POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

w Biurze Rachunkowym E-VAT Ewelina Sikora,
ul.Biała Droga 12e, 34-122 Wieprz

§ 1

Polityka bezpieczeństwa w zakresie ochrony danych osobowych w Biurze Rachunkowym E-VAT Ewelina Sikora, określa zasady przetwarzania danych osobowych oraz środki techniczne i organizacyjne zastosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.
Polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa przetwarzanych danych. Polityka bezpieczeństwa dotyczy danych osobowych przetwarzanych w zbiorach manualnych oraz w systemach informatycznych Biura Rachunkowego E-VAT Ewelina Sikora.

§ 2

Ilekroć w „Polityce Bezpieczeństwa" jest mowa o:
1. **Ustawie** - rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
2. **Danych osobowych** - za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. **Zbiorze danych** - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.
4. **Przetwarzaniu danych** - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.
5. **Usuwaniu danych** - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
6. **Integralności danych** — rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
7. **Poufności danych** — rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.
8. **Rozliczalności** - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
9. **Administratorze Danych Osobowych** - rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydującą o celach i środkach przetwarzania danych osobowych. W Biurze Rachunkowym E-VAT Ewelina Sikora funkcję sprawuje właściciel Ewelina Sikora.
10. **Administratorze Bezpieczeństwa Informacji** - osoba nadzorująca z upoważnienia Administratora Danych Osobowych przestrzeganie stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.
11. **ADO** – Administrator Danych Osobowych
12. **ABI** – Administrator Bezpieczeństwa Informacji
13. **Biuro Rachunkowe E-VAT** – skrót od pełnej nazwy Biuro Rachunkowe e-VAT Ewelina Sikora.

14. **Placówce** – Biuro Rachunkowe E-VAT Ewelina Sikora
15. **Identyfikatorze użytkownika** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym.
16. **Haśle** - rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym.
17. **Systemie informatycznym** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
18. **Zabezpieczeniu danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem

§3

Niniejsza Polityka bezpieczeństwa w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024) została opracowana zgodnie z wytycznymi: 1) rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004r. Nr 100, poz. 1024), 2) ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 z późn. zm.).
Polityka bezpieczeństwa reguluje sprawy ochrony danych osobowych, zawartych w systemach informatycznych oraz w postaci dokumentacji papierowej Biura Rachunkowego e-VAT. Opisane zasady określają granice zachowania użytkowników systemów informatycznych, wspomagających pracę w Biurze Rachunkowym E-VAT.
Dokument zwraca uwagę na konsekwencje, na jakie mogą się narazić osoby naruszające politykę bezpieczeństwa i nieprzestrzegające jej zasad. Zabezpieczenia odpowiednie do zagrożeń, ochrona przetwarzanych danych osobowych oraz niezawodność funkcjonowania są podstawowymi wymogami stawianymi systemom informatycznym.
Polityka bezpieczeństwa w Biurze Rachunkowym E-VAT obowiązuje więc pracowników będących bezpośrednio zatrudnionych przy przetwarzaniu danych osobowych. Dokument ten wskazuje sposób ochrony danych przetwarzanych w sposób tradycyjny oraz środki zabezpieczenia systemów informatycznych, postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.
Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy stwierdzono naruszenie zabezpieczeń systemu informatycznego. Wykonywanie postanowień tego dokumentu ma zapewnić odpowiednią reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemie informatycznym w Biura Rachunkowego E-VAT.

§4

Opis zdarzeń naruszających bezpieczeństwo danych osobowych. Zdarzenia zagrażające bezpieczeństwu danych osobowych podzielono na:

a) zagrożenia zamierzone, świadome i celowe - możliwość naruszenia poufności danych przez nieuprawniony dostęp z zewnątrz lub wewnątrz do systemu informatycznego, przejęcia lub podglądu tych danych przez osoby nieupoważnione,

b) losowe wewnętrzne takie jak: awarie sprzętowe, błędy oprogramowania itd. Istnieje niebezpieczeństwo zniszczenia danych, naruszenia poufności danych,

c) losowe zewnętrzne takie jak: klęski żywiołowe, przerwy w zasilaniu itp.; ich występowanie może prowadzić do utraty integralności danych, zniszczenia i uszkodzenia infrastruktury technicznej systemu, nie dochodzi do naruszenia poufności danych.

Główne zdarzenia naruszające bezpieczeństwo danych osobowych lub zakwalifikowane jako uzasadnione podejrzenie naruszenia to:

1) nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu np.: zalanie pomieszczeń, katastrofa budowlana itp.;

2) nadmierna wilgotność, wysoka temperatura i inne czynniki zewnętrzne,

3) awaria sprzętu lub oprogramowania, wyraźnie wskazujące na ingerencję osób trzecich,

4) komunikaty alarmowe systemu lub innego oprogramowania zaangażowanego w proces utrzymywania bezpieczeństwa zbiorów danych,

5) odstępstwa od oczekiwanego działania urządzeń systemu informatycznego wskazujące na możliwe naruszenie bezpieczeństwa danych,

6) naruszenie integralności systemu,

7) naruszenie struktury danych lub nieuprawniona modyfikacja, przejęcie lub podgląd danych osobowych przez osoby nieupoważnione,

8) naruszenie zabezpieczeń pomieszczeń, szaf, biurek i itp., w których przechowywane są zbiory danych w postaci nośników danych lub dokumentacji papierowej.

§ 5

Celem wdrożenia polityki bezpieczeństwa jest ochrona systemu informatycznego jako całości, jego poszczególnych elementów, przetwarzanych przez system zbiorów danych, obszaru, w którym przetwarzane są dane osobowe, a przede wszystkim zapewnienie technicznych i organizacyjnych uwarunkowań mających wpływ na zarządzanie systemami informatycznymi, w których przetwarzane są dane osobowe.

Polityka bezpieczeństwa zakłada pełne zaangażowanie współpracowników Biura Rachunkowego E-VAT dla zapewnienia bezpieczeństwa danych osobowych, przetwarzanych w sposób tradycyjny oraz za pomocą systemów informatycznych.

Administratorem Danych Osobowych przetwarzanych w Biurze Rachunkowym e-VAT jest właściciel.

Dla skutecznej realizacji zasad i reguł polityki bezpieczeństwa Administrator Danych Osobowych zapewnia:

1) odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne,

2) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,

3) monitorowanie zastosowanych środków ochrony.

Cele Biura Rachunkowego E-VAT w zakresie bezpieczeństwa danych osobowych:

1) ochrona zasobów informacyjnych i zapewnienie ciągłości działania procesów w biurze,

2) zapewnienie zgodności z prawem podejmowanych działań,

3) uzyskanie i utrzymanie odpowiednio wysokiego poziomu bezpieczeństwa zasobów Biura Rachunkowego E-VAT, rozumiane, jako zapewnienie poufności, integralności i dostępności zasobów oraz zapewnienie rozliczalności podejmowanych działań.

§6

Nadrzędną rolą w działaniach Administratora Danych Osobowych, wynikających z jego funkcji, jest ochrona powierzonych danych osobowych. Odpowiedzialność za te dane ponoszą wszyscy pracownicy biura, mający dostęp do danych osobowych w ramach swoich obowiązków służbowych. Zarządzanie bezpieczeństwem danych osobowych jest procesem ciągłym, realizowanym przy współdziałaniu osób upoważnionych do przetwarzania danych z Administratorem Danych Osobowych. Osoby upoważnione do przetwarzania danych osobowych w Biura Rachunkowego E-VAT zobowiązane są do:

1) przetwarzania danych osobowych zgodnie z obowiązującymi przepisami,

2) postępowania zgodnie z polityką bezpieczeństwa placówki,

3) ścisłego przestrzegania zakresu udzielonego upoważnienia, zachowania w tajemnicy danych osobowych, sposobu ich zabezpieczania oraz zapoznanie się z przepisami dotyczącymi ochrony danych osobowych,

4) natychmiastowego zgłoszenia Administratorowi Danych Osobowych lub Administratorowi Bezpieczeństwa Informacji podejrzenia lub stwierdzenia faktu naruszenia bezpieczeństwa danych osobowych przetwarzanych w biurze.

§7

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

1) przetwarzane zgodnie z prawem,

2) zbierane dla oznaczonych celów, zgodnych z prawem,

3) merytorycznie poprawne i adekwatne w stosunku do celów.

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

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

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

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

6. Prowadzi ewidencję osób uprawnionych do przetwarzania danych osobowych w poszczególnych systemach.

7. Organizuje szkolenia mające na celu zapoznanie każdej osoby, przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.

8. Odpowiada za to, by zakres czynności osoby zatrudnionej przy przetwarzania danych osobowych określał odpowiedzialność tej osoby za:

1) ochronę danych przed niepowołanym dostępem,

2) nieuzasadnioną modyfikację lub zniszczenie danych,

3) nielegalne ujawnienie danych w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.

§8

Administrator Bezpieczeństwa Informacji realizuje zadania w zakresie ochrony danych, a w szczególności:

1) ochrony danych osobowych, zawartych w zbiorach systemów informatycznych biura,

2) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa", w przypadku wykrycia nieuprawnionego dostępu do bazy danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,

3) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nich zatrudnionych.

§9

Obowiązki Administratora Bezpieczeństwa Informacji (ABI):

1. Nadzór na przestrzeganiem instrukcji określającej sposób zarządzania systemem informatycznym.
2. Nadzór nad właściwym zabezpieczeniem sprzętu oraz pomieszczeń, w których przetwarzane są dane osobowe.
3. Nadzór na wykorzystywanym w Biurze Rachunkowym E-VAT oprogramowaniem oraz jego legalnością.
4. Przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe.
5. Podejmowanie odpowiednich działań w celu właściwego zabezpieczenia danych.
6. Badanie ewentualnych naruszeń w systemie zabezpieczeń danych osobowych.
7. Podejmowanie decyzji o zainstalowaniu nowych urządzeń oraz oprogramowania wykorzystywanego do przetwarzania danych osobowych.
8. Nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych zawierających dane osobowe.
9. Definiowanie użytkowników i haseł dostępu.
10. Aktualizowanie oprogramowania antywirusowego i innego, chyba że aktualizacje te wykonywane są automatycznie.
11. Nadzór nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności.
12. Wdrożenie szkoleń z zakresu przepisów dotyczących ochrony danych osobowych oraz środków technicznych i organizacyjnych przy przetwarzaniu danych w systemach informatycznych.
13. Prowadzenie ewidencji osób, które zostały zapoznane z niniejszym dokumentem i zobowiązują się do stosowania zasad w nim zawartych wg wzoru stanowiącego załącznik nr 6.
14. Sporządzanie raportów z naruszenia bezpieczeństwa systemu informatycznego.

§10

1. Ewidencja osób posiadających upoważnienie do przetwarzania danych osobowych w podmiocie, zawiera załącznik nr 1
2. Wykaz pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe zawiera załącznik nr 2 do Polityki bezpieczeństwa.
3. Zobowiązanie do zachowania poufności, zawiera załącznik nr 3.
4. Rejestr czynności przetwarzania danych osobowych zawiera załącznik nr 4 do Polityki bezpieczeństwa.

5. Upoważnienie do przetwarzania danych osobowych zawiera załącznik nr 5.

6. Rejestr naruszeń ochrony danych osobowych zawiera załącznik nr 6.

7. Wzór zgłoszenia naruszenia ochrony danych osobowych zawiera załącznik nr 7.

8.Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych zawiera załącznik nr 8.

9. Polityka czystego biurka zawiera załącznik nr 9.

10. Procedura otwierania i zamykania budynku oraz pomieszczeń biurowych zawiera załącznik nr 10.

Załącznik nr 4 - Rejestr czynności przetwarzania danych osobowych

Rejestr czynności przetwarzania danych osobowych

w E-VAT Biurze Rachunkowym Ewelina Sikora, ul. Biała Droga 12e, 34-122 Wieprz

Czynność przetwarzania	obsługa stosunku pracy	obsługa klientów	
Cel przetwarzania	zarządzanie personelem, realizacja uprawnień i obowiązków pracodawcy wynikających z Kodeksu Pracy	realizacja uprawnień i obowiązków wynikających z podpisanych umów	
Podstawa przetwarzania	w zakresie danych, o których mowa w kodeksie pracy: umowa o pracę, w pozostałym zakresie - zgody pracownika.	w zakresie danych, o których mowa w umowie oraz OWU,	
Kategorie osób	Pracownicy zatrudnieni w e-VAT Biurze Rachunkowym, na podstawie umowy o pracę	klienci, z którymi Biuro zawarło umowę świadczenia usług	
kategorie danych	Imię i nazwisko, data urodzenia, PESEL, nr telefonu, e-mail służbowy i prywatny, miejsce zamieszkania	Imię i nazwisko, data urodzenia, PESEL, nr telefonu, e-mail służbowy i prywatny, miejsce zamieszkania, wartość przychodów, podatków,	
Kategorie odbiorców	Właściciel e-VAT Biuro Rachunkowe, dostawca powierzchni dyskowej	Właściciel e-VAT Biuro Rachunkowe, dostawca powierzchni dyskowej	
Sposób przetwarzania danych	papierowo i elektronicznie	papierowo i elektronicznie	
Okres przechowywania danych	Czas trwania stosunku pracy oraz okres archiwizacji i przechowywania dokumentów pracowniczych wymagany przepisami prawa	Czas trwania stosunku pracy oraz okres archiwizacji i przechowywania dokumentów pracowniczych wymagany przepisami prawa	
Stosowane środki bezpieczeństwa			

Załącznik - nr 2 do Polityki Bezpieczeństwa danych osobowych

Wykaz pomieszczeń oraz części pomieszczeń, w których przetwarzane są dane osobowe

w E-VAT Biurze Rachunkowym Ewelina Sikora, ul. Biała Droga 12e, 34-122 Wieprz

1. ……..
2. …….
3. …….
4. …….
5. …….
6. …….

Załącznik nr 1 - Do Polityki bezpieczeństwa danych osobowych

Wieprz, dnia……..

Ewidencja osób upoważnionych do przetwarzania danych osobowych

w E-VAT Biurze Rachunkowym Ewelina Sikora, ul. Biała Droga 12e, 34-122 Wieprz

1. Imię i nazwisko……..……data……podpis……..……
2. Imię i nazwisko……..……data……podpis……..……
3. Imię i nazwisko……..……data……podpis……..……
4. Imię i nazwisko……..……data……podpis……..……
5. Imię i nazwisko……..……data……podpis……..……
6. Imię i nazwisko……..……data……podpis……..……
7. Imię i nazwisko……..……data……podpis……..……
8. Imię i nazwisko……..……data……podpis……..……
9. Imię i nazwisko……..……data……podpis……..……
10. Imię i nazwisko……..……data……podpis……..……

Załącznik nr 3 – Wzór zobowiązania do zachowania poufności

Wieprz, dnia……

Pracownik: [Dane pracownika]

Zobowiązanie do zachowania poufności

w E-VAT Biurze Rachunkowym Ewelina Sikora, ul. Biała Droga 12e, 34-122 Wieprz

Oświadczam, że w związku z wykonywaniem obowiązków służbowych na rzecz Biura Rachunkowego E-VAT Ewelina Sikora oraz udzielonym mi upoważnieniem do przetwarzania danych osobowych:

(i) zostałem/am poinformowany/a o zasadach przetwarzania i ochrony danych osobowych w E-VAT Biurze Rachunkowym Ewelina Sikora, w tym o:

(a) treści Polityki ochrony danych osobowych z dnia 25.05.2018 r.

(b) procedurach oraz regulacjach dotyczących ochrony danych osobowych obowiązujących w E-VAT Biurze, w tym:

− Polityką czystego biurka z dnia 02.12.2024 r.,

− [•];

(c) przepisach dotyczących ochrony tajemnicy zawodowej doradcy podatkowego,

(d) zasadach ochrony danych osobowych wynikających z postanowień bezwzględnie obowiązującego prawa, w szczególności wynikających z 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);

(ii) treść informacji oraz regulacji, o których mowa w pkt (i) wyżej, oraz nałożonych na mnie na mocy Polityki obowiązków jest dla mnie jasna i zrozumiała.

W związku z powyższym zobowiązuje się do:

(i) niezwłocznego zastosowania się do nałożonych na mnie obowiązków w zakresie ochrony danych osobowych;

(ii) zapewnienia ochrony, poufności oraz integralności danych osobowych przetwarzanych w zbiorach przez E-VAT Biuro, w szczególności do zapewnienia należytego bezpieczeństwa danych osobowych przed ich ujawnieniem lub udostępnieniem (nawet przypadkowym) osobom trzecim i osobom nieuprawnionym, jak również przed ich nieuprawnionym lub przypadkowym uszkodzeniem, utratą lub zmodyfikowaniem,

(iii) zachowania tajemnicy i poufności dotyczącej wszelkich informacji przetwarzanych w toku zatrudnienia w Biurze E-VAT, w tym także po zaprzestaniu wykonywania prac;

(iv) zachowania w tajemnicy wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych w Biurze e-VAT;

(v) niezwłocznego zgłaszania przełożonemu wszelkich naruszeń ochrony danych osobowych, jak również wszelkich zaobserwowanych prób lub faktów naruszenia zabezpieczeń pomieszczeń lub systemów informatycznych.

Pracownik _____ (data i podpis)

Załącznik nr 5 – Wzór Upoważnienia do przetwarzania danych osobowych

Wieprz, dnia……..

Pracownik: [Dane pracownika]

Upoważnienie Pracownika do przetwarzania danych osobowych

w E-VAT Biurze Rachunkowym Ewelina Sikora, ul. Biała Droga 12e, 34-122 Wieprz

Działając w imieniu E-VAT Biuro Rachunkowe Ewelina Sikora, na podstawie art. 29 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) (zwanego dalej RODO) – nadaję:

[Imię i nazwisko upoważnionego],

zatrudnionemu na stanowisku: [Stanowisko]

upoważnienie do przetwarzania danych osobowych w zakresie pełnionych obowiązków służbowych na zajmowanym stanowisku, tj. uzyskuje Pani/Pan upoważnienie do przetwarzania danych osobowych w zakresie [Opis zakresu dostępu do danych osobowych, np. bez ograniczeń, pogląd danych osobowych, wprowadzanie i opracowywanie danych, usuwanie danych].

Upoważnienie obejmuje przetwarzanie danych osobowych:

(i) przetwarzanych na nośnikach papierowych;

(ii) przetwarzanych w systemach informatycznych:

(a) [•],

(b) [•];

(iii) Dane osobowe objęte Zbiorami danych:

(a) [•],

(b) [•].

Upoważnienie obejmuje uprawnienie do przetwarzania danych osobowych w okresie zatrudnienia.

Jednocześnie zobowiązuję Panią/Pana do przetwarzania danych osobowych, zgodnie z udzielonym upoważnieniem oraz z przepisami RODO, Ustawy z dnia [Data Ustawy, po jej uchwaleniu] o ochronie danych osobowych, Kodeksu pracy, a także z Polityką ochrony danych osobowych Pracodawcy.

Jednocześnie upoważniam Panią/Pana do tworzenia/posiadania dla potrzeb wykonywanej pracy zestawień, ewidencji oraz rejestrów z danymi osobowymi, z zachowaniem pełnej ich ochrony przy zastosowaniu środków technicznych i organizacyjnych wdrożonych u Pracodawcy.

Właściciel _____ [Data i podpis]

Załącznik nr 6 - Rejestr naruszeń ochrony danych osobowych

Lp.	Opis naruszenia	Data zajścia naruszenia	Kategoria osób, których dotyczy naruszenie	Zakres danych, których dotyczy naruszenie	Okoliczności naruszenia - opis charakteru naruszenia, analiza, zdarzenia, przyczyny wystąpienia	Opis skutków / konsekwencji naruszenia	Podjęte działania - opis środków zastosowanych lub proponowanych do wdrożenia w celu zaradzeniu naruszenia, w tym zastosowane środki w celu zminimalizowania jego negatywnych skutków	Rezultat działań naprawczych

Załącznik nr 7 - Wzór zgłoszenia naruszenia ochrony danych osobowych

Wieprz, dnia …….

E-VAT Biuro Rachunkowe Ewelina Sikora

Prezes Urzędu Ochrony Danych Osobowych
[Adres organu]

Zgłoszenie naruszenia ochrony danych osobowych

Działając w imieniu e-VAT Biuro Rachunkowe Ewelina Sikora z siedzibą w Wieprzu, w oparciu o przyznane mi uprawnienia oraz na podstawie art. 33 ust. 1 i 3 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), niniejszym zgłaszam następujące naruszenie ochrony danych osobowych:

Administrator Danych Osobowych oraz dane kontaktowe naruszenia:	
Data zaistnienia naruszenia:	
Kategorie i przybliżoną liczbę osób, których dane dotyczą:	
Kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie:	
Opisywać możliwe konsekwencje naruszenia ochrony danych osobowych:	
Opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych	

_____

[Podpis osoby upoważnionej]

Załącznik nr 8 - Instrukcja zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM, SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

w Biurze Rachunkowym E-VAT Ewelina Sikora,
ul.Biała Droga 12e, 34-122 Wieprz

§1

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. 2014 poz. 1182 z późn. zm.), Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024) nakłada na Administratora Danych Osobowych następujące obowiązki:

1) zapewnienie bezpieczeństwa i poufności danych, w tym zabezpieczenie ich przed ujawnieniem,

2) zabezpieczenie danych przed nieuprawnionym dostępem,

3) zabezpieczenie danych przed udostępnieniem osobom nieupoważnionym (nieuprawnionym pozyskaniem),

4) zabezpieczenie przed utratą danych,

5) zabezpieczenie przed uszkodzeniem lub zniszczeniem danych oraz przed ich nielegalną modyfikacją.

Ochronie podlegają dane osobowe, niezależnie od formy przechowywania, sprzęt komputerowy, systemy operacyjne i informatyczne oraz pomieszczenia, w których odbywa się proces przetwarzania.

Zawarte w instrukcji procedury i wytyczne są przekazywane osobom odpowiedzialnym za ich realizację stosownie do przyznanych uprawnień i zakresu obowiązków. Instrukcja określa ramowe zasady właściwego zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i system informatyczny, odpowiednie do zagrożeń i kategorii danych objętych ochroną.

§2

1. Celem instrukcji jest określenie sposobu zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.

2. Instrukcja Zarządzania Systemem Informatycznym, służącym do przetwarzania danych osobowych w Biurze Rachunkowym E-VAT, zwaną dalej instrukcją - określa sposób zarządzania oraz zasady administrowania systemem informatycznym, służącym do przetwarzania danych osobowych. Ilekroć w instrukcji jest mowa o:

1) biurze - rozumie się przez to Biuro Rachunkowe E-VAT Ewelina Sikora

2) kierowniku jednostki - rozumie się przez to właścicielu

3) danych osobowych - rozumie się przez to każdą informację, dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby,

4) zbiorze danych - rozumie się przez to każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony czy podzielony funkcjonalnie,

5) przetwarzaniu danych - rozumie się przez to jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,

6) usuwaniu danych - rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

7) Administratorze Danych Osobowych (ADO) - rozumie się przez to osobę odpowiedzialną w danej jednostce organizacyjnej za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane są dane osobowe oraz za podejmowanie odpowiednich działań w wypadku naruszeń w systemie zabezpieczeń. Funkcję ADO pełni właściciel,

8) Administratorze Bezpieczeństwa Informacji – rozumie się przez to osobę nadzorującą, (upoważnioną przez ADO), przestrzeganie stosowania środków technicznych i organizacyjnych, zapewniających ochronę przetwarzania danych osobowych w sposób odpowiedni do zagrożeń oraz kategorii danych objętych ochroną.

9) Administratorze Sieci/Systemu Operacyjnego - rozumie się przez to osobę nadzorującą i odpowiadającą za poprawną pracę powierzonego mu sprzętu sieciowego oraz systemu operacyjnego w danej jednostce organizacyjnej, w tym w szczególności:

a) mającą prawo do zmiany uprawnień wszystkich użytkowników,

b) za pomocą platformy zarządzania, dysponującą bezpośrednio wszystkimi zasobami podległej mu sieci,

c) pełniącą kontrolę nad dostępem użytkowników do systemów,

d) podejmującą samodzielnie lub na polecenie Administratora Bezpieczeństwa Informacji odpowiednie działania w wypadku naruszeń w systemie zabezpieczeń

e) funkcję tą pełni właściciel Biura Rachunkowego E-VAT.

9. Administratorze Aplikacji - rozumie się przez to osobę odpowiedzialną w danej jednostce organizacyjnej za bezpieczeństwo przetwarzania danych w ramach aplikacji, w tym administrującą prawami dostępu w ramach eksploatowanych aplikacji,

10. Użytkownikach systemu - rozumie się osoby upoważnione do przetwarzania danych osobowych w systemie informatycznym,

11. Obszarze kontrolowanym – rozumie się przez to obszar znajdujący się pod ochroną, o ograniczonym dostępie osób nieautoryzowanych, w którym odbywa się przetwarzanie danych, w tym danych osobowych.

§3

Niniejsza Instrukcja Zarządzania Systemem Informatycznym określa:

1) poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym,

2) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym,

3) stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem,

4) sposób przydziału haseł dla użytkowników i częstotliwość ich zmiany oraz osoby odpowiedzialne za te czynności,

5) procedury rozpoczęcia, zawieszenia i zakończenia pracy, przeznaczone dla użytkowników systemu;

6) metodę i częstotliwość tworzenia kopii awaryjnych.

7) metodę i częstotliwość sprawdzania obecności wirusów komputerowych oraz metodę ich usunięcia,

8) sposób, miejsce i okres przechowywania:

a) elektronicznych nośników informacji zawierających dane osobowe;

b) kopii zapasowych,

9) sposobu dokonywania przeglądów i konserwacji systemu i zbioru danych osobowych,

10) sposobu postępowania w zakresie komunikacji w sieci komputerowej,

11)procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych.

§4

Zasady nadawania i rejestrowania uprawnień do przetwarzania danych osobowych wraz ze wskazaniem osób odpowiedzialnych w tym zakresie właściciel Biura Rachunkowego E-VAT upoważnia pracowników do przetwarzania danych osobowych do niniejszej instrukcji. Upoważnienia do przetwarzania danych osobowych przechowywane są w teczkach akt osobowych pracowników oraz prowadzona jest ich ewidencja.

§5

Stosowane metody i środki uwierzytelnienia:

1) W systemach oraz programach komputerowych służących do przetwarzania danych osobowych stosowane jest uwierzytelnianie pracownika przy pomocy jego identyfikatora i hasła.

2) Pracownicy nie mogą używać tych samych identyfikatorów, ani wymieniać się identyfikatorami.

3) Identyfikator pracownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.

4) Hasło użytkownika bazy danej składa się z 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne.

5) Pracownik jest zobowiązany zmienić hasło, o ile system na to pozwala, co najmniej raz na 90 dni.

6) Każdy pracownik zarządza swoimi hasłami.

7) Hasło pracownika jest jego własnością i zna je wyłącznie dany pracownik oraz właściciel Biura Rachunkowego E-VAT.

8) Niedopuszczalne jest podglądanie haseł wprowadzanych do systemu przez innych pracowników. Jeżeli pracownik w pobliżu zaczyna wprowadzać hasło należy odwrócić wzrok.

§6

Zasady korzystania z systemu przez użytkowników (rozpoczęcia, zawieszenia i zakończenia pracy):

1) Rozpoczęcie pracy użytkownika w systemie informatycznym następuje po poprawnym uwierzytelnieniu (zalogowaniu się do systemu).

2) Rozpoczęcie pracy w aplikacji musi być przeprowadzone zgodnie z instrukcją zawartą w dokumentacji aplikacji.

3) Zakończenie pracy użytkownika następuje po poprawnym wylogowaniu się z systemu oraz poprzez uruchomienie odpowiedniej dla danego systemu opcji jego zamknięcia zgodnie z instrukcją zawartą w dokumentacji.
Niedopuszczalne jest zakończenie pracy w systemie bez wykonania pełnej i poprawnej operacji wylogowania z aplikacji i poprawnego zamknięcia systemu.

4) Monitory stanowisk komputerowych znajdujące się w pomieszczeniu, gdzie przebywają osoby, które nie posiadają uprawnień do przetwarzania danych osobowych, należy ustawić w taki sposób, aby uniemożliwić osobom postronnym wgląd w dane. Krzesło interesanta ustawione jest w taki sposób, by nie mógł patrzeć na ekran monitora.

5) Pomieszczenia, w których przetwarzane są dane osobowe należy zamykać na czas nieobecności osób zatrudnionych, w sposób uniemożliwiający dostęp do nich osobom trzecim.

§7

Środki stosowane do zabezpieczenia systemu informatycznego:

1) Na wszystkich stacjach roboczych oraz serwerach zainstalowane jest oprogramowanie antywirusowe.

2) Elektroniczne nośniki informacji należy każdorazowo sprawdzić programem antywirusowym przed użyciem, po zainstalowaniu ich w systemie.

3) W przypadku, gdy użytkownik stanowiska komputerowego zauważy komunikat oprogramowania zabezpieczającego system wskazujący na zaistnienie zagrożenia, zobowiązany jest zaprzestać jakichkolwiek czynności w systemie i niezwłocznie skontaktować się z ADO.

4) Zabrania się użytkownikom komputerów wyłączania, blokowania, odinstalowywania programów zabezpieczających komputer przed oprogramowaniem złośliwym oraz nieautoryzowanym dostępem.
Wszyscy pracownicy poinformowani są o zakazie instalowania nielegalnego oprogramowania.

§8

Udostępnianie danych osobowych instytucjom może odbywać się wyłącznie na pisemny uzasadniony wniosek, zgodnie z przepisami prawa.

§9

Zasady dokonywania przeglądów i konserwacji systemów oraz nośników informacji:

1) Przeglądy i konserwacje systemów oraz zbiorów danych wykonuje ADO na bieżąco.

2) Umowy dotyczące instalacji i konserwacji sprzętu należy zawierać z podmiotami, których kompetencje nie budzą wątpliwości, co do wykonania usługi. Naprawa sprzętu, na którym mogą znajdować się dane osobowe powinna odbywać się pod nadzorem osób użytkujących sprzęt w miejscu jego użytkowania.

3) W przypadku konieczności naprawy poza miejscem użytkowania sprzęt komputerowy przed oddaniem do serwisu powinien być odpowiednio przygotowany. Dane należy archiwizować na nośniki informacji, a dyski twarde wymontowywać na czas naprawy.

Załącznik nr 9 – Polityka czystego biurka

Polityka czystego biurka

Polityka obejmuje wszystkich pracowników oraz współpracowników Biura Rachunkowego E-VAT Ewelina Sikora. Nadzór nad wykonywaniem polityki powierza się właścicielowi.

Polityka Czystego Biurka

1. Polityka reguluje wymagania oraz procedury ochrony danych poufnych, w tym danych osobowych przetwarzanych w Biura Rachunkowego E-VAT Ewelina Sikora przez współpracowników w formie papierowej, w tym:

a. dokumentów papierowych;

b. korespondencji listownej;

c. akt sprawy;

d. dokumentów źródłowych przekazanych przez klientów E-VAT Biura;

e. korespondencji urzędowej.

2. Ilekroć w Polityce zostaną wykorzystane następujące definicje i zwroty, należy nadawać im następujące znaczenie:

a. Polityka – oznacza niniejszą Politykę Czystego Biurka wraz ze wszystkimi ewentualnymi załącznikami;

b. Pracownik – oznacza zarówno każdą osobę fizyczną zatrudnioną w Biurze Rachunkowym E-VAT na podstawie umowy o pracę, jak również współpracującą z Biurem Rachunkowym E-VAT na podstawie umowy cywilnoprawnej (w tym w zakresie prowadzonej jednoosobowej działalności gospodarczej) oraz studenta lub ucznia niebędących pracownikami Biurze Rachunkowym E-VAT w trakcie odbywania praktyk lub stażu zawodowego;

c. Biurze Rachunkowym E-VAT – oznacza Biuro Rachunkowe E-VAT Ewelina Sikora

3. Polityka obowiązuje wszystkich Pracowników Biurze Rachunkowym E-VAT, niezależnie od zajmowanego stanowiska i czasu zatrudnienia w Biurze Rachunkowym E-VAT.

4. Każdy Pracownik zobowiązany jest do ograniczenia dostępu osób postronnych do danych poufnych, w tym danych osobowych zawartych na nośnikach papierowych wykorzystywanych przez Pracownika przy wykonywaniu obowiązków służbowych.

5. W toku pracy każdy Pracownik zobowiązany jest do przechowywania na biurku lub przy stanowisku pracy tylko tych dokumentów, które są Pracownikowi niezbędne do wykonania bieżących zadań w danym momencie pracy. Jeżeli dane dokumenty nie będą już pracownikowi niezbędne do wykonania bieżących zadań, Pracownik zobowiązany jest do ich odłożenia. Postanowienia ust. 6 niżej stosuje się odpowiednio.

6. W przypadku opuszczenia przez pracownika – choćby chwilowo – biurka lub stanowiska pracy Pracownik zobowiązany jest do odłożenia i schowania wszystkich wykorzystywanych dokumentów zawierających dane poufne lub dane osobowe do zamykanej szuflady lub szafy, celem uniemożliwienia dostępu do dokumentów osobom postronnym.

7. W przypadku zakończenia przez Pracownika pracy w danym dniu, Pracownik jest obowiązany przed opuszczeniem siedziby Biurze Rachunkowym E-VAT do wykonania obowiązku, o którym mowa w ust. 6 wyżej oraz do zabezpieczenia dokumentów przed

dostępem jakichkolwiek osób postronnych. Po zakończonej pracy na biurku mogą znajdować się jedynie telefon stacjonarny i przybory biurowe.

8. Pracownik zobowiązany jest zapewnić, aby w toku pracy przy stanowisku pracy nie znajdowały się płyny lub inne substancje grożące zniszczeniem lub uszkodzeniem dokumentacji papierowej przy ich rozlaniu. Na tej samej podstawie Pracownik zobowiązany jest do powstrzymania się od spożywania posiłków przy biurku lub stanowisku pracy.

9. Niezależnie od postanowień ust. 4-8 wyżej, po zakończonej pracy Pracownik zobowiązany jest odłożyć laptop służbowy do zamykanej na klucz szafy, celem uniemożliwienia dostępu do danych zapisanych na komputerze służbowym osobom postronnym.

10. Jeżeli dany dokument nie będzie już wykorzystywany w Biurze Rachunkowym E-VAT, jak również w sytuacjach określonych w Polityce Ochrony Danych Osobowych z dnia 01.12.2024 r., Pracownik zobowiązany jest do zapewnienia niezwłocznego zniszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, o ile Polityka Ochrony Danych Osobowych z dnia 01.12.2024 r. nie przewiduje innego sposobu zadysponowania dokumentów lub nie nakazuje jego pozostawienia lub archiwizacji.

Załącznik nr 10 – Procedura otwierania i zamykania budynku oraz pomieszczeń biurowych

W Biurze Rachunkowym E-VAT z dniem 01.12.2024 r. wprowadza się procedurę otwierania i zamykania budynku oraz pomieszczeń biurowych położonych przy ul. Biała Droga 12e,, zwaną dalej „Polityką kluczy".
Nadzór nad wykonywaniem polityki powierza się……

Procedura otwierania i zamykania budynków oraz pomieszczeń biurowych

1) Procedura otwierania i przebywania w budynku

a) Siedzibą Biurze Rachunkowym E-VAT jest lokal biurowy znajdujący się przy ul.Biała Droga 12e, zwany dalej: Lokalem.

b) Do otwierania oraz zamykania Lokalu uprawnione są osoby wskazane w Załączniku nr 1 do Procedury.

c) W razie niemożności otwarcia lub zamknięcia pomieszczeń biurowych, pracownik niezwłocznie zawiadamia o tym fakcie Właściciela.

d) W pomieszczeniach biurowych, podczas godzin pracy, gdzie przebywa tylko jeden pracownik, jest on zobowiązany do każdorazowego zamknięcia pomieszczenia w przypadku jego opuszczenia.

e) Przebywanie pracowników w Lokalu po godzinach pracy powyżej 30 minut od zakończenia pracy jest niedozwolone, z zastrzeżeniem lit. f) oraz g) niżej.

f) Przebywanie pracowników w Lokalu po godzinach pracy lub dni wolne od pracy jest dopuszczalne za zgodą wyrażoną na piśmie lub na podstawie pisemnego polecenia służbowego członka Zarządu.

g) Od wymogów określonych w lit.

e) wyżej zwolnieni są: i) Właściciel, ii) inne osoby upoważnione pisemnie przez Właściciela.

2) Procedura zamykania budynku i pomieszczeń.

a) Po zakończeniu pracy pracownicy mają obowiązek zamknąć pomieszczenia na klucz.

b) Zamknięcie Lokalu następuje nie później niż o godzinie 18.00. W uzasadnionych przypadkach, za zgodą Właściciela lub osoby go zastępującej godzina zamknięcia może ulec zmianie.

3) Procedura przechowywania i dysponowania kluczami.

a) Osoby dysponujące kluczami zobowiązane są do odpowiedniego zabezpieczenia kluczy przed ich zgubieniem i kradzieżą.

b) W przypadku zagubienia, zaginięcia klucza lub stwierdzenia jego braku pracownik zgłasza ten fakt natychmiast Właścicielowi i w razie konieczności wydania kluczy zapasowych składa w tej sprawie wniosek.

c) Wydawanie kluczy zapasowych pracownikowi może odbywać tylko w uzasadnionych sytuacjach za zgodą Właściciela.

d) Zabrania się pracownikom samodzielnego dorabiania kluczy do Lokalu i pomieszczeń biurowych.

e) Zabrania się pozostawiania kluczy w zamkach od drzwi podczas obecności i nieobecności pracownika w pomieszczeniu biurowym.

f) Zabrania się udostępniania kluczy osobom nieupoważnionym.

4) Upoważnienia

a) Osoby wyszczególnione w Załączniku nr 1 do Procedury otrzymują stosowne upoważnienia do posiadania kluczy. Wzór upoważnienia stanowi Załącznik nr 2 do Procedury.

b) Upoważnienia wpina się do segregatora upoważnień, który znajduje się w biurze.

5) Postanowienia końcowe

a) Do Procedury dołączono następujące Załączniki:

i) Załącznik nr 1 - Wykaz osób uprawnionych;

ii) Załącznik nr 2 – Wzór upoważnienia do posiadania kluczy

Załącznik nr 1 - do Procedury otwierania i zamykania budynku oraz pomieszczeń biurowych

Wykaz osób uprawnionych do otwierania i zamykania budynku oraz pomieszczeń biurowych

Część 1 Wykaz osób stale uprawnionych do otwierania i zamykania Lokalu

Następujące osoby posiadają stały dostęp do Lokalu :

(i) ……..

(ii) …….

(iii) ……

Załącznik nr 2 - do Procedury otwierania i zamykania budynku oraz pomieszczeń biurowych

Wieprz, dnia …….

Upoważnienie do posiadania kluczy

Działając w imieniu Biuro Rachunkowe E-VAT Ewelina Sikora niniejszym upoważniam Pracownika ……. do stałego/czasowego posiadania kompletu kluczy głównych do Lokalu w ilości…….... sztuk.

Pracownik zobowiązany jest do odpowiedniego zabezpieczenia kluczy przed zgubieniem i kradzieżą.

_____

[Data i podpis Właściciela]

Niniejszym potwierdzam zapoznanie się z treścią upoważnienia oraz zobowiązania, jak również otrzymanie kluczy w ilości……. sztuk.

_____

[Data i podpis Pracownika]