Załącznik nr 1
Rejestr czynności przetwarzania danych osobowych

Rejestr czynności przetwarzania danych osobowych							
	Nazwa administratora danych lub podmiotu przetwarzającego				Akademia Kodu Michał Makaruk		
	Nazwa przedstawiciela administratora lub podmiotu przetwarzającego				Michał Makaruk		
	Współadministratorzy						
	Inspektor ochrony danych osobowych				Michał Makaruk		
	Cel przetwarzania	Opis kategorii osób	Kategorie odbiorców	Kategorie danych osobowych	Informacje o przekazaniu do państwa trzeciego lub organizacji międzynarodowej	Planowany termin usunięcia danych osobowych	Opis technicznych i organizacyjnych środków bezpieczeństwa
1	Realizowanie zamówień Użytkownika						
2	Nawiązywanie kontaktów z Użytkownikiem						
3	Zapewnienie wsparcia dla produktów i usług uzyskiwanych przez Użytkownika						
4	Realizowanie działań marketingowych (jeżeli						

	Użytkownik wyraził zgodę na przetwarzanie danych w celach marketingowych						
5	Personalizacja działania serwisów Akademii Kodu						

Załącznik nr 2
Wzór upoważnienia do przetwarzania danych osobowych.

UPOWAŻNIENIE DO PRZETWARZANIA
DANYCH OSOBOWYCH

nr . . . . . .

Działając w imieniu ... . niniejszym upoważniam:
Panią/Pana . . . . . .
. .
Stanowisko . . . . . do przetwarzania danych osobowych w . . . . . .
. . . . . w następującym zakresie*:

A. Okres upoważnienia:

□ na okres zatrudnienia / współpracy z . . . . . .
do dnia . . . . . włącznie

B. Zakres upoważnienia:

□ dane przetwarzane na nośnikach papierowych,
□ system informatyczny,
□ dane osobowe objęte zbiorem:
a) . . . . . .
.
b) . . . . . .
.
c) . . . . . .
.

* bez ograniczeń, podgląd danych, wprowadzanie danych, opracowywanie danych, zmienianie danych, usuwanie danych, na komputerach przenośnych)

. . . . . .

Administrator danych

Załącznik nr 3
Wzór Oświadczenia i zobowiązania osoby przetwarzającej dane osobowe

. . . . . , dn. . . . . r.

. . . . . (imię i nazwisko osoby upoważnionej)

. . . . . .(stanowisko)

. . . . . (miejsce pracy)

OŚWIADCZENIE

Oświadczam, że – w związku z wykonywaniem przeze mnie prac na rzecz Akademii Kodu Michał Makaruk oraz upoważnieniem mnie do Przetwarzania danych osobowych – zostałem/łam zapoznany/a ze stosownymi przepisami i standardami ochrony danych osobowych, zobowiązuję się do przestrzegania:

- Przepisów o ochronie adwokackiej tajemnicy zawodowej,
- Przepisów o ochronie danych osobowych, w tym 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
- Polityki Bezpieczeństwa informacji w . . .. ,
- Instrukcji zarządzania systemem Informatycznym w . . . . . ,

W związku z powyższym zobowiązuję się do:

a. zapewnienia ochrony danych osobowych przetwarzanych w zbiorach administratora, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem,
b. zachowania w tajemnicy, także po zaprzestaniu wykonywania prac, wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych w zbiorach . . . . . .
c. natychmiastowego zgłaszania do Administratora Danych zaobserwowania próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia, bezpieczeństwa zbioru/zbiorów lub systemów informatycznych.

akademia kodu

. . . . . .

[podpis pracownika/współpracownika]

Załącznik nr 4
Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego

. . . . . , dn. . . . . r.

Prezes Urzędu Ochrony Danych Osobowych
. . . . . .

ZGŁOSZENIE INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 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 (ogólne rozporządzenie o ochronie danych), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

1) Dane Administratora Danych osobowych:.....
2) Miejsce i dzień naruszenia:.....
3) Kategoria i przybliżona liczba osób, których dane dotyczą:.....
4) Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie:.....
5) Opis charakteru naruszenia ochrony danych:.....
6) Możliwe konsekwencje naruszenia ochrony danych osobowych:.....
7) Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych.....

.....

Załącznik nr 5

Rejestr przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych

REJESTR **przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa przetwarzania danych osobowych**										
Data zgłoszenia Naruszenia (dzień i godzina)	**Zgłaszający**	**Rodzaj naruszenia**	**Miejsce naruszenia**	**Opis naruszenia**	**Skutki naruszenia**	**Czy naruszenie podlega zgłoszeniu do organu nadzorczego**	**Czy naruszenie podlega zgłoszeniu osobie, której dane dotyczą**	**Podjęte działania – sposób usunięcia naruszenie**	**Data zakończenia czynności**	**Status**

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Niniejsza *Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych Akademii Kodu Michał Makaruk, ul. Ostrobramska 75c, 04-175 Warszawa, NIP: 4660376251, REGON: 146723662 (zwana dalej również: *„Akademią" lub „Administratorem"*) przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 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 (dalej RODO).

§ 1

1. Celem Instrukcji jest ustalenie zasad zabezpieczania i bezpiecznego przetwarzania informacji zbieranych w formie elektronicznej w Akademii.
2. Instrukcja obowiązuje wszystkie osoby realizujące jakiekolwiek zadania w Akademii, niezależnie od podstawy wykonywania tych zadań w Akademii, zwane dalej łącznie dla celów niniejszej Instrukcji *„pracownikami".*
3. Zakresem instrukcji objęte są działania związane z zabezpieczeniami sprzętu i oprogramowania komputerowego oraz postępowaniem personelu mającym na celu zapewnienie poufności gromadzonych danych.
4. Administrator danych odpowiada za zapewnienie stosowania odpowiednich zabezpieczeń bazy informacji zbieranych w formie elektronicznej.
5. Administrator odpowiada za organizację sieci, kontrolę przestrzegania zasad opisanych w instrukcji, instalację oprogramowania, nadzorowanie sieci.

§ 2

Definicje:

1) **Dane osobowe** – wszelkie informacje, w tym o stanie zdrowia, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
2) **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu Przetwarzania danych;
3) **Użytkownik** – osoba upoważniona przez Administratora do Przetwarzania danych osobowych w Akademii Kodu Michał Makaruk;
4) **Sieć lokalna** – połączenie Systemów informatycznych Administratora wyłącznie dla własnych potrzeb przy wykorzystaniu urządzeń i sieci telekomunikacyjnych;
5) **Zbiór danych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;
6) **Przetwarzanie danych** – 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;
7) **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym Przetwarzaniem;
8) **Identyfikator użytkownika** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do Przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie;

9) **Hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym (Użytkownikowi);

I. Procedury nadawania uprawnień do Przetwarzania danych i rejestrowania tych uprawnień w Systemie informatycznym

1) Za bezpieczeństwo Danych osobowych w Systemie informatycznym i za właściwy nadzór odpowiedzialny jest Administrator.
2) Do obsługi Systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do Przetwarzania danych, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie wydane przez Administratora,
3) Po upoważnieniu osoby do dostępu do przetwarzania danych osobowych w systemie informatycznym zostaje jej nadany Identyfikator użytkownika. Z chwilą nadania Identyfikatora osoba może uzyskać dostęp do systemów informatycznych w zakresie odpowiednim do danego upoważnienia.
4) Dla każdego Użytkownika Systemu informatycznego ustalony jest odrębny Identyfikator i Hasło.
5) Identyfikator użytkownika nie może być zmieniany, a po wyrejestrowaniu Użytkownika z Systemu informatycznego nie może być przydzielony innej osobie.
6) Identyfikator osoby, która utraciła uprawnienia do dostępu do Danych osobowych, zostaje niezwłocznie wyrejestrowany z Systemu informatycznego, w którym są przetwarzane, zaś Hasło dostępu zostaje unieważnione oraz zostają podjęte inne działania niezbędne w celu zapobieżenia dalszemu dostępowi tej osoby do danych.
7) Wszyscy użytkownicy systemów informatycznych zarejestrowani są w „Karcie użytkowników", stanowiącej załącznik do niniejszej Instrukcji.

8) W „Karcie użytkowników” zawarte są informacje o pracowniku, dacie uzyskania dostępu do systemów informatycznych oraz dacie pozbawienia tego dostępu.

II. Metody i środki Uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem

1) W Systemie informatycznym stosuje się Uwierzytelnianie na poziomie dostępu do systemu operacyjnego. Do Uwierzytelnienia Użytkownika na poziomie dostępu do systemu operacyjnego stosuje się Hasło oraz Identyfikator użytkownika.
2) Hasła użytkowników umożliwiające dostęp do Systemu informatycznego utrzymuje się w tajemnicy również po upływie ich ważności.
3) Hasło musi składać się z 8 znaków, w tym minimum z 2 cyfr i 2 znaków specjalnych. Hasła zmienia każdy pracownik nie rzadziej niż co 90 dni. Nowe hasło musi się różnić od poprzedniego minimum 3 znakami.
4) Zabrania się używania identyfikatora lub Hasła drugiej osoby.
5) Dla każdej osoby, której Dane osobowe są przetwarzane w Systemie informatycznym, system zapewnia odnotowanie:
    a. daty pierwszego wprowadzenia danych do systemu,
    b. identyfikatora Użytkownika wprowadzającego Dane osobowe do systemu,
    c. informacji o odbiorcach, którym Dane osobowe zostały udostępnione.

III. Procedury związane z wykonywaniem pracy przez Użytkowników systemu

1) Pracownik po przyjściu do pracy uruchamia stację roboczą.
2) Przed uruchomieniem komputera należy sprawdzić, czy nie zostały do niego podłączone żadne niezidentyfikowane urządzenia.
3) Po uruchomieniu pracownik loguje się przy pomocy identyfikatora Użytkownika oraz hasła do systemu informatycznego.
4) W trakcie pracy przy każdorazowym opuszczeniu stanowiska komputerowego należy dopilnować, aby na ekranie nie były wyświetlane Dane osobowe.
5) Przy opuszczaniu stanowiska na dłuższy czas należy ustawić ręcznie blokadę klawiatury i wygaszacz ekranu (wygaszacz nie rzadszy niż aktywujący się po 15 min braku aktywności).

IV. Kopie zapasowe.

1. Dla zabezpieczenia integralności danych dokonuje się archiwizacji danych w systemach Akademii.
2. Kopie zapasowe tworzone są:
    1) codziennie – na serwerze,
    2) raz na tydzień/miesiąc – na nośniku zewnętrznym.
3. Wszystkie dane archiwizowane winny być identyfikowane, tj. zawierać takie informacje jak datę dokonania zapisu oraz identyfikator zapisanych w kopii danych.
4. Nośniki z kopiami archiwalnymi powinny być zabezpieczone przed dostępem do nich osób nieupoważnionych, przed zniszczeniem czy kradzieżą.
5. Nośników z danymi zarchiwizowanymi nie należy przechowywać w tych samych pomieszczeniach, w których przechowywane są Zbiory danych osobowych używane na bieżąco.

6. Nośniki informacji, kopie zapasowe, które nie są przeznaczone do udostępnienia, przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym.
7. Kopie, które są już nieprzydatne, należy zniszczyć fizycznie lub stosując wymazywanie poprzez wielokrotny zapis nieistotnych informacji w obszarze zajmowanym przez dane kasowane.
8. Zabrania się wynoszenia jakichkolwiek nagranych nośników zawierających dane osobowe z miejsca pracy.

V. Sposób zabezpieczenia systemu informatycznego

1. Wszystkie komputery zabezpieczone są w licencjonowane oprogramowanie antywirusowe AVG, podlegające aktualizacji drogą Internetu. Programy antywirusowe zainstalowane są na serwerze i stacjach roboczych. Po każdej naprawie i konserwacji komputera sprzęt jest sprawdzany pod kątem występowania wirusów i konieczności ponownego zainstalowania programu antywirusowego. Elektroniczne nośniki informacji pochodzenia zewnętrznego podlegają automatycznemu sprawdzeniu programem antywirusowym przed rozpoczęciem korzystania z nich.
2. Dane uzyskiwane drogą teletransmisji podlegają sprawdzeniu przed udostępnieniem użytkownikom.
3. W przypadku wykrycia wirusa należy:
    a) uruchomić program antywirusowy i skontrolować użytkowany system,
    b) usunąć wirusa z systemu przy wykorzystaniu programu antywirusowego.

    Jeżeli operacja usunięcia wirusa się nie powiedzie, należy:
    a) zakończyć pracę w systemie komputerowym,
    b) odłączyć zainfekowany komputer od sieci,
    c) powiadomić o zaistniałej sytuacji Administratora.

VI. Poczta elektroniczna

1) Pracownicy mogą korzystać z poczty elektronicznej w celach służbowych oraz w celach prywatnych w zakresie ograniczonym swoimi obowiązkami.
2) Administrator może poznawać treść wiadomości elektronicznych wykorzystywanych przez pracowników znajdujących się we wszystkich systemach Administratora.
3) Zabronione jest otwieranie wiadomości e-mail pochodzących od nieznanego nadawcy bądź z podejrzanym tytułem (tzw. *phishing e-mail*). W szczególności zabronione jest otwieranie linków bądź pobieranie plików zapisanych w komunikacji zewnętrznej od nieznanego nadawcy.

VIII. Sposób realizacji wymogu zapisania w Systemie informatycznym informacji o odbiorcach danych.

1) Informacje o odbiorcach danych zapisywane są w Systemie informatycznym, z którego nastąpiło udostępnienie.
2) Informacja o odbiorcy danych zapisana jest w Systemie informatycznym przy uwzględnianiu daty i zakresu udostępnienia, a także dokładnego określenia odbiorcy danych.
3) Możliwe jest sporządzenie i wydrukowanie raportu zawierającego, w powszechnie zrozumiałej formie, powyższe informacje.

IX. Procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do Przetwarzania danych

1) Przeglądy kontrolne, serwis sprzętu i oprogramowania powinny być dokonywane przez firmy serwisowe, z którymi zostały zawarte umowy

zawierające postanowienia zobowiązujące je do przestrzegania zasad poufności informacji uzyskanych w ramach wykonywanych zadań.

2) Przy dokonywaniu serwisu należy przestrzegać następujących zasad:
    a) czynności serwisowe powinny być wykonywane w obecności osoby upoważnionej do Przetwarzania danych,
    b) Instrukcja zarządzania systemem informatycznym
    c) przed rozpoczęciem tych czynności dane i programy znajdujące się w systemie powinny zostać zabezpieczone przed ich zniszczeniem, skopiowaniem lub niewłaściwą zmianą,
    d) prace serwisowe należy ewidencjonować w książce zawierającej rodzaj wykonywanych czynności serwisowych, daty rozpoczęcia i zakończenia usługi, odnotowanie osób dokonujących czynności serwisowych, tj. imienia i nazwiska, a także osób uczestniczących w pracach serwisowych, w przypadku prac serwisowych dokonywanych przez podmiot zewnętrzny, wymagających dostępu do danych osobowych, z podmiotem takim powinny zostać zawarte stosowne umowy powierzenia