POLITYKA OCHRONY DANYCH OSOBOWYCH

Egzemplarz zatwierdzony: ☐ **TAK** ☐ **NIE**

Podpis Administratora:

.....

Centrum Bezpieczeństwa Informatycznego
22-300 Krasnystaw
ul. Okrzei 15/9E

NIP: 564 144 74 18
REGON: 110670379
BS Krasnystaw 97 8200 0008 2001 0025 6393 0001

tel. (+48) 82 561 13 02
e-mail: biuro@cbi24.pl
www.cbi24.pl

Spis treści

Rozdział I 4
Przepisy Ogólne 4
Art. 1. Informacje wstępne 4
Art. 2. Zakres stosowania Polityki 5
Art. 3. Deklaracja stosowania 5
Art. 4. Definicje 5
Rozdział II 8
Polityka Ochrony Danych Osobowych 8
Art. 5. Podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych 8
1. Administrator 8
2. Inspektor Ochrony Danych /IOD/ 10
3. Obsługa informatyczna 11
4. Użytkownicy 12
Art. 6. Zasady ochrony danych osobowych 12
Art. 7. Podstawy dopuszczalności przetwarzania danych osobowych 13
Art. 8. Obowiązek informacyjny przy przetwarzaniu danych 13
Art. 9. Prawa osób, których dane dotyczą 15
Art. 10. Procedura nadawania upoważnień do przetwarzania danych osobowych 15
Art. 11. Rejestrowanie czynności przetwarzania danych 16
Art. 12. Szkolenia z zakresu ochrony danych osobowych 18
Art. 13. Realizacja prawa dostępu do danych 19
Art. 14. Dostęp do danych osobowych przez podmioty trzecie 19
Art. 15. Zasady anonimizacji danych osobowych 20
Art. 16. Procedura przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej 22
Art. 17. Zasady dotyczące dokonywania transmisji i utrwalania obrad rady 23
Art. 18. Zasady postępowania z dokumentami papierowymi zawierającymi dane osobowe 25
Art. 19. Naruszenia ochrony danych osobowych 25

Rozdział III 25
Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych 25
Art. 20. Zasady zarządzania uprawnieniami Użytkowników w systemach informatycznych 25
Art. 21. Zasady zabezpieczenia dostępu do systemów informatycznych 26
Art. 22. Zasady zarządzania sprzętem elektronicznym i oprogramowaniem 27
Art. 23. Zasady wykonywania kopii bezpieczeństwa 27
Art. 24. Zasady korzystania z poczty elektronicznej 28
Art. 25. Zasady korzystania z Internetu 29
Art. 26. Zasady korzystania z bankowości elektronicznej 30
Art. 27. Zarządzanie pojemnością przestrzeni dyskowej 31
Art. 28. Zasady bezpiecznego przydzielania przestrzeni dyskowej 31
Art. 29. Komunikacja i czynności serwisowe na odległość 32
Art. 30. Zasady pracy z urządzeniami mobilnymi 32
Art. 31. Zasady zabezpieczania sprzętu elektronicznego i systemu informatycznego 33
Art. 32. Zasady korzystania z elektronicznych nośników danych 33
Art. 33. Zasady wykonywania przeglądów i konserwacji sprzętu elektronicznego i nośników danych 34
Art. 34. Zasada utylizacji i serwisu sprzętu elektronicznego 35
Rozdział IV 35
Inne środki organizacyjne i techniczne służące do zabezpieczania danych osobowych 35
Art. 35. Zasady bezpiecznej pracy 35
Art. 36. Zarządzanie ryzykiem 36
Art. 37. Audyt wewnętrzny w zakresie bezpieczeństwa informacji 37
Art. 38. Zarządzanie kluczami 37
Art. 39. Ochrona danych osobowych w fazie projektowania i domyślna ochrona danych 39
Rozdziała V 40
Postanowienia końcowe 40
Art. 40 Przetwarzanie danych osobowych w celu prowadzenia postępowań rekrutacyjnych 40
Art. 41 Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowych 41
Art. 42. Informacje dotyczące Polityki ochrony danych osobowych 42

Rozdział I
Przepisy Ogólne

Art. 1. Informacje wstępne

1. Polityka ochrony danych osobowych zwana dalej „Polityką" jest dokumentem wewnętrznym *Urzędu Gminy Złota* – zwanego dalej również „Jednostką", opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań wynikających z:

   1) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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) (Dz. Urz. UE L 119, s. 1, sprost.: Dz. Urz. UE L 127 z 23.05.2018, s. 2);
   2) Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (t. j. Dz. U. z 2019 r. poz. 1781 ze. zm.);
   3) Rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r., poz. 2247);
   4) Przepisów szczególnych, regulujących funkcjonowanie Jednostki i przetwarzanych w ramach jej działalności danych osobowych,
   5) Dobrych praktyk z zakresu bezpieczeństwa informacji oraz ochrony danych osobowych.

Art. 2. Zakres stosowania Polityki

Niniejsza Polityka ma zastosowanie do danych osobowych przetwarzanych przez Jednostkę w systemach informatycznych (sposób zautomatyzowany) oraz w postaci papierowej (niezautomatyzowany), a także w realizowanych projektach finansowanych ze środków zewnętrznych w ramach systemu SL2014.

Art. 3. Deklaracja stosowania

1. Administrator ustanawia Politykę oraz deklaruje:
   1) podejmowanie wszystkich działań niezbędnych dla zapewnienia legalności przetwarzanych danych,
   2) stałe podnoszenie świadomości oraz kwalifikacji osób przetwarzających dane w zakresie problematyki bezpieczeństwa tychże danych,
   3) stosowanie adekwatnych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanym danym,
   4) dążenie do zapewnienia poufności, dostępności oraz integralności danych osobowych.

Art. 4. Definicje

1) **Administrator** – Urząd Gminy Złota, reprezentowany przez Wójta; oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W rozumieniu niniejszej polityki ochrony danych pod pojęciem „Administratora" należy rozumieć Jednostkę
2) **aktywa** – wszelkie elementy posiadające wartość dla Jednostki (zasoby ludzkie, finansowe, informacyjne, organizacyjne, technologiczne, i fizyczne) mogące służyć do przetwarzania danych osobowych;
3) **dane osobowe** – 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;

4) **dane osobowe zwykłe** – wszelkie dane osobowe nienależące do szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, jak również danych dotyczących wyroków skazujących lub czynów zabronionych;

5) **szczególnych kategorii dane osobowe**– dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej (w tym o korzystaniu z usług opieki zdrowotnej) ujawniające informacje o stanie jej zdrowia; 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) oraz dane dotyczące seksualności lub orientacji seksualnej osoby fizycznej;

6) **dane dotyczące wyroków skazujących i czynów zabronionych** – dane dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa, które można przetwarzać wyłącznie pod nadzorem władz publicznych lub gdy pozwalają na to przepisy prawa krajowego lub prawa unijnego;

7) **Inspektor Ochrony Danych /IOD/** – osoba, wyznaczona przez Administratora lub podmiot przetwarzający, posiadająca odpowiednie kwalifikacje zawodowe (wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych osobowych) oraz umiejętności wymagane do wypełniania zadań związanych z ochroną danych, zwana w treści Polityki również jako „IOD";

8) **kopia zapasowa** – kopia danych lub oprogramowania, której celem wykonania jest odtworzenie systemu po awarii;

9) **Jednostka** – Urząd Gminy Złota;

10) **naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

11) **Obsługa informatyczna** – osoba lub podmiot wyznaczony przez Administratora do realizacji zadań w zakresie zarządzania, bieżącego nadzoru nad systemami

informatycznymi oraz serwisu sprzętu komputerowego w Jednostce;

12) **Odbiorca** - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią; Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców - przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

13) **Ograniczenie przetwarzania** – oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

14) **Podatność** - słabość aktywu (zasobu) lub zabezpieczenia które może być wykorzystane przez jedno lub więcej zagrożeń

15) **Podmiot przetwarzający** – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora na zlecenie;

16) **Polityka** – niniejsza Polityka ochrony danych osobowych;

17) **przetwarzanie** – operacja 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;

18) **Rejestr czynności przetwarzania danych osobowych**– rejestr czynności przetwarzania danych osobowych, o którym stanowi art. 30 ust. 1 RODO;

19) **Rejestr wszystkich kategorii czynności przetwarzania** – rejestr wszystkich kategorii czynności przetwarzania, o którym stanowi art. 30 ust. 2 RODO;

20) **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 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);

21) **Ryzyko** – potencjalna sytuacja, w której określone zagrożenie wykorzystując podatność aktywów lub grupy aktywów powodować może chociażby potencjalną szkodę majątkową lub niemajątkową dla Jednostki;

22) **System informatyczny** – system przetwarzania danych, w tym danych osobowych, łącznie z zasobami technicznymi (stanowisko pracy, jednostka centralna, system zarządzania, sieć teletransmisyjna), pracownikami oraz określonym obszarem działania (pomieszczeniami);

23) **Szacowanie ryzyka** – proces identyfikowania i analizy ryzyka oraz jego oceny;

24) **Użytkownik** - osoba posiadająca dostęp do systemu informatycznego przetwarzającego dane osobowe w Jednostce;

25) **Zagrożenie** – niepożądane działanie lub sytuacja, która może niekorzystnie wpłynąć na prawidłowość oraz bezpieczeństwo procesów realizowanych w Jednostce, potencjalna przyczyna wystąpienia incydentu;

26) **Zarządzanie ryzykiem** – skoordynowane działania w celu systematycznego stosowania zasad zarządzania, procedur, instrukcji a także kierowanie i sterowanie Jednostką z uwzględnieniem oszacowanego ryzyka;

27) **Zgoda** – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Rozdział II
Polityka Ochrony Danych Osobowych

Art. 5. Podmioty odpowiedzialne za ochronę i przetwarzanie danych osobowych

1. **Administrator**
   1) wdraża odpowiednie środki techniczne i organizacyjne, mające na celu zabezpieczanie przetwarzanych danych oraz zapewnianie poufności, integralności i dostępności danych,
   2) wyznacza IOD, o czym zawiadamia Prezesa Urzędu Ochrony Danych Osobowych,
   3) podejmuje odpowiednie działania w przypadku naruszenia ochrony danych

osobowych lub podejrzenia naruszenia ochrony danych osobowych zgodnie z procedurą stanowiącą integralną część niniejszej Polityki,

4) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie,
5) nadaje lub zatwierdza Użytkownikom uprawnienia do pracy w systemach informatycznych wykorzystywanych przez Jednostkę,
6) podejmuje decyzje dotyczące przeprowadzenia oceny skutków planowanych operacji przetwarzania danych po konsultacji z IOD,
7) zatwierdza Rejestr czynności przetwarzania danych osobowych oraz Rejestr wszystkich kategorii czynności przetwarzania,
8) wdraża niniejszą Politykę wraz z załącznikami,
9) dopełnia wszelkie pozostałe obowiązki wymagane przez RODO i inne przepisy regulujące zasady przetwarzania danych osobowych w Jednostce,
10) Administrator publikuje dane kontaktowe Inspektora Ochrony Danych i zawiadamia o nich organ nadzorczy, zgodnie z art. 37 ust. 7 RODO. Publikacja danych kontaktowych odbywa się w poprzez publiczne udostępnienie przez Administratora informacji o: imieniu i nazwisku Inspektora, numerze kontaktowym lub adresie e-mail, zgodnie z art. 11 w zw. z art. 10 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych,
11) włącza i współpracuje z IOD we wszystkich sprawach dotyczących ochrony danych osobowych, w tym informuje o nowych procesach przetwarzania danych osobowych,
12) Administrator w momencie projektowania /planowania nowych działań, które będą wiązały się z bezpośrednio lub pośrednio z przetwarzaniem danych osobowych (tzw. privacy by design) zobligowany jest do:
    a) przedstawienia opisu planowanego procesu przetwarzania danych osobowych i dokonania przy ewentualnej współpracy z IOD analizy zawierających:
        - szczegółową podstawę prawną podjęcia działań w projektowanym procesie, w tym w odniesieniu do podstawy legalizującej przetwarzanie danych osobowych (art. 6 ust. 1 lub 9 ust. 2 RODO),
        - zakres kategorii osób oraz rodzaju danych osobowych, które będą

przetwarzane w planowanym procesie,

- przewidywanych zasobów techniczno-organizacyjnych (tj. materialnych, sprzętowych oraz osobowych)
- proponowanych zabezpieczeń techniczno-organizacyjnych,
- planowanych terminów retencji danych,
- potencjalnego ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze w odniesieniu do zagrożeń wewnętrznych i zewnętrznych,
- potencjalnych odbiorców gromadzonych danych osobowych,

b) przedstawienia IOD informacji, o których mowa w pkt a) w celu przeprowadzenia analizy ryzyka

2. Inspektor Ochrony Danych /IOD/

1) weryfikuje przestrzeganie przepisów o ochronie danych osobowych i informuje Administratora oraz wszystkie osoby przetwarzające dane o obowiązkach na nich spoczywających,
2) wspólnie z Administratorem aktualizuje dokumentację z zakresu ochrony danych osobowych, tj. m.in. niniejszą Polityką,
3) opracowuje Rejestr czynności przetwarzania danych oraz Rejestr wszystkich kategorii czynności przetwarzania we współpracy z Administratorem lub wyznaczonymi osobami działającymi z upoważnienia administratora i dokonuje jego aktualizacji.
4) współpracuje z Administratorem w zakresie oceny skutków planowanych operacji przetwarzania danych oraz monitoruje jej wykonanie,
5) pełni funkcję punktu kontaktowego oraz współpracuje w przypadkach opisanych w przepisach z Prezesem Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem danych osobowych,
6) dokonuje analizy zgłoszonych naruszeń ochrony danych osobowych i rekomenduje podjęcie działań w jego obsłudze,
7) na wniosek Administratora opiniuje wnioski dotyczące realizacji praw osób, których dane dotyczą,

8) we współpracy z Administratorem dokonuje systemowego sprawdzenia procesu wydawania upoważnień do przetwarzania danych osobowych i uprawnień do systemów informatycznych,
9) na wniosek Administratora opiniuje umowy powierzenia przetwarzania danych osobowych,
10) przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych dla osób mających dostęp do danych,
11) bierze czynny udział w audytach zewnętrznych dotyczących przetwarzania danych osobowych w Jednostce.

3. Obsługa informatyczna

1) przydziela Użytkownikom identyfikator i hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa lub wyłącza konta Użytkowników zgodnie z zasadami określonymi w niniejszej Polityce oraz właściwych przepisach prawa,
2) dokonuje naprawy i konserwację sprzętu komputerowego,
3) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji,
4) wykonuje kopie zapasowe danych lub oprogramowania,
5) prowadzi inwentaryzację sprzętu komputerowego i oprogramowania,
6) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje IOD o naruszeniu i współdziała z nim przy ustalaniu i usuwaniu skutków naruszenia.
7) prowadzi regularne przeglądy infrastruktury IT.

4. Użytkownicy

1) Użytkownicy dopuszczeni przez Administratora do przetwarzania danych osobowych, zobowiązani są do:
   a) udziału w szkoleniach dotyczących ochrony danych osobowych,
   b) zapoznania się z przepisami prawa w zakresie ochrony danych osobowych,
   c) niezwłocznego zawiadomienia przełożonego o naruszeniach ochrony danych osobowych,
   d) stosowania określonych przez Administratora procedur i środków mających na celu zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym.
2) Ponadto osoby zajmujące kierownicze stanowiska w strukturze Jednostki oraz osoby zatrudnione na samodzielnych stanowiskach pracy są zobowiązani do:
   a) współdziałania z IOD w zakresie spraw dotyczących ochrony danych osobowych,
   b) sprawowania nadzoru nad pracą podległych osób w zakresie wykonywania czynności służbowych w sposób zapewniający ochronę danych osobowych,
   c) niezwłocznego zawiadomienia Administratora i IOD o naruszeniach ochrony danych osobowych.
   d) informowania IOD o realizacji nowych zadań lub projektów, które wiążą się z przetwarzaniem danych osobowych.

Art. 6. Zasady ochrony danych osobowych

1. Administrator zapewnia aby przetwarzanie danych osobowych odbywało się z poszanowaniem następujących zasad:
   1) dane osobowe muszą być przetwarzane zgodnie z prawem (legalizm);
   2) dane osobowe muszą być przetwarzane rzetelnie i uczciwie (rzetelność);
   3) dane osobowe muszą być przetwarzane w sposób przejrzysty dla osoby, której dane dotyczą (przejrzystość);
   4) dane osobowe muszą być przetwarzane w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których dane są przetwarzane (minimalizacja);
   5) dane osobowe muszą być przetwarzane z dbałością o prawidłowość i aktualność danych (prawidłowość);

6) dane osobowe muszą być przetwarzane nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania danych osobowych (ograniczenie przechowywania);
7) dane osobowe muszą być przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (ograniczenie celu);
8) dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych (bezpieczeństwo).

Art. 7. Podstawy dopuszczalności przetwarzania danych osobowych

1. Przetwarzanie danych osobowych zwykłych dopuszczalne jest tylko wtedy, gdy zostanie spełniona jedna z przesłanek wynikających z art. 6 ust. 1 RODO.
2. W przypadku przetwarzania szczególnych kategorii danych osobowych podstawą dopuszczalności przetwarzania danych mogą być wyłącznie przesłanki wynikające z art. 9 ust. 2 RODO.
3. W przypadku przetwarzania danych osobowych dotyczących wyroków skazujących i czynów zabronionych powinna zostać spełniona jedna z przesłanek wymienionych w art. 10 RODO.
4. W przypadku przetwarzania danych osobowych na podstawie zgody osoby, której dane dotyczą, należy stosować oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych, którego wzór stanowi **załącznik nr 1** do niniejszej Polityki (wzór służy do konstruowania szczegółowych zgód na przetwarzanie danych osobowych), a wzór oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych znajduje się w **załączniku nr 2**.

Art. 8. Obowiązek informacyjny przy przetwarzaniu danych

1. Administrator realizuje obowiązek informacyjny w stosunku do osób fizycznych od których bezpośrednio są zbierane dane osobowe zgodnie z art. 13 ust. 1 i 2 RODO oraz w stosunku do osób, których dane zostały zebrane z innego źródła aniżeli bezpośrednio od osoby, której dane dotyczą zgodnie z art. 14 ust.1 i 2 RODO.

2. Zwolnienie z realizacji obowiązku informacyjnego wynikającego z art. 13 ust. 1 i 2 RODO znajduje zastosowanie w sytuacji, gdy osoba, której dane dotyczą dysponuje już tymi informacjami oraz w przypadkach uregulowanych w powszechnie obowiązujących przepisach prawa.
3. Wzór ogólny klauzuli informacyjnej zawierającej informacje, o których mowa w art. 13 ust. 1 i 2 RODO - służącej za podstawę do konstruowania szczegółowych klauzul informacyjnych na potrzeby Jednostki, stanowi **załącznik nr 3** do niniejszej Polityki.
4. Administrator realizuje obowiązek informacyjny z art. 13 ust. 1 i 2 RODO w następujący sposób:
   a) Umieszczony w miejscu ogólnodostępnym w siedzibie Administratora;
   b) Indywidualnie;
   c) Realizowany na stanowiskach pracy;
   d) Umieszczony na stronie internetowej oraz na stronie BIP Jednostki;

   - oraz w sposób szczegółowo wskazany w źródłach prawa powszechnie obowiązującego.
5. Wzór ogólny klauzuli informacyjnej- zawierającej informacje, o których mowa w art. 14 ust. 1 i 2 RODO służącej za podstawę do konstruowania szczegółowych klauzul informacyjnych na potrzeby Jednostki, stanowi **załącznik nr 4** do niniejszej Polityki.
6. Zwolnienie z realizacji obowiązku informacyjnego na podstawie art. 14 ust.1 i 2, RODO znajduje zastosowanie gdy zostanie spełniona jedna z przesłanek wyszczególnionych w art. 14 ust. 5 RODO.
7. Administrator realizuje obowiązek informacyjny z art. 14 ust. 1 i 2 RODO w sposób szczegółowo wskazany w źródłach prawa powszechnie obowiązującego.

Art. 9. Prawa osób, których dane dotyczą

1. Osobie, której dane są przetwarzane, przysługują następujące prawa:
   1) prawo dostępu do danych,
   2) prawo do sprostowania danych,
   3) prawo do usunięcia danych,
   4) prawo do ograniczenia przetwarzania danych,
   5) prawo do przenoszenia danych,
   6) prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
2. Szczegółowe zasady realizowania w/w praw zostały opisane w **załączniku nr 5** do niniejszej Polityki.

Art. 10. Procedura nadawania upoważnień do przetwarzania danych osobowych

1. Do przetwarzania danych osobowych mogą mieć dostęp osoby posiadające pisemne upoważnienia do przetwarzania danych osobowych nadane przez Administratora, przy czym osoby te zobowiązane są złożyć oświadczenie o zachowaniu w tajemnicy danych osobowych lub winny podlegać odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.
2. Pracownik ds. kadr przygotowuje stosowne upoważnienie do przetwarzania danych osobowych.
3. Upoważnienie jest przygotowywane na podstawie wzoru upoważnienia do przetwarzania danych osobowych stanowiącego **załącznik nr 6** do niniejszej Polityki, natomiast wzór oświadczenia o zachowaniu w tajemnicy danych osobowych stanowi **załącznik nr 7**.
4. Administrator uprawniony jest do odwołania nadanego upoważnienia do przetwarzania danych osobowych w każdym czasie.
5. Zatwierdzone przez Administratora upoważnienie do przetwarzania danych osobowych pracownik ds. kadr rejestruje w ewidencji osób upoważnionych do przetwarzania danych, której wzór stanowi **załącznik nr 8** do niniejszej Polityki.
6. Upoważnienia do przetwarzania danych osobowych przechowywane są aktach osobowych oraz dokumentacji z zakresu ochrony danych osobowych.

7. W przypadku zmiany stanowiska lub zakresu obowiązków osoby upoważnionej albo w przypadku wystąpienia innych okoliczności, które wpływają bezpośrednio na rodzaj i zakres przetwarzanych danych osobowych osoba, o której mowa w ust. 2 zobowiązana jest do przygotowania nowego upoważnienia do przetwarzania danych osobowych.
8. Informacja o zmianie stanowiska lub zakresu obowiązków osoby upoważnionej, bądź wystąpienia innych okoliczności mających wpływ na rodzaj i zakres przetwarzanych danych osobowych, powinna być niezwłocznie przekazana do Obsługi informatycznej celem ewentualnej zmiany uprawnień do pracy w systemach informatycznych.
9. W przypadku ustania zatrudnienia lub zaistnienia innej przyczyny skutkującej odwołaniem upoważnienia, pracownik ds. kadr odnotowuje zmiany w ewidencji osób upoważnionych do przetwarzania danych osobowych – **załącznik nr 8**. Powyższe dotyczy każdej formy zatrudnienia, a także przetwarzania danych osobowych w związku z organizacją stażu, praktyki, wolontariatu w Jednostce.
10. Informacja o ustaniu zatrudnienia osoby upoważnionej lub zaistnienia innej przyczyny skutkującej odwołaniem upoważnienia powinna zostać niezwłocznie przekazana do Obsługi informatycznej celem odebrania takiej osobie wszystkich uprawnień do pracy w systemach informatycznych.

Art. 11. Rejestrowanie czynności przetwarzania danych

1. Wszystkie czynności przetwarzania realizowane przez Administratora zamieszcza się w Rejestrze czynności przetwarzania danych osobowych, który w celu jego obowiązywania wprowadza się odrębnym aktem administracyjnym.
2. Wszystkie czynności przetwarzania powierzone Administratorowi przez innego Administratora, Jednostka zamieszcza w Rejestrze wszystkich kategorii czynności przetwarzania, który w celu jego obowiązywania wprowadza się odrębnym aktem administracyjnym.
3. W przypadku zmian w przepisach prawa lub nałożenia na Jednostkę przez naczelne lub centralne organy administracji państwowej obowiązku wykonania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej,

w związku z realizacją których występuje konieczność przetwarzania danych osobowych, pracownicy uzyskujący taką informację zobowiązani są do poinformowania kierownika Wydziału, który we współpracy z Inspektorem Ochrony Danych, na podstawie przekazanych informacji dokonuje uzupełnienia lub zmian w Rejestrze czynności przetwarzania danych osobowych.

4. W przypadku uzyskania informacji przez pracownika Jednostki o powierzeniu przetwarzania danych osobowych Jednostce – na podstawie umowy lub innego instrumentu prawnego – pracownik ten jest zobowiązany do poinformowania kierownika Wydziału, który we współpracy z Inspektorem Ochrony Danych, na podstawie przekazanych informacji dokonuje uzupełnienia lub zmian w Rejestrze wszystkich kategorii czynności przetwarzania
5. Rejestry, o których mowa w ust. 1 i 2 przyjmują formę pisemną, w tym formę elektroniczną, która powinna być prowadzona w systemie informatycznym równolegle z formę pisemną.
6. Administrator jest zobowiązany do udostępnienia w/w rejestrów na żądanie organu nadzorczego. W/w Rejestry nie stanowią dokumentów udostępnianych na podstawie Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz. U. z 2020 r., poz. 2176).
7. IOD we współpracy z Administratorem, przygotowuje i aktualizuje rejestry, o których mowa w ust. 1 i 2.

Objaśnienie:

Rejestr czynności przetwarzania danych osobowych prowadzony jest przez Jednostkę w przypadku, w którym Jednostka występuje jako Administrator danych osobowych.

W Rejestrze tym zamieszcza się następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe Administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie - przedstawiciela administratora oraz inspektora ochrony danych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym

odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Rejestr wszystkich kategorii czynności przetwarzania prowadzony jest przez Jednostkę, w przypadku, w którym Jednostka występuje jako Podmiot przetwarzający dane osobowe na zlecenie.

W Rejestrze tym zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe Podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa Podmiot przetwarzający, a gdy ma to zastosowanie - przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
c) gdy ma to zastosowanie -przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentacja odpowiednich zabezpieczeń;
d) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Art. 12. Szkolenia z zakresu ochrony danych osobowych

1. Każda osoba, która uzyskuje upoważnienie do przetwarzania danych osobowych ma obowiązek zapoznać się z najważniejszymi informacjami o obowiązkach związanych z przetwarzaniem danych osobowych. Wzór informatora zawierającego w/w informacje stanowi **załącznik nr 9** do niniejszej Polityki.
2. IOD lub inna wyznaczona osoba, z własnej inicjatywy lub na wniosek Administratora,

przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych dla osób je przetwarzających.

3. Dodatkowo szkolenia wewnętrzne są przeprowadzane w przypadku każdej istotnej zmiany zasad lub przepisów dotyczących ochrony danych osobowych, odpowiednio uwzględniając postanowienie ust. 2.
4. Każde szkolenie wewnętrzne powinno być udokumentowane poprzez sporządzenie dokumentów potwierdzających uczestnictwo w takim szkoleniu przez jego uczestników (lista obecności lub zaświadczenie/certyfikat imienny dla Użytkownika).

Art. 13. Realizacja prawa dostępu do danych

1. Realizacja prawa dostępu do danych została opisana w **załączniku nr 5** do Polityki – art. 3 Prawo dostępu do danych.

Art. 14. Dostęp do danych osobowych przez podmioty trzecie

1. Administrator może przekazać podmiotowi trzeciemu (niebędącemu osobą, której dane dotyczą) przetwarzane przez siebie dane osobowe w ramach:
   1) udostępnienia jeżeli jest to przewidziane w powszechnie obowiązujących przepisach prawa,
   2) powierzenia jeżeli podmiot trzeci przetwarza dane w imieniu Administratora i na jego udokumentowane polecenie w rozumieniu art. 28 RODO.
2. W przypadku powierzenia przetwarzania danych konieczne jest zawarcie umowy powierzenia przetwarzania danych osobowych pomiędzy Administratorem oraz podmiotem przetwarzającym dane na zlecenie, który przetwarza dane w imieniu Administratora, bądź posłużenie się innym instrumentem prawnym, który podlega prawu Unii lub prawu polskiemu i wiąże zarówno podmiot przetwarzający, jak i Administratora.
3. IOD przygotowuje (we współpracy z osobami upoważnionymi, a także osobą reprezentującą Administratora) i weryfikuje umowy powierzenia przetwarzania danych lub inne instrumenty prawne przed ich zawarciem.
4. Administrator przyjął minimalne wymagania co do treści umowy powierzenia

przetwarzania danych, której wzór stanowi **załącznik nr 10** do Polityki.

5. Administrator po zawarciu każdej umowy powierzenia – poprzez pracownika ds. zarządzenia kryzysowego – odnotowuje ten fakt w rejestrze zawartych umów powierzenia, którego wzór stanowi **załącznik nr 11** do niniejszej Polityki.

Art. 15. Zasady anonimizacji danych osobowych

1. Osoba sporządzająca dokumenty przeznaczone do udostępnienia w Biuletynie Informacji Publicznej Jednostki, jest zobowiązana do oceny przedmiotowych dokumentów pod względem dopuszczalności publikacji danych osobowych osób fizycznych niepełniących funkcji publicznych lub kierowniczych.
2. Osoba sporządzająca dokumenty przeznaczone do udostępnienia w Biuletynie Informacji Publicznej Jednostki zobowiązana jest do dokonania analizy legalności publikacji danych osobowych zawartych w dokumentacji oraz w razie konieczności do dokonania ich anonimizacji.
3. Na podstawie obowiązujących przepisów o dostępie do informacji publicznej zaleca się zastosowanie następujących zasad anonimizacji danych:
   1) w przypadku udostępniania informacji o osobie fizycznej anonimizacji – co do zasady – podlegają:
      a) imię i nazwisko, chyba że dane te są zawarte w umowach podlegających publikacji w BIP,
      b) PESEL oraz NIP,
      c) data i miejsce urodzenia,
      d) numer dokumentu, za pomocą którego można zidentyfikować osobę fizyczną (np. dowód, paszport, prawo jazdy, legitymacja, koncesja, itp.),
      e) adres zamieszkania, zameldowania lub pobytu,
      f) numer tel. lub faksu,
      g) adres e-mail,
      h) numer konta bankowego,
      i) numer działki i obręb,
      j) numer księgi wieczystej,
      k) informacje o zobowiązaniach finansowych (chyba że dane te podlegają

publikacji w BIP),

l) informacje o stanie zdrowia, sytuacji finansowej, społecznej, itp.,

m) inne dane pozwalające zidentyfikować osobę fizyczną lub naruszyć jej prawa i wolności,

2) w przypadku udostępniania wyciągów z rachunków bankowych lub dokumentacji księgowej (w tym faktur) anonimizacji podlegają:

a) imię i nazwisko (chyba że dane te są zawarte w umowach podlegających publikacji w BIP),

b) PESEL oraz NIP,

c) adres zamieszkania, zameldowania lub pobytu,

d) numer konta bankowego,

3) Anonimizacji nie podlega jednak imię i nazwisko usługodawcy lub nazwa firmy realizującej usługę, informacja o wykonanej usłudze oraz kwota, za jaką usługa została wykonana.

4) w przypadku udostępniania kopii innych dokumentów Jednostki dodatkowo anonimizacji podlegają wszystkie informacje, które mogą bezpośrednio zidentyfikować osobę fizyczną lub inne osoby fizyczne biorące udział w realizacji spraw.

4. Zasady anonimizacji opisane w niniejszym rozdziale stanowią jedynie reguły ogólne anonimizacji i powinny być każdorazowo indywidualnie weryfikowane kiedy dochodzi do udostępniania danych.

5. Anonimizacji nie podlegają w żadnym przypadku:

1) nazwy organów, urzędów oraz instytucji publicznych,

2) nazwy organizacji międzynarodowych,

3) nazwy sądów,

4) nazwy spółek Skarbu Państwa,

5) dane osób reprezentujących Administratora,

6) dane pracowników Administratora w zakresie realizacji zadań określonych w regulaminie Jednostki,

7) dane członków zespołów, komisji rad i innych powołanych do realizacji zadań,

8) nazwy dokumentów, np. uchwała, zarządzenie, umowa, porozumienie, aneks, a także elementy dokumentów, które nie naruszają praw i wolności osoby,

9) imiona i nazwiska autorów cytowanych książek, komentarzy, artykułów naukowych, jeśli ich prace były wykorzystywane w treści dokumentów urzędowych podlegających udostępnieniu,
10) oznaczenie czasu, tj. informacje o latach, miesiącach, dniach, godzinach, przedziałach czasowych, jak też daty wytworzenia dokumentów, z wyjątkiem daty urodzenia osoby fizycznej,
11) dane, co do których wyrażona jest pisemna zgoda na ich ujawnienie w BIP (np. petycje).

Art. 16. Procedura przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej

1. Administrator udostępnia publicznie dane osobowe w Biuletynie Informacji Publicznej zgodnie z zasadami określonymi w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (t. j. Dz. U. z 2020 r. poz. 2176) i innych przepisach prawa powszechnie obowiązującego.
2. Administrator z uwzględnieniem zasady ograniczenia przechowywania zapewnia, że przechowuje dane osobowe publikowane w Biuletynie Informacji Publicznej w formie umożliwiającej identyfikację podmiotu danych przez okres nie dłuższy, niż jest to niezbędne do celów, w których te dane osobowe są przetwarzane (okres retencji).
3. W przypadkach, gdy okres retencji danych osobowych publikowanych w Biuletynie Informacji Publicznej nie wynika wyraźnie z przepisów prawa, Administrator ustala niniejsze okresy samodzielnie, uwzględniając ogólne zasady przetwarzania danych osobowych przewidziane w RODO, w tym przede wszystkim zasadę ograniczenia przechowywania określoną w art. 5 ust. 1 lit. e. Wszystkie ustalone okresy retencji zostają uwzględnione w treści Rejestru czynności przetwarzania danych osobowych prowadzonego przez Administratora, zwanego dalej Rejestrem.
4. Dane osobowe mogą być ponadto przetwarzane dłużej niż wynosi okres retencji, w przypadku, gdy są one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (na zasadach określonych w art. 89 ust. 1 RODO), pod warunkiem że wdrożone zostaną

odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności podmiotów danych.

5. Administrator – poprzez Informatyka Urzędu cyklicznie tj. nie rzadziej niż raz w roku posiada obowiązek dokonania przeglądu danych osobowych publikowanych w Biuletynie Informacji Publicznej. Poza okresowymi przeglądami Administrator przeprowadza również przeglądy tych danych, jeśli zajdzie przynajmniej jedna z poniższych sytuacji:
   1) zmienione zostaną powszechnie obowiązujące przepisy prawa mające wpływ na okres retencji,
   2) organ nadzorczy lub organ kontrolujący wydadzą zalecenia dotyczące przeglądu danych,
   3) zostanie wydana uzasadniona decyzja Administratora (o której osoby zatrudnione w organizacji Administratora oraz z nią współpracujące zostaną poinformowane).
6. Wszelkie przeglądy danych osobowych publikowanych w Biuletynie Informacji Publicznej podlegają dokumentowaniu w postaci stosownego dokumentu i są przechowywane u Sekretarza Urzędu.

Art. 17. Zasady dotyczące dokonywania transmisji i utrwalania obrad rady gminy

1. Administrator dokonuje transmisji i utrwalania obrad rady gminy zgodnie z art. 20 ust. 1b ustawy o samorządzie gminnym (t. j. Dz. U. z 2020, poz. 713 ze zm.) „Obrady rady gminy są transmitowane i utrwalane za pomocą urządzeń rejestrujących obraz i dźwięk. Nagrania obrad są udostępniane w Biuletynie Informacji Publicznej i na stronie internetowej gminy oraz w inny sposób zwyczajowo przyjęty".
2. Przed rozpoczęciem obrad, Przewodniczący rady Gminy:
   1) informuje radnych i innych uczestników, iż obrady są transmitowane na żywo oraz informuje o obowiązkach w zakresie nieujawniania, bez uzasadnionej potrzeby, danych osobowych osób niebędących funkcjonariuszami publicznymi, niepełniącymi funkcji publicznej, ani niezwiązanymi z tą funkcją.
   2) realizuje obowiązek informacyjny wynikający z art. 13 ust. 1 i 2 RODO, poprzez każdorazowe odczytywanie obowiązku informacyjnego przez rozpoczęciem sesji.

3. Administrator dokonuję teletransmisji sesji rady gminy indywidualnie poprzez wykupioną licencję programu komputerowego. W przypadku dokonywania transmisji i przechowywania nagrań z sesji rady miasta poprzez podmiot zewnętrzny, z którym Administrator zawarł umowę o świadczenie usługi, winna zostać zawarta również w w/w przedmiocie umowa powierzenia przetwarzania danych osobowych, a serwer podmiotu przetwarzającego winien znajdować się w na terytorium Europejskiego Obszaru Gospodarczego. W przypadku umieszczenia nagrania na serwerze państwa trzeciego należy uwzględnić wymagania stawiane w tym zakresie przez art. 44-49 RODO.
4. Administrator dysponuje własną kopią nagrania obrad, które przechowywane jest na dysku komputera użytkowanego do transmisji i obsługi sesji rady miasta oraz na zewnętrznym dysku sieciowym.
5. Administrator dysponuje własną kopią nagrania obrad, które udostępniane są na stronie internetowej oraz BIP jednostki na stronie – transmisjaobrad.info
6. Administrator lub wyznaczona przez Administratora osoba przygotowując protokół, stenogram lub nagranie z takiego posiedzenia, w związku z jego udostępnieniem publicznym – zobowiązany jest do ochrony prawa do prywatności osób fizycznych, w tym ochrony ich danych osobowych. W związku z powyższym, jeżeli przy przygotowaniu ww. materiałów pojawią się dane osobowe osób niebędących funkcjonariuszami publicznymi, niepełniącymi funkcji publicznych, ani niezwiązanych z tymi funkcjami, powinny być one anonimizowane.
7. Administrator lub wyznaczona przez Administratora dokonuje przeglądu nagrań z posiedzeń sesji rady jednostki samorządu terytorialnego, pod kątem ewentualnych nieprawidłowości związanych z brakiem anonimizacji danych osobowych osób prywatnych przed udostępnieniem nagrania z sesji na stronie internetowej i/lub w BIP-ie.
8. Powyższa zasady mają również zastosowanie do nagrań z posiedzeń innych organów władzy publicznej pochodzących z powszechnych wyborów.

Art. 18. Zasady postępowania z dokumentami papierowymi zawierającymi dane osobowe

1. W stosunku do dokumentów papierowych stanowiących wydruki z systemu informatycznego Jednostki oraz wszelkie dokumenty zawierające dane osobowe, osoby upoważnione obowiązują następujące środki ostrożności:
   1) wydruki z systemu informatycznego i wszelkie dokumenty zawierające dane osobowe powinny być niedostępne dla osób nieuprawnionych,
   2) wydruki z systemu informatycznego i wszelkie dokumenty zawierające dane osobowe nie mogą być pozostawione w drukarce lub kserokopiarce ogólnodostępnej,
   3) wydruki niepotrzebne i nieprzydatne powinny być na bieżąco niszczone za pomocą niszczarki właściwej klasy,
   4) dokumenty zawierające dane osobowe, których nie można zniszczyć z przyczyn technicznych lub formalnych, powinny być składowane w miejscu z ograniczonym dostępem, systematycznie weryfikowane, a następnie archiwizowane zgodnie z obowiązującymi w tym zakresie przepisami.

Art. 19. Naruszenia ochrony danych osobowych

1. Administrator stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych.
2. Procedura zarządzania naruszeniami ochrony danych stanowi **załącznik nr 12** do niniejszej Polityki.

Rozdział III

Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych

Art. 20. Zasady zarządzania uprawnieniami Użytkowników w systemach

informatycznych

1. Obsługa informatyczna na wniosek pracownika ds. kadr tworzy konta dostępu do systemów informatycznych, przy czym uzupełniony wniosek następnie zatwierdzany jest przez Administratora, który nadaje uprawnienia Użytkownikom do pracy w systemach informatycznych – wzór wniosku o nadanie/zmianę/odebranie uprawnień stanowi **załącznik nr 13** do niniejszej Polityki.
2. Obsługa informatyczna dokonuje modyfikacji, zmiany lub wyrejestrowania uprawnień Użytkowników systemów informatycznych na podstawie wniosku, złożonego przez osobę, o której mowa w ust. 1, zatwierdzonego przez Administratora.
3. Pracownik ds. kadr do ewidencji osób upoważnionych do przetwarzania danych osobowych – **załącznik nr 8** – oraz do upoważnienia do przetwarzania danych - **załącznik nr 6** - wpisuje systemy informatyczne do jakich osoba upoważniona do przetwarzania danych otrzymała dostęp. W przypadku zmiany lub odebrania uprawnień informacja ta jest odnotowywana ww. ewidencji w kolumnie „Dostęp do systemów informatycznych z uprawnieniami".

Art. 21. Zasady zabezpieczenia dostępu do systemów informatycznych

1. W przypadku dostępu Użytkowników do systemów informatycznych (dziedzinowych i operacyjnych) należy stosować metodę uwierzytelnienia poprzez wpisanie indywidualnego identyfikatora/ login'u oraz hasła.
2. Hasło powinno składać się z unikalnego zestawu znaków, zawierających małe i wielkie litery, cyfry oraz znaki specjalne. Hasła powinny być regularnie zmieniane przez Użytkowników oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione osobie nieuprawnionej. Hasło powinno się składać z min 8 znaków i powinno być zmieniane co 30 dni.
3. Użytkownik zobowiązany jest do zachowania hasła w poufności i niezapisywania haseł w sposób jawny.
4. Hasła administracyjne do urządzeń i systemów informatycznych, w tym baz danych, winny być przechowywane w zapieczętowanej kopercie w miejscu wskazanym przez Administratora.

Art. 22. Zasady zarządzania sprzętem elektronicznym i oprogramowaniem

1. Użytkownik zobowiązany jest korzystać ze sprzętu elektronicznego w sposób zgodny z jego przeznaczeniem i chronić go przed jakimkolwiek zniszczeniem lub uszkodzeniem.
2. Użytkownik ma obowiązek niezwłocznie zgłosić utratę lub zniszczenie powierzonego sprzętu Administratorowi.
3. Użytkownik nie może bez zgody Administratora instalować dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączać niezatwierdzonych urządzeń do systemu informatycznego.
4. Użytkownik nie może bez zgody Administratora korzystać z prywatnego sprzętu elektronicznego (np. laptopów, telefonów, aparatów fotograficznych, nośników typu pendrive) do wykonywania zadań służbowych. Szczegółowe zasady wykorzystywania prywatnego sprzętu określa **załącznik nr 14** do niniejszej Polityki.
5. Administrator ma prawo do monitorowania sprzętu służbowego wykorzystywanego przez Użytkowników. O fakcie monitorowania Administrator zobowiązany jest powiadomić Użytkowników, zgodnie z przepisami Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t. j. Dz. U. z 2020 r., poz. 1320 ze zm.) nie później niż 2 tygodnie przed jego uruchomieniem.
6. Użytkownik zobowiązany jest do korzystania wyłącznie z oprogramowania dopuszczonego do stosowania w Jednostce.

Art. 23. Zasady wykonywania kopii bezpieczeństwa

1. W celu zwiększenia poziomu bezpieczeństwa oraz zapewnienia ciągłości działania Jednostki tworzy się kopie zapasowe danych;
2. Kopią zapasową objęte są: bazy danych. Kopia zapasowa wykonywana jest codziennie w sposób ręczny. Wykonywana jest na nośnik HDD i przechowywana w serwerowni.
3. Kopie nie powinny znajdować się w tym samym pomieszczeniu co dane źródłowe.
4. Za sporządzenie kopii zapasowych odpowiedzialna jest Obsługa informatyczna

Jednostki.

5. Użytkownicy we własnym zakresie odpowiadają za sporządzanie kopii zapasowych dokumentów znajdujących się na lokalnych dyskach twardych;
6. Obsługa informatyczna Jednostki zobowiązana jest do testowania kopii zapasowych, w tym celu należy:
   1) uruchomić środowisko testowe do testowania kopii zapasowej,
   2) rozpocząć proces symulacji przywracania kopii zapasowej,
   3) zweryfikować poprawność przywróconych danych,
   4) zakończyć sprawdzenie poprawności wykonanej kopii zapasowej
   5) usunąć dane ze środowiska testowego.

Art. 24. Zasady korzystania z poczty elektronicznej

1. Użytkownik jest zobowiązany do korzystania z przyznanego mu adresu mailowego wyłącznie w celu prowadzenia korespondencji służbowej.
2. Użytkownik nie może używać służbowego adresu mailowego do celów prywatnych, w szczególności do rejestracji na portalach społecznościowych, dokonywania zakupów w sklepach internetowych.
3. Użytkownik powinien zachować szczególną ostrożność przy wpisywaniu adresu odbiorcy wiadomości.
4. Użytkownik podczas wysyłania maili do wielu adresatów jednocześnie, powinien użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości".
5. Użytkownik powinien zastosować zabezpieczenia kryptograficzne przy przesyłaniu załączników do wiadomości. Zabezpieczenia kryptograficzne mogą polegać na przesłaniu zahasłowanych plików w formie załącznika, niemniej hasło powinno być przekazane adresatowi za pośrednictwem innego źródła tj. sms, bądź podczas rozmowy telefonicznej po uprzednim zweryfikowaniu tożsamości adresata.
6. Użytkownik powinien zachować szczególną ostrożność podczas odbierania poczty elektronicznej, a w szczególności nie powinien otwierać plików i linków w niej zawartych, ani otwierać załączników jeżeli nie ma pewności co do autentyczności

adresata wiadomości. Tego typu maile większości przypadków mogą zawierać załączniki ze szkodliwym kodem, które po „kliknięciu" infekują komputer Użytkownika oraz może istnieć realne ryzyko zaimplementowania kodu w pozostałych komputerach sieci wewnętrznej Jednostki.

7. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowaniem przez kryptowirusy. W takim przypadku Użytkownik powinien poinformować o zdarzeniu Administratora.
8. Użytkownik powinien regularnie przeglądać folder spam i usuwać niepotrzebne wiadomości pocztowe.

Art. 25. Zasady korzystania z Internetu

1. Użytkownik powinien korzystać z dostępu do sieci Internet wyłącznie w celach niezbędnych do wykonywania zadań służbowych.
2. Użytkownik nie powinien otwierać stron internetowych zawierających treści nie związane bezpośrednio z merytoryką pracy, ze względu na możliwość przypadkowego pobrania złośliwego kodu, który może automatycznie zainfekować system operacyjny komputera.
3. Użytkownik ponosi pełną odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
4. Użytkownik nie może korzystać ze stron internetowych, na których prezentowane są treści o charakterze przestępczym, hackerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu może być zaimplementowany złośliwy kod, który może automatycznie zainfekować system operacyjny komputera w sposób niewidoczny dla Użytkownika).
5. Użytkownik nie może pobierać aplikacji z sieci Internet bez wcześniejszej zgody Administratora.
6. Użytkownik w przypadku korzystania z szyfrowanego połączenia przez przeglądarkę internetową, powinien zwrócić uwagę na pojawienie się odpowiedniej ikony (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć"

na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

7. Użytkownik powinien zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet.
8. Jeżeli strona internetowa podmiotu zawiera formularz kontaktowy, to taka strona powinna posiadać zabezpieczenie certyfikatem SSL, celem zaszyfrowania komunikacji pomiędzy przeglądarką internauty, a stroną internetową jednostki.

Art. 26. Zasady korzystania z bankowości elektronicznej

1. Użytkownik, który wykonuje przelewy bankowe zobowiązany jest do regularnej zmiany hasła oraz nieprzechowywania go w formie pisemnej wraz z loginem.
2. Użytkownik zobowiązany jest do zapamiętania lub przechowywania hasła dostępu oraz innych danych służących do uwierzytelniania i autoryzacji w bezpiecznym miejscu.
3. Użytkownik nie może opuścić stanowiska pracy bez wylogowania się i zamknięcia przeglądarki internetowej.
4. Użytkownik logujący się do bankowości elektronicznej nie powinien korzystać z nieznanych sieci bezprzewodowych.
5. W celu zalogowania się do systemu bankowości elektronicznej Użytkownik nie powinien wchodzić na stronę internetową banku za pośrednictwem linków znajdujących się w korespondencji elektronicznej.
6. Obsługa informatyczna jest zobowiązana do wyposażenia komputerów służących do korzystania z bankowości elektronicznej w aktualne oprogramowanie oraz zabezpieczenia systemu na poziomie wysokim (m.in. oprogramowanie antywirusowe, włączony firewall) oraz do wykonywania okresowej kontroli zgodności ustawień sprzętu informatycznego z przekazanymi przez bank, który obsługuje bankowość elektroniczną - zasadami dotyczącymi bezpieczeństwa teleinformatycznego.
7. Użytkownicy, obsługujący bankowość elektroniczną są zobligowani do zapoznania się z zasadami bezpieczeństwa teleinformatycznego przekazanymi przez bank, który obsługuje bankowość elektroniczną.

Art. 27. Zarządzanie pojemnością przestrzeni dyskowej

1. W przypadku wdrażania nowej wersji oprogramowania przez Obsługę informatyczną Jednostki, konieczne jest uprzednie wykonanie niezbędnych kopii zapasowych zarówno użytkowanych systemów, jak i plików źródłowych poszczególnych Użytkowników – czyli wszystko co może być przydatne do zapewnienia poufności, integralności dostępności i rozliczalności.
2. Z każdej wdrożonej zmiany w wersji oprogramowania Obsługa informatyczna Jednostki jest zobowiązana sporządzić właściwą dokumentację, tzw. bazę konfiguracji – raport (w wersji papierowej lub elektronicznej) pozwalającej na ewentualne przywrócenie systemów i oprogramowania do wersji sprzed zmiany, w którym opisane są informacje na temat wykrytych np. nieprawidłowości, sugestii dot. procesu, uwagi (z np. raportów audytowych IT), które sugerują konieczność wdrożenia nowej wersji oprogramowania.
3. Co najmniej raz na kwartał Obsługa informatyczna wykonuje weryfikację sprzętu i oprogramowania i określa konieczność wprowadzania zmian w oprogramowaniu jeśli zaistnieje taka konieczność.

Art. 28. Zasady bezpiecznego przydzielania przestrzeni dyskowej

1. Podczas przydzielania przestrzeni dyskowej należy w sposób racjonalny przydzielać zasoby, zachowując próg ostrzegawczy na poziomie 80% zajętości przestrzeni.
2. Obsługa informatyczna powinna wdrożyć mechanizmy umożliwiające w sposób racjonalny zarządzanie wyżej wymienioną przestrzenią dyskową dla każdego Użytkownika.
3. Raz na pół roku Obsługa informatyczna wykonuje analizę zajętości dysku. Do tego celu Obsługa informatyczna wykorzystuje wbudowane narzędzia konsoli zarządzania dyskami dostępnymi w systemach operacyjnych lub używa dedykowanego oprogramowania służącego do skanowania zajętości przestrzeni dyskowej.
4. W celu czyszczenia dysku ze zbędnych plików (pozostałości po działających lub odinstalowanych aplikacjach) oraz czyszczenia rejestru systemowego należy

na przykład zainstalować dedykowane do tego celu oprogramowanie, które po dokonaniu odpowiednich założeń systemowych dotyczących rozmiaru zbędnych plików umożliwi wyżej wymienione działania naprawcze.

Art. 29. Komunikacja i czynności serwisowe na odległość

1. Komunikacja z zewnątrz powinna być realizowana tylko poprzez mechanizmy szyfrujące zapewniające odpowiednie bezpieczeństwo (np. VPN, Team Viewer). W przypadku podmiotów zewnętrznych dokonujących czynności serwisowych (np. aktualizacja oprogramowania dziedzinowego) dostęp taki jest nadzorowany przez Obsługę informatyczną oraz każdorazowo powinien być poprzedzony autoryzacją (np. podaniem hasła do Team Viewer, które wygasa po skończonej sesji).
2. Komunikację należy prowadzić tylko za pomocą bezpiecznych metod transmisji, w tym włączenie transmisji szyfrowanej lub przeniesienie usług sieciowych na serwer posiadający taką możliwość.

Art. 30. Zasady pracy z urządzeniami mobilnymi

1. Administrator dopuszcza możliwość pracy z urządzeń mobilnych wyłącznie z urządzeń przeznaczonych do użytku służbowego.
2. Urządzenia mobilne służące do łączenia się systemami i sieciami zarządzanymi przez Administratora muszą być zgłoszone do Obsługi informatycznej, celem zabezpieczenia ich odpowiednimi środkami uwierzytelniania.
3. Administrator zabrania wykorzystywania służbowych urządzeń mobilnych do celów prywatnych oraz udostępniania ich osobom trzecim, jak również instalowania aplikacji, które nie są niezbędne do wykonywania obowiązków danego pracownika.
4. Administrator zabrania korzystania z publicznych sieci WIFI chyba że połączenie jest dodatkowo zabezpieczone kanałem VPN, oraz pozostawiania urządzenia bez nadzoru pracownika, w szczególności w miejscach ogólnodostępnych dla szerokiego grona osób trzecich,
5. Użytkownik nie może pozostawiać urządzenia bez opieki i nie może pożyczać osobie trzeciej.

6. Z siecią służbową Użytkownik może łączyć się tylko za pośrednictwem urządzeń zaakceptowanych przez Administratora.
7. Użytkownik powinien używać tylko rozwiązań posiadające silne mechanizmy szyfrowania transmisji i ochrony danych.
8. Obsługa informatyczna prowadzi ewidencję udostępnionych urządzeń mobilnych.

Art. 31. Zasady zabezpieczania sprzętu elektronicznego i systemu informatycznego

1. Komputery stacjonarne i przenośne powinny być zabezpieczone oprogramowaniem antywirusowym, który sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu.
2. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie powinno odbywać się przy wykorzystaniu ww. oprogramowania zainstalowanego na stacjach roboczych oraz komputerach przenośnych.
3. Obowiązkiem Obsługi informatycznej jest nadzór nad aktualizacją oprogramowania antywirusowego.
4. Użytkownik jest obowiązany każdorazowo zawiadomić Obsługę informatyczną o pojawiających się komunikatach, wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem – wirusa lub w przypadku sygnalizowanych problemów z działaniem oprogramowania antywirusowego.
5. Użytkownik, który posiada dostęp do systemów informatycznych powinien mieć zablokowaną możliwość instalowania nieautoryzowanego oprogramowania.

Art. 32. Zasady korzystania z elektronicznych nośników danych

1. Użytkownik może korzystać wyłącznie z szyfrowanych, elektronicznych nośników danych w szczególności pendriv-y, dysków zewnętrznych, nośników optycznych przeznaczonych do użytku służbowego.
2. Użytkownik korzystający z elektronicznych nośników danych w całym okresie użytkowania odpowiedzialny jest za bezpieczeństwo danych.
3. Użytkownik korzystający z ww. urządzeń zobowiązany jest do:
   1) przechowywania danych na dysku szyfrowanym,

2) transportu nośnika w sposób minimalizujący ryzyko kradzieży lub zniszczenia oraz stosownego zabezpieczenia nośnika przed uszkodzeniem,
3) zdecydowanego i skutecznego uniemożliwienia skorzystania z nośnika osobom nieuprawnionym (np. rodzina, dzieci, znajomi).

4. Obsługa informatyczna jest odpowiedzialna za prowadzenie inwentaryzacji sprzętu elektronicznego oraz utrzymywanie jej w aktualności.

Art. 33. Zasady wykonywania przeglądów i konserwacji sprzętu elektronicznego i nośników danych

1. Obsługa informatyczna dokonuje przeglądu i konserwacji sprzętu elektronicznego i nośników danych.
2. Użytkownik nie może samodzielne dokonywać napraw sprzętu elektronicznego, wymiany jego podzespołów oraz wykonywać innych czynności nie związanych bezpośrednio z jego eksploatacją lub nie dopuszczonych do wykonywania przez producenta sprzętu w instrukcji obsługi.
3. W przypadku serwisowania infrastruktury teleinformatycznej przez podmioty zewnętrzne, Obsługa informatyczna wymontowuje dyski twarde przed oddaniem ich do serwisu. W sytuacji, gdy do serwisu należy oddać cały zasób z dyskiem twardym, Administrator winien trwale usunąć wszystkie dane z dysku za pomocą certyfikowanych urządzeń. Jeżeli Administrator nie ma możliwości wymontowania dysku z urządzenia lub trwałego usunięcia danych, Administrator winien podpisać stosowną umowę powierzenia danych z firmą serwisową.
4. Użytkownik ma obowiązek niezwłocznie powiadomić Obsługę informatyczną o wszelkich nieprawidłowościach i awariach sprzętu informatycznego, mogących prowadzić do próby naruszenia lub naruszenia bezpieczeństwa danych osobowych.
5. W przypadku awarii systemu informatycznego i utraty informacji lub w przypadku zaistnienia możliwości uszkodzenia informacji Obsługa informatyczna jest zobowiązana do:
   1) przetestowania sieci informatycznej, systemu informatycznego oraz aplikacji służącej do przetwarzania danych,

2) ocenić zasadność odtworzenia danych przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych, a w przypadku uzasadnionej konieczności odtworzyć dane przy wykorzystaniu aktualnej kopii zapasowej lub kilku kopii zapasowych.

Art. 34. Zasada utylizacji i serwisu sprzętu elektronicznego

1. W przypadku wycofania sprzętu elektronicznego z użycia, dane osobowe na nim zapisane powinny być kasowane przy użyciu dedykowanego oprogramowania do bezpiecznego usuwania danych, najlepiej za pomocą certyfikowanego urządzenia np.: demagnetyzera.
2. W przypadku braku możliwości programowego usunięcia danych ze sprzętu elektronicznego podlega on fizycznemu zniszczeniu.
3. Zniszczenie sprzętu elektronicznego powinno być potwierdzane protokołem zniszczenia.

Rozdział IV

Inne środki organizacyjne i techniczne służące do zabezpieczania danych osobowych

Art. 35. Zasady bezpiecznej pracy

1. Każda osoba działająca z upoważnienia administratora i mająca dostęp do danych, zobowiązana jest do stosowania następujących zasad bezpieczeństwa:
   1) **polityki „czystego biurka"** - w trakcie pracy na biurku powinny znajdować się tylko te materiały, które są niezbędne do wykonywania obowiązków służbowych. W przypadku opuszczenia stanowiska pracy przez osobę upoważnioną, materiały zawierające dane, wymagające szczególnej ochrony powinny być zabezpieczone przed dostępem osób nieuprawnionych. Po zakończeniu dnia pracy każda osoba zobowiązana jest do zabezpieczenia wszelkich dokumentów i nośników zawierających istotne dane, w celu uniemożliwienia dostępu do nich osobom nieuprawnionym,
   2) **polityki „czystego ekranu"** - w przypadku chwilowego opuszczenia stanowiska pracy każda osoba zobowiązana jest do wylogowania się z systemu, bądź

zablokowania dostępu do pulpitu stacji roboczej w celu uniemożliwienia dostępu do systemu operacyjnego lub aplikacji osobom nieuprawnionym. Ponadto w trakcie pracy należy mieć otwarte tylko te aplikacje, które są niezbędne do wykonywania obowiązków służbowych,

3) takiego ustawienia monitora, aby osoby niepowołane nie mogły zapoznać się z informacjami wyświetlanymi na monitorze. W przeciwnym wypadku należy wyposażyć monitor w odpowiedni filtr prywatyzujący,
4) bieżącego niszczenia w niszczarce niepotrzebnej dokumentacji papierowej oraz przechowywania pozostałej dokumentacji papierowej w zabezpieczonych szafach, zamykanych przynajmniej na klucz,
5) niepozostawiania osób postronnych w pomieszczeniu, w którym przetwarzane są danę osobowe, bez obecności osoby upoważnionej,
6) zachowania w poufności wszelkich informacji, w tym danych osobowych poprzez złożenie stosownego oświadczenia,
7) niepozostawiania klucza w drzwiach biurowych po zewnętrznej stronie pomieszczenia,
8) niepozostawiania pomieszczeń biurowych bez opieki.

Art. 36. Zarządzanie ryzykiem

1. Administrator analizuje możliwe sytuacje i naruszenia ochrony danych osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania, ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zwane dalej „analizami ryzyka".
2. Administrator przeprowadza analizy ryzyka naruszenia praw lub wolności osób fizycznych dla czynności przetwarzania danych lub ich kategorii,
3. Analiza ryzyka powinna zapewniać:
   1) zidentyfikowanie ryzyka,
   2) oszacowanie ryzyka z punktu widzenia następstw dla działalności Jednostki oraz prawdopodobieństwa wystąpienia takiego ryzyka,

3) informowanie o następstwach wystąpienia ryzyka,
4) ustanowienie priorytetów w postępowaniu z ryzykiem,
5) regularne monitorowanie i przegląd różnych typów ryzyka oraz procesu zarządzania ryzykiem,
6) zbieranie informacji w celu doskonalenia podejścia do zarządzania ryzykiem.

4. Administrator dokumentuje wykonaną analizę ryzyka w postaci raportu.
5. Administrator dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w przypadkach, w których zgodnie z analizą ryzyka, ryzyko naruszenia praw i wolności osób jest wysokie oraz w każdym przypadku, gdy wymagają tego obowiązujące przepisy prawa i wytyczne Prezesa Urzędu Ochrony Danych Osobowych.

Art. 37. Audyt wewnętrzny w zakresie bezpieczeństwa informacji

1. Administrator zapewnia przeprowadzenie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji nie rzadziej niż raz na rok lub częściej zgodnie z powszechnie obowiązującymi w tym zakresie przepisami.
2. Z przeprowadzonego audytu powinien zostać sporządzony raport.

Art. 38. Zarządzanie kluczami

1. Wszystkie pomieszczenia biurowe w Jednostce co do zasady stanowią obszar przetwarzania danych osobowych.
2. Dodatkowo Administrator określił szczególne obszary przetwarzania danych objęte dodatkowymi zabezpieczeniami, do których dostęp mają tylko osoby upoważnione przez Administratora.
3. Opis środków technicznych służących do zabezpieczenia danych osobowych oraz wskazanie obszaru przetwarzania zawiera **załącznik nr 15** do niniejszej Polityki.
4. Administrator wyznaczył osoby, które są upoważnione do otwierania drzwi wejściowych do budynków Jednostki przed rozpoczęciem pracy Jednostki. Osoby, którym Administrator powierzył klucze zobowiązane są do nieudostępniania tych

kluczy osobom trzecim.

5. Klucze do poszczególnych pomieszczeń obszaru przetwarzania danych posiadają, na podstawie upoważnień do zarządzania kluczami do pomieszczeń biurowych, pracownicy, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie. Od momentu pobrania kluczy do momentu ich zdania na tych osobach spoczywa pełna odpowiedzialność za ich zabezpieczenie. Po otwarciu pomieszczeń biurowych, przed przystąpieniem do pracy, należy sprawdzić stan zastosowanych zabezpieczeń.
6. Fakt poboru klucza do pomieszczeń szczególnych należy odnotować w rejestrze poboru kluczy stanowiącym **załącznik nr 16** do niniejszej Polityki.
7. Zapasowe klucze do wszystkich pomieszczeń Jednostki winny zostać odpowiednio zabezpieczone i przechowywane są zamykanej skrzynce. Każdorazowe użycie klucza zapasowego powinno być zgłoszone do osoby upoważnionej przez Administratora.
8. Zabrania się pozostawiania kluczy do pomieszczeń z obszaru przetwarzania danych w drzwiach lub w miejscach ogólnie dostępnych, pomieszczenia te powinny być zamknięte na klucz na czas nieobecności osób upoważnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.
9. Zabrania się dorabiania kluczy bez zgody Administratora.
10. Zabrania się pozostawiania osób trzecich w pomieszczeniach biurowych Jednostki bez nadzoru osób upoważnionych przez Administratora.
11. Osoby upoważnione do przetwarzania danych osobowych mogą przebywać po godzinach pracy Jednostki na obszarze przetwarzania danych osobowych jedynie za zgodą Administratora.
12. W przypadkach przebywania osób upoważnionych w pomieszczeniach obszaru przetwarzania danych po wyznaczonych godzinach pracy, godzinach pełnienia obowiązków, wykonywania zadań na rzecz Administratora należy upewnić się czy zamknięto drzwi wejściowe do obszaru przetwarzania danych osobowych. Dodatkowo opuszczając obszar przetwarzania danych należy sprawdzić czy zamknięto wszystkie okna oraz drzwi wejściowe do pomieszczeń.

Art. 39. Ochrona danych osobowych w fazie projektowania i domyślna ochrona danych

1. Obowiązek uwzględnienia ochrony danych w fazie projektowania spoczywa na Administratorze. Administrator zobligowany jest do szczegółowej analizy i opisu planowanego procesu przetwarzania danych. Ponadto w przypadku, gdy do przetwarzania wykorzystywane będą narzędzia dostarczane Administratorowi przez zewnętrznych dostawców wymagane jest zaangażowanie tych podmiotów. W przypadku dostawcy będącego podmiotem przetwarzającym uwzględnienia ochrony danych w fazie projektowania oparte jest na zasadach wynikających z art. 28 RODO.
2. Kluczowym wymogiem związanym z ochroną danych osobowych w fazie projektowania i domyślną ochrony danych jest niedopuszczenie do przetwarzania danych w sposób, który naruszałby poszczególne wymogi RODO poprzez:
   a) zebranie informacji o celach danego projektu oraz planowanych środkach realizacji tych celów,
   b) określenie adekwatnych - dla danego projektu – środków technicznych i organizacyjnych służących do ochrony danych osobowych,
   c) ocenę czy z projektem łączą się ryzyka dla praw lub wolności i przyjęcia określonego mechanizmu postępowania z tym ryzykiem (ocena ryzyka może doprowadzić do konieczności przeprowadzenia pełnej oceny skutków a nawet uprzednich konsultacji z Prezesem Urzędu Ochrony Danych Osobowych),
   d) przypisanie ról w organizacji w zakresie dokonywania w/w ocen,
   e) przeszkolenie pracowników przed rozpoczęciem przetwarzania nowego projektu.
   f) planowanych terminów retencji danych
   g) szczegółowej podstawy prawnej podjęcia działań w danym procesie
   h) potencjalnych zagrożeń wewnętrznych i zewnętrznych
   i) potencjalnych odbiorców danych
3. Wymóg ochrony danych osobowych w fazie projektowania wymaga nie tylko oceny danego procesu przetwarzania danych przed jego rozpoczęciem, ale także monitorowania zgodności w czasie przetwarzania. Z punktu widzenia mechanizmu oceny nowych projektów i zarządzania projektami wprowadzono Rejestr czynności przetwarzania danych, który powinien podlegać bieżącym aktualizacjom.
4. Administrator zobowiązany jest do uwzględnienia procesu w stosownych

upoważnieniach dla osób obsługujących proces.

5. Administrator zobowiązany jest przedstawienia Inspektorowi Ochrony Danych w/w informacji w celu przeprowadzenia analizy ryzyka obejmującej nowy proces.

Rozdziała V

Postanowienia końcowe

Art. 40 Przetwarzanie danych osobowych w celu prowadzenia postępowań rekrutacyjnych

1. Jednostka przetwarza dane osobowe kandydatów w związku z prowadzonym postępowaniem rekrutacyjnym. Dane osobowe przetwarzane są w zakresie wynikającym z przepisów prawa. Jednostka nie pozyskuje zgód na przetwarzanie danych osobowych od kandydatów. Na podstawie art. 13 ust. 1 i 2 RODO, Jednostka realizuje w stosunku do kandydatów obowiązek informacyjny.
2. Klauzula informacyjna może stanowić integralną część wniosku rekrutacyjnego, z zastrzeżeniem sytuacji, w której wzór wniosku został określony przez organ prowadzący. Każdorazowa zmiana treści klauzuli informacyjnej zawierającej informacje, o których mowa w art. 13 ust. 1 i 2 RODO, wymaga przeprowadzenia uprzednich konsultacji z IOD.
3. Jednostka, jako Administrator wdraża odpowiednie środki techniczne i organizacyjne mające na celu zapewnienie bezpieczeństwa danych osobowych kandydatów.
4. W związku z prowadzonym postępowaniem rekrutacyjnym, Jednostka może korzystać z usług podmiotu zewnętrznego (m. in. w zakresie dostawy i obsługi systemu rekrutacyjnego) po uprzednim uregulowaniu kwestii powierzenia przetwarzania danych osobowych w formie umowy lub innego instrumentu prawnego, o czym stanowi art. 28 RODO – jeżeli podmiotowi zewnętrznemu będą ujawniane dane osobowe. Projekt ww. umowy lub innego instrumentu prawnego powinien być przekazany do zaopiniowania przez IOD. Jednostka informuje IOD o wszelkich zmianach w/w umowy lub innego instrumentu prawnego zaproponowanych przez podmiot przetwarzający dane na zlecenie, bądź zainicjowanych przez samą Jednostkę. W ramach

struktury organizacyjnej Jednostki, dane osobowe są ujawniane osobom działającym z upoważnienia Administratora.

5. Jednostka jest zobowiązana podać do publicznej wiadomości listę kandydatów zakwalifikowanych i niezakwalifikowanych. Lista podawana jest do publicznej wiadomości poprzez umieszczenie w widocznym miejscu w siedzibie jednostki. Przepisy prawa mogą dodatkowo nakładać na Jednostkę obowiązek przekazania do publicznej wiadomości ww. listy w inny sposób, aniżeli wymieniony powyżej. Jednostka wdraża odpowiednie środki techniczne i organizacyjne mające na celu uniemożliwienie dostępu osobom nieuprawnionym do treści wniosków rekrutacyjnych złożonych przez kandydatów.

Art. 41 Przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowych

1. Osoba lub odpowiednia jednostka wydziałowa Administratora odpowiedzialna za dobór narzędzi służących do przetwarzania danych osobowych, w ramach korzystania z których to dane osobowe będą przekazywane do państwa trzeciego lub organizacji międzynarodowej (tj. poza Europejski Obszar Gospodarczy), bądź osoba/jednostka podejmująca decyzję w zakresie doboru ww. narzędzi, zobowiązana jest poinformować o tym fakcie inspektora ochrony danych (tj. o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej).
2. W sytuacji, gdy dobór narzędzi do przetwarzania danych osobowych nastąpi w drodze wyłonienia najkorzystniejszej oferty w ramach postępowania o udzielenie zamówienia publicznego, inspektor ochrony danych jest zawiadamiany o zamiarze przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej przez Sekretarza Urzędu. Zawiadomienie inspektora ochrony danych o zamiarze przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej powinno zawierać m. in. informację o nazwie państwa trzeciego lub organizacji międzynarodowej, a także informację o celu przekazania danych osobowych; kategorii osób, których dane dotyczą oraz ich rodzaju. Zawiadomienie przekazywane jest na adres poczty elektronicznej inspektora ochrony danych. Informacje zawarte

w zawiadomieniu są niezbędne do ustalenia przez inspektora ochrony danych właściwej podstawy przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.

3. Na podstawie ww. informacji, inspektor ochrony danych dokonuje aktualizacji rejestru czynności przetwarzania danych osobowych oraz właściwych klauzul informacyjnych, o ile przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej jest dopuszczalne w świetle rozdziału V RODO. W przypadku braku podstaw do przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, inspektor ochrony danych informuje administratora o braku przesłanki legalizującej transfer danych osobowych".

Art. 42. Informacje dotyczące Polityki ochrony danych osobowych

1. Każda osoba mająca dostęp do danych osobowych Jednostki zobowiązana jest zapoznać się z niniejszą Polityką oraz potwierdzić ten fakt własnoręcznym podpisem na wykazie, którego wzór stanowi **załącznik nr 17** do niniejszej Polityki.
2. Niniejsza Polityka winna podlegać przeglądom we współpracy z Inspektorem Ochrony Danych i aktualizacji w przypadku zmian w otoczeniu organizacyjno-prawnym Administratora.
3. Dokument niniejszej Polityki obowiązuje w wersji elektronicznej i znajduje się w ogólnodostępnym folderze sieciowym dostępnym z poziomu komputerów służbowych Użytkowników Administratora.
4. Aktualizacja Polityki odbywać się będzie centralnie tj. w celu uniknięcia pomyłki co do obowiązującej w danym momencie wersji Polityki, Administrator umieszcza w ogólnodostępnym folderze sieciowym obowiązującą wersję dokumentu, usuwając przy tym wersję poprzednią.
5. Mając na względzie treść ust. 4, w ogólnodostępnym folderze sieciowym znajdować się może zawsze tylko jedna wersja dokumentu Polityki.
6. Przekazanie informacji o zmianach powinno zostać dokonane poprzez zobowiązanie Użytkowników do zapoznania się w określonym czasie z treścią zaktualizowanej

Polityki i podpisaniu przez nich ponownie wykazu osób zapoznanych z Polityką – **załącznik nr 17**.

7. Dokument aktualnej Polityki przechowywany jest również w wersji tradycyjnej (papierowej) i dostępny jest u pracownika ds. zarządzania kryzysowego. Administrator udostępnia niniejszą Politykę każdemu Użytkownikowi na żądanie.

Art. 42. Wykaz załączników

1) Załącznik nr 1 – Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych,
2) Załącznik nr 2 – Wzór oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych,
3) Załącznik nr 3 – Wzór ogólnej klauzuli informacyjnej z art. 13 ust. 1 i 2,
4) Załącznik nr 4 – Wzór ogólnej klauzuli informacyjnej z art. 14 ust. 1 i 2,
5) Załącznik nr 5 – Procedura realizacji praw osób których dane dotyczą,
6) Załącznik nr 6 – Wzór upoważnienia do przetwarzania danych osobowych,
7) Załącznik nr 7 – Wzór oświadczenia o zachowaniu w tajemnicy danych osobowych,
8) Załącznik nr 8 – Ewidencja osób upoważnionych do przetwarzania danych osobowych,
9) Załącznik nr 9 – Informator dla Użytkowników z zakresu ochrony danych osobowych,
10) Załącznik nr 10 – Wzór umowy powierzenia przetwarzania danych osobowych,
11) Załącznik nr 11 – Wzór rejestru zawartych umów powierzenia przetwarzania danych osobowych,
12) Załącznik nr 12 – Procedura zarządzania naruszeniami ochrony danych osobowych
13) Załącznik nr 13 – Wzór wniosku o nadanie/zmianę/odebranie uprawnień w systemach informatycznych,
14) Załącznik nr 14 – Zasady wykorzystywania sprzętu prywatnego,
15) Załącznik nr 15 – Wzór opisu środków technicznych stosowanych do zabezpieczania danych osobowych i wykaz obszaru przetwarzania,
16) Załącznik nr 16 – Wzór rejestru poboru kluczy,
17) Załącznik nr 17 – Wykaz osób zapoznanych z Polityką ochrony danych osobowych.

Zał. nr 1 do Polityki	**Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych**

_____, _____

(miejscowość) (data)

Wyrażam zgodę na przetwarzanie moich danych osobowych w rodzaju: .....

w celach ..... zgodnie z art. 6 ust. 1 lit a)* lub art. 9 ust. 2 lit. a)* Rozporządzeniem 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 (publ. Dz. Urz. UE L Nr 119, s. 1).

Niniejsza zgoda jest dobrowolna i może być cofnięta w dowolnym momencie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

_____

(czytelny podpis, data)

*niepotrzebne skreślić

Zał. nr 1 do Polityki	**Wzór oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych**

OBOWIĄZKE INFORMACYJNY

1) Administratorem Państwa danych jest..... (adres: ....., adres e-mail: ....., numer telefonu: .....).
2) Administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych za pośrednictwem adresu email: ..... lub pisemnie pod adresem Administratora.
3) Państwa dane osobowe będą przetwarzane w w/w celu.
4) Państwa dane osobowe będą przetwarzane do czasu cofnięcia zgody na przetwarzanie danych osobowych.
5) Podstawą prawną przetwarzania danych jest art. 6 ust. 1 lit. a) ww. Rozporządzenia.
6) Państwa dane osobowe będą przetwarzane w sposób zautomatyzowany, lecz nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym o profilowaniu.
7) Państwa dane osobowych nie będą przekazywane poza Europejski Obszar Gospodarczy (obejmujący Unię Europejską, Norwegię, Liechtenstein i Islandię).
8) W związku z przetwarzaniem Państwa danych osobowych, przysługują Państwu następujące prawa:
   a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
   b) prawo do sprostowania (poprawiania) swoich danych osobowych;
   c) prawo do ograniczenia przetwarzania danych osobowych;
   d) prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   e) prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa), w sytuacji, gdy uzna Pani/Pan, że przetwarzanie danych osobowych narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO);
9) Podanie przez Państwa danych osobowych jest dobrowolne. Nieprzekazanie danych skutkować będzie brakiem realizacji celu, o którym mowa w pkt 3.
10) Państwa dane mogą zostać przekazane podmiotom zewnętrznym na podstawie umowy powierzenia przetwarzania danych osobowych, a także podmiotom lub organom uprawnionym na podstawie przepisów prawa.

Zał. nr 2 do Polityki	**Wzór oświadczenia o wycofaniu zgody na przetwarzanie danych osobowych**

_____, _____

(miejscowość) (data)

Oświadczenie

o wycofaniu zgody na przetwarzanie danych osobowych

Na mocy przysługującego mi uprawnienia, wynikającego z art. 7 ust. 3 zd. 1. 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; tzw. „RODO"), niniejszym wycofuję wyrażoną przeze mnie zgodę na przetwarzanie danych osobowych _____, w celach: _____, przetwarzanych przez: _____.

_____

(czytelny podpis, data)

Zał. nr 3 do Polityki	**Wzór ogólnej klauzuli informacyjnej z art. 13 ust. 1 i 2**

Klauzula informacyjna

Na podstawie art. 13 ust. 1 i 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.U.UE.L. z 2016r. Nr 119, s.1 ze zm.) - dalej: „RODO" informuję, że:

1) Administratorem Państwa danych jest .....
2) Administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych za pośrednictwem adresu email: ..... lub pisemnie pod adres Administratora.
3) Państwa dane osobowe będą przetwarzane w celu ....., tj. gdyż jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze (art. 6 ust. 1 lit. c RODO) w zw. z Ustawą z dnia ..... W przypadku dobrowolnego udostępniania przez Państwa danych osobowych innych niż wynikające z obowiązku prawnego, podstawę legalizującą ich przetwarzanie stanowi wyrażona zgoda na przetwarzanie swoich danych osobowych (art. 6 ust. 1 lit. a RODO). Udostępnione dobrowolnie dane będą przetwarzane w celu .....
4) Państwa dane osobowe będą przetwarzane przez okres niezbędny do realizacji ww. celu z uwzględnieniem okresów przechowywania określonych w przepisach szczególnych, w tym przepisów archiwalnych tj. ..... lat. Natomiast z przypadku danych podanych dobrowolnie – co do zasady do czasu wycofania przez Państwa zgody na ich przetwarzanie.
5) Państwa dane osobowe będą przetwarzane w sposób zautomatyzowany, lecz nie będą podlegały zautomatyzowanemu podejmowaniu decyzji, w tym o profilowaniu.
6) Państwa dane osobowych nie będą przekazywane poza Europejski Obszar Gospodarczy (obejmujący Unię Europejską, Norwegię, Liechtenstein i Islandię).
7) W związku z przetwarzaniem Państwa danych osobowych, przysługują Państwu następujące prawa:
   a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
   b) prawo do sprostowania (poprawiania) swoich danych osobowych;
   c) prawo do ograniczenia przetwarzania danych osobowych;
   d) w przypadku gdy przetwarzanie odbywa się na podstawie wyrażonej zgody (art. 6 ust. 1 lit. a RODO) - prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
   e) prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa), w sytuacji, gdy uzna Pani/Pan, że przetwarzanie danych osobowych narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO);
8) Podanie przez Państwa danych osobowych w związku z ciążącym na Administratorze obowiązkiem prawnym jest obowiązkowe, a ich nieprzekazanie skutkować będzie

brakiem realizacji celu, o którym mowa w punkcie 3. Nieprzekazanie danych udostępnianych dobrowolnie pozostaje bez wpływu na rozpoznanie sprawy.

9) Państwa dane mogą zostać przekazane podmiotom zewnętrznym na podstawie umowy powierzenia przetwarzania danych osobowych, a także podmiotom lub organom uprawnionym na podstawie przepisów prawa.

Zał. nr 4 do Polityki	**Wzór ogólnej klauzuli informacyjnej z art. 14 ust. 1 i 2**

Klauzula informacyjna

Na podstawie art. 14 ust. 1 i 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.U.UE.L. z 2016r. Nr 119, s.1 ze zm.) - dalej: „RODO" informuję, że:

1) Administratorem Państwa danych jest .....
2) Administrator wyznaczył Inspektora Ochrony Danych, z którym mogą się Państwo kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych za pośrednictwem adresu email: ..... lub pisemnie pod adres Administratora.
3) Państwa dane osobowe będą przetwarzane w celu ....., tj. gdyż jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze (art. 6 ust. 1 lit. c RODO) w zw. z Ustawą z dnia .....
4) Administrator przetwarza Państwa dane osobowe t.j. .....
5) Państwa dane osobowe będą przetwarzane przez okres niezbędny do realizacji ww. celu z uwzględnieniem okresów przechowywania określonych w przepisach szczególnych, w tym przepisów archiwalnych tj. ..... lat.
6) Państwa dane nie będą przetwarzane w sposób zautomatyzowany, w tym nie będą podlegać profilowaniu.
7) Państwa dane osobowych nie będą przekazywane poza Europejski Obszar Gospodarczy (obejmujący Unię Europejską, Norwegię, Liechtenstein i Islandię).
8) W związku z przetwarzaniem Państwa danych osobowych, przysługują Państwu następujące prawa:
   a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
   b) prawo do sprostowania (poprawiania) swoich danych osobowych;
   c) prawo do ograniczenia przetwarzania danych osobowych;
   d) prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych (ul. Stawki 2, 00-193 Warszawa), w sytuacji, gdy uzna Pani/Pan, że przetwarzanie danych osobowych narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych (RODO);
9) Państwa danych osobowe zostały pozyskane od .....
10) Państwa dane mogą zostać przekazane podmiotom zewnętrznym na podstawie umowy powierzenia przetwarzania danych osobowych, a także podmiotom lub organom uprawnionym na podstawie przepisów prawa.

Zał. nr 5 do Polityki	**Procedura realizacji praw osób, których dane dotyczą**

Art 1 Cel procedury

Celem procedury jest wdrożenie ogólnych zasad postępowania w przypadku realizacji praw osób, których dane dotyczą na mocy 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) (Dz. Urz. UE L 119, s. 1) - zwane dalej RODO.

Art 2 Postanowienia ogólne

1. Pracownik ds. zarządzania kryzysowego koordynuje przyjmowanie i rozpatrywanie wniosków obywateli w zakresie praw związanych z ochroną danych osobowych wpływających do Administratora.
2. Korespondencję przesłaną na adresy poczty elektronicznej inspektor@cbi24.pl Inspektor Ochrony Danych przekazuje do pracownika ds. zarządzania kryzysowego.
3. W przypadku korespondencji, o której mowa w ust. 1 i 2, wyżej wskazany pracownik weryfikuje kompletność danych adresowych oraz informacji umożliwiających zidentyfikowanie komórki merytorycznej odpowiadającej za przetwarzanie tych danych.
4. W przypadku braku wystarczających informacji umożliwiających zidentyfikowanie osoby kierującej wniosek, pracownik o którym mowa powyżej występuje do osoby fizycznej o uszczegółowienie informacji.
5. Pracownik ds. zarządzania kryzysowego przekazuje korespondencję do właściwej komórki, która jest zobowiązana do zrealizowania wniosku.
6. Realizacja praw osób, których dane dotyczą powinna następować niezwłocznie. Termin ten nie może być dłuższy, niż miesiąc od dnia otrzymania wniosku.
7. W razie potrzeby termin ten może zostać przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W takim przypadku Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia na piśmie bądź elektronicznie, chyba że osoba, której dane dotyczą zażąda tej informacji w innej formie.
8. Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie, przy czym nie później niż w terminie miesiąca od otrzymania żądania, ma obowiązek poinformowania osoby, której dane dotyczą o powodach

niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Art 3 Prawo dostępu do danych

1. Osoba, której dane są przetwarzane przez Administratora, posiada uprawnienie do uzyskania informacji w każdym czasie potwierdzenia czy Administrator przetwarza jej dane osobowe.
2. W przypadku przetwarzania danych przez Administratora, osoba fizyczna ma prawo do uzyskania do nich dostępu oraz do uzyskania informacji o:
   1) celu przetwarzania danych,
   2) kategorii odnośnych danych osobowych,
   3) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych,
   4) planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe – podanie kryteriów ustalania tego okresu.
   5) prawie do żądania od Administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczących osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
   6) prawie do wniesienia skargi do organu nadzorczego,
   7) źródle danych, jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą.
3. W każdym przypadku przed udzieleniem informacji zawierających dane osobowe na wniosek, osoba obsługująca zobowiązana jest zweryfikować czy wnioskodawca jest upoważniony do takiego udostępnienia na podstawie przepisów prawa lub stosownego pełnomocnictwa udzielonego przez osobę, której dane dotyczą.
4. Weryfikacja winna nastąpić co do zasady na podstawie okazanego dokumentu tożsamości ze zdjęciem (dowód osobisty, prawo jazdy, paszport itp.), a tylko wyjątkowo na podstawie innych dostępnych informacji o wnioskodawcy takich jak np.: imię, nazwisko, adres, numer telefonu, adres e-mail, imię matki lub ojca, numer PESEL lub inne informacje zamieszczone w dokumentach zgromadzonych przez Administratora.
5. Jeżeli osoba fizyczna, której dane dotyczą, zwróci się z wnioskiem o dostarczenie kopii jej danych osobowych podlegających przetwarzaniu, żądanie takie jest realizowane

bezpłatnie po jednoznacznej weryfikacji tożsamości osoby wnioskującego.

6. Za wszelkie kolejne kopie, o które zwróci się wnioskodawca, można pobrać opłatę. Opłata powinna obejmować jedynie faktyczne koszty sporządzenia kopii, tj. koszt papieru, koszty kserowania.
7. Jeżeli wnioskodawca, którego dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się drogą elektroniczną po jednoznacznej weryfikacji tożsamości osoby, np. podaniu daty urodzenia, podaniu innej informacji, która była podana we wcześniejszej korespondencji, a co do której można mieć pewność, że będzie ją posiadać jedynie osoba, której dane dotyczą.
8. Kopię danych, o której mowa w ust. 3, wydaje się w postaci wydruku danych po ich przepisaniu lub skopiowaniu do ustrukturyzowanego powszechnie używanego formatu nadającego się do odczytu maszynowego. Nie należy wydawać skanów dokumentów ani ich kserokopii, gdyż mogą zawierać dodatkowe dane niedotyczące osoby występującej z wnioskiem.
9. Prawo do uzyskania kopii, o której mowa w ust. 3, nie może niekorzystnie wpływać na prawa i wolności innych.

Art 4 Prawo do sprostowania danych

1. Każdej osobie, której dane są przetwarzane przez Administratora przysługuje prawo do sprostowania dotyczących jej danych osobowych, które są nieprawidłowe lub nieaktualne.
2. Ponadto osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych poprzez przedstawienie odpowiedniego oświadczenia.
3. Osoba upoważniona do przetwarzania danych przez Administratora, która w ramach wykonywanych zadań przetwarza dane osoby występującej z żądaniem z ust. 1 i 2, obowiązana jest dokonać weryfikacji przetwarzanych danych. Uzupełnienie tych danych następuje z uwzględnieniem celów przetwarzania.
4. Niniejsza procedura nie znajduje zastosowania do prostowania danych osobowych, w odniesieniu do których tryb ich sprostowania lub uzupełnienia określają odrębne przepisy, np. procedura sprostowania błędów i omyłek zawartych w decyzji administracyjnej w trybie art. 113 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2018 r. poz. 2096).

Art 5 Prawo do żądania usunięcia danych

1. Osobie, której dane są przetwarzane przez Administratora przysługuje prawo żądania niezwłocznego usunięcia jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, Powyższe prawo jest realizowane w przypadku gdy zostanie spełniona jedna z poniższych przesłanek:
   1) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
   2) osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych,
   3) osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania,
   4) dane osobowe były przetwarzane w sposób niezgodny z prawem,
   5) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator.
2. Jeżeli dane osobowe zostały upublicznione, a na mocy ust. 1 istnieje obowiązek usunięcia tych danych osobowych, to (biorąc pod uwagę dostępną technologię i koszt realizacji) należy podjąć niezbędne działania by poinformować innych Administratorów przetwarzających te dane osobowe, że osoba fizyczna której dane dotyczą, żąda, by Administratorzy usunęli wszelkie odniesienia do tych danych, kopie tych danych osobowych lub ich kopie.
3. Prawo do żądania usunięcia danych nie ma zastosowania gdy przetwarzanie tych danych jest niezbędne do:
   1) korzystania z prawa do wolności wypowiedzi i informacji,
   2) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega Administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,
   3) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, o ile prawdopodobne jest, że realizacja uprawnienia do „bycia zapomnianym", uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania.
   4) do ustalenia, dochodzenia lub obrony roszczeń.

Art 6 Prawo do żądania ograniczenia przetwarzania

1. Osoba, której dane są przetwarzane przez Administratora, ma prawo żądania ograniczenia przetwarzania jej danych osobowych, gdy:
   1) osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych (w tym przypadku ogranicza się przetwarzanie na okres pozwalający sprawdzić prawidłowość danych),
   2) przetwarzanie jest niezgodne z prawem, a osoba fizyczna, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
   3) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,
   4) osoba fizyczna, której dane dotyczą, wobec przetwarzania wniosła sprzeciw (w tym przypadku ogranicza się przetwarzanie do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie Administratora są nadrzędne wobec podstaw sprzeciwu).
2. Ograniczenie przetwarzania oznacza, że dane osobowe można jedynie przechowywać. Inne formy przetwarzania mogą mieć miejsce wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.
3. Ograniczenia przetwarzania dokonuje się poprzez odpowiednie oznaczenie danych osobowych, których dotyczy żądanie, przetwarzanych zarówno w formie tradycyjnej, jak i elektronicznej, tak aby każda osoba upoważniona do przetwarzania danych była świadoma, że dane te można jedynie przechowywać.
4. Przed uchyleniem ograniczenia przetwarzania Administrator informuje o tym osobę, która żądała takiego ograniczenia.

Art 7 Prawo do przeniesienia danych

1. Osoba, której dane są przetwarzane przez Administratora ma prawo do przeniesienia swoich danych, gdy podstawą ich przetwarzania jest udzielona zgoda, zawarta umowa albo gdy przetwarzanie danych odbywa się w sposób zautomatyzowany (czyli przy użyciu systemów informatycznych).

2. Prawo do przeniesienia danych dotyczy tylko tych danych, które dana osoba dostarczyła wcześniej Administratorowi.
3. Prawo do przenoszenia danych oznacza w szczególności prawo do:
   1) otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła Administratorowi,
   2) prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła Administratorowi, innemu administratorowi, bez przeszkód ze strony Administratora danych, o ile jest to technicznie możliwe.
4. Wykonywanie tego prawa nie może niekorzystnie wpływać na prawa i wolności innych osób.
5. Prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

Art 8 Prawo do wniesienia sprzeciwu wobec przetwarzania danych

1. Jeżeli przetwarzanie danych przez Administratora oparte jest na przesłance wykonania zadania realizowanego w interesie publicznym, jakim jest m.in. dostęp do informacji publicznej, osoba, której dane dotyczą, z przyczyn związanych z jej szczególną sytuacją, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych.
2. Administrator, po wniesieniu sprzeciwu przez osobę, której dane dotyczą powinien zaprzestać przetwarzania tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.
3. W momencie złożenia sprzeciwu wobec przetwarzania Administrator niezwłocznie ogranicza przetwarzanie i weryfikuje czy istnieją ważniejsze uzasadnione podstawy do przetwarzania niż interes osoby wnioskującej.
4. Jeżeli Administrator posiada podstawę prawną, o której mowa powyżej, informuje osobę wnioskującą o odmowie realizacji prawa wraz z uzasadnieniem decyzji. W przypadku, gdy uzasadniona jest przesłanka do zrealizowania żądania, postępuje się zgodnie z ust. 2.

Zał.nr 6 do Polityki	**Wzór upoważnienia do przetwarzania danych osobowych**

.....dnia.....roku

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

NR ...../.....

Na podstawie art. 29 i 32 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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)

UPOWAŻNIAM

.....

imię i nazwisko

.....

stanowisko, komórka organizacyjna

do przetwarzania danych osobowych

.....

Upoważnienie wydaje się na czas nieokreślony, nie później niż do czasu wygaśnięcia podstawy zatrudnienia, przy czym Administrator posiada uprawnienie do jego odwołania w każdej chwili.

_____

(pieczęć i podpis Administratora)

Ponadto pracownik posiada dostęp do następujących systemów informatycznych przetwarzających dane osobowe:

lp.	systemy informatyczne	uprawnienia*	data nadania/ zmiany
1.			
2.			
3.			
4.			

* Uprawnienia:
O-odczyt
W-wydruk
M-modyfikacja (zmiana, wprowadzanie danych)

Zał.nr 6 do Polityki	**Wzór upoważnienia do przetwarzania danych osobowych**

Zał. nr 7 do Polityki	**Wzór oświadczenia o zachowaniu w tajemnicy danych osobowych**

_____, _____

(miejscowość) (data)

Ja niżej podpisany/podpisana* ..... zobowiązuję się do zachowania w tajemnicy danych osobowych, do których jako pracownik będę posiadał dostęp w związku z wykonywaniem przeze mnie zadań służbowych i obowiązków pracowniczych, zarówno w trakcie obowiązującego stosunku pracy, jak i bezterminowo po ustaniu zatrudnienia.

Ponadto oświadczam, że zostałem zapoznany z przepisami dotyczącymi ochrony danych osobowych, w szczególności:

- Rozporządzeniem 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) (Dz. U. UE. L. 2016, poz. 119.1),
- ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781 ze zm.),
- dokumentacją ochrony danych osobowych przyjętą w Jednostce.

Niniejsze zobowiązanie nie dotyczy informacji poufnych, których ujawnienie organom sądowym lub administracyjnym oraz innym podmiotom i organom państwowym jest wymagane przez bezwzględnie obowiązujące przepisy prawa.

_____

(czytelny podpis, data)

Zał. nr 8 do Polityki	**Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych**

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Nr upoważnienia	Imię i nazwisko	Stanowisko	Data nadania	Data ustania	Dostęp do systemów informatycznych z uprawnieniami

Zał. nr 9 do Polityki	**Informator dla Użytkowników z zakresu ochrony danych osobowych**

Użytkowniku:

- opróżniaj regularnie folder „Kosz" w komputerze,
- nie przetrzymuj na pulpicie pojedynczych plików oraz folderów,
- nie przekazuj swojego loginu oraz hasła współpracownikom i innym osobom postronnym,
- zmieniaj hasło regularnie,
- w pracy używaj tylko służbowych nośników danych zabezpieczonych hasłem,
- nie używaj obcych nośników danych,
- dokumenty papierowe niszcz zawsze w niszczarkach,
- elektroniczne nośniki danych oddaj informatykowi do zniszczenia,
- regularnie twórz kopię zapasową swoich zasobów dyskowych,
- nie używaj nielegalnych publikacji, zdjęć oraz programów,
- nośniki danych sprawdzaj zawsze systemem antywirusowym,
- zbierając dane od klientów Jednostki, spełnij wobec nich „obowiązek informacyjny",
- zbieraj tylko tyle danych, ile wymaga realizacja usługi, o którą wystąpił klient Jednostki, oraz ile dopuszcza prawo,
- gdy udostępniasz dane osobowe lub informacje, upewnij się, że przekazujesz je tylko ich właścicielom lub podmiotom upoważnionym na podstawie przepisów prawa,
- gdy udzielasz informacji telefonicznej, zweryfikuj tożsamość osoby, w celu sprawdzenia czy ma ona prawo do uzyskania tych informacji,
- gdy wysyłasz wiadomość e-mail z załącznikiem zawierającym dane osobowe klienta Jednostki, zahasłuj ten załącznik,
- gdy korzystasz z listy mailingowej, wysyłaj informacje do klientów Jednostki, używając pola „kopia ukryta" w wiadomości e-mail,
- gdy udostępniasz informację publiczną, trwale zanonimizuj informacje o kliencie Jednostki, aby nie naruszyć jego praw i wolności i żeby wnioskodawca nie mógł go zidentyfikować,
- jeżeli klient zawnioskuje o realizację swoich praw wynikających z RODO, poinformuj o tym przypadku IOD,
- wykorzystuj służbową pocztę e-mail tylko do celów służbowych,
- nie otwieraj załączników z niewiadomego źródła,
- nie wykorzystuj opcji „autouzupełnianie" w wypełnianych formularzach,
- nie zapamiętuj swoich haseł w przeglądarkach,

- przy pracy na urządzeniu przenośnym upewnij się, że jest ono zabezpieczone przed dostępem osób trzecich,
- nie podłączaj służbowych urządzeń przenośnych do obcych sieci wi-fi,
- nie pozostawiaj w pomieszczeniach biurowych Jednostki osób postronnych bez asysty,
- gdy opuszczasz stanowisko pracy, zawsze blokuj stację roboczą,
- kończ pracę w systemach, zawsze wylogowując się z nich poprawnie,
- nie pozostawiaj niezamkniętych pomieszczeń biurowych oraz nie zostawiaj w drzwiach tych pomieszczeń kluczy,
- gdy kończysz pracę, zabezpiecz przed dostępem osób nieupoważnionych dokumenty papierowe oraz elektroniczne nośniki danych, a także wszystkie szafy, w których przechowywane są dokumenty,
- po zakończeniu pracy zabezpiecz wszystkie pomieszczenia, w których pracujesz,
- zadbaj o stosowne uprawnienia, gdy pozostajesz w pomieszczeniu biurowym po godzinach pracy,
- jeśli udostępniasz informacje dotyczące bezpieczeństwa informacji, skontaktuj się z IOD,
- jeśli przekazujesz dane osobowe podmiotom zewnętrznym, skonsultuj z IOD zasadność zawarcia umowę powierzenia,
- zgłoś do kierownika Jednostki i IOD potrzebę gromadzenia nowych danych osobowych lub aktualizację danych dotychczasowych,
- zgłaszaj wszystkie incydenty bezpieczeństwa lub ochrony danych do kierownika Jednostki oraz IOD,
- dbaj o otrzymany od pracodawcy sprzęt służbowy,
- zgłaszaj wszystkie awarie sprzętu do obsługi informatycznej Jednostki,

Informatyku:

- wykonaj konfigurację dla wnioskowanych zasobów oraz właściwie i zgodnie z wnioskiem przygotuj konto w systemach,
- reaguj na zgłaszane incydenty, zabezpiecz ewentualne dowody i powiadom o nich niezwłocznie IOD,
- do sieci Jednostki podłączaj tylko osoby posiadające odpowiednie uprawnienia lub umowy,
- zabezpiecz hasłem służbowe nośniki oraz dyski urządzeń przenośnych,
- prowadź ciągły nadzór nad ruchem sieciowym oraz zarządzaj pojemnością systemów.

Zał.nr 10 do Polityki	**Wzór umowy powierzenia przetwarzania danych osobowych**

UMOWA

POWIERZENIA DANYCH OSOBOWYCH DO PRZETWARZANIA

zawarta w dniu _____ r. w _____

pomiędzy:

_____

z siedzibą w _____. (___ - _____),

ul. _____ ,

NIP _____, reprezentowaną przez:

_____ – *(funkcja)*

zwaną w treści Umowy „**Administratorem**",

a

_____

z siedzibą w _____. (___ - _____),

ul. _____ , NIP

_____, reprezentowaną przez:

_____ – *(funkcja)*

zwaną w treści Umowy **„Procesorem"** lub **„Przetwarzającym"**,

w dalszej części Umowy Administrator i Procesor są nazywani łącznie **„Stronami"** lub każde oddzielnie **„Stroną"**.

§ 1

Przedmiot Umowy, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą

1. Umowa ma charakter umowy powierzenia danych osobowych w rozumieniu art. 28 ust. 1 i 3 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; Dz. U. UE. L. 2016, poz. 119.1), zwanego w dalszej części Umowy jako: „Rozporządzenie".
2. Procesor uprawniony jest do przetwarzania danych osobowych wyłącznie w celu wykonania umowy głównej, tj. umowy z dnia _____ , której przedmiotem jest _____, które będzie zwane w dalszej części Umowy jako „przetwarzanie" .
3. Przetwarzanie dotyczyć będzie kategorii osób:....., oraz rodzaju danych osobowych: .....

4. Przetwarzanie danych następować będzie w sposób ciągły w formie ..... oraz obejmuje następujące operacje.....

§ 2

Czas trwania Umowy

1. Umowa zostaje zawarta na czas określony od dnia _____ do dnia _____.
2. Procesor nie ma prawa do wykorzystania zgromadzonych na podstawie niniejszej Umowy danych osobowych w jakimkolwiek celu po jej rozwiązaniu, niezależnie od podstawy takiego rozwiązania.

§ 3

Warunki powierzenia danych osobowych do przetwarzania

1. Procesor przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora, przez które Strony rozumieją niniejsza Umowę lub indywidualne polecenia i instrukcje przekazywane w sposób, o którym mowa w § 4 ust. 2 zdanie drugie oraz:
   a) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
   b) podejmuje odpowiednie środki techniczne oraz organizacyjne, mające na celu zapewnienia bezpieczeństwa danych osobowych;
   c) nie korzysta z usług innego podmiotu przetwarzającego, bez uprzedniej pisemnej zgody Administratora;
   d) w miarę możliwości pomaga Administratorowi, poprzez odpowiednie środki techniczne i organizacyjne, wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w art. 12-23 Rozporządzenia;
   e) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36 Rozporządzenia;
   f) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, w tym również te, zawarte na nośnikach danych, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych, przy czym w sposób, o którym mowa w § 4 ust. 3 zdanie drugie składa

Administratorowi oświadczenie o trwałym usunięciu lub zwrocie wszystkich danych lub wskazuje podstawę prawną pozwalającą na ich dalsze przetwarzanie;

g) udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 Rozporządzenia oraz umożliwia Administratorowi (lub upoważnionemu przez niego audytorowi) przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich;

h) w przypadku przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, przed rozpoczęciem przetwarzania informuje w sposób wskazany w § 4 ust. 3 zdanie drugie Administratora o takim obowiązku prawnym, o ile prawo nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny, natomiast w przypadku indywidualnej woli przekazania przez Procesora powierzonych danych osobowych do państwa trzeciego lub organizacji międzynarodowej – dokonuje tego przetwarzania jedynie na odrębne polecenie Administratora, dokonane w sposób, o którym mowa w § 4 ust. 2 zdanie drugie.

i) zobowiązuje się do niezwłocznego poinformowania Administratora o jakimkolwiek postępowaniu, w szczególności administracyjnym lub sądowym, dotyczącym przetwarzania przez Procesora danych osobowych, o jakiejkolwiek decyzji administracyjnej lub orzeczeniu dotyczącym przetwarzania tych danych, skierowanych do Procesora, a także o wszelkich planowanych - o ile są mu wiadome - lub realizowanych kontrolach i inspekcjach dotyczących przetwarzania przez tego Procesora danych osobowych, w szczególności prowadzonych przez inspektorów upoważnionych przez Prezesa Ochrony Danych Osobowych. Poinformowanie następuje w sposób, o którym mowa w § 4 ust. 3 zdanie drugie.

2. Jeżeli powierzone dane osobowe są przetwarzane w formie elektronicznej na serwerach i nośnikach danych Procesora, te serwery i nośniki nie mogą znajdować się poza obszarem Unii Europejskiej i Europejskiego Obszaru Gospodarczego.
3. Procesor zobowiązuje się do każdorazowego i niezwłocznego informowania Administratora o przypadkach naruszenia przepisów prawa dotyczących ochrony powierzonych danych osobowych, w tym w szczególności przepisów Rozporządzenia, zaistniałych w okresie obowiązywania niniejszej Umowy.
4. W przypadku stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 Rozporządzenia, Procesor zgłasza je Administratorowi bez zbędnej zwłoki. Zgłoszenie naruszenia ochrony danych osobowych Administratorowi zawiera w swej treści

elementy wskazane w art. 33 ust. 3 RODO oraz winno nastąpić w sposób, o którym mowa w § 4 ust. 3 zdanie drugie.

5. Na wypadek zawinionego naruszenia przez Procesora zasad przetwarzania danych osobowych (określonych w przepisach powszechnie obowiązującego prawa, Rozporządzenia oraz niniejszej Umowy), skutkującego zobowiązaniem Administratora na mocy prawomocnego orzeczenia sądu, ugody sądowej bądź porozumienia mediacyjnego do wypłaty odszkodowania, zadośćuczynienia lub kary pieniężnej, Procesor zobowiązuje się zrekompensować Administratorowi udokumentowane straty z tego tytułu w pełnej wysokości.
6. Procesor jest zwolniony z odpowiedzialności za szkody spowodowane przetwarzaniem przez niego danych naruszającym przepisy prawa, jeżeli nie można mu przypisać winy za zdarzenie, które doprowadziło do powstania szkody.
7. Procesor zapewnia, że dane osobowe nie będą udostępniane jego pracownikom i zleceniobiorcom przed podpisaniem przez nich oświadczeń lub umów o zachowaniu poufności. Zachowanie poufności nie ustaje po rozwiązaniu lub wygaśnięciu stosunku pracy lub umowy cywilnoprawnej, niezależnie od przyczyny tego rozwiązania lub wygaśnięcia.
8. Procesor zobowiązuje się do monitorowania i stosowania przepisów prawa, powszechnie dostępnych wskazówek i zaleceń organu nadzorczego oraz unijnych organów doradczych, zajmujących się ochroną danych osobowych, w zakresie przetwarzania powierzonych mu danych, po uprzednim uzgodnieniu wpływu tych regulacji na przetwarzanie danych z Administratorem.

§ 4

Kontrola przetwarzania danych powierzonych

1. Administrator przez cały okres obowiązywania Umowy jest uprawniony do kontroli poprawności zabezpieczenia i przetwarzania danych powierzonych Procesorowi. Kontrola może zostać przeprowadzona m.in. w formie bezpośredniej inspekcji polegającej na dopuszczeniu przedstawicieli Administratora do wszystkich obszarów przetwarzania danych osobowych objętych niniejszą Umową we wszystkich lokalizacjach Procesora, w sposób nieutrudniający nadmiernie jego bieżącej działalności. Procesor zobowiązany jest do przedstawienia odpowiednich dokumentów do kontroli oraz wyjaśnień na piśmie na każde wezwanie Administratora,.
2. W przypadku, gdy kontrola, o której mowa w ust. 1, wykaże jakiekolwiek nieprawidłowości Administrator ma prawo żądać od Procesora niezwłocznego wdrożenia zaleceń

Administratora wynikających z ustaleń pokontrolnych. Zalecenia te przedstawiane będą w formie pisemnej pod adres siedziby Procesora lub formie elektronicznej pod adres e-mail ..... – przy czym obydwie formy zostają zastrzeżone pod rygorem nieważności.

3. Procesor niezwłocznie informuje Administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie Rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych. Poinformowanie winno nastąpić w formie pisemnej pod adres siedziby Administratora lub formie elektronicznej pod adres e-mail ..... – przy czym obydwie formy zostają zastrzeżone pod rygorem nieważności.

§ 5

Podpowierzenie danych

1. Procesor może powierzać przetwarzanie powierzonych mu danych osobowych objętych Umową innym podmiotom na stałe współpracującym z Procesorem (tzw. podpowierzenie) wyłącznie po uprzedniej zgodzie Administratora wyrażonej w sposób, o którym mowa w § 4 ust. 3 zdanie drugie.
2. Podpowierzając przetwarzanie danych osobowych innym podmiotom, Procesor jest obowiązany zapewnić w dalszej umowie powierzenia spełnienie przez ten podmiot wszelkich wymogów w zakresie ochrony danych osobowych na poziomie, co najmniej takim samym jak przewidziany w niniejszej Umowie.

§ 6

Poufność

1. Procesor zobowiązuje się do zachowania w tajemnicy wszelkich danych osobowych, informacji i materiałów przekazanych lub udostępnionych mu lub o których wiedzę powziął w związku z realizacją Umowy, a także powstałych w wyniku jej wykonania informacji i materiałów w formie pisemnej, graficznej lub jakiejkolwiek innej formie. Informacje i materiały są objęte tajemnicą nie mogą być bez uprzedniej pisemnej zgody Administratora udostępniane jakiejkolwiek osobie trzeciej, ani też ujawnione w inny sposób, chyba że w dniu ich ujawnienia były powszechnie znane albo muszą być ujawnione zgodnie z powszechnie obowiązującymi przepisami prawa, orzeczeniem sądu lub organu państwowego.
2. Procesor zapewnia, że osoby upoważnione do przetwarzania danych osobowych będą obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

Obowiązek zachowania tajemnicy nie ustaje po zaprzestaniu przetwarzania danych z jakiejkolwiek podstawy. Przepis § 3 ust. 7 Umowy stosuje się odpowiednio.

§ 7

Współpraca Stron

1. Strony ustalają, że podczas realizacji Umowy powierzenia będą ze sobą ściśle współpracować, informując się wzajemnie o wszystkich okolicznościach mających lub mogących mieć wpływ na wykonanie powierzenia danych osobowych.
2. Strony będą dokonywały uzgodnień i podejmowały decyzje operacyjne poprzez swoich przedstawicieli odpowiedzialnych za realizację Umowy w formie ustnej, pisemnej lub elektronicznej,.
3. Strony zobowiązują się, że wszelkie decyzje dotyczące polubownego zakończenia sporu z osobą fizyczną na skutek naruszenia ochrony jej danych osobowych, w szczególności fakt i wysokość wypłaty ewentualnego odszkodowania, podejmą wspólnie.

§ 8

Wypowiedzenie umowy

1. Każdej ze Stron przysługuje uprawnienie do rozwiązania Umowy z zachowaniem terminu wypowiedzenia określonego w umowie głównej.
2. Administrator ma prawo wypowiedzieć Umowę w trybie natychmiastowym, w przypadku rażącego naruszenia postanowień Umowy przez Procesora, który:
   a) wykorzystał dane osobowe w sposób niezgodny z Umową, w szczególności przetwarzał je dla własnych celów lub celów innych podmiotów, a także celów niezgodnych z powszechnie obowiązującymi przepisami prawa lub postanowieniami niniejszej Umowy;
   b) wykonuje Umowę niezgodnie z obowiązującymi w tym zakresie przepisami prawa lub instrukcjami Administratora w tym zakresie;
   c) nie zaprzestał niewłaściwego przetwarzania danych osobowych mimo uprzedniego wezwania Administratora do usunięcia naruszeń i bezskutecznego upływu wyznaczonego terminu 14 dni na zaniechanie naruszeń.
3. W przypadku wypowiedzenia Umowy w trybie natychmiastowym, o którym mowa w ust. 2, umowa główna ulega również rozwiązaniu, przy czym Procesor zrzeka się jakichkolwiek roszczeń wynikających z przedwczesnego rozwiązania umowy głównej.

§ 9

Postanowienia Końcowe

1. Z tytułu wykonywania niniejszej Umowy Procesorowi nie przysługuje dodatkowe wynagrodzenie.
2. Wszelkie zmiany niniejszej Umowy wymagają formy pisemnej pod rygorem nieważności.
3. Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Administratora.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

(Administrator)	(Procesor)

Zał. nr 11 do Polityki	**Wzór rejestru zawartych umów powierzenia przetwarzania danych osobowych**

Lp.	**Numer umowy**	**Data zawarcia umowy - obowiązywania umowy**	**Strona umowy**	**Zakres powierzenia**
1.				
2.				
3.				
4.				
5.				
6.				

Zał. nr 12 do Polityki	**Procedura zarządzania naruszeniami ochrony danych osobowych**

Art. 1. Istota naruszenia ochrony danych

Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

a) nieautoryzowany dostęp do danych,
b) nieautoryzowane modyfikacje lub zniszczenie danych,
c) udostępnienie danych nieautoryzowanym podmiotom,
d) nielegalne ujawnienie danych,
e) pozyskiwanie danych z nielegalnych źródeł.

Art. 2. Postępowanie w przypadku naruszenia danych osobowych

1. Użytkownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt naruszenia Administratorowi i Inspektorowi ochrony danych.
2. Typowe sytuacje, gdy bezpośredni przełożony powinien powiadomić Administratora i Inspektora ochrony danych:

a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
b) dokumentacja jest niszczona bez użycia niszczarki,
c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie,
d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.,
e) niewylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, niezamknięcie pomieszczenia z komputerem, niewykonanie

w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych,

f) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe,
g) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia,
h) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
i) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
j) telefoniczne próby wyłudzenia danych osobowych;
k) kradzież komputerów lub twardych dysków z danymi osobowymi;
l) utrata kontroli nad kopią danych osobowych;
m) maile zachęcające do ujawnienia identyfikatora i/lub hasła;
n) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
o) istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki"
p) hasła do systemów przechowywane są w pobliżu komputera.

3. Użytkownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia .
4. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora danych.

Inspektor Ochrony Danych podejmuje następujące kroki:

1. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
2. odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
3. nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

4. Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - **Załącznik nr 1**.
5. Inspektor ochrony danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) - **Załącznik nr 2** - rejestr naruszeń i incydentów ochrony danych osobowych, zawierający również wskazanie działań korygujących i zapobiegawczych.

Art. 3. Zgłaszanie naruszenia ochrony danych do Urzędu Ochrony Danych Osobowych

1. W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia – **Załącznik nr 3.**
2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
   a) opisywać charakter naruszenia ochrony danych osobowych, 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,
   b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
   c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
   d) opisywać środki zastosowane lub proponowane przez Administratora w celu zapobiegania naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach - środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania

zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

Art. 4. Zawiadomienie osoby której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art.33 ust. 3 lit. b), c) i d).
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

a) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

b) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, w zakresie o którym mowa w art. 34 ust. 1 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 (publ. Dz. Urz. UE L Nr 119, s. 1).

c) jeżeli wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Załącznik nr 1 Raport naruszenia ochrony danych

1. Data ..... Godzina .....

2. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem

   .....

   (imię, nazwisko, stanowisko służbowe,):

3. Lokalizacja zdarzenia

   .....

   (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

4. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

   .....

5. Podjęte działania:

   .....

6. Wstępna ocena przyczyn wystąpienia naruszenia:

   .....

7. Postępowanie wyjaśniające i naprawcze:

   .....

....

(podpis pracownika) *(data i podpis Inspektora Ochrony Danych)*

Zał. nr 12 do Polityki	**Procedura zarządzania naruszeniami ochrony danych osobowych**

Zał. nr 12 do Polityki	**Procedura zarządzania naruszeniami ochrony danych osobowych**

Załącznik nr 2 Rejestr naruszeń i incydentów ochrony danych osobowych

L p.	**Data naruszenia**	**Kategoria osób, których dane zostały naruszone**	**Kwalifikacj a naruszenia (niskie lub wysokie)**	**Zastosowane środki zaradcze**	**Zgłoszenie do organu nadzorczego (dotyczy lub nie dotyczy)**	**Zawiadomienie osoby której dane dotyczą (dotyczy lub nie dotyczy)**
1.						
2.						
3.						
4.						
5.						
6.						

Zał. nr 12 do Polityki	**Procedura zarządzania naruszeniami ochrony danych osobowych**

Zał. nr 12 do Polityki	**Procedura zarządzania naruszeniami ochrony danych osobowych**

Załącznik nr 3 Zgłoszenie o naruszeniu ochrony danych osobowych organowi nadzorczemu

_____, _____
(miejscowość) (data)

Nazwa Jednostki .....

adres (dane korespondencyjne):

.....

.....

Urząd Ochrony Danych Osobowych

ul. Stawki 2

00-193 Warszawa

Zgłoszenie naruszenia ochrony danych osobowych

Na podstawie obowiązku wynikającego z art. 33 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).

Data naruszenia	
Liczba osób których dane dotyczą	
Liczba wpisów danych osobowych i kategoria tych danych	
Dane Inspektora Danych osobowych	
Dane Organu Nadzorczego	
Charakter Naruszenia:	
Konsekwencje naruszenia:	
Zastosowane i proponowane środki zaradcze:	

Zał. nr 12 do Polityki	**Procedura zarządzania naruszeniami ochrony danych osobowych**

(Podpis Administratora)

Zał. nr 12 do Polityki	**Procedura zarządzania naruszeniami ochrony danych osobowych**

Załącznik nr: 4 Zawiadomienie o naruszeniu ochrony danych osoby, której dane zostały naruszone

_____, _____
(miejscowość) (data)

Nazwa Jednostki .....

adres (dane korespondencyjne):

.....

.....

Sz. P.

.....

.....

Zawiadomienie o naruszeniu ochrony danych osobowych

Na podstawie obowiązku wynikającego z art. 34 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 związku z naruszeniem Pana/Pani danych osobowych w zakresie ..... zawiadamiamy co następuje:

Konsekwencją wyżej wymienionej sytuacji jest podjęcie przez osoby nieupoważnione informacji w zakresie.....

Zawiadamiający podjął wszelkie możliwe środki celem minimalizacji skutków naruszenia między innymi: zawiadomienie do organu nadzorczego, zawiadomienie organów ścigania, wcześniejsza szyfryzacja danych.

Celem uzyskania dodatkowych informacji należy kontaktować się z .....

_____
(Podpis Administratora)

Zał. nr 13 do Polityki	**Wzór wniosku o nadanie/zmianę/odebranie uprawnień w systemach informatycznych**

WNIOSKUJĘ O:

☐ nadanie ☐ zmianę ☐ odebranie

uprawnień dla

....
imię i nazwisko Użytkownika

.....
stanowisko, komórka organizacyjna

Wypełnić w przypadku przyznania uprawnień

LP	System informatyczny**	Uprawnienia^
1.	Nazwa: ..... Login: ..... Data przyznania uprawnienia:	
2.	Nazwa: ..... Login: ..... Data przyznania uprawnienia:	
3.	Nazwa: ..... Login: ..... Data przyznania uprawnienia:	

** Systemy informatyczne, do których użytkownik ma dostęp lub jest mu odbierany
^Uprawnienia: O-odczyt; W-wydruk; M-modyfikacja (zmiana, wprowadzanie danych)

.....

.....
(podpis osoby składającej wniosek - data)

(podpis osoby z Obsługi informatycznej - data)

.....
(Zatwierdzenie Administratora – pieczęć i podpis,data)

Zał. nr 13 do Polityki	**Wzór wniosku o nadanie/zmianę/odebranie uprawnień w systemach informatycznych**

Wypełnić w przypadku zmiany lub odebrania uprawnień

LP	System informatyczny**		Uprawnienia^
	Odebrany	**Przyznany**	
1.	Nazwa: .... Login..... Data odebrania uprawnienia	Nazwa: .... Login..... Data przyznania uprawnienia:	
2.	Nazwa: .... Login..... Data odebrania uprawnienia	Nazwa: .... Login..... Data przyznania uprawnienia:	
3.	Nazwa: .... Login..... Data odebrania uprawnienia	Nazwa: .... Login..... Data przyznania uprawnienia:	

** Systemy informatyczne, do których użytkownik ma dostęp lub jest mu odbierany
^Uprawnienia: O-odczyt; W-wydruk; M-modyfikacja (zmiana, wprowadzanie danych)

.....

.....
(podpis osoby składającej wniosek - data)

(podpis osoby z Obsługi informatycznej - data)

.....
(Zatwierdzenie Administratora – pieczęć i podpis,data)

Zadania Administratora:

1. Administrator zwraca się z prośbą do Użytkownika o przyniesienie prywatnego sprzętu w celu odpowiedniej konfiguracji i zabezpieczenia.
2. W przypadku braku zgody Użytkownika na ingerencję w jego prywatny sprzęt Administrator określa minimalne zasady bezpiecznej pracy.
3. Na nieskonfigurowanym sprzęcie Użytkownika, Użytkownik za zgodą Administratora może wykonywać najprostsze prace takie jak pisanie pism, tworzenie tabel, prezentacji, itp., które następnie będą wysyłane poprzez służbowy e-mail jako zaszyfrowane dokumenty.
4. W miarę możliwości przekaż pracownikowi służbowy sprzęt dostępowy do Internetu.
5. Administrator ustala osoby kontaktowe w zakresie różnych działań służbowych (np. informatyka, księgowość) i informuje Użytkowników o wyznaczonych osobach.
6. Administrator ustala jakie dokumenty w formie papierowej mogą być wynoszone przez Użytkowników poza jednostkę i jakie warunki bezpieczeństwa należy spełnić przy wynoszeniu dokumentacji służbowej
   (Nie dotyczy dokumentów posiadających klauzule tajności).
7. Administrator ustala jakie dokumenty mogą być drukowane oraz skanowane na sprzęcie prywatnym lub zapewnia odpowiedni sprzęt Użytkownikowi.
8. Administrator ustala zasady niszczenia wydruków technicznych lub błędnych wykonanych na sprzęcie prywatnym lub zapewnia odpowiedni sprzęt Użytkownikowi.
9. Administrator powinien odebrać od Użytkownika oświadczenie o zapoznaniu się z zasadami pracy na sprzęcie prywatnym oraz stosowaniu się do niniejszych zasad.
10. Administrator zapewnia szkolenie Użytkownikom z zasad pracy na sprzęcie prywatnym i wsparcie obsługi informatycznej w przypadku problemów lub wątpliwości.

Zadania dla Obsługi informatycznej:

11. W przypadku zgody Użytkownika na ingerencję w prywatny sprzęt należy wykonać tylko najistotniejsze czynności, które nie ingerują w prywatne zasoby Użytkownika.
12. Należy sprawdzić jaki został zainstalowany system operacyjny na sprzęcie Użytkownika. W przypadku systemów niewspieranych przez Microsoft należy skonsultować z Administratorem dalszą możliwość pracy na sprzęcie prywatnym – należy wykonać test równowagi (mini analizę ryzyka dla takiej sytuacji).
13. W przypadku realizacji dalszej konfiguracji należy zaktualizować system operacyjny na komputerze oraz ustawić aktualizacje automatyczne.

14. Należy przygotować i skonfigurować prywatny komputer Użytkownika aby logował się tylko do zabezpieczonej i odpowiednio skonfigurowanej sieci VPN.
15. Należy monitorować ruch sieciowy pod kątem wystąpienia niepożądanego ruchu.
16. Za zgodą Użytkownika należy wyłączyć możliwość dostępu do BIOS komputera zabezpieczając go hasłem.
17. Za zgodą Użytkownika należy wyłączyć w BIOS możliwość boot'owania z innych nośników niż dysk twardy komputera.
18. Należy zaszyfrować dyski twarde, nośniki danych lub karty pamięci, na których będą gromadzone informacje służbowe.
19. Należy sprawdzić czy został zainstalowany program antywirusowy, a jeśli nie jako niezbędne minimum należy włączyć, należy zaktualizować Windows Defender oraz ustawić jego automatyczną aktualizację.
20. Należy zaktualizować inne oprogramowanie oraz przeglądarki internetowe, które będą wykorzystywane przez pracownika.
21. Należy włączyć i skonfigurować firewall aby uniemożliwić podłączenie komputera Użytkownika do niezabezpieczonych sieci Wi-Fi.
22. Należy założyć Użytkownikowi konto dostępu do służbowej części komputera bez uprawnień administratora. Konto to będzie wykorzystywane do na sprzęcie prywatnym.
23. Należy ustawić hasło logowania do konta zgodne z przyjętą polityką haseł.
24. Należy ustawić wygaszacz ekranu zabezpieczony hasłem nie dłuższym niż 10 min.
25. W przypadku przekazania przez Administratora służbowego punktu dostępowego do Internetu należy odpowiednio go skonfigurować (szyfrowana transmisja) i zabezpiecz dostęp hasłem.
26. Należy wymusić szyfrowanie połączeń ze służbową pocztą e-mail.
27. Należy aktualizować oprogramowanie serwera poczty e-mail oraz monitorować ruch na serwerze.
28. W przypadku używania przez Użytkownika smartfonu do pracy oraz obsługi poczty służbowej należy odpowiednio go zabezpieczyć.
29. W przypadku potrzeby wymiany danych pomiędzy Użytkownikami należy założyć wspólny, zabezpieczony katalog mając na uwadze właściwe uprawnienia Użytkowników.
30. Należy określić maksymalną wielkość pliku, którą można przesłać na wspólny zasób.
31. Należy ustalić zasady oraz punk kontaktowy w przypadku awarii lub innych problemów technicznych.

32. W przypadku korzystania z komunikatora internetowego należy odpowiednio go skonfigurować, zabezpieczyć hasłem, sprawdzić czy posiada właściwą ochronę kryptograficzną oraz sprawdzać aktualizacje dla serwera i klienta.
33. Należy zabezpieczyć alternatywne połączenie z Jednostką o tych samych parametrach i zabezpieczeniach w przypadku problemów z już istniejącym.
34. Należy przeskanować komputer aplikacją antywirusową.
35. Należy przeprowadzić szkolenie dla Użytkowników w zakresie pracy na sprzęcie prywatnym.
36. W przypadku ingerencji w komputer prywatny Użytkownika należy usunąć wszystkie wprowadzone zmiany, pliki, katalogi oraz punkty dostępowe.
37. W przypadku braku zgody na ingerencję w prywatny sprzęt Użytkownika należy przekazać minimalne wymagania jakie musi spełnić Użytkownik oraz jego sprzęt.
38. W powyższym przypadku nie należy zezwalać na logowanie się Użytkownika do systemów dziedzinowych Jednostki.

Zadania dla użytkownika:

39. Użytkownik powinien założyć osobny katalog służbowy, w którym będą przechowywane dokumenty Administratora.
40. Użytkownik powinien używać do logowania się na komputerze do katalogu służbowego haseł zgodnych z polityką haseł przyjętą w Jednostce.
41. Należy używać tylko rekomendowanych przez Administratora przeglądarek internetowych.
42. Nie należy zapamiętywać haseł w przeglądarkach internetowych.
43. Wykorzystując prywatny sprzęt do swoich celów (np. zakupy, gry, itp.) należy zachować daleko idące środki ostrożności.
44. Nie należy instalować żadnego oprogramowania bez uprzedniej konsultacji z Obsługą informatyczną.
45. Nie należy logować się na prywatnym komputerem do publicznych sieci Wi-Fi.
46. Użytkownik, który wyraził zgodę na konfigurację prywatnego sprzętu przez Obsługę informatyczną powinien łączyć się z zasobami Jednostki tylko za pomocą skonfigurowanego przez Obsługę informatyczną bezpiecznego łącza VPN.
47. Jeśli Użytkownik nie wyraził zgody na konfigurację prywatnego sprzętu przez Obsługę informatyczną najprawdopodobniej nie będziesz miał dostępu do systemów dziedzinowych Jednostki.
48. Do celów służbowych Użytkownik zobowiązany jest korzystać tylko z służbowej poczty e-mail.

49. Przed wysłaniem wiadomości Użytkownik powinien upewnić się, że wiadomość jest wysyłana do właściwego adresata, szczególnie gdy są wysyłane dane osobowe lub inne istotne informacje.
50. Użytkownik nie powinien otwierać wiadomości od nieznanych nadawców, a szczególnie załączników niewiadomego pochodzenia oraz klikać w żadne linki lub odnośniki.
51. W przypadku drukowania służbowych dokumentów na prywatnym sprzęcie Użytkownik powinien je odpowiednio zabezpieczyć.
52. W przypadku wykorzystywania do kontaktów komunikatora internetowego Użytkownik nie może używać w tym samym czasie innych narzędzi do komunikacji.
53. W przypadku przesyłania plików lub dokumentów za pomocą poczty e-mail lub komunikatorów internetowych Użytkownik zawsze powinien zabezpieczyć je hasłem. Hasło należy przekazać innym kanałem kontaktowym (np. wiadomością SMS).
54. W przypadku braku zgody Użytkownika na ingerencję w ustawienia na komputerze prywatnym przez Obsługę informatyczną bezwzględnie należy usunąć wszystkie dokumenty, zapamiętane hasła oraz konta służbowe.
55. W przypadku wyrażonej zgody przez Użytkownika na wprowadzenie ustawień na komputerze prywatnym przez Obsługę informatyczną należy mieć na względzie, aby informatycy przywrócili ustawienia do stanu początkowego.
56. W przypadku utraty sprzętu Użytkownik zobowiązany jest niezwłocznie skontaktować się z wyznaczoną osobą do kontaktu i zadbać jeżeli jest taka możliwość, o zdalne usunięcie danych z urządzenia.

Zał. nr 15 do Polityki	**Opis środków technicznych stosowanych do zabezpieczania danych osobowych i wykaz obszaru przetwarzania**

Obszarem przetwarzania danych osobowych jest siedziba Administratora Danych Osobowych zlokalizowana w budynku ***przy ulicy Sienkiewicza 79, 28-425 Złota.***

Obszar przetwarzania danych osobowych w Jednostce stanowią niżej wskazane pomieszczenia, w których realizowane są procesy przetwarzana danych osobowych:

Obszarem przetwarzania danych osobowych w Jednostce są pomieszczenia znajdujące się na parterze oraz piętrze budynku w którym realizowane są zadania administracyjno-organizacyjne, rozumiane jako procesy przetwarzana danych osobowych.

Techniczne środki zabezpieczające

Administrator zabezpiecza przetwarzane dane osobowe wykorzystując środki techniczne w postaci:

- zabezpieczenia pomieszczeń, gdzie przetwarzane są dane osobowe poprzez zastosowanie drzwi antywłamaniowych;
- dezintegracji w sposób mechaniczny za pomocą niszczarki, dokumentów w formie papierowej zawierających dane osobowe uznanych - przez Administratora lub osoby przez niego upoważnione - za nieprzydatne w procesie przetwarzania danych, w celu uniemożliwienia zapoznania się z treścią dokumentu przez osoby nieuprawnione,
- wdrożenia procedury sporządzania kopii informatycznych nośników danych oraz systemów informatycznych wykorzystywanych w jednostce do przetwarzania danych osobowych;
- zastosowania praktyki zabezpieczenia komputerów wykorzystywanych w jednostce do procesów przetwarzana danych osobowych w system loginów i haseł oraz zastosowanie w nich wymuszonego mechanizmu zmiany haseł;
- zastosowania praktyki zabezpieczenia komputerów wykorzystywanych w jednostce do procesów przetwarzana danych osobowych programem antywirusowym, który sprawuje ciągły nadzór (praca w tle) nad pracą systemu operacyjnego;
- gaśnice wolnostojące zlokalizowane w siedzibie Administratora;
- osoby wyznaczone do zarządzania kluczami do budynku oraz pomieszczeń służbowych posiadają stosowne upoważnienia.

Zał. nr 15 do Polityki	**Opis środków technicznych stosowanych do zabezpieczania danych osobowych i wykaz obszaru przetwarzania**

Wykaz osób posiadających klucze do drzwi zewnętrznych budynku Urzędu Gminy w Złotej

Budynek przy ul. Sienkiewicza 79

1. Wójt Złotej
2. Kierownik Referatu Organizacyjnego i Spraw Obywatelskich
3. Zastępca Skarbnika
4. Sekretarz Gminy
5. Sprzątaczka
6. Kierownik GOPS
7. Skarbnik
8. Podinspektor

Zał. nr 15 do Polityki	**Opis środków technicznych stosowanych do zabezpieczania danych osobowych i wykaz obszaru przetwarzania**

Upoważnienie do zarządzania kluczami do budynku Urzędu Gminy w Złotej

Zgodnie z Polityką ochrony danych powierzam Pani/Panu ..... , zatrudnionej/zatrudnionemu w Urzędzie Gminy w Złotej, na stanowisku ..... komplet kluczy do budynku Urzędu Gminy w Złotej przy ul. Sienkiewicza 79.

.....
podpis Wójta

Oświadczam, że przyjmuję pełną odpowiedzialność za powierzone klucze i zobowiązuję się do ich wykorzystania jedynie w celach realizacji powierzonych mi zadań zgodnie z niniejszym upoważnieniem.

.....
data i podpis pracownika

Zał. nr 15 do Polityki	**Opis środków technicznych stosowanych do zabezpieczania danych osobowych i wykaz obszaru przetwarzania**

Upoważnienie do zarządzania kluczami do pomieszczeń biurowych

Zgodnie z Polityką ochrony danych powierzam Pani/Panu ..... , zatrudnionej/zatrudnionemu w Urzędzie Gminy w Złotej, na stanowisku ..... klucze do pomieszczenia biurowego w którym wykonuje powierzone obowiązki.

.....
podpis Wójta

Oświadczam, że przyjmuję pełną odpowiedzialność za powierzone klucze i zobowiązuję się do ich wykorzystania jedynie w celach realizacji powierzonych mi obowiązków zgodnie z niniejszym upoważnieniem.

.....
data i podpis pracownika

Zał. nr 16 do Polityki	**Rejestr poboru kluczy**

LP	Data	Nr strefy	Godzina pobrania	Imię i nazwisko pobierającego	Godzina zdania	Imię i nazwisko zdającego
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						

Zał. nr 16 do Polityki	**Rejestr poboru kluczy**

14.						
15.						
16.						
17.						

Zał. nr 17 do Polityki	**Wykaz osób zapoznanych z Polityką ochrony danych osobowych**

Lp.	**Imię i nazwisko pracownika**	**Podpis**
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		