

Załącznik do Zarządzenia
Nr 897/2017
Burmistrza Pyrzyc
z dnia 5 maja 2017r

PLAN SPRAWDZEŃ ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI Z ZAKRESU PRZESTRZEGANIA ZASAD OCHRONY DANYCH OSOBOWYCH NA ROK 2017

Plan sprawdzeń został sporządzony zgodnie z §3 ust. 2 pkt. 1 Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez Administratora Bezpieczeństwa Informacji.

Przedmiotem sprawdzenia jest zbadanie zgodności zasad przetwarzania danych osobowych obowiązujących w Urzędzie Miejskim w Pyrzycach z przepisami o ochronie danych osobowych.

Termin sprawdzeń : **01.06.2017 – 30.11.2017r**

Czynności objęte dokumentowaniem – odebranie od użytkowników wyjaśnień ustnych, przeprowadzenie oględzin, zabezpieczenie dowodów z dokumentu.

Sposób dokumentowania - sporządzanie notatek, kopii otrzymanych dokumentów oraz dokumentów z systemu informatycznego.

Plan sprawdzeń obejmuje w szczególności:

- badanie zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa;
- określenie stanu faktycznego w zakresie przetwarzania danych osobowych;
- sprawdzenie zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych;
- kontrolę przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych.

Zakres sprawdzeń i ich szczegółowa tematyka została opisana w poniższej tabeli.

BURMISTRZ
Marzenna Podzińska

L	Przedmiot sprawdzenia	Zakres poszczególnych sprawdzeń	Data rozpoczęcia	Data zakończenia	Wydział podlegający kontroli
1.	Realizacja procedur wdrożonych przez ADO w zakresie ochrony danych osobowych	<ul style="list-style-type: none"> ❖ Ustawienie sprzętu komputerowego w pomieszczeniach – czy uniemożliwia dostęp do ekranu monitorów osobom postronnym ❖ Polityka czystego biurka ❖ Polityka kluczy ❖ Sprawdzamy czy w sposób bezpieczny niszczone są dokumenty przeznaczone do zniszczenia ❖ Sprawdzenie czy osoby dopuszczone do przetwarzania danych osobowych otrzymały pisemne upoważnienia oraz oświadczenia o zapoznaniu z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych osób dopuszczonych do przetwarzania danych osobowych. ❖ Ustalamy, czy osoby, które nie powinny mieć już prawa dostępu do danych osobowych (np. byli pracownicy) mają odwołane upoważnienia ❖ Ewidencja wydanych upoważnień oraz jej zgodność z wydanymi upoważnieniami 	01-06-2017r	20-06-2017r	<p>Wydział Organizacyjny:</p> <ul style="list-style-type: none"> - pomieszczenie serwerowni - pokój 138 - punkt informacyjny - sekretariat <p>Wydział Budżetu i Finansów:</p> <ul style="list-style-type: none"> - pokoje 280, 276, 263, 263A, 254, 267, 252, 251, 268
2.	Funkcjonowanie zastosowanych zabezpieczeń fizycznych oraz funkcjonowanie systemów zabezpieczeń Systemowych	<ul style="list-style-type: none"> ❖ Spełnienie wymogów z poziomu ochrony systemów informatycznych służących do przetwarzania danych osobowych przed osobami trzecimi. ❖ Sprawdzenie mechanizmów automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy 	01-06-2017r	20-06-2017r	<p>Wydział Organizacyjny:</p> <ul style="list-style-type: none"> - pomieszczenie serwerowni - pokój 138 - punkt informacyjny - sekretariat <p>Wydział Budżetu i Finansów:</p> <ul style="list-style-type: none"> - pokoje 280, 276, 263, 263A, 254, 267, 252, 251, 268

	<p>użytkownika.</p> <ul style="list-style-type: none"> ❖ Sprawdzenie czy zbiór danych osobowych przechowywany jest w pomieszczeniu zabezpieczonym drzwiami zwykłymi (niewzmacnianymi, nie przeciwpożarowymi). ❖ Przestrzeganie zasady rozporządzenia i zakończenia pracy w systemie. ❖ Zabezpieczenie systemowe i fizyczne sprzętu komputerowego. ❖ Tworzenie kopii zapasowych. ❖ Odnutowywanie przez systemy służące do przetwarzania danych osobowych czynności wykonywane na danych osobowych przez użytkowników. <p>Zapewnienie odpowiedniego poziomu bezpieczeństwa :</p> <ul style="list-style-type: none"> a) dbałości o aktualizację oprogramowania, b) minimalizowaniu ryzyka utraty informacji w wyniku awarii, c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją, d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa, e) zapewnieniu bezpieczeństwa plików systemowych, f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa, h) kontroli zgodności systemów 	01-10-2017r	20.10.2017r	<p>Wydział Planowania Inwestycji i drogownictwa: - pokoje 260, 261, 262, 262A</p>
--	--	-------------	-------------	--

	teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;				
3.	Prawidłowość funkcjonowania mechanizmów kontroli dostępu do zbiorów danych	<ul style="list-style-type: none"> ❖ Dostęp pracowników do zbiorów danych oraz zakres dostępu pracowników i weryfikacja wydanych upoważnień (w tym byłych pracowników oraz odwołanie upoważnień). ❖ Zasady nadawania/zmieniania/odbierania uprawnień do systemów informatycznych. ❖ Stosowanie identyfikatorów i haseł dla użytkowników zgodnie z wymogami formalnymi. 	01-06-2017r 01-07-2017r	20-06-2017r 20-09-2017r	<p>Wydział Organizacyjny:</p> <ul style="list-style-type: none"> - pomieszczenie serwerowni - pokój 138 - punkt informacyjny - sekretariat <p>Wydział Budżetu i Finansów:</p> <ul style="list-style-type: none"> - pokoje 280, 276, 263, 263A, 254, 267, 252, 251, 268 <p>Wydział Planowania Inwestycji i drogownictwa:</p> <ul style="list-style-type: none"> - pokoje 260, 261, 262, 262A <p>Wydział Organizacyjny</p>
4.	Inwentaryzacji opisującej sposób przetwarzania danych osobowych w Urzędzie	<ul style="list-style-type: none"> ❖ Weryfikacja dokumentacji z zakresu ochrony danych osobowych funkcjonującej w Urzędzie ❖ Zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa (Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 r. Nr 100, poz. 1024) – art. 39a ustawy) 	01-06-2017r	20-06-2017r	<p>Wydział Organizacyjny</p>

<p>5. Weryfikacja zbioru/ów danych osobowych oraz oprogramowani.</p> <p>Zbiory:</p> <ol style="list-style-type: none"> 1. Księgowość finansowa oraz rozliczenia należności podatkowych i opłat 2. Planowanie przestrzenne. 3. Dziennik Korespondencji Przychodzącej 4. Dziennik Korespondencji przychodzącej BIF 5. Dziennik Korespondencji przychodzącej USC 6. Rejestr decyzji na zajęcie pasa drogowego i uzgodnień drogowych 7. Ewidencja uczestników zamówień publicznych 8. Rejestr Ofert 9. Rejestr wniosków o udzielenie informacji publicznej <p>Systemy informatyczne:</p> <ul style="list-style-type: none"> - pakiety biurowe; - Formularze IPS(IPS Przedsiębiorstwo Informatyczne - e-Petron2 (Petron) 			<p>❖ Weryfikacja zbiorów</p> <p>❖ Sprawdzamy, czy wszystkie dane są przetwarzane legalnie, czyli czy został spełniony jeden z warunków postawionych w art. 23. ust.1 ustawy</p>
		<p>01-07-2017r</p> <p>01-10-2017r</p>	<p>20-09-2017r</p> <p>20.10.2017r</p>
			<p>-pomieszczenie serwerowni</p> <p>- pokój 138</p> <p>-punkt informacyjny</p> <p>-sekretariat</p> <p>Wydział Budżetu i Finansów:</p> <p>- pokoje 280, 276, 263, 263A, 254, 267, 252, 251, 268</p> <p>Wydział Planowania Inwestycji i drogownictwa:</p> <p>- pokoje 260, 261, 262, 262A</p>

<p>- DOC.pl System Wsparcia Gmin w realizacji zadań wynikających z regulacji Ustawy o Utrzymaniu Czystości i Porządku w Gminach (u.c.p.g.) – (RAD Sp. z o.o.)</p> <p>- Ewidencja i rozliczanie podatku VAT II inst. (ZSI SIGID)</p> <p>- Ewidencja i rozliczanie podatku VAT (ZSI SIGID)</p> <p>-Kadry i Place (Unit Szczecin)</p> <p>- System Finansowo - Księgowy S-Finks (Unit Szczecin)</p> <p>- Płatnik ZUS (ASSECO)</p> <p>- Biznes Pl@net (Bank BGZ BNP Paribas S.A.)</p> <p>- Bestia (SPIN S.A.)</p> <p>- Ewidencja opłat dzierżawnych II instalacja (ZSI SIGID)</p> <p>- Księgowość budżetowa jednostki i zarządu III inst</p>			
---	--	--	--

<p>(ZSI SIGID)</p> <ul style="list-style-type: none"> - Księgowość budżetowa jednostki i zarządu II inst (ZSI SIGID) - Księgowość budżetowa jednostki i zarządu I inst (ZSI SIGID) - Podatek od nieruchomości dla osób fizycznych (ZSI SIGID) - Podatek od nieruchomości dla osób prawnych (ZSI SIGID) - Podatek rolny/leśny/nieruchomości dla osób fizycznych (ZSI SIGID) - Podatek rolny/leśny dla osób prawnych (ZSI SIGID) - Podatek od środków transportowych (ZSI SIGID) - Ewidencja opłat dzierżawnych (ZSI SIGID) - Ewidencja opłat za wieczyste użytkowanie (ZSI SIGID) - Program obsługi kasy (ZSI SIGID) - Ewidencja i drukowanie faktur (ZSI SIGID) - Kadry i płace 			
---	--	--	--

<p>pracowników urzędu i oświaty (ZSI SIGID)</p> <ul style="list-style-type: none"> - Kadry i place pracowników urzędu i oświaty II inst (ZSI SIGID) - Ewidencja środków trwałych i wyposażenia (ZSI SIGID) - Programy obsługi mandatów kredytowych (ZSI SIGID) 				
---	--	--	--	--

Dokumentowanie czynności w toku sprawdzenia zawiera w szczególności:

1. Sporządzeniu notatki z czynności, w szczególności z zebranych wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;
2. Odebraniu wyjaśnień osoby, której czynności objęto sprawdzeniem;
3. Sporządzeniu kopii otrzymanego dokumentu, sporządzeniu kopii obrazu wyświetlonego na ekranie urządzenia stanowiącego część systemu informatycznego służącego do przetwarzania lub zabezpieczania danych osobowych;
4. Sporządzeniu kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych osobowych lub zapisów konfiguracji technicznych środków zabezpieczeń tego systemu.

Sporządził: Administrator Bezpieczeństwa Informacji



Zatwierdził: Administrator Danych

BURMISTRZ

Maryna Podzińska

