Nasz znak:	Dotyczy pisma znak:	z dnia:	Data
RO.1431.31.2022		03.07.2022	31.08.2022

W odpowiedzi na wniosek o udostępnienie informacji publicznej w trybie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) z dnia 3 lipca 2022 r. przesłany za pośrednictwem poczty elektronicznej, Burmistrz Tykocina informuje j.n:

1. **Czy na stronie www są pełne danych IOD?**TAK
2. **Wnosimy o dokumentację potwierdzająca realizację zadań przez IOD lub opis jego działań od dnia 25 maja 2018 roku (zadań wynikających z art. 39 rozporządzenia RODO)**

IOD od dnia 25 maja 2018 roku wykonywał zadania w zakresie:

a) informowania administratora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowania przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania;

c) udzielania na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d) współpracy z organem nadzorczym;

e) pełnienia funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

3. **Czy zostały opracowane i wdrożone przepisy wewnętrzne, procedury, instrukcje i inne dokumenty dotyczące przetwarzania danych osobowych oraz bezpieczeństwa informacji. Jeśli tak to jakie?**

Urząd dysponuje Polityką Bezpieczeństwa Informacji. Polityka Bezpieczeństwa Informacji określa podstawowe zasady zarządzania bezpieczeństwem informacji oraz podmioty odpowiedzialne za ochronę informacji w Urzędzie Miejskim w Tykocinie. Zasady zarządzania bezpieczeństwem informacji w Urzędzie zostały opracowane zgodnie z obowiązującymi przepisami oraz w oparciu o wymagania Polskich Norm i standardów w obszarze bezpieczeństwa informacji.

4. **Wnosimy o przedłożenie dokumentu potwierdzającego zapoznanie się pracowników z treścią obowiązujących przepisów wewnętrznych, ewentualnie wskazanie w jaki sposób zostali oni zapoznani.**

Pracownicy otrzymali treść przepisów wewnętrznych do wglądu i zapoznania się, dodatkowo przeprowadzone zostało wewnętrzne szkolenie obejmujące tematyką regulacje wewnętrzne.

5. **Informacje dotyczące szkoleń pracowników w zakresie ochrony danych osobowych przeprowadzanych po 25 maja 2018 roku (informacje tj. data szkolenia, zakres szkolenia, osoba prowadząca, listy obecności, czas trwania).**

Szkolenie 16.01.2020 „Polityka ochrony danych osobowych w Urzędzie Miejskim w Tykocinie" (2,5h na grupę szkoleniową). Prowadzącym był nasz IOD.

Zakres obejmował: podstawy prawne przetwarzania danych, zadania i kompetencje Urzędu Ochrony Danych Osobowych, omówienie wewnętrznej dokumentacji z zakresu ochrony danych, zadania IOD, administratora oraz pracowników, zasady przetwarzania danych, prawa osób których dane dotyczą, obowiązek informacyjny, naruszenia ochrony danych, omówienie wybranych kar nałożonych przez UODO. Ponadto każdy pracownik po zatrudnieniu zostaje przeszkolony przez IOD w sposób indywidualny w zakresie ochrony danych osobowych w Urzędzie

6. **Czy został opracowany Rejestr czynności przetwarzania danych osobowych oraz jego zmiany.**

Tak, Urząd prowadzi rejestr czynności przetwarzania.

7. Czy został opracowany Rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany?

Tak, Urząd prowadzi rejestr kategorii czynności przetwarzania.

8. W jaki sposób realizowany jest obowiązek informacyjny – art. 13 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne

Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, administrator podczas pozyskiwania danych osobowych wykonuje obowiązek informacyjny. Klauzule informacyjne dostępne są w BIP, pozostałe klauzule zamieszcza się na wnioskach i drukach. Obowiązek ten jest wypełniany przy wszystkich czynnościach tego wymagających

***9.* W jaki sposób realizowany jest obowiązek informacyjny – art. 14 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne.**

Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są nie od tej osoby, administrator podczas pozyskiwania danych osobowych wykonuje obowiązek informacyjny.

10. Wnosimy o regulacje dotyczące monitoringu wizyjnego (jeśli jest). Procedura i Regulamin w tym zakresie.

Urząd opracował klauzulę informacyjną dotycząca monitoringu wizyjnego. Informacja o zakresie stosowania monitoringu została przekazana pracownikom oraz umieszczona w regulaminie pracy.

***11.* Czy IOD w ramach monitorowania przeprowadza regularne i systematyczne sprawdzenia/audyty w zakresie prawidłowości przetwarzania danych osobowych oraz przestrzegania rozporządzenia RODO, ustawy o.d.o. oraz regulacji wewnętrznych? Dokumentacja w tym zakresie (plany, sprawozdania, raporty, itp.).**

IOD dokonuje na bieżąco weryfikacji poprawności przetwarzania danych osobowych. Zidentyfikowane nieprawidłowości korygowane są na bieżąco. Wytworzone dokumenty zawierające zagrożenia oraz podatności nie podlegają udostępnieniu na podstawie ustawy o dostępie do informacji publicznej.

12. W trybie dostępu do informacji publicznej – zwracamy się z prośbą o informację, czy w związku z monitoringiem wizyjnym miejsc publicznych prowadzonym przez Państwa jednostkę była prowadzona była ocena skutków w rozumieniu art. 35 ust. 1 rodo stosownie do treści tego przepisu:

Analiza skutków nie jest wymagana.

13. Mając na uwadze powyższe wnosimy o informację czy została opracowana polityka retencji danych? Jakich czynności ona dotyczy?

Retencja danych określona została w rejestrze czynności przetwarzania.

Wnosimy o wykazanie kwalifikacji IOD w zakresie wiedzy prawniczej? Czy IOD jest prawnikiem? Jakie posiada doświadczenie? Kto i w jaki sposób weryfikował kwalifikacje IOD?

IOD posiada kompetencje, o których mowa w art. 37 ust. 5 tj. „ Inspektor ochrony danych jest wyznaczony na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania zadań, o których mowa w art. 39.

Żaden przepis prawa nie wymaga tego, aby IOD legitymował się dyplomem potwierdzającym uzyskanie wykształcenia prawniczego. Weryfikacja została przeprowadzona przez pracowników Administratora.

W jaki sposób odbywają się systematyczne szkolenia pracowników prowadzone przez IOD. Proszę wskazać, kiedy miały one miejsce oraz zakres szkolenia – pomijając ogólny instruktaż i zapoznanie się z przepisami dot. ochrony danych.

Szkolenie 16.01.2020 „Polityka ochrony danych osobowych w Urzędzie Miejskim w Tykocinie" (2,5h na grupę szkoleniową). Prowadzącym był nasz IOD.

Zakres obejmował: podstawy prawne przetwarzania danych, zadania i kompetencje Urzędu Ochrony Danych Osobowych, omówienie wewnętrznej dokumentacji z zakresu ochrony danych, zadania IOD, administratora oraz pracowników, zasady przetwarzania danych, prawa osób których dane dotyczą, obowiązek informacyjny, naruszenia ochrony danych, omówienie wybranych kar nałożonych przez UODO. Ponadto każdy pracownik po zatrudnieniu zostaje przeszkolony przez IOD w sposób indywidualny w zakresie ochrony danych osobowych w Urzędzie

Czy na bieżąco przekazywane są IOD do akceptacji pod względem prawidłowości w zakresie ochrony danych osobowych projekty dokumentów tj. projekty umów, informacji udostępnianych w Biuletynie Informacji Publicznych, projekty przepisów wewnętrznych związanych z udostępnianiem bądź pozyskiwaniem danych osobowych.- TAK

Pozostałe pytania:

1. **Czy podmiot prowadzi BIP i pod jakim adresem internetowym-** TAK, http://bip.um.tykocin.wrotapodlasia.pl/
2. **Z usług jakiego dostawcy BIP podmiot korzysta. Czy jest to www.nbip.pl lub www.bip.edu.pl czy inny (podać jaki)?** System udostępniony przez Województwo Podlaskie w ramach projektu „Wdrażanie

elektronicznych usług dla ludności województwa podlaskiego cz. II, projekt administracja samorządowa", w ramach Regionalnego Programu Operacyjnego województwa podlaskiego na lata 2007-2013 Osi priorytetowej IV Społeczeństwo Informacyjne.

3. **Jakie są umowne okresy świadczenia tej usługi. Jaka jest wartość umów brutto w poszczególnych okresach? Dane odrębnie za poszczególne okresy w latach 2017-do czerwca 2022.**
System udostępniony bezpłatnie przez Województwo Podlaskie w ramach projektu „Wdrażanie elektronicznych usług dla ludności województwa podlaskiego cz. II, projekt administracja samorządowa", w ramach Regionalnego Programu Operacyjnego województwa podlaskiego na lata 2007-2013 Osi priorytetowej IV Społeczeństwo Informacyjne. Od 20.05.2021 r. zawarto porozumienie o udostępnieniu systemu BIP na czas nieokreślony

4. **Proszę podać liczbę informacji publicznych opublikowanych w BIP w latach 2017-do czerwca 2022r**
2017- 146
2018- 210
2019- 310
2020- 306
2021- 236
2022- 91

5. **Proszę podać liczbę wniosków o informację publiczną jakie wpłynęły do podmiotu, liczbę wniosków na które udzielono odpowiedzi wraz wnioskowaną informacją, liczbę wniosków na które udzielono odpowiedzi odmownej udzielenia informacji, liczbę wniosków na które nie udzielono odpowiedzi, liczbę postępowań sądowych w związku wnioskami o informację publiczną. Jeśli sąd określił, że podmiot pozostawał w bezczynności podać ile razy to określił i w poszczególnych latach Dane odrębnie za rok 2017, 2018,2019, 2020, 2021.**

Lata	Liczba wniosków które wpłynęły	Liczba wniosków na które udzielono odpowiedzi	Liczba wniosków których odmówiono udzielenia odpowiedzi	Liczba wniosków na które nie udzielono odpowiedzi	Liczba postępowań sądowych
2017	50	50	0	0	0
2018	61	61	0	0	0
2019	63	62	1	0	1
2020	90	90	0	0	0
2021	80	80	0	0	0
2022 (wg stanu na dzień 30.06.2022	30	30	0	0	0

Sąd określił, ze podmiot pozostawał w bezczynności jeden raz w roku 2019 (wyrok z 2019 roku, wniosek z 2019 roku).

6. **Wnosimy o udostępnienie wszystkich wniosków o informację publiczną na stronie BIP-** Żaden przepis prawa nie wymaga aby wnioski o informację publiczną zostały udostępnione na stronie BIP podmiotu. Zgodnie z art. 10 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) „informacja publiczna, która nie została udostępniona w Biuletynie Informacji Publicznej lub portalu danych, jest udostępniana na wniosek"

7. **Wnosimy o udostępnienie wszystkich wniosków o informację publiczną jako informację publiczną w latach 2016 do czerwca 2022r.**

Odpowiadając na Pani wniosek o udostępnienie informacji publicznej z dnia 3 lipca 2022 r. w zakresie udostępnienia informacji publicznej wskazanej w I Wniosku pyt. 7, tj. dotyczącej udostępnienia wszystkich wniosków o informację publiczną jako informację publiczną jako informację publiczną w latach 2016 do czerwca 2022 r., po analizie jego treści uprzejmie informujemy, że nie dysponujemy zbiorem o jaki Pani wnioskuje, a zakres wnioskowanej informacji obejmuje obowiązek przetworzenia, o którym mowa w art. 3 ust. 1 pkt 1 ustawy o dostępie do informacji publicznej.

W piśmie z dnia 15 lipca 2022 r. została Pani wezwana do wykazania, w terminie siedmiu dni od daty otrzymania niniejszego pisma, w jakim zakresie udostępnienie wyżej wymienionych informacji we wniosku, jest szczególnie istotne dla interesu publicznego. Na dzień 31.08.2022 r. do Urzędu Miejskiego w Tykocinie ta informacja przez Wnioskodawcę nie została uzupełniona.
Wobec powyższego, mając na względzie przepisy art. 3 ust. 1 pkt 1 i art. 16 ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902), działając na podstawie art. 64 § 2 w związku z art. 63 §1-3a Kodeksu postępowania administracyjnego (k.p.a.) – wzywam do uzupełnienia braku formalnego wniosku z dnia 3 lipca 2022 r. poprzez złożenie wniosku opatrzonego własnoręcznym podpisem lub bezpiecznym podpisem elektronicznym oraz wskazanie adresu wnioskodawcy

w terminie siedmiu (7) dni od daty otrzymania niniejszego pisma,

pod rygorem pozostawienia wniosku bez rozpoznania (art. 64 § 2 k.p.a.).

Nieusunięcie wyżej wymienionych braków wniosku w powyższym terminie spowoduje pozostawienie wniosku bez rozpoznania (art. 64 § 2 k.p.a.).

Zgodnie z utrwalonym orzecznictwem, wszystkie przypadki, w których ma dojść do podjęcia przez organ aktu administracyjnego, w tym zwłaszcza kwalifikowanego, jakim jest decyzja administracyjna, bezwzględnie wymagać będą własnoręcznego podpisu wnioskodawcy (bezpiecznego podpisu elektronicznego) na wniosku o udostępnienie informacji publicznej, a jego brak winien być usuwany w postępowaniu naprawczym, regulowanym w art. 64 § 2 k.p.a. Zgodnie z art. 16 ust. 2 uodip, do decyzji odmownej oraz o umorzeniu postępowania stosuje się przepisy k.p.a., co oznacza, że Kodeks ten ma zastosowanie do całego procesu wydawania decyzji, a więc także do kwestii usuwania braków formalnych wniosku.

Wniosek z dnia 3 lipca 2022 r. przesłany drogą mailową nie jest opatrzony podpisem oraz nie zawiera adresu wnoszącego podanie, a tym samym nie odpowiada warunkom, jakie przepisy Kodeksu postępowania administracyjnego statuują w odniesieniu do podań (przepis art. 63 § 1 – 3a k.p.a. Zgodnie z art. 64 § 2 k.p.a., jeżeli podanie nie czyni zadość innym wymaganiom ustalonym w przepisach prawa, należy wezwać wnoszącego do usunięcia braków w terminie siedmiu dni z pouczeniem, że nieusunięcie tych braków spowoduje pozostawienie podania bez rozpoznania.

8. Wnosimy o udostępnienie informacji publicznej w zakresie ilości dni urlopu wypoczynkowego pozostałych do wykorzystania kierownikowi jednostki oraz poszczególnym zastępcom (jeśli są) a także, czy w tym roku którejś z tych osób został lub zostanie wypłacony ekwiwalent za niewykorzystany urlop (jeśli tak w jakiej kwocie i komu)

Kierownik jednostki- 44 dni
Zastępca kierownika jednostki- 16 dni
W 2022 roku nie wypłacono i na dzień udzielenia odpowiedzi na wniosek nie ma podstaw do wypłaty ekwiwalentu za niewykorzystany urlop wypoczynkowy.
Celem zachowania pełnej przejrzystości działań - wnosimy o opublikowanie treści wnioski na stronie internetowej podmiotu wraz z odpowiedziami i uchybieniami na na podstawie art. 8 ust. 1 ww. Ustawy o petycjach Chcemy działać w pełni jawnie i transparentnie. Treść wniosku oraz odpowiedzi została opublikowana w BIP.

PYTANIA Z KRAJOWYCH RAM INTEROPERACYJNOŚCI

Pytania informacja publiczna?

1. **Kto dokonuje corocznych audytów z KRI?**
   Audyty z zakresu KRI dokonywane zostały przez ASI we współpracy z IOD. W 2022 roku audyt z zakresu bezpieczeństwa informacji wykonała firma realizująca diagnozę cyberbezpieczeństwa.
2. **Czy IOD realizuje zadania w związku z KRIO?**
   IOD uczestniczy w audytach z zakresu KRI.
3. **Kto przeprowadza audyt bezpieczeństwa?**

Wewnętrzną kontrolę stanu bezpieczeństwa danych osobowych i przestrzegania zasad i przepisów z zakresu ochrony danych osobowych powinien regularnie, w przyjęty przez siebie sposób, przeprowadzać **inspektor ochrony danych**.

Audyty bezpieczeństwa z zakresu KRI dokonywane zostały przez ASI we współpracy z IOD. W 2022 roku audyt z zakresu bezpieczeństwa informacji wykonała firma realizująca diagnozę cyberbezpieczeństwa.

Pytania informacja publiczna:

Lp.	Zagadnienie	*Tak*	Nie	Uwagi
Utrzymywanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.				
1.	Czy prowadzona jest ewidencja:			
	a) sprzętu informatycznego w ramach ewidencji majątkowej? CZY IOD KONTROLUJĘ EWIDENCJĘ	x		
	b) oprogramowania (np. licencje)? IOD KONTROLUJĘ EWIDENCJĘ	x		częściowo
	c) umów serwisowych?	x		
2.	Czy przypisano konkretnym osobom obowiązki w zakresie prowadzenia powyższych ewidencji - w tym oprogramowania i nośników oprogramowania? Jeśli TAK proszę o przedłożenie dokumentu. CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W		x	IOD nie kontrolował zakresu obowiązków pracowników pod kątem przypisania obowiązku prowadzania powyższych ewidencji.
3.	Czy posiadam zinwentaryzowany sprzęt / oprogramowanie wraz z określeniem ważności danego komponentu dla całej jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	x		częściowo
4.	Czy pracownicy mogą używać swojego sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych? IOD KONTROLUJĘ EWIDENCJĘ		x	
5.	Czy pracownicy mogą podłączać swój sprzęt (laptopy, telefony, tablety) do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		x	
6.	Czy zapisuję każdy fakt podłączenia zewnętrznego sprzętu do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*		x	
7.	Czy monitoruję podłączenia ewentualnych nieautoryzowanych punktów bezprzewodowych do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE*		x	

	PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W			
Przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.				
1.	Czy znam najistotniejsze zagrożenia dla zinwentaryzowanych systemów IT? *Jeśli TAK proszę o ich wskazanie*. TAK	Należy w tym miejscu podkreślić, że prawo dostępu do informacji publicznej obejmuje prawo żądania udzielenia informacji o określonych faktach i stanach istniejących w chwili udzielania informacji. Informacja publiczna dotyczy sfery faktów, a prawo dostępu do informacji publicznej oznacza dostęp do informacji już będącej w posiadaniu podmiotu zobowiązanego, utrwalonej i nie może być utożsamiane z prawem do inicjowania działań mających na celu wytworzenie informacji jakościowo nowej. Informacja o którą Pani pyta w ww. pkt wniosku nie mieści się w pojęciu ustawy o dostępie do informacji publicznej i nie może być udostępnione w trybie tej ustawy.			
2.	Czy wiem, które systemy są krytyczne dla działania jednostki? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W TAK (IOD w tym zakresie nie przeprowadził sprawdzenia)*			
3.	Czy mam pewność, że każdy krytyczny system jestem w stanie odtworzyć z kopii zapasowych w odpowiednim czasie? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W Każdy system krytyczny posiada kopie bezpieczeństwa.*			
4.	Czy mam opracowane plany działania w momencie naruszenia bezpieczeństwa IT w mojej organizacji (np. procedury reagowania na incydenty IT)? Urząd posiada procedurę reakcji na incydenty.			
5.	Czy znam potencjalne zagrożenia dla systemów, które znajdują się w mojej infrastrukturze lub w infrastrukturze zewnętrznej (outsourcing)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W Tak znane są potencjalne zagrożenia dla systemów IT.*	Należy w tym miejscu podkreślić, że prawo dostępu do informacji publicznej obejmuje prawo żądania udzielenia informacji o określonych faktach i stanach istniejących w chwili udzielania informacji. Informacja publiczna dotyczy sfery faktów, a prawo dostępu do informacji publicznej oznacza dostęp do informacji już będącej w posiadaniu podmiotu zobowiązanego, utrwalonej i nie może być utożsamiane z prawem do inicjowania działań mających na celu wytworzenie informacji jakościowo nowej. Informacja o którą Pani pyta w ww. pkt wniosku nie mieści się w pojęciu ustawy o dostępie do informacji publicznej i nie może być udostępnione w trybie tej ustawy.		
Podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji wraz z bezzwłoczną zmianą uprawnień, w przypadku zmiany zadań.				
1.	Czy wskazana/e jest/są w jednostce osoba/y odpowiedzialna/e za bezpieczeństwo IT w jednostce? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	x		

	Jeśli TAK proszę o przedłożenie dokumentu.			
2.	Czy osoby te posiadają stosowne kompetencje? Jeśli TAK proszę o potwierdzenie tego faktu.	x		Osoby posiadają wieloletnie doświadczenie, uczestniczyły w specjalistycznych szkoleniach
3.	Czy wszyscy pracownicy zaangażowani w proces przetwarzania informacji posiadają pisemne uprawnienia?	x		
4.	Czy uprawnienia, o których mowa w pkt 3 uprawniają jedynie do przetwarzania informacji w stopniu adekwatnym do realizowanych zadań? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	x		
5.	Czy identyfikatory i hasła nadawane są po uprzednim pisemnym złożeniu wniosku?	x		
6.	Czy na bieżąco aktualizowane są uprawnienia do dostępu (np. w momencie zmiany zakresu obowiązków)? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	X		
7.	Czy prowadzona jest formalna listę zadań /obowiązków /uprawnień takich osób? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	x		
Ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Należy zaznaczyć stosowane w jednostce rozwiązania.				
1.	Bieżące czynności monitorowania dostępu w tym logi (serwery, systemy, urządzenia sieciowe).	x		
2.	Podstawowe elementy ochrony przed nieautoryzowanymi działaniami związanymi z przetwarzaniem informacji:	x		
a.	ochrona sieci na poziomie portów LAN		x	
b.	BIOS		x	
c.	centralny system kontroli dostępu logicznego do pojedynczych komputerowych stanowisk pracy, serwerów i zasobów sieci - na poziomie domeny Windows		x	
d.	niezależne od domenowych systemy kontroli dostępu logicznego do kluczowych systemów informatycznych; *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	x		
e.	system ochrony zewnętrznej klasy firewall	x		
f.	system ochrony zewnętrznego dostępu logicznego (urządzanie sieciowe-serwer VPN); – zabezpieczenie	x		

	kodem PIN dostępu do wydruków;			
g.	stosowanie tokenów z hasłami jednorazowymi		x	
Podstawowe zasady gwarantujące bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE PRACĘ NA ODLEGŁOŚĆ CZY TYLKO PRZEDSTAWIA DOKUMENTY*				
1.	Czy wprowadzono regulacje wewnętrzne jednostki w zakresie zdalnego dostępu do zasobów informatycznych/pracy na odległość? *Jeśli TAK proszę o przedłożenie dokumentu*		x	
2.	Czy w umowach zawieranych z podmiotami zewnętrznymi określono zakres i tryb dostępu do własnych zasobów IT? Jeśli TAK proszę o udokumentowanie.		x	
3.	Czy w pracy na odległość stosuję bezpieczne metody połączenia?	x		
4.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, posiadają aktualne oprogramowanie antywirusowe/są w pełni zaktualizowane?	x		
5.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, są chronione przed utratą danych (np. w wyniku kradzieży)? Jeśli TAK proszę wskazać, w jaki sposób.	x		Kopie bezpieczeństwa
Zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*				
1.	Czy jednostka posiada zapisy gwarantujące odpowiedni poziom bezpieczeństwa IT w umowach zawieranych z dostawcami sprzętu/ oprogramowania? Jeśli TAK proszę o udokumentowanie.	x		
2.	Czy posiadam krytyczne systemy, dla których nie ma zapisów umownych dotyczących bezpieczeństwa (np. zapewnienie możliwości wgrania aktualizacji komponentów, na których bazuje dany system)?		x	
Zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. CZY IOD PRZEPROWADZIŁ ANALIZĘ RYZYKA I OCENĘ SKUTKÓW DLA PRZETWARZANIA DANYCH W URZĄDZENIACH MOBILNYCH?*				
1.	Czy obowiązują odpowiednie regulacje dotyczące zapisu danych na nośnikach przenośnych? Jeśli TAK proszę o przedłożenie.	x		
2.	Czy posiadam mechanizmy uniemożliwiające dostęp do danych na urządzeniu mobilnym po jego utraceniu (np. pin/szyfrowanie przestrzeni dyskowej na urządzeniu)?	x		
3.	Czy istnieje możliwość zdalnego, trwałego usunięcia danych z tego typu urządzenia?		x	
4.	Czy kontroluję to, co użytkownicy mogą realizować na urządzeniach mobilnych (np. uruchamianie dowolnych aplikacji)?	x		

5.	Czy mam zapewnione bezpieczne połączenie urządzeń mobilnych z moją infrastrukturą (np. tylko protokoły szyfrowane)?	x		
6.	Czy pracownicy mogą podłączać swoje urządzenia mobilne do mojej infrastruktury IT?		x	
Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. ANALIZA RYZYKA W/W*				
1.	Czy realizuję bieżące aktualizacje zarówno na stacjach PC (system operacyjny / java / adobe reader / flash itp.), jak i serwerach?	x		
2.	Czy aktualizuję oprogramowanie firmware na urządzeniach sieciowych – szczególnie tych, które mają bezpośredni styk z Internetem?	x		
3.	Czy posiadam aktualne sygnatury dla systemu antywirusowego?	x		
4.	Czy mam przygotowaną procedurę odtworzenia danej stacji roboczej / serwera po wykryciu na nim wirusa?	x		
5.	Czy mam informacje o systemach, dla których aktualizacja nie powiodła się?	x		
6.	Czy wiem, które systemy IT są krytyczne dla prawidłowego działania jednostki?	x		
7.	Czy zapewniono ciągłość działania w przypadku wystąpienia awarii ww. systemów?	x		
8.	Czy użytkownicy sieci przesyłają wrażliwe informacje w formie jawnej (np. za pośrednictwem e-mail lub przenosząc na pendrive / telefonie)?		x	
9.	Czy obowiązuje w jednostce instrukcja reagowania na incydenty bezpieczeństwa IT?	x		
10.	Czy wiem, z jakimi innymi wymaganiami prawnymi muszą być zgodne użytkowane systemy?	x		
11	Czy zapewniam odpowiednio bezpieczny dostęp do poczty elektronicznej (dostęp tylko szyfrowany)?	x		
12.	Czy umożliwiony jest zdalny dostęp do poczty elektronicznej?	x		
13.	Czy dostęp do Internetu w jednostce jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp)?	x		
14.	Czy w odpowiedni sposób zapewnia się ochronę przed fizyczną ingerencją w infrastrukturę IT (np.: odpowiednie zabezpieczenia serwerowni, okablowania)	x		
Zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.				
1.	Czy istnieją w jednostce procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?	x		
2.	Czy okresowo testuje się procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?		x	

Czy jedynym kryterium wyboru dla IOD i innych usług bezpieczeństwa informacji niezależnie od formy świadczenia tych usługi jest cena? Jeśli tak to prosimy o wyjaśnienie czy w związku z tym oznacza to, że ochrona informacji ma niski priorytet w zarządzaniu Państwa organizacją? Jeśli nie, to jakie inne

kryteria Państwo stosujecie i z jaką wagą. Prosimy o uszczegółowienie tej kwestii. Nie. M.in. cena, kompetencje, szeroko rozumiane doświadczenie.
Czy Państwa jednostka organizacyjna wdrożyła wewnętrzną procedurę schematów podatkowych (MDR – Mandatory Disclosure Rules), zgodnie z wymaganiami ustawy ordynacja podatkowa ? TAK

Mariusz Dudziński
Burmistrz Tykocina
/podpis elektroniczny/

I N F O R M A C J A

Wypełniając obowiązki określone w art. 13 ust. 1 i 2 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 (dalej: „RODO") informuje się, że:

1. Administratorem Pani(a) danych osobowych jest Burmistrz Tykocina, z siedzibą przy ul. 11 Listopada 8, 16-080 Tykocin, tel. 85 718 16 27.
2. Kontakt z inspektorem ochrony danych jest możliwy poprzez adres email: iod@umtykocin.pl.
3. Pani(a) dane osobowe przetwarzane są w celu rozpatrzenia wniosku o dostęp do informacji publicznej na podstawie art. 6 ust. 1 lit. c RODO w związku z ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej.
4. Administrator nie zamierza przekazywać Pani(a) danych do państwa trzeciego ani do organizacji międzynarodowych.
5. Dane mogą zostać udostępnione podmiotom upoważnionym na podstawie przepisów prawa oraz podmiotom z którymi administrator podpisał umowę powierzenia.
6. Podane dane osobowe przechowywane będą do zakończenia postępowania w sprawie rozpoznania wniosku o udostępnienie informacji publicznej a następnie przez okres 10 lat.
7. Posiada Pani(a) prawo do:
   a. żądania od administratora dostępu do danych osobowych na podstawie art. 15 RODO,
   b. sprostowania danych na podstawie art. 16 RODO,
   c. ograniczenia przetwarzania danych osobowych na podstawie art. 18 RODO,
   d. w przypadku uznania, iż przetwarzanie przez Administratora Pana(i) danych osobowych narusza przepisy RODO przysługuje Pani(u) prawo wniesienia skargi do organu nadzorczego , którym jest Prezes Urzędu Ochrony Danych Osobowych z siedzibą przy ul. Stawki 2, 00-193 Warszawa.
8. Nie przysługuje Pani(u)prawo do:
   a. usunięcia danych osobowych w związku z art. 17 ust. 3 RODO,
   b. przenoszenia danych osobowych w związku z art. 20 ust. 1 RODO,
   c. sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.
9. Podanie przez Panią(a) danych osobowych nie jest obowiązkowe. Niepodanie danych kontaktowych uniemożliwić może przekazanie odpowiedzi na złożony wniosek o udostępnienie informacji publicznej.
10. Dane nie będą przetwarzane w celu zautomatyzowanego podjęcia decyzji.