Raport z przeglądu obowiązujących procedur
w zakresie ochrony danych osobowych

Nazwa administratora: Publiczne Przedszkole nr 10

Adres administratora: ul. Edukacyjna 44-335 Jastrzębie-Zdrój

Adres (miejsce) przetwarzania danych osobowych: j.w.

Dotyczy sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych oraz politykami przyjętymi przez administratora

1. Zakres audytu wraz z opisem stanu faktycznego:

L.p.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI	UWAGI TAK/NIE/ ND
1.	DOKUMENTACJA	Sprawdzenie, czy Polityka Ochrony Danych Osobowych jest aktualna względem obowiązującego stanu prawnego oraz faktycznego.	TAK
2.	DOKUMENTACJA	Sprawdzenie, czy pracownicy mają upoważnienie do przetwarzania danych osobowych – jeżeli jest wymagane.	TAK
3.	DOKUMENTACJA	Sprawdzenie, czy podmioty danych maja możliwość zapoznania się z klauzulą informacyjną RODO	TAK
4.	DOKUMENTACJA	Sprawdzenie, czy dokonano analizy ryzyka dla przetwarzanych danych osobowych	TAK
5.	DOKUMENTACJA	Sprawdzenie, czy administrator prowadzi rejestr czynności przetwarzania	TAK
6.	DOKUMENTACJA	Sprawdzenie, czy jest prowadzony rejestr kategorii przetwarzania, jeżeli organizacja jest procesorem dla danych osobowych.	TAK
7.	DOKUMENTACJA	Sprawdzenie, czy dokonano oceny skutków dla ochrony danych , jeżeli wystąpiła taka konieczność.	ND
8.	DOKUMENTACJA	Ustalenie, czy dokumentacja z danymi osobowymi jest przechowywana nie dłużej niż do ustania celu lub wymagań przepisów prawa.	TAK

L.p.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI	UWAGI TAK/NIE/ ND
9.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Kontrolowanie osób przetwarzających dane osobowe - czy stosują się do „zasady czystego biurka".	TAK
10.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajdują się szafy zamykane na klucz, w których przechowuje się dokumentację zawierającą dane osobowe podlegające ochronie. Czy szafy są odpowiednie dla przechowywanej w nich dokumentacji i ewentualnych zagrożeń?	TAK
11.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Czy biuro/pomieszczenie, w którym przetwarzane są dane osobowe zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych	TAK
12.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy upoważnione osoby świadczące usługi w terenie znają zasady właściwej ochrony przed dostępem osób nieuprawnionych dokumentów zawierających dane osobowe.	ND
13.	FIZYCZNA OCHRONA DANYCH OSOBOWYCH	Sprawdzenie, czy w pomieszczeniu znajduje się niszczarka dokumentów (jeśli takie urządzanie nie znajduje się w pomieszczeniu, należy skontrolować pracownika, w jaki sposób niszczy zbędną dokumentację, która nie podlega archiwizacji). Szczególnie powinno się zwrócić uwagę, czy niepotrzebne dokumenty nie są przypadkiem wyrzucane do kosza na śmieci – dokumenty powinny być niszczone w sposób mechaniczny lub manualny, tak, by uniemożliwić ich odczytanie osobom postronnym.	TAK
14.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, mające na celu sprawdzenie, czy komputer jest zabezpieczony hasłem.	TAK
15.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Monitorowanie, czy osoby przetwarzające dane osobowe w systemie informatycznym logują się za pomocą WŁASNEGO identyfikatora i hasła.	TAK
16.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie aktywności systemu antywirusowego, na komputerach, które m.in. służą do obsługi systemów przetwarzających dane osobowe.	TAK
17.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Kontrolowanie, czy pracownik korzysta z wygaszacza ekranu.	TAK

L.p.	ZAKRES KONTROLI	PODEJMOWANE CZYNNOŚCI	UWAGI TAK/NIE/ ND
18.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy monitor komputera został usytuowany w sposób uniemożliwiający wgląd do danych - osobom postronnym.	TAK
19.	OCHRONA ŚRODOWISKA KOMPUTEROWEGO	Sprawdzenie, czy serwer oraz dysk do przechowywania kopii bezpieczeństwa są właściwie zabezpieczone i czy wejście do serwerowni jest autoryzowane.	TAK
20.	STRONA INTERNETOWA	Sprawdzenie, czy na stronie internetowej jednostki nie są upublicznione nadmiarowe dane oraz ustalenie, czy administrator pozyskał zgody na publikacje wizerunku na stronie internetowej.	TAK
21.	STRONA INTERNETOWA	Sprawdzenie, czy administrator opublikował na stronie internetowej lub na BIP imię i nazwisko oraz kontaktowy adres e-mail do inspektora ochrony danych.	TAK
22.	UMOWA POWIERZENIA	Sprawdzenie czy administrator podpisał z procesorem umowę powierzenia	TAK
23.	MONITORING	Czy administrator stosuje monitoring wizyjny lub w inny sposób monitoruje pracę pracowników (np. monitoring poczty elektronicznej, rozmów telefonicznych. GPS). Jeżeli tak to należy ustalić czy:	TAK
		- Administrator dopełnił obowiązków informacyjnych oraz procedur wynikających z przepisów prawa	TAK
		- Administrator zapewnia właściwą ochronę oraz autoryzowany dostęp do nagrań z monitoringu.	TAK
24.	KONTROLA PRAKTYKI	Przeprowadzenie analizy - jakie obecnie pracownicy mają problemy w zakresie przetwarzania danych osobowych oraz czy ostatnio miały miejsce zdarzenia typu: próby nieuprawnionego dostępu do danych osobowych,działanie zewnętrznych aplikacji, wirusów czy złośliwego oprogramowania; nieuprawniony dostęp do otwartych aplikacji w systemie informatycznym; próba nieuprawnionej interwencji przy sprzęcie komputerowym; wynoszenie niezabezpieczonych dysków z miejsca pracy; udzielanie informacji osobom postronnym, pomijając formalny tryb administracyjny	nie zgłoszono

2. Do protokołu załączony został wykaz pomieszczeń , w których przetwarza się dane osobowe oraz sprzętu komputerowego, na którym dane są przetwarzane.

3. Termin przeglądu: 13.11.2018

4. Wnioski z przeglądu/stwierdzone uchybienia Dostęp do przedszkola autoryzowany. Teren monitorowany. Dane osobowe zabezpieczone w szafach zamykanych na klucz

5. Ewentualne spostrzeżenia i zalecenia: Brak

Podpisy osób uczestniczących w przeglądzie:

6. Inspektor ochrony danych: Bernadetta Domder

Inspektor Ochrony Danych
Bernadetta Domder
tel. 600 854 652 e-mail: iodpusz@wp.pl

7. Inne osoby uczestniczące: 1) Anna Łukasik 2) Mirosława [illegible]

Pomieszczenia i komputery:

Pomieszczenie, w których przetwarzane są dane osobowe (należy podać numer biura i lokalizację)	Sprzęt informatyczny wykorzystywany w przetwarzaniu danych osobowych - należy podać rodzaj komputera (stacjonarny, przenośny)
gabinet dyrektora	komputer stacjonarny
gabinet intendent	komputer stacjonarny