Załącznik nr 1 do Polityki – „Wzór Rejestru Czynności Przetwarzania Danych"

LP.	Nazwa czynności przetwarzania	Jednostka organizacyjna (wydział, referat itp.)	Cel przetwarzania	Kategoria osób	Kategoria danych	Podstawa prawna	Źródło danych	Planowany termin usunięcia kategorii danych *(jeżeli jest to możliwe)*	Nazwa współadministratora i dane kontaktowe *(jeśli dotyczy)*	Nazwa podmiotu przetwarzającego i dane kontaktowe *(jeśli dotyczy)*	Kategoria odbiorców *(innych niż podmiot przetwarzający)*	Nazwa systemu lub oprogramowania	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa zgodnie z art. 32 ust. 1 *(jeżeli jest to możliwe)*	DPIA (TAK/NIE)	Transfer do kraju trzeciego lub org. międzynarodowej	
															Transfer do kraju trzeciego lub organizacji międzynarodowej (nazwa kraju i podmiotu)	Jeśli transfer i art. 49 ust. 1 akapit drugi - dokumentacja odpowiednich zabezpieczeń

Załącznik nr 2 do Polityki – „Wzór umowy powierzenia przetwarzania danych"

Umowa Nr .....

Zawarta w dniu ..... r. w..... pomiędzy:

.....zwanym w dalszej części niniejszej umowy „Zleceniodawcą" reprezentowanym przez:

....

a

.....

zwanym w dalszej części niniejszej umowy „Wykonawcą"

reprezentowanym przez:

.....

o następującej treści:

§ 1

Powierzenie przetwarzania danych osobowych

1. W związku z realizacją umowy nr ..... z dnia ..... r. pomiędzy (.....) a (.....), o ..... Zleceniodawca powierza Wykonawcy trybie art. 28 ust.3 rozporządzenia Parlamentu Europejskiego i Rady (EU) 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). zwanego dalej RODO przetwarzanie danych osobowych.
2. Zleceniodawca oświadcza, że jest administratorem danych, które powierza.
3. Powierzone dane zawierają informacje o osobach fizycznych będących osobami fizycznymi.
4. Zleceniodawca powierza Wykonawcy przetwarzanie danych osobowych w zakresie określonym w § 2.

§ 2

Zakres i cel przetwarzania danych

1. Wykonawca będzie przetwarzał, powierzone na podstawie niniejszej Umowy, następujące kategorie danych osobowych:

   .....
2. Powierzone przez Zleceniodawcę dane osobowe będą przetwarzane przez Wykonawcę wyłącznie w celu wykonywania przez Wykonawcę na rzecz Zleceniodawcy usług szczegółowo opisanych w umowie , o której mowa w § 1 ust. 1 i w sposób zgodny z niniejszą Umową.

§ 3

Sposób wykonania Umowy w zakresie przetwarzania danych osobowych

1. Wykonawca zobowiązuje się, przy przetwarzaniu danych osobowych, o których mowa w § 2 ust 1, do ich zabezpieczenia poprzez podjęcie środków technicznych i organizacyjnych, o których mowa w art. 28 RODO.

2. Wykonawca oświadcza, że:

   1) prowadzi dokumentację opisującą sposób przetwarzania danych osobowych,

   2) znajdujące się w jego posiadaniu urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zapewniają właściwy do zagrożeń poziom bezpieczeństwa,

   3) stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, a w szczególności zabezpieczenia danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem RODO, zmianą, utratą, uszkodzeniem lub zniszczeniem, w zakresie, za który odpowiada Wykonawca.

3. Wykonawca zobowiązuje się przetwarzać powierzone mu dane osobowe zgodnie z niniejszą Umową, RODO oraz z innymi przepisami prawa powszechnie obowiązującego, które chronią prawa osób, których dane dotyczą.

4. Wykonawca zobowiązuje się niezwłocznie zawiadomić Zleceniodawcę o:

   1) każdym prawnie umocowanym żądaniu udostępnienia danych osobowych właściwemu organowi państwa, chyba, że zakaz zawiadomienia wynika z przepisów prawa, a szczególności przepisów postępowania karnego, gdy zakaz ma na celu zapewnienia poufności wszczętego dochodzenia,

   2) każdym nieupoważnionym dostępie do danych osobowych,

   3) każdym żądaniu otrzymanym od osoby, której dane przetwarza, powstrzymując się jednocześnie od odpowiedzi na żądanie.

5. Zleceniodawca ma prawo do kontroli sposobu wykonywania niniejszej Umowy poprzez przeprowadzenie zapowiedzianych na 7 dni kalendarzowych wcześniej doraźnych kontroli dotyczących przetwarzania danych osobowych przez Wykonawcę oraz żądania składania przez niego pisemnych wyjaśnień.

6. Na zakończenie kontroli, o których mowa w ust. 8, przedstawiciel Zleceniodawcy sporządza protokół w 2 egzemplarzach, który podpisują przedstawiciele obu stron. Wykonawca może wnieść zastrzeżenia do protokołu w ciągu 5 dni roboczych od daty jego podpisania przez strony.

7. Wykonawca zobowiązuje się dostosować do zaleceń pokontrolnych mających na celu usunięcie uchybień i poprawę bezpieczeństwa przetwarzania danych osobowych.

8. Wykonawca zobowiązuje się odpowiedzieć niezwłocznie i właściwie na każde pytanie Zleceniodawcy dotyczące przetwarzania powierzonych mu na podstawie Umowy danych osobowych.

9. Wykonawca może „podpowierzyć" usługi objęte umową, o której mowa w § 1 ust. 1 i niniejszą umową podwykonawcom jedynie za zgodą Zleceniodawcy.

§4

Odpowiedzialność Wykonawcy

1. Wykonawca jest odpowiedzialny za udostępnienie lub wykorzystanie danych osobowych niezgodnie z Umową, a w szczególności za udostępnienie osobom nieupoważnionym.
2. W przypadku naruszenia przepisów RODO lub niniejszej Umowy z przyczyn leżących po stronie Wykonawcy, w następstwie, czego Zleceniodawca, jako administrator danych osobowych zostanie zobowiązany do wypłaty odszkodowania lub zostanie ukarany karą grzywny, Wykonawca zobowiązuje się pokryć Zleceniodawcy poniesione z tego tytułu straty i koszty.

§5

Czas obowiązywania Umowy powierzenia

Niniejsza Umowa powierzenia zostaje zawarta na czas określony od dnia ..... do dnia ..... .

§ 6

Warunki wypowiedzenia Umowy

1. Zleceniodawca ma prawo rozwiązać niniejszą Umowę bez zachowania terminu wypowiedzenia, gdy Wykonawca:
   1) wykorzystał dane osobowe w sposób niezgodny z niniejszą Umową,
   2) powierzył przetwarzanie danych osobowych podwykonawcom bez zgody Zleceniodawcy,
   3) nie zaprzestanie niewłaściwego przetwarzania danych osobowych,
   4) zawiadomi o swojej niezdolności do dalszego wykonywania niniejszej Umowy, a w szczególności niespełniania wymagań określonych w §3.
2. Rozwiązanie niniejszej Umowy przez Zleceniodawcę jest równoznaczne z wypowiedzeniem umowy, o której mowa w § 1 ust. 1.

§ 7

Rozwiązanie Umowy

Wykonawca, w przypadku wygaśnięcia umowy, o której mowa §1 ust.1 i niniejszej umowy niezwłocznie, ale nie później niż w terminie do 5 dni kalendarzowych, zobowiązuje się zwró-

cić lub usunąć wszelkie dane osobowe, których przetwarzanie zostało mu powierzone, w tym skutecznie usunąć je również z nośników elektronicznych pozostających w jego dyspozycji i potwierdzić powyższe przekazanym Zleceniodawcy protokołem.

§8

Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§9

W sprawach nieuregulowanych w niniejszej umowie mają zastosowanie przepisy Kodeksu Cywilnego.

§10

Spory wynikłe z tytułu Umowy będzie rozstrzygał Sąd właściwy dla miejsca siedziby Zleceniodawcy.

§ 11

Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze stron.

....

za Zleceniodawcę za Wykonawcę

Załącznik nr 3 do Polityki – „Wzór ewidencji umów powierzenia przetwarzania danych osobowych"

Lp.	Nazwa podmiotu przetwarzającego	Data podpisania umowy	Data zakończenia umowy	Zakres i kategoria powierzonych danych danych	Nazwa strony trzeciej jeśli taką wskazano

Załącznik nr 4 do Polityki – „Wzór wniosku o wpis aktualizacyjny do RCPD"

.....

Miejscowość, data

Wniosek o wpis aktualizacyjny

Wnoszę o wpisanie / usunięcie / aktualizację czynności przetwarzania danych do RCPD

1. Nazwa czynności przetwarzania danych

.....

2. Jednostka organizacyjna (departament, dział itp.)

.....

3. Cel przetwarzania

.....

4. Kategorie osób

.....

5. Kategorie danych

.....

6. Podstawa prawna

.....

7. Źródło danych

.....

8. Planowany termin podjęcia przetwarzania kategorii danych

.....

9. Planowany termin usunięcia kategorii danych

.....

.....

Data i podpis wnioskującego

Załącznik nr 5 do Polityki – „Wzór zgody na przetwarzanie danych"

Zgoda na przetwarzanie danych osobowych

Poinformowano mnie o przysługującym mi prawie cofnięcia niniejszej zgody w dowolnym momencie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Aby wycofanie zgody było tak łatwe jak jej wyrażenie Administrator zapewnia mi dostęp w swojej siedzibie do niniejszego formularza i umożliwia złożenie podpisu pod klauzulą „Cofam zgodę na przetwarzanie danych".

Wyrażam dobrowolnie i świadomie zgodę na przetwarzanie przez Administratora

Starostę Lęborskiego

z siedzibą **w Starostwie Powiatowym w Lęborku**

84-300 Lębork, ul. Czołgistów 5,

w celu

.....

.....

poniżej wymienionych moich danych osobowych

.....

.....

I poświadczam ten fakt własnoręcznym podpisem pod klauzulą „Wyrażam zgodę na przetwarzanie danych".

Wyrażam zgodę na przetwarzanie danych

.....

Data i własnoręczny podpis

Cofam zgodę na przetwarzanie danych

.....

Data i własnoręczny podpis

Załącznik nr 6 do Polityki – „Wzór klauzuli informacyjnej"

KLAUZULA INFORMACYJNA – wzór ogólny

Zgodnie z art. 13 ust. 1 i ust. 2 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. informuję, iż:

1. administratorem Pani/Pana danych osobowych jest Starostwo Powiatowe w Lęborku reprezentowane przez Starostę Lęborskiego z siedzibą w 84-300 Lębork, ul. Czołgistów 5;
2. inspektorem ochrony danych w Starostwie Powiatowym w Lęborku jest Pan Krzysztof Pukaczewski (**e-mail: iodo@starostwolebork.pl*);
3. Pani/Pana dane osobowe przetwarzane będą w celu realizacji ustawowych zadań Starosty jako organu administracji na podstawie art. 6 ust. 1 lit. ... *(*należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e/f. *Przy podpunkcie f należy wskazać uzasadniony interes ADO lub strony trzeciej)* ogólnego rozporządzenia o ochronie danych osobowych oraz na podstawie ..... *(*należy podać podstawy prawne dla konkretnego wydziału/referatu)*
4. odbiorcą Pani/Pana danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa;
5. Pani/Pana dane osobowe nie będą przekazywane do państwa trzeciego/organizacji międzynarodowej;
6. Pani/Pana dane osobowe będą przechowywane w czasie określonym przepisami prawa, zgodnie z instrukcją kancelaryjną obowiązującą w Starostwie Powiatowym w Lęborku;
7. posiada Pani/Pan prawo dostępu do treści swoich danych osobowych oraz prawo ich sprostowania, usunięcia lub ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;
8. ma Pan/Pani prawo wniesienia skargi do Urzędu Ochrony Danych Osobowych gdy uzna Pani/Pan, iż przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r.;
9. podanie przez Pana/Panią danych osobowych jest ... *(*wybrać odpowiednio: wymogiem ustawowym/warunkiem umownym/warunkiem zawarcia umowy)*. Jest Pan/Pani zobowiązana do ich podania a konsekwencją niepodania danych osobowych będzie ... *(* jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych)*.

Załącznik nr 7 do Polityki – „Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji".

Procedury bezpieczeństwa fizycznego i bezpieczeństwa informacji

I

Procedura nadawania upoważnień do przetwarzania danych i uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków związanych z przetwarzaniem danych osobowych. Wniosek o wydanie upoważnienia jest kierowany do Sekretarza przez przełożonego osoby, która powinna uzyskać upoważnienie lub w przypadku osób pracujących na samodzielnym stanowisku na wniosek zainteresowanego. Pracownik w Urzędzie przygotowuje treść upoważnienia w dwóch egzemplarzach do zaopiniowania i podpisu Administratorowi. W przypadku akceptacji upoważnień przez Administratora, pracownik wyznaczony w Urzędzie przekazuje jeden egzemplarz upoważnienia oraz wniosek do akt personalnych pracownika z podpisem pracownika potwierdzającym odbiór upoważnienia. Drugi egzemplarz upoważnienia Pracownik wyznaczony w Urzędzie przekazuje pracownikowi. Fakt wydania upoważnienia Pracownik wyznaczony w Urzędzie odnotowuje w Ewidencji osób upoważnionych. **Załącznik nr 10 do Polityki – „Wzór upoważnienia do przetwarzania danych osobowych"** określa treść upoważnienia. Na zasadach powyżej opisanych następuje cofnięcie upoważnienia czy jego rozszerzenie. Druk wzoru wniosku o wydanie upoważnienia określa **Załącznik nr 8 do Polityki – „Wniosek o nadanie / rozszerzenie / cofnięcie upoważnienia do przetwarzania danych osobowych"** a **Załącznik nr 9 do Polityki – „Ewidencja osób upoważnionych do przetwarzania danych osobowych"** określa zakres informacji ujętych w ewidencji. Możliwe jest prowadzenie ewidencji w rozbiciu na komórki organizacyjne Urzędu.

Uprawnienia w systemie informatycznym, w którym przetwarza się dane osobowe nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków związanych z przetwarzaniem danych osobowych z wykorzystaniem systemów informatycznych. Wniosek o wydanie uprawnienia jest kierowany do Administratora przez przełożonego osoby, która powinna uzyskać uprawnienie pracy w systemie informatycznym lub w przypadku osób pracujących na samodzielnym stanowisku na wniosek zainteresowanego. W przypadku akceptacji wniosku przez Administratora, Administrator przekazuje podpisany wniosek Administratorowi Systemów Informatycznych (ASI). ASI powiadamia ustnie przełożonego pracownika oraz zainteresowanego o nadaniu uprawnień w systemie informatycznym. Wnioski pozytywnie zaopiniowane przez Administratora są zagregowane i pod nadzorem ASI. Na zasadach powyżej opisanych następuje cofnięcie uprawnienia czy jego rozszerzenie. Druk wzoru wniosku o wydanie uprawnienia określa **Załącznik nr 11 do Polityki – „Wniosek o nadanie**

/ rozszerzenie / cofnięcie uprawnienia w systemie informatycznym".

Każdy pracownik przed dopuszczeniem do przetwarzania danych osobowych zostaje zapoznany przez Pracownika wyznaczonego w Urzędzie z zasadami ochrony danych osobowych opisanych w Polityce ochrony danych osobowych. Pracownik po zapoznaniu z wspomnianymi zasadami podpsuje klauzulę poufności, której wzór stanowi **Załącznik nr 12 do Polityki – „Wzór klauzuli poufności"**. Każdy z pracowników Urzędu jest przeszkolony z zakresu tematyki ochrony danych osobowych przez IOD po podjęciu zatrudnienia oraz w razie zmiany istotnych warunków zewnętrznych (np. zmiany przepisów) lub wewnętrznych (np. zmiana stanowiska pracy).

II

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzeniem i użytkowaniem

Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu. Każdy identyfikator użytkownika zabezpieczony jest hasłem.

1. Hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,
   - hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
   - hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,
   - hasło nie może być jednakowe z identyfikatorem użytkownika,
   - hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.
2. Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
3. Hasło musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.

4. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie Administratora.

5. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

III

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych

Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń. W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić Administratora.

Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.

W przypadku czasowego opuszczenia stanowiska pracy, użytkownik musi wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.

Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych płyty CD, pendrive i inne, zawierających dane osobowe. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następują poprzez wylogowanie się z tego systemu.

IV

Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Kopie zapasowe powinny być kontrolowane przez administratora danych, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.

Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.

W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

V

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych

Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.

Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być wynoszone poza pomieszczenia stanowiące obszar przetwarzania danych osobowych.

Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem.

W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.

VI

Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

1) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

- poprzez zainstalowanie programu antywirusowego;
- poprzez zainstalowanie firewall (zapora sieciowa);
- poprzez zabezpieczenie sieci radiowej odpowiedniej mocy uwierzytelnieniem;

2) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez zastosowanie zasilacza awaryjnego ups.

Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem w pomieszczeniu zamkniętym;

b) usuwa się niezwłocznie po ustaniu ich użyteczności.

VII

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych przez firmy zewnętrzne na podstawie zawartych umów. W umowie musi znajdować się zapis o powierzeniu danych osobowych.

W przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora lub ASI.

Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.

Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni ASI.

Załącznik nr 8 do Polityki – „Wzór wniosku o nadanie / rozszerzenie / cofnięcie upoważnienia do przetwarzania danych osobowych"

.....

Miejscowość i data

Wniosek

o nadanie / rozszerzenie / cofnięcie upoważnienia do przetwarzania danych osobowych

Wnioskuję o wydanie upoważnienia/ rozszerzenie/ cofnięcie upoważnienia z dnia .....

Pani /Panu* .....

(imię i nazwisko pracownika)

zatrudnionej/emu w ..... na stanowisku ..... do przetwarzania danych osobowych wynikających z zakresu obowiązków pracowniczych z powodu:

a) podjęcia pracy na stanowisku .....
b) zmiany stanowiska.....
c) zmiany zakresu obowiązków pracowniczych.....
d) utworzenia nowego zbioru danych osobowych.....
e) naruszenia zasad i sposobu przetwarzania danych osobowych .....

1. Czynność przetwarzania danych osobowych zgodna z RCPD:

   .....

2. Rodzaj uprawnień: Z - pełne prawa do zarządzania bazą danych, P- prawo do przeglądania,

   .....

3. Sposób i miejsce przetwarzania danych osobowych

   .....

.....

Data i podpis Kierownika referatu/ pracownika na samodzielnym stanowisku pracy

---

* niepotrzebne skreślić

Załącznik nr 9 do Polityki – „Ewidencja osób upoważnionych do przetwarzania danych osobowych"

Lp.	Imię i nazwisko	Stanowisko służbowe	Data nadania upoważnienia	Data ustania upoważnienia	Czynność przetwarzania danych wg RCPD	Identyfikator *(Jeżeli dane są przetwarzane w systemie informatycznym)*

Załącznik nr 10 do Polityki – „ Wzór upoważnienia do przetwarzania danych osobowych"

.....

Miejscowość i data

UPOWAŻNIENIE Nr .....

do przetwarzania danych osobowych

I.

Na podstawie art. 29 RODO z dniem ..... upoważniam Panią/Pana*) .....

.....

(imię i nazwisko)

zatrudnioną/zatrudnionego w .....

(nazwa komórki organizacyjnej)

do przetwarzania danych osobowych, w celach związanych z wykonywaniem obowiązków na stanowisku: .....

(zajmowane stanowisko)

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej i elektronicznej*)

II.

Upoważniam Panią/Pana*) do przetwarzania danych osobowych w ramach czynności przetwarzania danych:

.....

(wpisać zgodnie z RCPD)

III.

1. Upoważnienie wygasa z chwilą ustania Pana/Pani*) zatrudnienia na stanowisku ..... w .....

(wskazać stanowisko pracy) *(nazwa instytucji lub komórki organizacyjnej)*

2. Jednocześnie informuję, że zobowiązany(a) jest Pan(i) do zachowania powyższych informacji w tajemnicy. Obowiązek ten istnieje również po ustaniu zatrudnienia.

.....

Data i podpis Administratora

Uwaga:

Niniejsze upoważnienie zostało sporządzone w dwóch jednobrzmiących egzemplarzach, które otrzymują:

Osoba upoważniona;

Administrator

*) *niepotrzebne skreślić*

Załącznik nr 11 do Polityki – „Wniosek o nadanie / rozszerzenie / cofnięcie uprawnienia w systemie informatycznym".

.....

Miejscowość i data

Wniosek

o nadanie / rozszerzenie / cofnięcie uprawnienia w systemie informatycznym

Wnioskuję o wydanie uprawnienia/ rozszerzenie/ cofnięcie uprawnienia* z dnia .....

Pani /Panu* .....

(imię i nazwisko pracownika)

zatrudnionej/emu w ..... na stanowisku ..... do przetwarzania danych osobowych w poniższym systemie / systemach*:

.....
.....
.....
.....
.....
.....
.....
.....
.....

.....

Data i podpis Kierownika referatu/ pracownika na samodzielnym stanowisku pracy

---

Akceptuję / nie akceptuję wniosku*

.....

Data i podpis Administratora

* niepotrzebne skreślić

Załącznik nr 12 do Polityki – „Wzór klauzuli poufności"

KLAUZULA POUFNOŚCI

OŚWIADCZENIE

Oświadczam, że zapoznano mnie z obowiązującymi w Starostwie Powiatowym w Lęborku zasadami ochrony danych osobowych oraz przepisami prawa i zobowiązuję się do ich stosowania.

Świadomy/a jestem obowiązku zachowania w tajemnicy danych osobowych i sposobów ich zabezpieczenia, również po ustaniu zatrudnienia lub zakończeniu współpracy.

Pouczono mnie o konsekwencjach prawnych nieprzestrzegania obowiązujących w Starostwie Powiatowym w Lęborku zasad ochrony danych i / lub przepisów krajowych o ochronie danych osobowych.

....

(miejscowość, data) *(czytelny podpis)*

Załączniku nr 13 do Polityki – „Wzór protokołu analizy ryzyka"

Protokół analizy ryzyka

1. Nazwa analizowanej czynności przetwarzania danych lub ich kategorii
   .....
2. Data wykonania analizy
   .....
3. Skład zespołu analizującego ryzyko
   .....
   .....
   .....
   .....
4. Charakter przetwarzania
   .....
5. Zakres przetwarzania
   .....
6. Kontekst przetwarzania
   .....
7. Cel przetwarzania
   .....
8. Ryzyko naruszenia praw lub wolności osób fizycznych (prawdopodobieństwo i waga zagrożenia)
   Skutek - .....
   Prawdopodobieństwo - .....
   Poziom zagrożenia - .....
9. Rekomendacja do przeprowadzenia oceny skutków przetwarzania danych
   .....

.....

Data i podpis Administratora

Ocena skutków przetwarzania danych		
Data wykonania oceny		
Czynność przetwarzania		
Osoby zaangażowane w przetwarzanie		
Kategoria przetwarzanych danych		
Cel przetwarzania danych – kontekst		
Podstawa przetwarzania danych		
Adekwatność przetwarzania danych		
Realizacja obsługi praw osób		
Stosowane środki ochronne		
Zagrożenia dla poufności (P) Skala od 0 do 4 = 1 od 5 do 8 = 2 od 9 do 12 = 3	1. nieuprawniony dostęp do pomieszczenia, w którym przetwarzane są dane osobowe;	
	2. ujawnienie haseł dostępu do zasobów z danymi osobowymi;	
	3. nieuprawnione przeniesienie informacji zawierających dane osobowe na inny nośnik;	
	4. utrata nośnika zawierającego dane osobowe;	
	5. klęska żywiołowa, w wyniku której utracono poufność danych osobowych;	
	6. nieuprawnione wyniesienie danych osobowych zawartych na nośniku elektronicznym lub innym;	

	7. udostępnianie danych osobowych osobom nieupoważnionym;	
	8. wejście w posiadanie danych osobowych przez osobę nieuprawnioną;	
	9. pokonanie zabezpieczeń fizycznych lub programowych;	
	10. naprawy i konserwacje systemów lub sieci teleinformatycznej służących do przetwarzania danych osobowych przez osoby nieuprawnione do przetwarzania danych osobowych;	
	11. podsłuch lub podgląd danych osobowych;	
	12. stosowanie korupcji oraz szantażu w celu wydobycia określonych informacji od wybranych pracowników firmy;	
	Stwierdzony poziom zagrożenia dla poufności wg skali od 1 do 3	
Zagrożenia dla integralności (I) **Skala od 0 do 4 = 1** **od 5 do 8 = 2** **od 9 do 12 = 3**	1. nielegalny dostęp do danych osobowych, w tym do stanowiska komputerowego;	
	2. błędy, pomyłki;	
	3. awarie sprzętowe (serwer i inne komponenty);	
	4. awarie oprogramowania;	
	5. brak kopii bezpieczeństwa;	
	6. brak narzędzi, urządzeń i innych składników wspomagających integralność (np. brak archiwum)	
	7. zaniechania organizacyjne personelu;	
	8. uszkodzenie, celowe lub przypadkowe systemu operacyjnego lub urządzeń sieciowych;	

	9. celowe lub przypadkowe uszkodzenie, zniszczenie lub nieuprawniona modyfikacja danych;	
	10. działanie złośliwego oprogramowania (wirusy);	
	11. pożar, zalanie, ekstremalna temperatura, itp.;	
	12. zagrożenia zewnętrzne (np. klęski żywiołowe, atak terrorystyczny).	
	Stwierdzony poziom zagrożenia dla integralności wg skali od 1 do 3	
Zagrożenia dla rozliczalności (R) **Skala od 0 do 4 = 1** **od 5 do 8 = 2** **od 9 do 12 = 3**	1. brak kontroli nad dokumentami wykonywanymi na stanowisku w zakresie ich kopiowania i drukowania;	
	2. brak formalizacji zastępstw pracowniczych;	
	3. możliwość wprowadzenia zmian w treści dokumentu zawierającego dane osobowe;	
	4. błędy oprogramowania lub sprzętu;	
	5. nieprzydzielenie użytkownikom indywidualnych zasobów informacyjnych;	
	6. brak ciągłości w administracji systemem informatycznym;	
	7. brak mechanizmów okresowej kontroli zasad wspierających rozliczalność;	
	8. możliwość zniszczenia lub uszkodzenia danych w sposób zamierzony;	
	9. brak rejestracji udostępnienia danych osobowych;	
	10. możliwość wyłudzenia dostępu do danych (np. podszywanie się pod innego użytkownika);	
	11. przebywanie w strefach przetwarzania osób nieupoważnionych w trakcie lub po pracy;	
	12. wykonywanie pracy w sposób zdalny.	

	Stwierdzony poziom zagrożenia dla rozliczalności wg skali od 1 do 3					
Powaga ryzyka	Poufność (P)		Mnożnik (P) x (I) x (R)		Stwierdzona powaga ryzyka Skala od 1 do 3 = niska od 4 do 8 = średnia od 9 do 18 = wysoka	
	Integralność (I)					
	Roliczalność (R)					
Plan reakcji na ryzyko						
Ryzyko szczątkowe Jeśli mnożnik (P) x (I) x (R) równy 27						
Metoda monitorowania ryzyka						
Konsultacje z UODO						
Podpisy osób uczestniczących w ocenie skutków przetwarzania danych						

Załączniku nr 15 do Polityki – „Wzór rejestru naruszeń bezpieczeństwa".

Lp.																			