nieprawidłowe usunięcie danych z nośnika np. pendrive);
- naruszenie zabezpieczenia systemu informatycznego np. przechwycenie danych przez program szpiegowski;
- odtajnienie hasła;
- zmiany funkcjonalności aplikacji;
- obniżenie jakości, prędkości, transmisji danych w sieci telekomunikacyjnej;
- niewykonanie kopii zapasowej;
- brak możliwości odtworzenia kopii zapasowej;
- powtarzające się zaniki zasilania;
- wykorzystywanie przetwarzanych danych osobowych niezgodnie z przepisami prawa powszechnie obowiązującego;
- nieprawidłowości w zakresie zabezpieczenia pomieszczeń gdzie przetwarzane są dane osobowe np. dopuszczenie osoby nieupoważnionej do wglądu w dane osobowe, niewylogowanie się po opuszczeniu stanowiska pracy;
- wystąpienie jednej z sytuacji kryzysowych, o których mowa powyżej;
- użytkowanie stacji roboczej przez osobę nie będącą użytkownikiem systemu;
- usuwanie, oddawanie lub modyfikowanie bez wiedzy i zgody użytkownika jego dokumentów;
- przechowywanie kopii zapasowych w tych samych pomieszczeniach, w których przechowywane są zbiory danych osobowych eksploatowane na bieżąco.

- Zastosowane środki techniczne:
  - dostęp do danych osobowych ograniczony jest autoryzacją użytkownika poprzez wpisanie loginu i hasła;
  - każdemu użytkownikowi uprawnionemu do przetwarzania danych osobowych przydzielany jest indywidualny login i hasło; hasło jest znane tylko przez użytkownika co pozwala na zachowanie zasady niezaprzeczalności zdarzeń; wymogi dotyczące haseł zostały opisane w Instrukcji;
  - od chwili otrzymania loginu użytkownik odpowiedzialny jest za wszystkie czynności, które zostały wykonane przy jego użyciu;
  - użytkownicy, bez zezwolenia Administratora Danych, nie mogą wynosić poza pomieszczenia stanowiące obszar przetwarzania danych osobowych dokumentów lub elektronicznych nośników informacji zawierających dane osobowe lub kopii tych danych (nie dotyczy przetwarzania danych osobowych na komputerach przenośnych);

- dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym – z wyjątkiem systemów służących do przetwarzania danych osobowych ograniczone wyłącznie do edycji tekstu w celu udostępnienia ich na piśmie – system zapewnia odnotowanie:
    - daty pierwszego wprowadzenia danych do systemu;
    - loginu użytkownika, który dane wprowadził;
    - źródła danych w przypadku, gdy dane pozyskiwane są nie od osoby, której dotyczą;
    - informacji o odbiorcach danych, o ile są przekazywane (data, zakres udostępnienia);
    - informacji o braku zgody osoby na przetwarzanie danych osobowych w celach marketingowych;
- w celu ochrony zbioru danych osobowych przed utratą lub celowym zniszczeniem, wszystkie bazy zawierające dane osobowe są kopiowane w określonych przez Administratora Danych odstępach czasowych;
- stacje robocze służące do przetwarzania danych osobowych zostały wyposażone w system operacyjny oraz pakiet biurowy z automatyczną aktualizacją. Stosuje się aktywną ochronę antywirusową w czasie rzeczywistym na każdym komputerze podłączonym do sieci. Oprogramowanie zostało skonfigurowane w taki sposób aby aktualizacje bez wirusów pobierane były automatycznie, a żaden z użytkowników nie miał możliwości wyłączenia programu antywirusowego.

- Zastosowane środki organizacyjne:
    - do przetwarzania danych osobowych może zostać dopuszczona osoba, która otrzymała od Administratora Danych upoważnienie do przetwarzania danych osobowych, którego wzór stanowi Załącznik nr 2 do Polityki;
    - warunkiem udzielenia upoważnienia do przetwarzania danych osobowych jest zaznajomienie użytkownika przetwarzającego dane osobowe z:
        - wymaganiami prawa powszechnie obowiązującego w zakresie ochrony danych osobowych;
        - Polityką;
        - Instrukcją.
    - Administrator Danych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi Załącznik nr 3 do Polityki;
    - wszystkie programy zainstalowane na stacjach roboczych pochodzą z legalnych źródeł, Administrator Danych posiada dokumenty potwierdzające legalność używanego w Podmiocie oprogramowania;
    - wdrożenie niniejszej Polityki oraz Instrukcji;
    - monitory użytkowników powinny zostać ustawione w taki sposób, że osoby postronne nie mają wglądu w treść wyświetlaną na ekranie;
    - na stacjach roboczych, na których przetwarzane są dane osobowe zainstalowano automatyczne wygaszacze ekranu blokujące po 10 minutach bezczynności dostęp do stacji roboczej;
    - użytkownicy zobowiązani są przy każdym opuszczeniu stanowiska pracy do zablokowania stacji roboczej;

- każdy użytkownik, który przetwarza dane osobowe w formie papierowej zobowiązany jest do zabezpieczenia ich przed osobami niemającymi upoważnienia do przetwarzania danych osobowych poprzez odpowiednie ich przechowywanie oraz niszczenie;
- niepotrzebne w danym momencie dokumenty w formie papierowej i nośniki elektroniczne, należy bezwzględnie chować w zamykanych szafach. Pod żadnym pozorem dokumenty i nośniki nie powinny pozostać niezabezpieczone po zakończeniu pracy. Wszystkie niepotrzebne dokumenty niszczone są przy pomocy niszczarki do papieru. Niedopuszczalne jest pozostawienie wydruków zawierających dane osobowe w miejscach ogólnodostępnych – zasada „czystego biurka";
- do momentu zniszczenia, dokumenty należy przechowywać w miejscu do którego osoby postronne nie mają dostępu;
- w przypadku naprawy sprzętu komputerowego zawierającego dane osobowe, dane te są wcześniej usuwane. W przypadku braku możliwości usunięcia danych – naprawa odbywa się pod nadzorem Administratora Danych lub osoby upoważnionej przez Administratora Danych;
- Administrator Danych przewiduje możliwość powierzenia przetwarzania danych osobowych innemu podmiotowi. Administrator Danych zawiera, z każdym podmiotem, któremu zostanie powierzone przetwarzanie danych osobowych, umowy o powierzeniu przetwarzania danych osobowych, w której określony zostanie zakres przetwarzania, cel ich przetwarzania oraz wymagane zabezpieczenia danych osobowych gwarantowane przez te podmioty.

- Każdy użytkownik przetwarzający dane osobowe przy użyciu komputera przenośnego zobowiązany jest do:
  - stosowania środków ochrony kryptograficznej wobec przetwarzanych danych osobowych zlokalizowanych na dysku komputerów przenośnych;
  - zachowania szczególnej ostrożności podczas transportu, przechowywania i użytkowania komputera przenośnego;
  - stosowania bezwzględnego zakazu pozostawiania komputera przenośnego w samochodzie lub przechowalni bagażu;
  - korzystania z komputera przenośnego tak aby zminimalizować ryzyko wglądu w wyświetlane na monitorze dane osobowe przez osoby nieupoważnione;
  - bezwzględnego zakazu udostępniania komputera przenośnego zawierającego dane osobowe osobom nieupoważnionym;
  - aktualizacji oprogramowania antywirusowego zainstalowanego na komputerze;
  - niezwłocznego poinformowania Administratora Danych o ewentualnej kradzieży lub zgubieniu komputera przenośnego;
  - w przypadku korzystania z komputera przenośnego w miejscach publicznych ograniczenia możliwości wglądu w treść wyświetlanych na monitorze komputera danych osobom nieupoważnionym;
  - sporządzania kopii zapasowych danych zgromadzonych na stacji roboczej oraz zabezpieczenia kopii przed dostępem osób nieupoważnionych.

**§ 18**

- Administrator Danych lub osoba przez niego upoważniona dokonuje okresowych kontroli i oceny funkcjonowania mechanizmów zabezpieczeń oraz przestrzegania zasad postępowania w przypadku naruszenia ochrony danych osobowych.

- Administrator Danych prowadzi rejestr dokonywanych kontroli oraz ustaleń, wniosków i zaleceń w nich wynikających, a także nadzoruje ich wykonywanie.

**§ 19**

- Zgromadzone w Podmiocie dane osobowe przekazywane są uprawnionym podmiotom na mocy obowiązujących przepisów prawa. Administrator Danych sprawuje nadzór nad tym jakie dane i w jakim zakresie, a także komu zostały udostępnione.
- Użytkownik, który udostępnia dane osobowe podmiotowi uprawnionemu, przed ich udostępnieniem zobowiązany jest sprawdzić czy istnieją przesłanki prawne umożliwiające przekazanie danych oraz poinformować Administratora o fakcie udostępnienia tych danych osobowych.
- W sytuacji otrzymania wniosku o udostępnienie danych osobowych od osoby, której one dotyczą, użytkownik lub Administrator Danych przygotowuje odpowiedź niezwłocznie.

## ROZDZIAŁ V
## Postępowanie w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych

**§ 20**

- Przed przystąpieniem do pracy użytkownik obowiązany jest dokonać sprawdzenia stanu stacji roboczej oraz oględzin swojego stanowiska pracy, w tym zwrócić szczególną uwagę, czy nie zaszły okoliczności wskazujące na naruszenie lub próby naruszenia ochrony danych osobowych.
- W przypadku stwierdzenia naruszenia lub zaistnienia okoliczności wskazujących na naruszenia ochrony danych osobowych, użytkownik zobowiązany jest do bezzwłocznego powiadomienia o tym fakcie Administratora Danych.
- Powyższe postanowienia mają zastosowanie zarówno w przypadku naruszenia lub podejrzenia naruszenia ochrony danych osobowych gromadzonych w systemach informatycznych, jak i w formie tradycyjnej.

**§ 21**

Do czasu przybycia Administratora Danych lub upoważnionej przez niego osoby, zgłaszający:

- powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również od podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;
- zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osób nieupoważnionych;
- podejmuje, stosownie do zaistniałej sytuacji, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

**§ 22**

Administrator Danych lub osoba przez niego upoważniona podejmuje kroki zmierzające do likwidacji naruszeń zabezpieczenia danych osobowych i zapobieżenia wystąpieniu ich w przyszłości.

**§ 23**

- W przypadku zaginięcia komputera lub nośników magnetycznych, na których były zgromadzone dane osobowe, użytkownik powiadamia Administratora Danych, a w przypadku kradzieży występuje o powiadomienie jednostki policji.

- W sytuacji, o której mowa w § 23 ust. 1 Polityki Administrator Danych podejmuje niezbędne kroki do wyjaśnienia okoliczności zdarzenia, sporządza protokół z zaginięcia, który powinna podpisać także osoba, której skradziono lub której zaginął sprzęt.
- W przypadku kradzieży komputera razem z nośnikiem magnetycznym Administrator Danych podejmuje działania zmierzające do odzyskania utraconych danych oraz nadzoruje proces przebiegu wyjaśnienia sprawy.

**§ 24**

Osoba zatrudniona przy przetwarzaniu danych osobowych za naruszenie obowiązków wynikających z niniejszej Polityki oraz przepisów prawa powszechnie obowiązującego ponosi odpowiedzialność przewidzianą w Kodeksie pracy lub innych aktach prawnych w zależności od rodzaju i skutków naruszeń.

## ROZDZIAŁ VI
## Postanowienia końcowe

**§ 25**

Polityka jest dokumentem wewnętrznym w Podmiocie i nie może być udostępniania osobom nieupoważnionym w jakiejkolwiek formie.

**§ 26**

- W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy prawa powszechnie obowiązującego.
- Wszelkie załączniki do niniejszej Polityki stanowią jej integralną część.
- Użytkownicy zobowiązani są do bezwzględnego stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.