Witam.

Zapoznaliśmy się i przeanalizowaliśmy komplet dokumentów udostępniony nam 12 kwietnia i mamy niestety szereg uwag.

Część uwag, tych obejmujących kilka dokumentów lub wymagających opisu, przedstawimy poniżej. Reszta pomniejszych wprowadzona jest jako komentarz w trybie recenzji w poszczególnych dokumentach, które załączamy i prosimy o zapoznanie się z nimi.

1. **Audyt.**
2. Audyt nie zawiera pełnego opisu stanu Ochrony Danych Osobowych w ZSSiL3 sprzed audytu, a jedynie części informatycznej i to, jak się wydaje, nie do końca wnikliwie. De facto audyt stwarza wrażenia jakby przed wizytą firmy Serwkom w ZSSiL3 panował jeden wielki chaos co nie jest zgodne z rzeczywistością. Polityka bezpieczeństwa była, wdrożona i aktualizowana. Instrukcja zarządzania systemem informatycznym była. Polityka haseł działała. Instrukcja na wypadek naruszenia była. Zgody na przetwarzanie danych były zbierane na bieżąco. Zgody „na wizerunek” również. Oświadczenia o poufności również.

Być może były to dokumenty i procedury niedoskonałe, ale w audycie nie wykazano błędów i potrzeby naprawy czy choćby napisania od nowa ze względu np. na nakład pracy.

1. Być może audyt powinien zawierać oszacowane ryzyko, a dokładniej dwa: „przed Serwkom” i „po Serwkom” wykonane już zgodnie z zaproponowaną dokumentacją
2. Audyt jak i całokształt dokumentów dość jednoznacznie wymusza powołanie ABI i zastępców co nie jest obowiązkowe i jak się wydaje rzetelne wypełnianie zadań związanych z ochroną danych nie wymaga posiadania ABI
3. Rejestracja zbioru REKRUTACJA. Zbiór Rekrutacja (a dokładniej dwa zbiory) był zgłoszony do rejestracji już w 2014 r. (audytor oglądał kopię zgłoszenia) a to że GIODO nadal nie dopisało go do zarejestrowanych zbiorów nie jest winą ZSSiL3. Audyt o tym nie wspomina.

Obecnie wysłano zgłoszenie aktualizacyjne w związku ze zmianą firmy dostarczającej system rekrutacyjny

1. audyt stwierdza dla kilku komputerów cyt. *klucz w systemie niezgodny z COA i dostępny w internecie*. Dla nie-informatyka jest to jednoznaczne ze stwierdzeniem „piracki z internetu”. Podobnie wspomniane jest o kluczu Office 2003 dostępnym w internecie. Wydaje się, że w takim wypadku audytor powinien wprowadzić dodatkowe uwagi na temat sposobów aktywacji systemów OEM SLP czy KMS/MAK w przypadku licencji VL. Inaczej powstaje wrażenie używania przez ZSSiL3 nielegalnego oprogramowania.
2. audyt wspomina o rozważeniu kupna serwera dla stacji przetwarzających dane osobowe jednak Polityka i Instrukcja zakładają od razu istnienie takiego serwera i nawet nie wspominają o komputerach samodzielnych w sieci równoległej/bezserwerowej co ma na razie miejsce w ZSSiL3. Zgodnie z wykładnią GIODO dokumenty Polityki nie powinny mieć charakteru abstrakcyjnego więc w momencie wdrożenia Polityki musimy posiadać sieć serwerową inaczej będziemy z Polityką automatycznie niezgodni.
3. audyt zaleca aktualizację wszystkich systemów do windows 8.1 i 10 wspominając o zakończeniu wsparcia dla Windows 7, które przecież kończy się w 2020 r. Zapomina natomiast o systemie Vista. System 10 nie jest natomiast nadal systemem dojrzałym.
4. **ABI.**

Powtarzający się w całości dokumentacji poważny problem powołania i obowiązków ABI. W żadnym z dokumentów nie odnaleźliśmy możliwości „nie powołania” ABI. Wydaje się, że wszędzie powinno istnieć założenie, że coś wykonuje powołany ABI lub ADO lub pełnomocnik ds. ODO w zależności od uprawnień wewnętrznych i oczywiście zgodności z Ustawą. W przeciwnym wypadku istnieje niejako wymuszenie powołania ABI, najlepiej zewnętrznego bądź na etacie. Podobnie jak w przypadku serwerów (pkt 1e) Polityka i powiązane dokument nie dopasowują się do ZSSiL3 tylko dopasowują ZSSiL3 do Polityki. (opierając się na tym, iż powołanie ABI nie jest obowiązkowe, jak i posiadanie serwera)

1. **Używanie skrótu Szkoły**

Prosimy aby w całości dokumentacji używać pełnej nazwy Szkoły lub skrótu ZSSiL3 lub ZSSiL nr 3 nie zaś skrótu ZSSiL

1. **Umowa powierzenia danych dla DBFO.**

Czy w świetle nowelizacji Ustawy z dnia 1.04.2016 r. konieczna jest ta umowa?

1. **Zgoda na publikację wizerunku.**

Do tej pory stosowana w ZSSiL3 zgoda na publikację wizerunku była bardziej szczegółowa niż zaproponowana przez firmę Serwkom. W związku z doświadczeniami posiadała rozróżnienia na publikację na www , gazetkach, folderach reklamowych itp. Dlaczego wprowadzono inną, ogólniejszą zgodę jak się wydaje niedostosowaną do naszych potrzeb?

1. **Harmonogram kontroli wewnętrznych.**

Nie odnaleźliśmy w dokumentacji formularza/podpowiedzi/przykładu planu audytu wewnętrznego dokonywanego przez ABI lub ADO (minimum raz w roku) wynikającego z Ustawy jak i dokumentów wdrażanych np. Procedury nadzoru nad dokumentacja i zapisami i Procedury –audytu wewnętrznego.

1. **Forma papierowa czy tradycyjna**

Czy w całości dokumentacji nie powinniśmy używać stwierdzenia „w formie tradycyjnej” (w kontrze do systemu informatycznego) zamiast „w formie papierowej” aby pozostawać w zgodzie z nowelizacją Ustawy od 1.01.2015 r. W przepływach danych sama firma Serwkom używa stwierdzenia „postać tradycyjna”.

1. **Zmiana firmy dostarczającej system rekrutacji**

W trakcie dość długiego procesu tworzenia dokumentacji przez firmę Serwkom zmienił się dostawca systemu informatycznego z OTAGO na Vulcan więc automatycznie struktura zbiorów danych stała się nieaktualna jeszcze przed wdrożeniem Polityki i dok. powiązanych

1. **Wykaz zbiorów czy rejestr zbiorów**

Czy Wykaz zbiorów danych osobowych nie powinno się to nazywać Jawny rejestr … i zawierać dodatkowe informacje jak daty utworzenia zbioru, wykreślenia zbioru, podmiot któremu powierzono, administrator, cel, zakres itp. zgodnie z art. 36a ust. 2 pkt 2 Ustawy

1. **Kopie zapasowe – storage sieciowy**

Wydaje się, że zgodnie z rozmowami prowadzonymi z panem Januszem Gałusem przed zawarciem umowy z firmą Serwkom Szkoła wraz z dokumentacją i audytem miała otrzymać propozycję (np. w formie ofertowej) na wdrożenie storage’u sieciowego w systemie bezserwerowym i systemie serwerowym (z serwerem oferowanym np. przez Serwkom) bo problem niedostatecznych backupów był zidentyfikowany jako najistotniejszy już we wstępnej rozmowie

1. **POD**
2. Generowanie ewidencji (listy) osób z uprawnieniami przetwarzania danych osobowych – daty nadania, modyfikacji i odebrania wypełniają się automatycznie datą generowania listy. Każdą datę trzeba więc poprawiać ręcznie i daty się nie zapisują (?) przez co przy ponownym generowaniu trzeba wpisywać poprawiać je ponownie
3. Czy dokument Opis struktury zbiorów danych nie powinien być ilościowo i nazewnictwem identyczny z listą uprawnień w POD?
4. Zbiór Kartoteka ucznia zawiera dane wrażliwe, dostęp ma wyłącznie Dyrektor, pedagog i psycholog. Jak ich wyróżnić od „zwykłych” nauczycieli i specjalisty ds. uczniów, którzy nie mają dostępu do danych wrażliwych? Czy zbiór danych wrażliwych uczniów/opiekunów nie powinien być wydzielony jako oddzielny zbiór?

**Strona 24** *Polityki Bezpieczeństwa* Ochrony Danych osobowych- czy do aktyw informacyjnych należą: materiały dydaktyczne, dokumenty stanowiące podstawę oceniania i pytania i zadania egzaminacyjne?

**Strona 25** za organizację systemu ochrony informacji niejawnych w ZSSL odpowiada Pełnomocnik ds. ochrony informacji niejawnej ????( tzn. kto?)

**Strona 27 i 28 –** kto kwalifikuje informacje jako publiczna, do użytku wewnętrznego, służbowego ( jakie to dokumenty???), wszystkie??

**Strona 34 –** zabezpieczenia w postaci nadzoru przez pracownika w trybie 24 godzinnym???

**Strona 36 –** zasilacze bezprzewodowe ( UPS) ???

**Strona 38 –** oprogramowanie poza siedzibą ZSSiL ( jak to wykazać by to nie zablokowało pracy np. przy EXPO)

**Strona 41 –** uprawnieni Pracownicy/współpracownicy posiadają? ( **mogą**) i dalej a do sal??

Opis podstawowych procesów i obowiązków związanych z przetwarzaniem danych osobowych

Ad.3 + załaczniki