

# System Zarządzania Bezpieczeństwem Informacji

## w Zespole Szkół Zawodowych Nr 1

### im. Marszałka Józefa Piłsudskiego w Skierniewicach

(wdrożenie z zakładanym terminem realizacji do 31.12.2023)

#### I. Wykonawca:

##### **Radca Prawny Kamil Suplewski**

OIRP Warszawa: WA-13308

+48 506 577 332, kamil.suplewski@gmail.com

prawnik-suplewski.business.site

#### I. Cele:

##### 1. Audyt zgodności ochrony bezpieczeństwa informacji:

Ustalenie i zweryfikowanie zachodzących procesów przetwarzania informacji. Wskazanie obszarów, w których ochrona nie jest wystarczająca, adekwatna lub występują ewentualne uchybienia w tym zakresie. Przedstawienie działań dostosowujących do przepisów prawa i standardów postępowania, w szczególności wynikających z rodziny norm ISO z grupy 270(...) i 31(...), w szczególności norm ISO 27005 i ISO 31000.

##### 2. Wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji:

Wprowadzenie mechanizmów mających zabezpieczyć przepływ informacji, w tym ze szczególnym naciskiem na zgodność z RODO, z uwzględnieniem specyfiki samorządowej placówki edukacyjnej, ustalonej organizacji i kultury pracy oraz indywidualnych potrzeb ZSZ NR 1. Opracowanie i wdrożenie odpowiednich procedur postępowania, oraz wymaganej dokumentacji, w szczególności wynikających z w/w rodziny norm ISO oraz spodziewanych przyszłych przedsięwzięć.

##### 3. Pełnienie funkcji Inspektora Ochrony Danych Osobowych (IOD / DPO - Data Protection Officer)

Przyjęcie obowiązków wynikających z art.39 RODO, w tym między innymi: stała obsługa i monitoring procesów przetwarzania danych osobowych; modyfikowanie przyjętych rozwiązań pod kontem aktów prawnych przyjmowanych w krajowym porządku prawnym, a także z uwzględnieniem wytycznych Prezesa Urzędu Ochrony Danych Osobowych oraz Europejskiej Rady Ochrony Danych; reprezentacja przed sądami powszechnymi i urzędami w postępowaniach związanych z ochroną danych osobowych.

A także pełnienie funkcji Inspektora Ochrony Bezpieczeństwa Informacji (IBI / ISO – Information Security Officer), co oznacza przyjęcie i stałe wypełnianie obowiązków, jakie nakładają na IBI regulacje obowiązujące i wprowadzane w ZSZ NR 1 (Polityka Bezpieczeństwa Informacja i akty akcesoryjne).

#### II. Ogólny zakres działań:

A. Holistyczna weryfikacja procesów dot. informacji pod kątem zgodności z przepisami prawa krajowego, europejskiego oraz międzynarodowego prywatnego i publicznego, a także ustalonych w praktyce standardów postępowania, ze szczególnym uwzględnieniem zagadnień ochrony danych osobowych, w tym weryfikacja:

- spełnienia przesłanek legalizujących przetwarzanie informacji (danych osobowych),
- stosowanych klauzul informacyjnych i ich rozszerzenie w celu dostosowania do przepisów,
- stosowanych zgód i ich modyfikacja w celu dostosowania do przepisów, w szczególności RODO,
- podlegania obowiązkowi prowadzenia rejestru czynności przetwarzania danych osobowych oraz rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora,

- podlegania obowiązkowi wyznaczenia Inspektora Ochrony Danych Osobowych,
- stosowanych umów powierzenia i ich uzupełnienie w celu dostosowania do przepisów,
- stosowanych technicznych i organizacyjnych środków ochrony informacji, w szczególności przy uwzględnieniu sposobu przetwarzania danych osobowych oraz ich ocena pod kątem zgodności z prawem,
- zasadności i ew. zgodności przekazywania informacji, w tym danych osobowych do państw trzecich,
- wykorzystywanych wzorów dokumentów, w tym weryfikacja języka stosowanego w komunikacji, ustalenie obszarów, które będą wymagały zmian,

**a ponadto:**

- analiza możliwości realizacji nowych obowiązków administratora i praw podmiotów danych,
- rekomendacje w zakresie realizacji *Privacy by Design i by Default*,
- identyfikacja i weryfikacja zasobów teleinformatycznych oraz ich zabezpieczeń,
- sformułowanie wytycznych pod kątem zbudowania Systemu Zarządzania Bezpieczeństwem Informacji.

**B. Asysta wdrożeniowa, obejmująca wsparcie przy wdrożeniu rekomendacji z zakresu bezpieczeństwa informacji, audyt powdrożeniowy, dalsze aktualizacje.**

1. Opracowanie procedury mapowania procesów wewnętrznych, oceny ryzyka,
2. Opracowanie rejestru czynności przetwarzania oraz rejestru kategorii czynności,
3. Przygotowanie wewnętrznych polityk ochrony informacji, dokumentacji oceny skutków i uprzednich konsultacji,
4. Opracowanie polityki zarządzania naruszeniami oraz polityki zgłaszania naruszeń,
5. Doradztwo przy opracowaniu procedur wewnętrznych w zakresie realizacji praw podmiotów danych w tym prawa do informacji, dostępu do danych, przenoszenia danych i ograniczenia przetwarzania,
6. Przygotowanie wzoru informacji,
7. Przygotowanie w niezbędnym zakresie wzorów dokumentacji do realizacji *Privacy by Design i by Default*,
8. Przygotowania wzorów upoważnień,
9. Przygotowanie umów powierzenia i aneksów do umów powierzenia
10. Doradztwo w procesie wdrażania wytycznych z zakresu bezpieczeństwa.

#### **IV. Harmonogram prac**

##### **Etap 1 - identyfikacja wymagań**

Identyfikacja wymagań, w zakresie adekwatnym do procesów i zakresu działalności organizacji. Ocena aktualnych rozwiązań na zgodność z wymaganiami ochrony informacji na poziomie dokumentacji oraz praktyk działania.

Technika realizacji - wywiady z kluczowym personelem (istnieje możliwość kontaktu na odległość, bezpośrednie spotkania generalnie nie są koniecznością), oraz analiza posiadanej dokumentacji. Istotne będzie współdziałanie z dotychczasowym Administratorem Bezpieczeństwa Informacji, Administratorem Systemów Informatycznych (ew. z innymi osobami pełniącymi podobne funkcje), o ile taki istnieje. Na tym etapie stworzony zostanie profil organizacyjny pod kątem ochrony bezpieczeństwa informacji, co pozwoli też określić dokładniej ramy czasowe realizacji dalszych etapów.

##### **Etap 2 - planowanie i wdrożenie**

1. Zmiany w strukturze organizacyjnej, w tym w organizacji systemów IT - kwestie typowo projektowe dla modyfikacji już istniejących lub zakupu nowych;
2. Opracowanie dokumentacji, w tym: Dokumentacja ogólna, Oceny ryzyka, Zarządzanie ryzykiem, Polityki, procedury i instrukcje.

3. Zaprojektowanie i przygotowanie systemu LMS (learning management system), z opcją szkoleń w systemie distance (e-learning), dobrymi praktykami oraz przygotowanie siatki szkoleń i materiałów - szkolenia z dokumentacji i z procedur.

### **Etap 3 – Audyt po-wdrożeniowy**

Etap ten zostanie wykonany na działającym systemie. Dla lepszych wyników realizacja tego etapu od realizacji poprzednich oddzielał będzie odstęp co najmniej pół roku. W tym czasie nastąpi weryfikacja przyjętych rozwiązań pod kątem realizacji założonych celów, oraz opracowanie planu dalszych działań/zmian. Wyniki zostaną przedstawione i omówione z kierownictwem jednostki.

## **V. Doświadczenie Wykonawcy:**

Zakończone wdrożenia, a w części także pełnienie funkcji IOD (DPO) i IBI (ISO):

- **„Groupe Positive”** (previously „Groupe Sarbacane” - A global corporation governed by EU law, located in the French Republic, operating mainly in the area of IT and R&D - advanced IT solutions to support the processing of highly complex information resources.)
  - Sarbacane
  - Sarbacane Chat
  - Primotexto
  - Lyout
  - Tipimail
  - Datananas
  - Marketing 1BY1
  - rapidmail
  - 4Dem
  - Signitic
  - noCRM.io
  - user.com
- **Grupa Kapitałowa MIRBUD:**
  - Mirbud S.A. z/s w Skierniewicach (w ramach tej Spółki – Czasopismo Głos),
  - JHM Development S.A. z/s w Skierniewicach,
  - Expo Mazury S.A. z/s w Ostródzie,
  - Marywilska 44 S.A. z/s w Warszawie,
  - Przedsiębiorstwo Budowy Dróg i Mostów Kobylarnia S.A. z/s w Kobylarnii,
- **Genotic, Inc.** z/s w San Francisco, CA, USA
- **TaskPilot, Inc.** z/s w San Francisco, CA, USA
- **User.com** Sp. z o.o. z/s w Warszawie
- Pływalnia Miejska „Nawa” Sp. z o.o. z/s w Skierniewicach
- Kompania Leśna Sp. z o.o. z/s w Nowym Dworze Parceli
- Kompania Leśna Sp.j. z/s w Nowym Dworze Parceli
- Liceum Ogólnokształcące im. Bolesława Prusa w Skierniewicach
- Zespół Szkół Zawodowych nr 2 im. chor. Józefa Paczkowskiego w Skierniewicach
- Zespół Szkół Numer 3 im. Wisławy Szymborskiej w Skierniewicach
- Żłobek Miejski z Oddziałami Integracyjnymi w Skierniewicach
- Żłobek Miejski z Oddziałami Integracyjnymi „Tuptuś” w Rawie Mazowieckiej
- Miejski Ośrodek Pomocy Rodzinie w Skierniewicach
- Fundacja CivilHub z/s w Warszawie
- Grzegorz Warzecha Fundacja Rodzinna z/s w Warszawie
- Userengage Sp. z o.o. z/s w Warszawie
- Expose Sp. z o.o. z/s w Warszawie

- Aperto Sp. z o.o. z/s w Warszawie
- Mandali Sp. z o.o. z/s w Łodzi
- Blue Sp. z o.o. z/s w Skierniewicach
- Międzynarodowe Studium Dziewulskich Sylwia Dziewulska z/s w Warszawie
- Concept Beauty Sp. z o.o. z siedzibą w Warszawie
- Przedsiębiorstwo Produkcyjno Handlowo Usługowe "Gomak" Sp. z o.o. z siedzibą w Godzianowie
- Eurotom Tomasz Chodkiewicz z siedzibą w Nowym Dworze Parceli
- Firma Handlowa "Fruktus" R. Dziuba, M. Dziuba Spółka Jawna z siedzibą w Skierniewicach
- Krajewscy S.C. Jerzy Krajewski, Marcin Krajewski z siedzibą w Skierniewicach
- Stowarzyszenie Przewoźników Taksówkowych „Mobil-Taxi” z siedzibą w Skierniewicach
- Stowarzyszenie Skierniewickich Przewoźników NOVA-TAXI 196-69 z siedzibą w Skierniewicach
- Stowarzyszenie Razem dla Skierniewic z siedzibą w Skierniewicach
- "Karczma u Boryny" z siedzibą w Lipcach Reymontowskich
- etc...

**Na oryginalne właściwe:**  
**Data, pieczęć i podpis Mecenasa**  
Skierniewice, dn.11.12.2023r.

Akceptuję:  
Skierniewice, dn.13.12.2023r.

**Na oryginalne właściwe:**  
**Data, pieczęć i podpis Dyrektora**