

17.12.2019 r.

Audyt wewnętrzny

Andrzej Hawran

/usługobiorca/

kontakt:

(preferowany) mail: sekretariateiuap@radca-hawran.pl
dyrektoreiuap@radca-hawran.pl

tel. 505 667 853, 507 940 096

pn – pt. godz. 7.00 - 15.00

www: <https://radca-hawran.pl/uslugi-dla-administracji-publicznej/>

znak: NOWE.52.1720.1.2019.11

**SPRAWOZDANIE Z ZADANIA AUDYTOWEGO
przeprowadzonego
w Urzędzie Gminy Nowe**

Temat zadania: monitorowanie przestrzegania rozporządzenia oraz innych przepisów unii i państw członkowskich oraz polityk administratora.

Obszar działalności: : Urząd Gminy Nowe, Stanowisko: Inspektor Ochrony Danych Osobowych

Cel zadania:

1. zebranie informacji i wydanie opinii o funkcjonującym systemie zarządzania bezpieczeństwem informacji.
2. racjonalne zapewnienie Burmistrza Gminy Nowe, że podejmowane działania w obszarze bezpieczeństwa informacji są realizowane.

Zakres podmiotowy zadania: badaniem objęto Urząd Gminy Nowe.

Zakres przedmiotowy zadania: objęte badaniem zostanie wykonywanie obowiązków wynikających z przepisów prawa związanych z ochroną danych osobowych.

Data rozpoczęcia zadania: 21.11.2019 r.; rozpoczęcie zadania.

USTALENIA:

1. przepisy prawa powszechnie obowiązujące
2. przepisy prawa wewnętrznie obowiązujące
3. informacje na stronie BIP
4. pismo z 25.11.2019r.
5. pismo z 25.11.2019r.
6. pismo z 15.12.2019r.
7. pismo z 16.12.2019r.

Zarządzeniem nr 274/2018 z dnia 8 czerwca 2018 r. powołano w Gminie Nowe Inspektora ODO Agnieszka Stawicka.

Zarządzeniem nr 275/2018 z dnia 8 czerwca 2018 wprowadzono Politykę Ochrony Danych w Gminie Nowe.

Polityka Ochrony Danych składa się::

- zał. 1 — wykaz osób zapoznanych z Polityką,
- zał. 12 - ewidencja osób upoważnionych,
- zał. 17 — rejestr umów powierzenia danych,
- zał. 19 — rejestr naruszeń,

Zarządzeniem nr 269/2018 z dnia 24 kwietnia 2018 r. wprowadzono rejestr czynności przetwarzania Gminy Nowe.

Zarządzeniem nr 76/2019 z dnia 13 maja 2019 r. wprowadzono rejestr kategorii czynności przetwarzania danych osobowych.

Dokonano aktualizacji:

- aktualizacja Polityki Ochrony Danych w obszarze zał. 13 — środki techniczne i organizacyjne zarządzeniem nr 99/2019 z dnia 29 sierpnia 2019r.

Dokonano przeglądu aktualności Polityki w zakresie Systemów informatycznych wykorzystywanych w Urzędzie, w których są przetwarzane dane osobowe oraz sposobu postępowania z kluczami do budynku i pomieszczeń biurowych. Opracowano szczegółowe zasady postępowania z kluczami wraz z wykazem osób upoważnionych do otwierania budynku, pobierania/ otrzymania kluczy do pomieszczeń).

Zarządzeniem nr 59/2019 z dnia 13 marca 2019 r. dokonano aktualizacji rejestru czynności przetwarzania danych.

Systemy informatyczne zostały zinwentaryzowane i stanowią element zał. 13 do Polityki, ponadto dodatkowo informatyk prowadzi spis systemów informatycznych. Nazwy systemów informatycznych funkcjonujących w Urzędzie Gminy Nowe:

1. PB_EWID (Ewidencja Ludności – Urząd Stanu Cywilnego).
2. BUDŻET (Księgowość budżetowa z planowanie).
3. PODATKI.
4. KSGZOB (Księgowość zobowiązań).
5. KASA.
6. JGU (System wymiaru podatków lokalnych od osób prawnych).
7. AUTA (System wymiaru podatku od środków transportowych).
8. DZIERŻAWY (System ewidencji i wymiaru dzierżaw czasowych).
9. OPLOK (System wymiaru opłat lokalnych – opłata za odpady).
10. PŁACE (Program kadrowo-płacowy).
11. REJESTR VAT (System ewidencji zakupu, sprzedaży, fakturowania i VAT).
12. UŻYTKOWANIE WIECZYSTY (Program do zintegrowanego zarządzania umowami i opłatami z tytułu użytkowania wieczystego).
13. EGZEKUCJE.
14. PŁATNIK (ZUS).
15. PROGMAN MAJĄTEK WEB (Ewidencja środków trwałych).

W okresie ostatnich 5 lat w obszarze działalności nie zostały przeprowadzone kontrole zewnętrzne.

W okresie ostatnich 3 lat w obszarze działalności IOD przeprowadził kontrolę wewnętrzną:

1. w dniu 16 czerwca 2018r. w zakresie:
 - a) zasady wdrożenia odpowiednich środków technicznych i organizacyjnych,
 - b) wskazano na przykładowe tzw. dobre praktyki w zakresie ochrony danych osobowych w zakresie zabezpieczeń systemu informatycznego, przetwarzania wizerunku,
 - c) prawnych zasad funkcjonowania monitoringu przekazano informacje o zmianach w przepisach,
 - d) system nadzoru nad kluczami do szaf tzw. polityka kluczy do szaf,
 - e) polityka czystego biurka
 - f) odpowiednie ustawienie monitora
 - g) pseudonimizacja - Rekrutacja pracowników
 - h) sposób w jaki jest prowadzona lista obecności pracowników
 - i) sytuacje udzielania informacji bankom o pracownikach ubiegających się o kredyt,
 - j) miejsce przechowywania akt osobowych,
 - k) ZFSS

- l) wskazano na konieczność zawarcia umowy powierzenia
- m) wyjaśniono zasady stosowania obowiązku informacyjnego (art. 13 RODO),
- 2. 25.09.2018 r. — dokonano przeglądu środków technicznych i organizacyjnych, sporządzono notatkę ze spotkania z rekomendacjami.
- 3. 28.08.2019r. -dokonano analizy stosowania klauzul informacyjnych zgodnie ze zmianami w przepisach ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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).
Przeanalizowano obowiązek informacyjny:
 - 1. ustawa z dnia 29 stycznia 2004 r. - prawo zamówień publicznych- art.8a,
 - 2. ustawa z dnia 27 marca 2003r. o planowaniu i zagospodarowaniu przestrzennym
 - 3. wskazano rekomendacje w zakresie deklaracji śmieciowej,
 - 4. opracowano politykę kluczy (aktualizacja zał. 12 do Polityki)

W okresie ostatnich 2 lat w obszarze działalności zostały przeprowadzone następujące kontrole funkcjonalne.

W dniu 07.03.2019 r. został przeprowadzony w Urzędzie Gminy Nowe audyt bezpieczeństwa informacji przez firmę: Centrum Bezpieczeństwa Informatycznego. Celem audytu było przedstawienie zaobserwowanego przez audytorów stanu bezpieczeństwa informacji w jednostce oraz wskazanie ewentualnych podatności mających wpływ na przetwarzane dane. Audyt został przeprowadzony pod kątem zgodności z obowiązującymi przepisami prawa w zakresie przetwarzania informacji oraz dobrych praktyk i standardów bezpieczeństwa. Audyt został zrealizowany na podstawie udostępnionej dokumentacji (procedur), sprzętu oraz w oparciu o przepisy prawne:

- a) Ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tj. Dz. U. z 2017 r. poz. 570 z późn. zm.);
- b) Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U. 2017 poz. 2247 z późn. zm.);
- c) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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);
- d) Normy ISO: 27001:2017, 27005:2017.

Na podstawie stanu faktycznego (07.03.2019 do 18.04.2019) sporządzono dnia 18.04.2019 raport pn.: „Urząd Gminy Nowe Raport z audytu" wraz z rekomendacjami.

W dniu 13 marca 2019 r. przeprowadzono analizę zagrożeń i ryzyka przy przetwarzaniu danych osobowych w Urzędzie Gminy Nowe przez firmę: Centrum Bezpieczeństwa Informatycznego. Analiza została zrealizowana na podstawie udostępnionej dokumentacji (procedur), wywiad zebrany od administratora sieci, audyt IT oraz w oparciu o przepisy prawne:

- Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i ich swobodnym przepływem Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (RODO) art. 24 i 32 oraz odpowiednie motywy preambuły RODO —(51), (75), (76), (82), (83), (90), (91).

- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz.1000).
Na podstawie stanu faktycznego sporządzono raport pn.: "Analiza zagrożeń i ryzyka przy przetwarzaniu danych osobowych" wraz z rekomendacjami.

Lp.	Pytanie	TAK	NIE	ND	Uzupełnienie odpowiedzi bądź inna odpowiedz; Dowód /opisowo bądź skan/	uwagi
1	I. Podstawy prawne przetwarzania					
2	RODO art. 6, motyw 40-57. Czy dokonano przeglądu procesów związanych z przetwarzaniem danych osobowych pod kątem ustalenia podstawy prawnej przetwarzania danych osobowych	1				
3	Czy do zidentyfikowanych zbiorów danych/procesów przetwarzania danych określono podstawę prawną	1				
4	II. Zgoda na przetwarzanie danych osobowych					
5	Identyfikacja zakresu danych dla przetwarzania których wymagana jest zgoda. Czy jednostka zidentyfikowała dane osobowe, do przetwarzania których wymagana jest zgoda	1				
6	Czy określono wzory zgód uwzględniających wymogi RODO	1				
7	RODO; art. 4 pkt 11, motyw 32. Zgoda powinna być jednoznaczna, dobrowolna, świadoma i ma postać pisemnego lub ustnego oświadczenia. Czy treść zgody potwierdza dobrowolne, konkretne, świadome i jednoznaczne wyrażenie woli	1				
8	RODO; art. 4 pkt 11, art. 7, motyw 32. Zgoda powinna być udokumentowana. Czy administrator jest w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych osobowych	1				
9	RODO; art. 7. Zgoda musi zostać przedstawiona w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii. Czy zgoda została przedstawiona osobie, której dane dotyczą w sposób pozwalający wyraźnie odróżnić ją od innych kwestii	1				
10	motyw 32. Do każdego celu przetwarzania powinna być uzyskana zgoda. Jeśli przetwarzanie służy różnym celom, czy uzyskano zgodę osoby, której dane dotyczą na wszystkie cele	1				
11	motyw 42. Oświadczenie powinno być zrozumiałe i mieć łatwo dostępną formę. Czy oświadczenie o wyrażeniu zgody przygotowane przez administratora ma zrozumiałą i łatwo dostępną treść i formę, jest sformułowane jasnym i prostym językiem i nie zawiera nieuczciwych warunków	1				
12	motyw 42. Osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych. Czy ze zgody wynika tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych	1				
13	RODO art. 7 ust 3. Osoba, której dane dotyczą powinna mieć możliwość cofnięcia zgody. Czy osoba, której dane dotyczą została poinformowana o możliwości cofnięcia zgody	1				
14	RODO Art. 7 ust 4 motyw 43. Równość stron. Czy od zgody nie uzależnia się wykonania umowy, jeśli przetwarzanie danych osobowych jest niezbędne do wykonywania tej umowy	1				
15	III. Prawa osoby której dane dotyczą					
16	RODO art. 12, 14 ust. 3 pkt a-c i ust.5 , art. 15 ust. 3; motyw: motywy 39, 58, 59, 60, 61, 64, 68. Każda osoba powinna mieć kontrolę nad dotyczącymi jej danymi osobowymi. Czy opracowano procedurę udzielania informacji osobom, których dane osobowe dotyczą	1				
17	RODO Art.13 Administrator ma obowiązek w prostej i zrozumiałej formie udzielić informacji, wg katalogu ustalonego przez ustawodawcę unijnego, osobie	1				

	której dane osobowe dotyczą. Czy opracowano treść klauzuli informacyjnej dla osób, od których dane osobowe będą (pozyskiwane, zbierane) przetwarzane				
18	RODO Art.13 Jeżeli odpowiedź na powyższe pytanie jest twierdząca, to czy wzór klauzuli zawiera:	1			
19	a) tożsamość i dane kontaktowe administratora	1			
20	b) dane kontaktowe inspektora danych osobowych gdy został powołany	1			
21	c) cele przetwarzania oraz podstawę prawną przetwarzania	1			
22	d) odbiorców danych	1			
23	e) zamiar przekazywania danych do państwa trzeciego lub organizacji międzynarodowej	1			
24	f) okres przechowywania danych lub kryteria ustalania tego okresu	1			
25	g) prawo dostępu do danych sprostowania, usunięcia, ograniczenia, przetwarzania, wniesienia sprzeciwu, przenoszenia danych	1			
26	h) prawo do cofnięcia zgody w dowolnym momencie	1			
27	i) prawo wniesienia skargi do organu nadzorczego	1			
28	j) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu	1			
29	k) informacje o obowiązku podania danych i z czego wynika	1			
30	RODO, Art. 12, 14 ust. 3 pkt a-c i ust.5 , Art. 15 ust. 3 motyw: motywy 39, 58, 59,60,64,68. Administrator ma obowiązek w prostej i zrozumiałej formie udzielić informacji, wg katalogu ustalonego przez ustawodawcę unijnego, osobie której dane osobowe dotyczą. Czy opracowano klauzulę informacyjną dla osób, których dane będą przetwarzane, a których dane pozyskano w sposób inny niż od osoby której dane dotyczą	1			
31	RODO Art. 14. Jeżeli odpowiedź na powyższe pytanie jest twierdząca, to czy klauzula ta zawiera:	1			
32	a) tożsamość administratora i dane kontaktowe	1			
33	b) cele przetwarzania i podstawę prawną przetwarzania	1			
34	c) dane kontaktowe do IOD.	1			
35	d) kategorie odnośnych danych osobowych	1			
36	e) informacje o odbiorcach danych osobowych lub kategoriach odbiorców	1			
37	f) zamiar przekazywania danych do państwa trzeciego lub organizacji międzynarodowej	1			
38	g) okres przechowywania danych lub kryteria ustalania tego okresu	1			
39	h) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust 1 lit. f wskazanie prawnie uzasadnionego interesu administratora lub osobę trzecią				
40	i) prawo dostępu do danych , sprostowania, usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania, o prawie do przenoszenia danych	1			
41	j) prawo do cofnięcia zgody w dowolnym momencie jeżeli przetwarzanie odbywa się na podstawie art. 6 ust.1 lit a (zgoda) lub art. 9 ust.2 lit. A	1			
42	k) prawo wniesienia skargi do organu nadzorczego	1			
43	l) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie czy pochodzą one ze źródeł publicznie dostępnych	1			
44	m) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu (zasady i konsekwencje)	1			
45	n) inne informacje (np. dalsze przetwarzanie)	1			

46	RODO Art. 13 ust.4 motyw 62. Czy dokonano przeglądu danych osobowych już przetwarzanych pod względem uzyskania zapewnienia, że osoba, której dane przetwarzamy dysponuje informacjami	1				
47	IV. Administrator					
48	RODO art. 4 pkt 7. Identyfikacja Administratora danych (kolejno administratora). Czy wskazano kto jest administratorem danych	1				
49	RODO art. 24 motyw 74. Czy w jednostce istnieją formalne procedury lub jednolite i powtarzalne praktyki dotyczące zabezpieczeń organizacyjnych mających wpływ na te bezpieczeństwo przetwarzanych danych osobowych, w szczególności dotyczące:	1				
50	a) zarządzania incydentami	1				
51	b) sposobu nadzoru, w tym kontroli, sprawdzeń, audytów i raportowania alertów	1				
52	RODO Art. 24 motyw: 74, 156. Czy w jednostce wdrożono procedury lub jednolite i powtarzalne praktyki dotyczące kontroli logicznej w procesach przetwarzania danych osobowych, w szczególności:	1				
53	a) anonimizację	1				
54	b) środki ochrony kryptograficznej	1				
55	c) środki kontroli integralności danych	1				
56	d) środki kontroli dostępu do danych	1				
57	e) środki kontroli dotyczące rozliczalności wykonywanych operacji	1				
58	f) środki bieżącego monitoringu	1				
59	g) zastosowane środki ochrony przed działaniem oprogramowania szkodliwego typu wirusy, środki szpiegujące, środki służące ochronie przed wykradaniem danych itp.	1				
60	h) środki ochrony sieci przed działaniem osób z zewnątrz	1				
61	RODO Art. 24 motyw: 74. Czy w jednostce wdrożono środki ochrony fizycznej, w tym: środków bezpieczeństwa infrastruktury technicznej wykorzystywanej do przetwarzania danych	1				
62	a) środków bezpieczeństwa infrastruktury technicznej wykorzystywanej do przetwarzania danych	1				
63	RODO Art. 24 motyw: 74. b) środków bezpieczeństwa dokumentacji papierowej, w tym papierowych rejestrów zawierających dane osobowe	1				
64	RODO Art. 24 motyw: 74 c) środków ochrony przed awarią zasilania lub zakłóceniami w sieci zasilającej	1				
65	RODO art. 38. Czy IOD był szkolony/ podnosił kwalifikacje z zakresu przetwarzania danych osobowych, w szczególności ze zmian wynikających z RODO	1				
66	Czy zapewniono innym (niż IOD) pracownikom jednostki szkolenia itp. z zakresu zmian wynikających z RODO	1				
67	V. Umowy powierzenia					
68	RODO Art. 28 ust 3 i 9, motyw 81. Umowy powierzenia przetwarzania danych osobowych. Czy Administrator powierzył przetwarzanie danych osobowych, związane ze świadczeniem określonych usług, na podstawie zawartej umowy: w formie pisemnej, w tym w wersji elektronicznej	1				
69	Czy opracowano wzory umów o powierzeniu przetwarzania danych osobowych związanych ze świadczeniem usług	1				
70	RODO Art. 28 ust 3 motyw: 81. Jeżeli odpowiedź na powyższe pytanie jest twierdząca, czy wzory umów zawierają:	1				
71	a) przedmiot przetwarzania	1				

72	b) czas trwania przetwarzania	1				
73	c) charakter i cel przetwarzania	1				
74	d) rodzaj danych osobowych	1				
75	e) kategorie osób których dane dotyczą	1				
76	f) obowiązki i prawa administratora	1				
77	RODO Art. 28 ust 3 pkt b, h, 32-36. g) obowiązki podmiotu przetwarzającego	1				
78	RODO Art. 28 ust 3. Czy umowy o powierzeniu przetwarzania danych osobowych zawierają następujące obowiązki przetwarzającego:	1				
79	RODO Art. 28 ust. 2, 4 i 3 d. a) warunki korzystania z usług innego podmiotu przetwarzającego (podwykonawcy).	1				
80	RODO Art 30 ust 2. b) prowadzenie rejestru wszystkich kategoriach czynności przetwarzania danych osobowych dokonywanych w imieniu administratora.		1			
81	c) zgłoszenia naruszenia ochrony danych osobowych	1				
82	RODO Art. 28 ust3b. d) zobowiązanie do zachowania tajemnicy.	1				
83	RODO Art. 28 ust 3 c. e) wymagane środki zabezpieczające przetwarzane dane.	1				
84	RODO Art. 28 ust3 f. f) pomoc administratorowi w ocenie skutków dla ochrony danych	1				
85	RODO Art. 28 ust.3 g. g) archiwizowania lub zwrotu lub usunięcia danych osobowych po zakończeniu przetwarzania danych osobowych.	1				
86	Czy powierzono wyznaczonemu pracownikowi monitorowanie zawieranych umów na przetwarzanie danych osobowych, w związku ze świadczeniem określonych usług w celu zabezpieczenia ochrony powierzanych danych osobowych	1				
87	VI. Inspektor ochrony danych					
88	RODO Art. 37 Projekt UODO art. 7 UOFP art. 9. Obowiązek wyznaczenia inspektora ochrony danych (dalej IOD). W jaki sposób kierownik jednostki spełnił obowiązek dotyczący wyznaczenia inspektora ochrony danych (dalej IOD)	1				
89	RODO Art. 38 ust 6. . Czy wyznaczony IOD będzie wykonywał inne zadania i obowiązki		1			
90	RODO Art. 38 ust 6. Jeśli TAK to czy dodatkowe zadania i obowiązki będą powodowały konflikt interesów		1			
91	RODO Art. 38 motyw: 97. Status IOD. Czy IOD włączany jest we wszystkie procesy przetwarzania danych od 25 maja 2018 r.		1			
92	RODO Art. 38 ust. 3. Czy zapewniono, iż IOD podlega bezpośredniej podległości pod administratora (25 maja 2018r.)			1		
93	RODO Art. 39 motyw: 97. Zadania IOD. Czy pisemnie powierzono IOD zadania, o których mowa w art. 39 RODO	1				
94	RODO Art. 38 ust. 4 . Czy utworzono na stronie www. jednostki, zakładki RODO/ochrona danych osobowych/, która uwzględniałaby w szczególności dane osobowe IOD oraz jego zadania	1				
95	UODO Art. 36a.2.c. Czy w 2018r. IOD przeprowadzał z pracownikami jednostki szkolenia, oficjalne spotkania lub udokumentowane pogadanki z zakresu przepisów o ochronie danych osobowych, które uwzględniały istotne zmiany wynikające z RODO	1				
96	VII. Rejestrowanie czynności przetwarzania danych osobowych					
97	RODO Art. 30 pkt. 1 i 3 motyw: 82 Rejestr czynności przetwarzania danych osobowych za które odpowiada administrator.	1				

98	RODO Art. 30 pkt. 1 a - g. Zawartość rejestru czynności przetwarzania danych osobowych. Czy przygotowywany przez administratora rejestr czynności przetwarzania danych osobowych za które odpowiada zawiera wszystkie wymagane elementy	1				
99	RODO Art. 30 pkt. 1 a. a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych	1				
100	RODO Art. 30 pkt. 1 b. b) Cele przetwarzania	1				
101	RODO Art. 30 pkt. 1 c. c) Opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych,	1				
102	RODO Art. 30 pkt. 1 d. d) Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub organizacjach międzynarodowych	1				
103	RODO Art. 30 pkt. 1 e. e) Gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazania, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń,	1				
104	RODO Art. 30 pkt. 1 g. . f) Jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.	1				
105	RODO Art. 30 pkt. 2 motyw: 82. Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora przez podmiot przetwarzający/przedstawiciel podmiotu przetwarzającego. Czy jednostka jest podmiotem przetwarzającym	1				
106	RODO Jw. 30 pkt. 3 Standardy kontroli zarządczej. Dokumentowanie. Czy opracowano rejestr wszystkich kategorii czynności	1				
107	RODO Jw. 30 pkt. 1 a – d. Zawartość rejestru wszystkich kategorii czynności przetwarzania danych osobowych. Czy przygotowywany przez podmiot przetwarzający rejestr wszystkich kategorii czynności przetwarzania danych osobowych zawiera wszystkie wymagane elementy	1				
108	VIII. Zabezpieczenie danych na podstawie oszacowanego ryzyka					
109	RODO Art. 32. Nie naruszanie praw i wolności, w szczególności prawa do ochrony danych osobowych. Czy w jednostce opracowano procedury zarządzania ryzykiem uwzględniające aspekty RODO	1				
110	motyw 74, 75, 76, 77, 78, 83, RODO art. 32. Przeprowadzenie analizy ryzyka. Czy w jednostce przeprowadzono analizę uwzględniającą ryzyko naruszenia praw lub wolności osób fizycznych wynikające z przetwarzania danych osobowych?. (w szczególności ryzyko wynikające z: przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych).	1				
111	motyw 74, 75, 76, 77, 78, 83, art. 32 ust.1 RODO. Wdrożenie odpowiednich środków technicznych i organizacyjnych opartych na analizie ryzyka. Czy wyniki analizy ryzyka wykazały potrzebę wdrożenia odpowiednich (dodatkowych) środków technicznych lub organizacyjnych	1				
112	motyw 74, 75, 76, 77, 78, 83, art. 32 RODO. Wdrożenie odpowiednich środków technicznych i organiza-				1	Na etapie reali-

	cyjnych opartych na analizie ryzyka. Czy w jednostce wdrożono odpowiednie środki techniczne i organizacyjne oparte na wykonanej analizie ryzyka, wyniki analizy ryzyka wykazały potrzebę wdrożenia odpowiednich (dodatkowych) środków technicznych lub organizacyjnych					zacji
113	IX. Ocena skutków dla ochrony danych					
114	motyw: 84, 89-93, RODO art. 35. Dokonanie oceny skutków dla ochrony danych w przypadku, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych. Czy występują operacje przetwarzania danych, dla których poziom ryzyka naruszenia praw lub wolności osób fizycznych oceniono jako wysoki		1			
115	motyw: 84, 89-93, RODO art. 35. Dokonanie oceny skutków dla ochrony danych w przypadku, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.. Czy wśród planowanych operacji przetwarzania danych występują operacje, dla których poziom ryzyka naruszenia praw lub wolności osób fizycznych oceniono jako wysoki		1			
116	motyw: 84, 89-93, RODO art. 35. Dokonanie oceny skutków dla ochrony danych w przypadku, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych. Czy dla planowanych operacji przetwarzania danych, dla których poziom ryzyka naruszenia praw lub wolności osób fizycznych oceniono jako wysoki, przewiduje się dokonanie (dokonano) ocenę skutków dla ochrony danych	1				
117	motyw: 84, 89-93, RODO art. 35 ust.7 . Dokonanie oceny skutków dla ochrony danych w przypadku, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych. Czy jednostka określiła sposób dokonania oceny skutków dla ochrony danych (np. w formie procedury)	1				
118	X. Pseudoanonimizacja					
119	RODO: Art. 4 pkt.5 motyw: 26. Pseudoanonimizacja danych osobowych. Czy w jednostce jest/ będzie stosowana pseudoanonimizacja danych w procesie przetwarzania danych osobowych		1			
120	XI. Informowanie o naruszeniach ochrony danych					
121	RODO Art. 33 motyw: 85. Informowanie organu nadzorczego i osoby, której dane dotyczą o naruszeniach. Czy IOD i ASI zna nowy obowiązek zgłaszania naruszeń ochrony danych osobowych do organu nadzorczego w ciągu 72 h po stwierdzeniu naruszenia	1				
122	RODO Art. 34 motywy: 86. Czy IOD i ASI zna nowy obowiązek zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych	1				
123	motyw: 88. Czy istnieje procedura zgłaszania naruszeń ochrony danych osobowych? Jeśli na powyższe pytanie odpowiedziano TAK proszę odpowiadać na kolejne pytania w tym obszarze.	1				
124	Zakres procedury. Czy w procedurze uwzględniono definicję naruszenia wymagającego zgłoszenia do organu nadzorczego	1				
125	RODO Art. 33 motywy: 85, 87-88. Informowanie organu nadzorczego o naruszeniach. Czy w procedurze uwzględniono maksymalny czas zgłoszenia naruszenia do organu nadzorczego? (natychmiast po stwierdzeniu naruszenia, bez zbędnej zwłoki, max. do 72 h).	1				

126	RODO Art. 33 ust 5. Czy w procedurze uwzględniono obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze	1				
127	RODO Art. 34 motyw: 86-88. Informowanie osoby, której dane dotyczą o naruszeniach. Czy w procedurze uwzględniono czas na poinformowanie osoby, której dane dotyczą, o naruszeniu	1				
	razem	106	7	1		

Opinia audytora wewnętrznego:

**W BADANYM OBSZARZE AUDYTU WEWNĘTRZNEGO
/por. temat zadania/
AUDYTOR WEWNĘTRZNY NIE DOSTRZEGŁ UCHYBIEN**

Skoro uchybień nie dostrzeżono, nie sformułowano zaleceń w badanym obszarze.

**BADANIE AUDYTOWE OPOWIADA SIĘ
ZA POZYTYWNA OCENĄ AUDYTOWANEGO
W OPARCIU O PRZYJĘTE KRYTERIUM.**

**Audytora wewnętrznego
Andrzej Hawran**
/podpis na oryginale/

zaświadczenie Ministra Finansów
nr 264/2004

Doręczenie wyłącznie elektronicznie na adres:

1. burmistrz@gminanowe.pl