INSTRUKCJA ZARZĄDZANIA
SYSTEMEM INFORMATYCZNYM
PRZETWARZAJĄCYM DANE OSOBOWE
W FIRMIE

SŁAWOMIR PIWOWARCZYK
KAMIENICA 65, 32-075 GOŁCZA
NIP: 678 262 88 45, REGON: 356 287 951

.....	.....	.....
pieczęć firmowa	podpis administratora danych osobowych	data

Wstęp

Realizując konstytucyjne prawo każdej osoby do ochrony życia prywatnego oraz postanowienia ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182 ze zm.), jak również wydane w oparciu o delegacje ustawową rozporządzenia wykonawcze do ww. ustawy, w celu zastosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, wprowadza się następujący zestaw procedur, stanowiący Instrukcję zarządzania systemem informatycznym przetwarzającym dane osobowe.

Rozdział 1
Postanowienia ogólne

§ 1

Ilekroć w Instrukcji jest mowa o:

1. **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2014 r., poz. 1182 ze zm.);
2. **danych osobowych** – rozumie się przez to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań;
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. **systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
6. **zabezpieczeniu danych** w systemie informatycznym – rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
7. **usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
8. **administratorze danych** – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, decydujące o celach i środkach przetwarzania danych osobowych;
9. **administratorze systemu** – rozumie się przez to osobę zarządzającą systemem informatycznym przetwarzającym dane osobowe;

10. **użytkowniku systemu** – rozumie się przez to osobę, której został przydzielony przez administratora systemu indywidualny identyfikator w systemie informatycznym w powiązaniu z niezbędnymi uprawnieniami dostępowymi w tym systemie;
11. **elektronicznym nośniku** – rozumie się przez to elektroniczne urządzenie, na którym przechowuje się dane osobowe w celu jego ponownego odtworzenia w systemie informatycznym;
12. **zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie;
13. **odbiorcy danych** – rozumie się przez to każdego, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, przedstawiciela, o którym mowa w art. 31a ustawy, podmiotu, o którym mowa w art. 31 ustawy, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
14. **państwie trzecim** – rozumie się przez to państwo nienależące do Europejskiego Obszaru Gospodarczego;
15. **obszarze przetwarzania danych** – należy przez to rozumieć wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
16. **wykazie zbiorów** – należy przez to rozumieć wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
17. **opisie struktury zbiorów** – należy przez to rozumieć opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
18. **opisie przepływu danych** – należy przez to rozumieć opis sposobu przepływu danych pomiędzy poszczególnymi systemami informatycznymi;
19. **środkach technicznych i organizacyjnych** – należy przez to rozumieć środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Rozdział 2
Procedura nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności

§ 2

Uwzględniając kategorie przetwarzanych danych oraz zagrożenia bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym, zastosowano poziom bezpieczeństwa wysoki.

§ 3

Osobą odpowiedzialną za nadawanie uprawnień w systemie informatycznym jest administrator danych.

§ 4

Procedura nadawania, modyfikowania i odbierania uprawnień użytkownikowi w systemie informatycznym obejmuje w kolejności:

1. zapoznanie osoby z przepisami dotyczącymi ochrony danych osobowych oraz procedurami bezpieczeństwa systemu informatycznego;
2. nadanie upoważnienia do przetwarzania danych osobowych oraz odebranie oświadczenia o zachowaniu poufności danych osobowych i przestrzeganiu wewnętrznej dokumentacji ochrony danych osobowych;

3. zwrócenie się z wnioskiem do administratora systemu o nadanie uprawnień w systemie informatycznym w niezbędnym zakresie;
4. nadanie uprawnienia w systemie informatycznym w niezbędnym zakresie, po zweryfikowaniu przez administratora systemu treści upoważnienia do przetwarzania danych osobowych lub innej podstawy prawnej pozwalającej na przydzielenie uprawnień;
5. modyfikacja i odbieranie uprawnień użytkownika w systemie informatycznym zgodnie z procedurą opisaną w pkt 3–4.

§ 5

Procedura rejestrowania uprawnień użytkownika w systemie informatycznym jest przeprowadzana przez administratora tego systemu i obejmuje w kolejności:

1. przypisanie indywidualnego identyfikatora użytkownika w systemie informatycznym do konkretnej osoby, przy zapewnieniu, że identyfikator ten nie był wcześniej przydzielony innemu użytkownikowi, wraz z datą przyznania i odebrania uprawnień;
2. przypisanie zakresu przydzielonych uprawnień w systemie informatycznym do konkretnego identyfikatora użytkownika.

Rozdział 3
Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

§ 6

W zakresie uwierzytelniania użytkownika w systemie informatycznym zastosowano identyfikator i hasło.

§ 7

Hasło zastosowane do uwierzytelnienia użytkownika w systemie informatycznym składa się z co najmniej 8 znaków, w tym musi zawierać małe i duże litery oraz liczbę lub znak specjalny. Hasło jest zmieniane w cyklach nie dłuższych niż 30 dni.

§ 8

Zmiana hasła dokonywana jest przez użytkownika manualnie.

§ 9

Hasło zastosowane do uwierzytelnienia administratora systemu w systemie informatycznym składa się z co najmniej 8 znaków, w tym musi zawierać małe i duże litery oraz liczbę lub znak specjalny. Każdorazowe użycie konta administratora systemu jest odnotowywane w tym systemie w formie logów dostępowych. Hasło jest zmieniane w cyklach nie dłuższych niż 6 miesięcy.

§ 10

Użytkownicy systemów informatycznych są zapoznawani z zagrożeniami wynikającymi ze stosowania haseł jako formy ich uwierzytelniania w systemie informatycznym.

Rozdział 4
Procedury rozpoczęcia, zawieszenia i zakończenia pracy użytkowników systemu informatycznego

§ 11

Przed rozpoczęciem pracy w systemie informatycznym użytkownik weryfikuje bezpieczeństwo treści wyświetlanych na ekranie ze względu na przebywanie osób nieupoważnionych w obszarze przetwarzania.

§ 12

Przed przerwaniem pracy w systemie informatycznym i tymczasowym odejściem od punktu dostępowego systemu informatycznego użytkownik blokuje swój dostęp poprzez manualne uruchomienie wygaszacza ekranu chronionego hasłem.

§ 13

Po zakończeniu pracy w systemie informatycznym użytkownik zamyka system informatyczny, do którego ma dostęp.

Rozdział 5
Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

§ 14

Kopie zapasowe danych są tworzone z centralnego zasobu (serwera plików) w następujących cyklach: kopia całościowa wykonywana raz w miesiącu.

§ 15

Kopie wykonywane na dysk zewnętrznym lub nośniku elektronicznym typu pendrive. W przypadku zużycia lub uszkodzenia nośnika zewnętrznego lub elektronicznego, należy uszkodzony nośnik zutylizować w sposób uniemożliwiający odczytanie danych na nim zawartych.

Rozdział 6
Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe

§ 16

W przypadku korzystania z elektronicznych nośników zawierających dane osobowe, w szczególności takich jak płytki CD/DVD/BR, Pendrive, Karty SD, zewnętrzne dyski twarde, taśmy magnetyczne, są one przechowywane w sposób uniemożliwiający do nich dostęp osobom nieupoważnionym.

§ 17

W celu usunięcia danych osobowych z elektronicznego nośnika danych użytkownicy stosują metodę trzykrotnego nadpisania pełnej zawartości nośnika danymi niezawierającymi danych osobowych.

§ 18

W przypadku zużycia lub uszkodzenia elektronicznego nośnika zawierającego kopie zapasowe, w celu jego utylizacji uszkadza się go mechanicznie w taki sposób, aby odtworzenie danych było niemożliwe.

Rozdział 7
Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

§ 19

W systemie informatycznym zostało zainstalowane automatycznie aktualizujące się oprogramowanie antywirusowe: **Microsoft Security Essentials/Windows Defender.**

§ 20

Na styku sieci wewnętrznej z siecią publiczną zastosowano zaporę ogniową: systemowa w ramach programu antywirusowego **Microsoft Security Essentials/Windows Defender oraz zapora sieciowa na routerze D-Link.**

§ 21

Użytkownicy systemu niezwłocznie informują administratora systemu o zagrożeniach monitowanych przez oprogramowanie antywirusowe.

Rozdział 8
Sposób odnotowania informacji o odbiorcach danych, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

§ 22

Administrator danych udostępnia dane odbiorcom danych samodzielnie tj. z pominięciem przyznawania dostępu odbiorcom danych do systemu informatycznego administratora danych.

Rozdział 9
Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych

§ 23

Administrator systemu informatycznego prowadzi okresowe przeglądy systemu informatycznego w celu określania ich poziomu sprawności, biorąc pod uwagę racjonalne wykorzystanie sprzętu oraz bezpieczeństwo danych przetwarzanych z jego wykorzystaniem.

§ 24

Administrator systemu przeprowadza ww. przegląd nie rzadziej niż raz na 5 lat.

§ 25

W przypadku konieczności dokonania naprawy elementu infrastruktury systemu informatycznego przez osobę nieupoważnioną (np. zewnętrzny serwis informatyczny), wszelkie czynności dokonywane są pod bezpośrednim nadzorem osób upoważnionych.

Rozdział 10
Postanowienia końcowe

§ 26

Wszelkie zasady opisane w niniejszej Instrukcji są przestrzegane przez użytkowników i administratorów systemów ze szczególnym uwzględnieniem dobra osób, których dane te dotyczą.

§ 27

Instrukcja obowiązuje od dnia jej zatwierdzenia przez administratora danych.