From: [redacted]
Sent: Thursday, November 11, 2021 11:04 AM
Subject: WNIOSEK

INFORMACJA PUBLICZNA DLA KIEROWNIKÓW JEDNOSTEK

KOLEJNE KARY:

https://uodo.gov.pl/pl/138/1244

https://uodo.gov.pl/pl/138/1453

https://glos.pl/uodo-kara-upomnienia-dla-szkoly-za-przetwarzanie-danych-osobowych-uczniow

Temat monitoringu wizyjnego jest przedmiotem naszego zainteresowania. O jego funkcjonowaniu w Państwa podmiocie wiemy wciąż niewiele. Informacja o monitoringu jest informacją publiczną np. koszt, cel, spełnienie wymogów związanych z instalacją, okres przechowywania.

Właśnie dlatego postanowiliśmy zgłębić temat wysyłając wnioski o udostępnienie informacji publicznej z prośbą o udzielenie następujących odpowiedzi:

1. Czy podmiot posiada monitoring wizyjny?
2. Jaka jest podstawa prawna instalowania monitoringu?
3. Czy adresaci są i w jaki sposób informowani o ich obecności?
4. W jaki sposób zostały spełnione obowiązki informacyjne?
5. Jakie obowiązki przeprowadził administrator w związku z zainstalowaniem monitoringu (ocena skutków, obowiązki informacyjne, konsultacje z organem prowadzący, zapoznanie pracowników)
6. Czemu na stronie www nie ma pełnych danych IOD?

   Przecież przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (art. 11) wprost zobowiązują podmiot, który wyznaczył IOD, by udostępnił jego dane na swojej stronie internetowej. Administrator, który wyznaczył IOD powinien opublikować jego następujące dane: imię i nazwisko oraz adres poczty elektronicznej lub numer telefonu.

7. Czy były przeprowadzone konsultacje z organem prowadzącym?

8. 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:

„Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może spowodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę".

Natomiast zgodnie z art. 35 ust. 3 rodo:

„Ocena skutków dla ochrony danych, o której mowa w ust. 1, wymagana w szczególności w przypadku systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie".

Jednocześnie zgodnie z art. 35 ust. 7 rodo ocena skutków obligatoryjnie zawiera co najmniej

a)systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;

b)ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;

c)ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1; oraz

d)środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy".

Jeżeli ocena skutków (stosownie do treści art. 35 ust. 1 rodo) była prowadzona to wnosimy przesłanie tej oceny.

10. 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).

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

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

13. 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).

14. Rejestr czynności przetwarzania danych osobowych oraz jego zmiany.

15. Rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.

16. Dokumentacja w zakresie analizy ryzyka związanego z przetwarzaniem danych osobowych.

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

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

19. Informacje dotyczące monitoringu wizyjnego (jeśli jest). Procedura i Regulamin w tym zakresie.

20. 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.).

Przedmiotowy wniosek/wnioski - nie powinny być rozpatrywane w trybie KPA. Urząd powinien procedować nasze wnioski W TRYBIE Ustawy o dostępie do informacji publicznej

Pozwalamy sobie również przypomnieć, zgodnie z art. 2 ust. 2 Ustawy o dostępie do informacji publicznej " (...) Od osoby wykonującej prawo do informacji publicznej nie wolno żądać wykazania interesu prawnego lub faktycznego.

Celem naszych wniosków jest - sensu largo - usprawnienie, naprawa - na miarę istniejących możliwości - funkcjonowania struktur Administracji Publicznej - głownie w Gminach/Miastach jednostkach organizacyjnych, uczelni - gdzie jak wynika z naszych wniosków - stan faktyczny wymaga wszczęcia procedur sanacyjnych.

W przypadku braku uzyskania odpowiedzi na zadane pytania będziemy zmuszeni złożyć skargę do sądu na bezczynność.

Odpowiedzi proszę wysłać na na adres naszego maila.

[redacted]

URZĄD MIASTA
GORZOWA WIELKOPOLSKIEGO

Urząd Miasta
ul. Sikorskiego 3-4
66-400 Gorzów Wlkp.

T: +48 95 735 55 00
F: +48 95 735 56 70
E: kancelaria@um.gorzow.pl
I: www.gorzow.pl

Gorzów Wielkopolski, dnia 24.11.2021 r.

WOR - III.1431.287.2021.KPa

[redacted]

Odpowiadając na złożony w dniu 11 listopada 2021 r. wniosek o udostępnienie informacji publicznej, poniżej przekazuję odpowiedzi w zakresie właściwości Urzędu Miasta Gorzowa Wielkopolskiego.

Ad 1. Prezydent Miasta zastosował wewnętrzny monitoring na terenie obiektu urzędu miasta.

Ad 2. Podstawą prawną zainstalowania monitoringu jest art. 9a ustawy z dnia 08 marca 1990 r. o samorządzie gminnym (Dz. U. z 2021 r. poz. 1372 ze zm.).

Ad 3. W miejscu zastosowania monitoringu umieszczono informację o treści:

OBIEKT MONIOTOROWANY
Administratorem danych osobowych jest Prezydent Miasta Gorzowa Wlkp.
Szczegółowe informacje na temat przetwarzania danych osobowych można uzyskać w siedzibie Administratora lub na stronie
https://bip.wrota.lubuskie.pl/umgorzow/411/Klauzula_informacyjna_dotyczaca_monitoringu_wizyjnego_w_Urzedzie_Miasta/

Ad 4. Jak pkt 3.

Ad 5. Jak punkty 3,7,8.

Ad 6. Informacja na temat danych osobowych inspektora ochrony danych znajduje się w Biuletynie Informacji Publicznej pod linkiem:
https://bip.wrota.lubuskie.pl/umgorzow/412/Inspektor_Ochrony_Danych/

Ad 7. Administrator nie prowadził konsultacji z organem nadzorczym, gdyż zgodnie z art. 36 ust. 1 zidentyfikował i uznał, że przetwarzanie danych w postaci wizerunku cech szczególnych osób i numerów identyfikacyjnych (np. numery tablic rejestracyjnych i numerów bocznych pojazdów) nie powoduje wysokiego ryzyka w zakresie ich przetwarzania. Jednocześnie w myśl zapisów RODO zminimalizował ryzyko przetwarzania danych osobowych poprzez zastosowanie środków i zabezpieczeń chroniących prawa i wolności osób, których dane dotyczą.

Ad 8. Oceny skutków nie przeprowadzono. Zgodnie z „Wykazem rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony" do grupy - Systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie wykorzystujące elementy rozpoznawania cech lub właściwości obiektów, które znajdą się w monitorowanej przestrzeni - nie są zaliczane systemy monitoringu wizyjnego, w których obraz jest nagrywany i wykorzystywany tylko w przypadku potrzeby analizy incydentów naruszenia prawa (a taka rolę spełnia zastosowany w urzędzie monitoring).
Komunikat Prezesa Urzędu Ochrony Danych Osobowych ogłoszony w Monitorze Polskim z dnia 17 czerwca 2019 r. *http://monitorpolski.gov.pl/MP/2019/666*

Ad 10. Odnosząc się do powyższego żądania udostępnienia dokumentacji potwierdzającej realizację zadań przez IOD od dnia 25 maja 2018 r. (zadań wynikających z art. 39 RODO) należy stwierdzić, że jest ono nieprecyzyjne i zbyt ogólne.
Nie wskazano żądanych dokumentów tj. jaka konkretnie informacja publiczna pozostaje w kręgu żądania. Wniosek tak sformułowany nie jest żądaniem udostępnienia informacji publicznej i nie może być prawidłowo rozpoznany ze względu na niedookreślony zakres żądania. Żądanie udostępnienia „wszelkiej dokumentacji", dokumentacji potwierdzającej wykonywanie szeroko zakreślonych w przepisie czynności - nie jest więc wnioskiem o dostęp do informacji publicznej i nie może być prawidłowo rozpoznany ze względu na nieokreślony zakres żądania. Tak sformułowany wniosek nie wskazuje na informacje publiczne, których udostępnienia domaga się wnioskodawca.
Niesprecyzowane wnioski o informacje – obiektywnie niepozwalające ustalić treści żądania – nie stanowią wniosków o informację publiczną w rozumieniu art. 1 ust. 1 w zw. z art. 10 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, a w rezultacie nie podlegają rozpatrzeniu w jej trybie.
Ponadto dokumentacja dotycząca realizacji zadań przez IOD, dotyczy m.in. realizowanych sprawdzeń, opinii dotyczących stosowanych zabezpieczeń. Dokumentacja zawiera zatem środki techniczne oraz organizacyjne, które mają zagwarantować ciągłą dostępność, rozliczalność oraz integralność danych. Ujawnienie tych informacji mogłoby mieć zatem negatywny wpływ na poziom bezpieczeństwa danych zapewniany przez organ, do którego skierowano wniosek.

Ad 11. Administrator opracował i wdrożył dokumenty bezpieczeństwa przetwarzania danych m.in.:

1) Politykę bezpieczeństwa danych osobowych w urzędzie miasta wraz z Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.
2) Procedury:
   a) nadawania upoważnień do przetwarzania danych osobowych;
   b) ustalania okresów przechowywania danych;
   c) obowiązku informacyjnego wraz ze wzorami klauzul informacyjnych;

d) powierzenia przetwarzana danych osobowych wraz z umową;
e) oceny ryzyka;
f) realizacji praw osób fizycznych;
g) postępowania w przypadku naruszenia ochrony danych osobowych;
h) nadawania/zmiany/odbierania uprawnień do przetwarzania danych osobowych w SI;
i) przetwarzania danych osobowych w BiP;
j) anonimizacji danych osobowych w dokumentach w wersji papierowej i informatycznej.

3) Politykę czystego biurka.
4) Regulamin użytkowania urządzenia mobilnego; itp.

Ad 12. Pracownicy urzędu zapoznani zostali z Polityką bezpieczeństwa danych osobowych w urzędzie miasta wraz z Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych oraz opracowanymi procedurami, co potwierdzili własnoręcznym podpisem w stosownym oświadczeniu (oświadczenia jako dokument wewnętrzny przechowuje IOD).
Procedury dostępne są na: portalu wewnętrznym urzędu - w katalogu wiedzy – zakładce: ochrona danych osobowych.

Ad 13. IOD prowadził dla pracowników urzędu szkolenia zbiorowe, indywidualne oraz konsultacje dla poszczególnych komórek organizacyjnych z zakresu ochrony danych osobowych na podstawie zapisów RODO, ustawy o ochronie danych osobowych. Ponadto w załączeniu przekazuję wykaz szkoleń wraz z zakresem i podmiotem prowadzącym szkolenia (Załącznik nr 1).
Żądanie przez wnioskodawcę list obecności, potwierdzeń odbycia szkoleń przez pracowników nie stanowi informacji publicznej i nie podlega udostępnieniu w myśl ustawy o dostępie do informacji publicznej. Dokumenty te (listy obecności) nie zawierają danych publicznych i związane są z aktywnością organu związaną z wewnętrzną organizacją jego funkcjonowania. Mają walor wyłącznie organizacyjny oraz porządkowy i stanowią narzędzie pracodawcy w zakresie kierowania sposobem wykonywania pracy, sposobem dokumentowania odbycia przez pracownika szkoleń organizowanych w celu podnoszenia kwalifikacji zawodowych pracowników.
Nie każdy przejaw działalności i nie każdy wytworzony przez organ „dokument" zawiera informację publiczną, która podlega udostępnieniu w oparciu o przepisy ustawy o dostępie do informacji publicznej. Część dokumentów służących jedynie potrzebom podmiotu zobowiązanego, pomimo że związana jest z jego działalnością, określanych jako dokumenty wewnętrzne, nie jest informacją publiczną i nie podlega ujawnieniu. W przeciwieństwie do dokumentu urzędowego, którym zgodnie z art. 6 ust. 2 ustawy o dostępie do informacji publicznej jest treść oświadczenia woli lub wiedzy, utrwalona

i podpisana w dowolnej formie przez funkcjonariusza publicznego w rozumieniu przepisów kodeksu karnego, w ramach jego kompetencji, skierowana do innego podmiotu lub złożona do akt sprawy. Przez dokument wewnętrzny rozumie się taki dokument, który został wytworzony w zakresie działania danego podmiotu, ale nie przesądzający o kierunkach jego działania, a w przypadku list obecności ma charakter wyłącznie organizacyjny.

Ad 14. Z uwagi na fakt, że Rejestr czynności przetwarzania danych osobowych zawiera ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, nie podlega ujawnianiu i powszechnemu dostępowi.
Żądany rejestr nie zawiera informacji o sprawach publicznych. Jest dokumentem zawierającym informacje o sposobie gromadzenia danych osobowych, jest nośnikiem informacji o charakterze wewnętrznym, porządkowym, ewidencyjnym wspomagającym pracę administratora i inspektora ochrony danych tak aby przetwarzanie odbywało się zgodnie z przepisami RODO oraz gwarantowało realizację zasady rozliczalności przed organem nadzoru.
Rejestr czynności przetwarzania danych osobowych nie odnosi się do publicznej sfery działania organu i jako taki nie zawiera informacji publicznej (patrz Wyrok WSA w Łodzi z dnia 12 lutego 2019 r. Sygn. Akt. II SAB/Łd 181/18).

Ad 15. Z uwagi na fakt, że Rejestr kategorii czynności przetwarzania danych osobowych zawiera ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, nie podlega ujawnianiu i powszechnemu dostępowi.
Żądany rejestr nie zawiera informacji o sprawach publicznych. Jest dokumentem zawierającym informacje o sposobie gromadzenia danych osobowych, jest nośnikiem informacji o charakterze wewnętrznym, porządkowym, ewidencyjnym wspomagającym pracę administratora i inspektora ochrony danych tak aby przetwarzanie odbywało się zgodnie z przepisami RODO oraz gwarantowało realizację zasady rozliczalności przed organem nadzoru.
Rejestr kategorii czynności przetwarzania danych osobowych nie odnosi się do publicznej sfery działania organu i jako taki nie zawiera informacji publicznej (patrz Wyrok WSA w Łodzi z dnia 12 lutego 2019 r. Sygn. Akt. II SAB/Łd 181/18).

Ad 16. Odnosząc się do udostępnienia dokumentacji w zakresie analizy ryzyka, informuję, iż dokument ten ma charakter wewnętrzny - organizacyjny i porządkowy i nie może być udostępniony w trybie ustawy o dostępie do informacji publicznej.
Analiza ryzyka stanowi dokumentację wewnętrzną wspomagającą pracę administratora i inspektora ochrony danych w zakresie wdrażania odpowiednich środków technicznych i organizacyjnych, tak aby przetwarzanie odbywało się zgodnie z przepisami rozporządzenia oraz gwarantowało realizację zasady rozliczalności przed organem nadzoru.

Ad 17. Obowiązek informacyjny realizowany jest w formie elektronicznej oraz w formie pisemnej (tradycyjnej, za pośrednictwem operatora pocztowego), w zależności od konkretnej sprawy załatwianej przez klienta urzędu.

Obowiązek informacyjny w urzędzie **spełniany jest:**

1) w formie elektronicznej (na stronie internetowej UM, w BIP-ie);
2) w formie pisemnej w przestrzeni powszechnie dostępnej (tablica ogłoszeń na Sali Obsługi Klienta, poczekalnie wydziałów/biur, stanowiska pracy, przy których obsługiwani są klienci urzędu);
3) w trakcie prowadzenia korespondencji (przy pierwszym kontakcie/w piśmie, które kierowane jest do osoby, której dane dotyczą);
4) w formie ustnej - podczas osobistego kontaktu z klientem (wymagane potwierdzenie).

Poniżej przekazuję linki do przykładowych klauzul informacyjnych zamieszczonych na bip Gorzowa:

https://bip.wrota.lubuskie.pl/umgorzow/299/Klauzula_informacyjna/

https://bip.wrota.lubuskie.pl/umgorzow/407/Klauzula_informacyjna_dotyczaca_transmisji_obrad_Rady_Miasta/

https://bip.wrota.lubuskie.pl/umgorzow/422/Klauzula_informacyjna_w_zwiazku_z_udostepnieniem_informacji_publicznej/

Ad 18. Jak wyżej.

Ad 19. Zarządzeniem Nr 87/W/II/2019 Prezydent Miasta Gorzowa Wielkopolskiego z dnia 11 marca 2019 r. wprowadził do użytku „Regulamin funkcjonowania monitoringu wizyjnego w Urzędzie Miasta Gorzowa Wielkopolskiego".

Ad 20. Audyty/sprawdzenia z zakresu RODO realizowane są poprzez sprawdzenia planowe wynikające z planu sprawdzeń oraz incydentalne w przypadku zgłoszeń dokonanych przez pracowników komórek organizacyjnych urzędu bądź w przypadku zidentyfikowania problemów związanych z ochroną danych osobowych.

Zakres realizowanych sprawdzeń obejmuje m.in.

1) Stosowanie w praktyce zasad określonych w Polityce bezpieczeństwa przetwarzania danych osobowych w Urzędzie Miasta Gorzowa Wlkp. oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Urzędzie Miasta Gorzowa Wlkp.;
2) Sprawdzenie czy w Regulaminie wewnętrznym wydziału/biura znajdują się zapisy dotyczące ochrony danych osobowych przez pracowników;
3) Legalność przetwarzania danych osobowych art. 5 ust. 1 RODO;
4) Identyfikacja danych osobowych. Sprawdzenie rejestru czynności przetwarzania i jeśli to ma zastosowanie rejestru kategorii czynności przetwarzania;
5) Zgodność przetwarzania danych z prawem art. 6 ust. 1 i art. 9 ust. 2;

6) Sprawdzenie zakresu i celu przetwarzania danych, poprawności i adekwatności danych oraz czasu ich przechowywania;
7) Realizacja obowiązku informacyjnego art.13 i 14 RODO;
8) Realizacja praw osób, których dane dotyczą art. 15 – 21 RODO;
9) Upoważnienia do przetwarzania danych osobowych oraz oświadczenia o zapoznaniu z przepisami oraz wewnętrznymi dokumentami z zakresu ochrony danych osobowych – aktualność, zgodność z zakresem obowiązków;
10) Sprawdzenie poprawności procedur nadawania upoważnień (weryfikacja upoważnień) do przetwarzania danych osobowych;
11) Szkolenie osób przetwarzających dane osobowe – art. 39 ust. 1 lit. b RODO;
12) Powierzanie danych osobowych do przetwarzania – art. 28 RODO - sprawdzenie umów powierzenia pod kątem poprawności na zgodność z przepisami art 28 RODO.
13) Udostępnianie danych osobowych;
14) Nadawanie /zmienianie/odbieranie uprawnień do SI;
15) Techniczne i organizacyjne zabezpieczenie obszaru przetwarzania danych osobowych. Ocena realizacji:
    a) czy ustawienie sprzętu komputerowego uniemożliwia dostęp do ekranu monitorów osobom postronnym;
    b) czy stosowana jest Polityka kluczy;
    c) czy stosowana jest Polityka czystego biurka,
    d) sposób zabezpieczenia danych osobowych w formie papierowej (czy są przechowywane w sposób uniemożliwiający dostęp do nich osobom nieupoważnionym);
    e) sposób niszczenia niepotrzebnych dokumentów, danych wygenerowanych z systemów;
    f) przestrzeganie zasady rozpoczęcia i zakończenia pracy w systemie;
    g) zabezpieczenie fizyczne sprzętu komputerowego;
    h) blokowanie systemu, podczas opuszczenia stanowiska pracy w trakcie dnia pracy;
16) Transfer danych do tzw. państw trzecich – Rozdział 7 UODO.
17) Zabezpieczenie fizyczne pomieszczeń, w których gromadzone i przetwarzane są dane osobowe – art. 24 RODO:
    a) przechowywanie dokumentów;
    b) bezpieczeństwo sprzętu informatycznego;
    c) zabezpieczenia danych osobowych;
    d) usuwania danych osobowych;
    e) niszczenia dokumentów papierowych;
    f) polityka „czystego biurka";

g) sprzątanie pomieszczeń wydziału/biura;

18) Dokumentacja Dyrektora wydziału określona w § 9 ust. 1 pkt. 13 Polityki bezpieczeństwa:

a) wykaz przetwarzanych zbiorów danych osobowych w wydziale;

b) ewidencja osób upoważnionych do przetwarzania danych osobowych w wydziale.

Przekazane wyżej informacje odnoszą się do zakresu działania prezydenta miasta, jako kierownika jednostki - Urzędu Miasta Gorzowa Wielkopolskiego.

Natomiast w zakresie kompetencji kierowników jednostek organizacyjnych informuję, iż ustawa o dostępie do informacji publicznej w swoich uregulowaniach proceduralnych nie przewiduje przekazania wniosku wg właściwości, ani organowi niższej instancji w rozumieniu administracyjnego toku instancji, ani jednostce podległej adresatowi wniosku (zob. wyrok WSA w Szczecinie z 13.03.2014 r., II SAB/Sz 119/13. Obowiązku takiego nie można również wywieść z treści art. 65 Kpa (wyrok NSA z 16.12.2009 r., I OSK 1116/09). Zatem w zakresie udzielenia informacji odnoszących się do kierowników jednostek organizacyjnych, należy zwrócić się z wnioskiem o udzielenie informacji publicznej bezpośrednio do kierowników tych jednostek. Jednostki organizacyjne, jako podmioty utworzone przez gminę w celu realizacji zadań publicznych, mieszczą się w katalogu podmiotów zobowiązanych do udzielania informacji publicznej, wymienionych w art. 4 ust. 1 ustawy o dostępie do informacji publicznej (Dz. U. z 2020 r., poz. 2176 ze zm.).

Wykaz jednostek miasta znajduje się w Biuletynie Informacji Publicznej Urzędu Miasta Gorzowa Wielkopolskiego pod adresem:
https://bip.wrota.lubuskie.pl/umgorzow/60/Jednostki_Miasta/

z up. PREZYDENTA MIASTA
Eugeniusz Kurzawski
Sekretarz Miasta

Załącznik nr 1

Informacje dotyczące szkoleń pracowników w zakresie ochrony danych osobowych przeprowadzanych z zakresu RODO

Lp.	Rok	Temat szkolenia/konferencji/warsztatów	Organizator
1.	2018	Szkolenie – Dokumentacja ochrony danych i obowiązki Inspektora Ochrony Danych w świetle RODO	Firma Zontek i Wspólnicy Sp. Komandytowa
2.		Szacowanie ryzyka w procesie analizy ryzyka ogólnego oraz oceny skutków dla przetwarzania danych (DPIA) w oparciu o wytyczne RODO, Grupa robocza art. 29 (EROD), Komunikat Prezesa UODO z dnia 17.06.20219r, ISO 27001, 27002,27005,29134, 31000	ISO LEX Audyt i szkolenia
3.		Szkolenia wewnętrzne – Nowe uwarunkowania prawne ochrony danych osobowych wynikające z RODO 10.04.2018, 12.04.2018, 16.04.2018, 17.04.2018, 18.04.2018, 19.04.2018, 26.04.2018, 10.05.2018, 15.05.2018, 17.05.2018, 29.05.2018, 02.10.2018,	Inspektor Ochrony Danych
4.		Kurs z zakresu ochrony danych osobowych	Centrum Kształcenia MBM Tychy
5.	2019	Szkolenie – Dokumentacja ochrony danych i obowiązki Inspektora Ochrony Danych w świetle RODO	Firma Zontek i Wspólnicy Sp. Komandytowa
6.		Szkolenia wewnętrzne - Ochrona danych osobowych w systemach informatycznych jak i w wersji papierowej 19.02.2019, 14.05.2019, 16.05.2019, 27.05.2019, 28.05.2019, 12.09.2019, 08.10.2019, 03.12.2019,	Inspektor Ochrony Danych
7.	2020	Szkolenie – Dokumentacja ochrony danych i obowiązki Inspektora Ochrony Danych w świetle RODO	Firma Zontek i Wspólnicy Sp. Komandytowa
8.		Analiza Ryzyka Ogólnego oraz Ocena Skutków dla Przetwarzania Danych (DPIA)	ISO-LEX Sylwia Kochan
9.		Szkolenie – Bezpieczeństwo informacji w oparciu o ustawę z dnia 14.12.20218r o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, a także w oparciu o rozporządzenie RM z dnia 21.05.2019r w sprawie trybu i sposobu realizacji zadań przez IOD w ślad za dyrektywą parlamentu europejskiego i rady (UE) 2016/580 z dnia 27.04.2016r w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postepowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar w sprawie przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U.UE L z dnia 04.05.2016r),	ISO LEX Audyt i szkolenia
10.		Szkolenia wewnętrzne - Ochrona danych osobowych w systemach informatycznych jak i w wersji papierowej 03.03.2020, 18.06.2020,	Inspektor Ochrony Danych
11.	2021	Szkolenie – Naruszenia ochrony danych podczas pracy zdalnej. Wycieki danych. Zasady bezpieczeństwa pracy zdalnej	Zrzeszenie Gmin Województwa Lubuskiego
12.		Szkolenie – Krajowe Ramy Interoperacyjności	ISO-LEX Sylwia Kochan
13.		Szkolenia wewnętrzne - Ochrona danych osobowych w systemach informatycznych jak i w wersji papierowej 09.03.2021, 18.05.2021, 14.06.2021, 29.06.2021, 13.07.2021, 16.09.2021, 28.09.2021, 07.10.2021, 13.10.2021, 20.10.2021.	Inspektor Ochrony Danych