Kuźnica, dn. 02 września 2022 roku

Or.1431.30.2022

Anna M
rodo.rodo55@wp.pl

Odpowiadając na wniosek o udostępnienie informacji publicznej z dnia 03 lipca 2022r. (data wpływu do Urzędu 04 lipca 2022 r.) informuję, jak niżej:

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie: „1. Czy na stronie www są pełne danych IOD?"

Informacja na temat danych osobowych inspektora ochrony danych znajduje się w https://kuznica.ug.gov.pl/.

Odpowiedź dotyczy realizacji żądania zawartego we wniosku o następującej treści - cyt.: „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).

Odnosząc się do żądania udostępnienia dokumentacji potwierdzającej realizację zadań przez inspektora ochrony danych od dnia 25 maja 2018 r (zadań wynikających z art. 39 RODO) należy stwierdzić, że jest ono nieprecyzyjne i zbyt ogólne, a co za tym idzie nie stanowi informacji publicznej, która mogłaby być udostępniona w trybie i na zasadach przewidzianych w ustawie o dostępie do informacji publicznej. Przywołany przez wnioskodawcę przepis art 39 RODO określa jedynie zadania inspektora ochrony danych oraz wskazuje ogólnie sposób ich realizacji. Ustawodawca wylicza wprawdzie zadania takie jak: informowanie o obowiązkach dotyczących ochrony danych i doradzanie w tym zakresie, monitorowanie przestrzegania przepisów o ochronie danych i polityk ochrony danych, podział obowiązków, działania edukacyjne i uczestniczenie w zadaniach audytowych, udzielanie zaleceń co do oceny skutków dla ochrony danych i monitorowanie jej wykonania, współpracę z organem nadzorczym, pełnienie funkcji punktu kontaktowego dla organu nadzorczego i prowadzenie konsultacji z organem nadzorczym. W ust. 2 ww. przepisu ustawodawca określa sposób ogólny, w jaki inspektor ochrony danych powinien wykonywać swoje zadania. Zgodnie z tym przepisem przy wykonywaniu tych zadań inspektor powinien uwzględnić ryzyko związane z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Prawodawca unijny nie wskazuje jednak konkretnych rozwiązań w zakresie wykonywania przez inspektora ochrony danych swoich zadań, jak i nie wskazuje rodzaju dokumentów które powinny powstać w tym procesie oraz nie przesądza czy i w jaki sposób inspektor ochrony danych ma dokumentować powierzone mu zadania. Nie można uznać za prawidłowy wniosek o udostępnienie informacji publicznej, w którym wnioskodawca nie wskazuje konkretnie określonej informacji, lecz czyni to bardzo ogólnie. Wnioskodawca nie wskazał jakich konkretnie dokumentów się domaga tj. jaka konkretnie informacja publiczna pozostaje w kręgu jego zainteresowania. Wnioski tak sformułowane nie są żądaniem udostępnienia informacji publicznej i nie mogą być prawidłowo rozpoznane ze względu na niedookreślony zakres żądania. Żądanie udostępnienia „wszelkiej dokumentacji", czy tak jak w tym wypadku, 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. W tym miejscu przychylić się należy do poglądu

wyrażonego w orzecznictwie, że niesprecyzowane wnioski o informacje – obiektywnie niepozwalające ustalić treści żądania wnioskodawcy – 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. W orzecznictwie sądów administracyjnych utrwalił się pogląd, zgodnie z którym przepisy Kodeksu postępowania administracyjnego stosuje się (z modyfikacjami) jedynie do decyzji o odmowie udostępnienia informacji publicznej oraz umorzeniu postępowania o udostępnienie informacji w przypadku określonym w art. 14 ust. 2 (art. 16 ust. 2 u.d.i.p.), a nie do całego postępowania zainicjowanego wnioskiem o udzielenie informacji publicznej, co oznacza, że w przypadku – jak miało to miejsce w niniejszej sprawie – nieprecyzyjnego i niekonkretnego sformułowania wniosku o udostępnienie informacji publicznej, której podmiot zobowiązany zamierza udzielić, nie ma on podstawy prawnej do żądania usunięcia braków podania poprzez jego doprecyzowanie, lecz winien udostępnić informacje w takim zakresie w jakim żądanie wynika z wniosku w sposób nie budzący wątpliwości. Inaczej rzecz ujmując to na podmiocie wnoszącym o udostępnienie informacji publicznej ciąży obowiązek sformułowania wniosku w sposób na tyle jednoznaczny i precyzyjny, by mógł on zostać rozpoznany w pełnym oczekiwanym przez stronę zakresie (**por. wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu w sprawie II SAB/Po 78/15**). Powyższe w żadnym stopniu nie narusza przy tym konstytucyjnego prawa obywatela do uzyskania dostępu do informacji o sprawach publicznych, albowiem nawet w sytuacji nieprecyzyjnego, względnie nieprzejrzystego sformułowania wniosku o udostępnienie informacji i nieuzyskania w następstwie tego całości oczekiwanej informacji, brak jest przeszkód dla ponownego złożenia wniosku o udostępnienie informacji, sformułowanego już w sposób umożliwiający jego jednoznaczne odczytanie. Dokumentacja dotycząca realizacji zadań przez inspektora ochrony danych, dotyczy m.in. realizowanych sprawdzeń, opinii dotyczących stosowanych zabezpieczeń. Dokumentacja prowadzona przez inspektora ochrony danych 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 podmiot, do którego skierowano wniosek.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:

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

Odnosząc się do udostępnienia informacji na temat rodzaju opracowanej i wdrożonej przez administratora dokumentacji, dotyczącej przetwarzania danych osobowych, zapewnienia bezpieczeństwa informacji informuję, iż dokumenty te mają charakter wewnętrzny - organizacyjny i porządkowy, a informacja o nich nie podlega udostępnieniu w trybie ustawy o dostępie do informacji publicznej. Stanowią one 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 RODO oraz gwarantowało realizację zasady rozliczalności przed organem nadzoru. Z uwagi na fakt, że powyższe dokumenty zawierają ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, nie podlegają ujawnianiu i powszechnemu dostępowi. Żądane dokumenty nie zawierają informacji o sprawach publicznych, lecz informację o sposobie i zasadach przetwarzania danych osobowych u administratora. Są więc nośnikiem informacji o charakterze wewnętrznym, porządkowym, ewidencyjnym, który ma

służyć zapewnieniu m.in. porządku i bezpieczeństwa. Takie dokumenty nie odnoszą się natomiast do publicznej sfery działania podmiotu i jako takie nie zawierają informacji publicznej (por. Wyrok WSA w Łodzi z dnia 12 lutego 2019 r. sygn. akt. II SAB/Łd 181/18). Zgodnie z wyrokiem NSA z 4.04.2019 r., I OSK 1709/17 uznać należy, że dokument wewnętrzny to dokument wytworzony na potrzeby danego podmiotu i zawiera tylko dane związane z jego funkcjonowaniem, a więc nie wykorzystywane w stosunku do podmiotów zewnętrznych. W dokumentach uznanych jako składowe Systemu Zarządzania Bezpieczeństwem Informacji np. politykach bezpieczeństwa, procedurach, instrukcjach oraz raportach z audytów mogą znajdować się rozwiązania techniczno-organizacyjne służące ochronie informacji w podmiocie, a więc dostęp do powyższych dokumentów powinien być ograniczony tylko do grupy osób ponoszących odpowiedzialność w zakresie zarządzania bezpieczeństwem informacji. Omawiane stanowisko jest zbieżne z wytycznymi Urzędu Ochrony Danych Osobowych pośrednio lub bezpośrednio z wyrokami sądów (wyrok WSA w Warszawie z 8 grudnia 2005 r., II SA/Wa 1539/05). Organ w pełni podziela ww. stanowiska.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:
„4. Wnosimy o przedłożenie dokumentu potwierdzającego zapoznanie się pracowników z treścią obowiązujących przepisów wewnętrznych, ewentualnie wskazanie w jaki sposób zostali oni zapoznani."
Pracownicy zapoznawani są z treścią obowiązujących przepisów wewnętrznych poprzez udostępnienie im treści postanowień do wiadomości i stosowania. W sytuacjach, w których określone regulacje wewnętrzne wymagają potwierdzenia zapoznania się przez pracownika w formie złożenia oświadczenia na piśmie, takowe oświadczenie jest przez pracownika składane, lub elektronicznie poprzez Infointegrum.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:
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).

- w 2018 r. dnia 26.05.2018 r. pt. Ochrona Danych Osobowych. Szkolenie prowadziła Pani Ewa Rybus-Tołłoczko. Ze szkolenia została sporządzona lista obecności, w której uczestnicy potwierdzili odbycie szkolenia, czas trwania 5 godz.;
- w 2019 r. dnia 23.03.2019 r. pt. Zapewnienie przestrzegania przepisów z zakresu ochrony danych osobowych przez pracowników Urzędu Gminy Kuźnica przy realizacji zadań – Bezpieczeństwo informacji w Urzędzie. Szkolenie prowadziła Pani Aneta Kuberska. Ze szkolenia została sporządzona lista obecności, w której uczestnicy potwierdzili odbycie szkolenia, czas trwania 6 godz.;
- w 2021 r. dnia 16.09.2021 r. Szkolenie dla pracowników samorządowych z zakresu cyberbezpieczeństwa w ramach operacji „SILNE WSPARCIE" realizowane przez Zespół Działań Cyberprzestrzennych Dowództwa Wojsk Obrony Terytorialnej. Ze szkolenia została sporządzona lista obecności, w której uczestnicy potwierdzili odbycie szkolenia, czas trwania 4 godz.
- w 2022 r. dnia 11.06.2022 r. Szkolenie: Zapewnienie przestrzegania przepisów z zakresu ochrony danych osobowych przez administratora i jego pracowników. Szkolenie prowadziła Pani Aneta Kuberska. Ze szkolenia została sporządzona lista obecności w której uczestnicy potwierdzili odbycie szkolenia, czas trwania 6 godz.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:
„6. Czy został opracowany Rejestr czynności przetwarzania danych osobowych oraz jego zmiany."
Rejestr czynności przetwarzania został opracowany i jest aktualizowany.
Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:
„7. Czy został opracowany Rejestr kategorii czynności przetwarzania danych osobowych oraz jego zmiany.".
Rejestr kategorii czynności przetwarzania danych osobowych został opracowany i jest aktualizowany.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:
„8. W jaki sposób realizowany jest obowiązek informacyjny – art. 13 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne."
Osoby, których dane dotyczą, są informowane przy pierwszym kontakcie poprzez udostępnienie klauzul informacyjnych wyłożonych przy stanowiskach pracy, bądź zintegrowanych z wnioskiem czy formularzem lub dołączonych do nich (zależnie od wymagań w przepisach szczegółowych). Klauzule są też wywieszone na tablicach informacyjnych. W przypadku, w którym z jakiś powodów informacja o przetwarzaniu danych nie została podana przy pierwszym kontakcie, zamieszcza się ją w powiadomieniach i zawiadomieniach oraz wezwaniach kierowanych do osoby, której dane dotyczą. Klauzule informacyjne zostały utworzone dla wszystkich czynności przetwarzania, w których dane są pozyskiwane bezpośrednio od osób.

KLAUZULA INFORMACYJNA DOTYCZĄCA PRZETARGÓW

Informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą
Zgodnie z art.13 ust.1 i ust.2 rozporządzenia Parlamentu Europejskiego i rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych) informujemy, że:
1. Administratorem Pani/Pana danych osobowych jest Urząd Gminy Kuźnica (dalej: „ADMINISTRATOR"), z siedzibą: pl. 1000-lecia Państwa Polskiego 1, 16-123 Kuźnica.
Z Administratorem można się kontaktować pisemnie, za pomocą poczty tradycyjnej na adres: pl. 1000-lecia Państwa Polskiego 1, 16-123 Kuźnica lub drogą e-mailową pod adresem: sekretariat@kuznica.ug.gov.pl.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można się skontaktować pod adresem mailowym: iod@kuznica.ug.gov.pl
3. Państwa dane osobowe są przetwarzane na podstawie art. 6 ust. 1 lit. c, e 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) oraz ustawy Prawo zamówień publicznych.
4. Przetwarzanie danych osobowych odbywa się dla potrzeb niezbędnych do przeprowadzenia procesu realizacji zamówienia publicznego.
5. Odbiorcami Państwa danych osobowych będą wyłącznie podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa.
6. Państwa dane osobowe przechowywane będą w czasie określonym przepisami prawa, zgodnie z instrukcją kancelaryjną.

7. Posiadają Państwo prawo do żądania od Administratora dostępu do danych osobowych, ich sprostowania lub ograniczenia przetwarzania.
8. Skargę nas działania Administratora można wnieść do Prezesa Urzędu Ochrony Danych Osobowych.
9. Podanie danych osobowych jest dobrowolne, ale niezbędne do zabezpieczenia interesu Państwa i Administratora na wypadek postępowania reklamacyjnego lub dochodzenia roszczeń oraz oceny jakości usług.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie: „9". W jaki sposób realizowany jest obowiązek informacyjny – art. 14 RODO? Opisać. Przedstawić obowiązujące klauzule informacyjne".

Obowiązek informacyjny zrealizowano poprzez przygotowanie szczegółowych klauzul informacyjnych dla wszystkich czynności przetwarzania danych osobowych, pozyskiwanych z innych źródeł niż osoba, której dane dotyczą.

Wzór klauzuli, wyciąg z regulaminu realizacji praw osób, których dane dotyczą

KLAUZULA INFORMACYJNA

Informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą

Zgodnie z art.14 ust.1 i ust.2 rozporządzenia Parlamentu Europejskiego i rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólnego rozporządzenia o ochronie danych), informujemy, że:

1. Administratorem Pani/Pana danych osobowych gromadzonych przez Urząd Gminy jest Wójt Gminy Kuźnica, z siedzibą w Kuźnica pl. 1000-lecia Państwa Polskiego 1.
2. Administrator wyznaczył inspektora ochrony danych, z którym może się Pani/Pan skontaktować w sprawach związanych z przetwarzaniem danych osobowych oraz wykonywaniem praw przysługujących na mocy niniejszego rozporządzenia, za pośrednictwem adresu e-mail: iod@kuznica.ug.gov.pl.
3. Pani/Pana dane osobowe przetwarzane będą w celu ... (należy podać cel przetwarzania) na podstawie ... (należy podać podstawę prawną przetwarzania np. art. 6 ust 1 pkt a/b/c/d/e);
4. Odbiorcą Pani/Pana danych osobowych będą ..... (podać kategorię odbiorców, o ile istnieją);
5. Pani/Pana dane osobowe będą przechowywane przez okres ... (jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu wyłonienia zwycięscy konkursu, do czasu zakończenia rekrutacji itd.);
6. Posiada Pani/Pan prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania (jeżeli przetwarzanie odbywa się na podstawie zgody), którego dokonano na podstawie zgody przed jej cofnięciem;
7. Ma Pan/Pani prawo wniesienia skargi do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych;

8. Pani / Pana dane w postaci: .....zostały uzyskane przez administratora od ...;
9. Pani/Pana dane będą / nie będą/ przetwarzane w sposób zautomatyzowany w tym również w formie profilowania.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie: „10. Wnosimy o regulacje dotyczące monitoringu wizyjnego (jeśli jest). Procedura i Regulamin w tym zakresie.".

Odnosząc się do udostępnienia dokumentacji w zakresie dotyczącym monitoringu wizyjnego związanego z przetwarzaniem danych osobowych, w tym procedury i regulaminu informuję, iż dokument ten ma charakter wewnętrzny i nie może być udostępniony w trybie ustawy o dostępie do informacji publicznej. Stanowi on 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 RODO oraz gwarantowało realizację zasady rozliczalności przed organem nadzoru w sytuacjach wystąpienia incydentów. Jest to nośnik informacji o charakterze wewnętrznym, który ma służyć zapewnieniu m.in. porządku i bezpieczeństwa. Procedura nie odnosi się do publicznej sfery działania podmiotu i jako taka nie zawiera informacji publicznej (por. Wyrok WSA w Łodzi z dnia 12 lutego 2019 r. sygn. akt. II SAB/Łd 181/18). Zgodnie z wyrokiem NSA z 4.04.2019 r., I OSK 1709/17 uznać należy, że dokument wewnętrzny to dokument wytworzony na potrzeby danego podmiotu i zawiera tylko dane związane z jego funkcjonowaniem, a więc nie wykorzystywane w stosunku do podmiotów zewnętrznych – nie stanowi informacji publicznej.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie: „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.)."

Informuję, że audyty/sprawdzenia z zakresu RODO realizowane są poprzez bieżące sprawdzenia (ze względu na specyfikę jednostki) 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.

- kompletność zidentyfikowanych czynności przetwarzania danych osobowych,
- zakres i cel przetwarzania danych,
- przesłanki legalności przetwarzania danych osobowych, w tym danych szczególnej kategorii,
- zabezpieczenia: organizacyjne i techniczne danych osobowych,
- zakres i poprawność konstruowania umów powierzenia przetwarzania danych,
- obowiązek informacyjny (w zakresie realizacji).

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. Pytanie:
„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:

„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".

Podstawą prawną monitoringu w Urzędzie Gminy jest Art. 6 ust. 1 lit c RODO.

Wobec powyższego, w związku z art. 35 ust. 10 RODO ust. 1- 7 nie stosuję się jeżeli przetwarzanie na podstawie art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych przepisów.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. Pytanie:
„13. Mając na uwadze powyższe wnosimy o informację czy została opracowana polityka retencji danych? Jakich czynności ona dotyczy?"
Polityka retencji danych nie została opracowana. Okres przechowywania danych wynika z Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych oraz z przepisów szczególnych.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:
„Wnosimy o wykazanie kwalifikacji IOD w zakresie wiedzy prawniczej? Czy IOD jest prawnikiem? Jakie posiada doświadczenie?
Inspektor ochrony danych nie posiada wykształcenia prawniczego i nie jest prawnikiem. Posiada ponad 20 letni staż pracy w administracji. Od 2016 roku jako ABI a od 2018 roku do chwili obecnej IOD.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:
„Kto i w jaki sposób weryfikował kwalifikacje IOD? „
Weryfikacji kandydata na inspektora ochrony danych dokonał Administrator w osobie Wójta Gminy, na podstawie nabytych kwalifikacji i doświadczenia zawodowego przez pracownika.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:
„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."
Realizacja, przez inspektora ochrony danych, szkoleń pracowników Administratora odbywa się na bieżąco, dotyczy konkretnych sytuacji i potrzeb. Utrzymywany jest stały kontakt inspektora z pracownikami.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:
„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. Inspektor ochrony danych na bieżąco otrzymuje do konsultacji (akceptacji) projekty dokumentów, w tym także projekty przepisów wewnętrznych i informacji udostępnianych w BIP, celem dokonania oceny prawidłowości ich zapisów w zakresie obejmującym ochronę danych osobowych.

Pozostałe pytania:
1.Urząd Gminy Kuźnica prowadzi BIP pod adresem: bip.kuznica.ug.gov.pl.

2. Urząd Gminy Kuźnica użytkuje obecnie Biuletyn Informacji Publicznej Wrót Podlasia, którym zarządza Urząd Marszałkowski Województwa Podlaskiego.

3. Nie dotyczy.

4. Urząd Gminy Kuźnica nie jest w stanie udzielić odpowiedzi na to pytanie.

5. Liczba wniosków, które wpłynęły do Urzędu Gminy Kuźnica w 2017 r. wynosi 84, Liczba wniosków, na które udzielono odpowiedzi wraz z wnioskowaną informacją w roku 2017 wyniosła 54, natomiast na pozostałe 30 odpowiedzi zostały udzielone częściowo, ponieważ część pytań nie stanowiła informacji publicznej, nie dotyczyła organu lub organ nie był w posiadaniu żądanych informacji/dokumentów.

Liczba wniosków, które wpłynęły do Urzędu Gminy Kuźnica w 2018 r. wynosi 51. Liczba wniosków, na które udzielono odpowiedzi wraz z wnioskowaną informacją w roku 2018 wyniosła 39, natomiast na pozostałe 12 odpowiedzi zostały udzielone częściowo, ponieważ część pytań nie stanowiła informacji publicznej, nie dotyczyła organu lub organ nie był w posiadaniu żądanych informacji/dokumentów.

Liczba wniosków, które wpłynęły do Urzędu Gminy Kuźnica w 2019 r. wynosi 56. Liczba wniosków, na które udzielono odpowiedzi wraz z wnioskowaną informacją w roku 2019 wyniosła 38, na 6 wniosków odmówiono decyzją udzielenia informacji publicznej natomiast na pozostałe 12 odpowiedzi zostały udzielone częściowo, ponieważ część pytań nie stanowiła

informacji publicznej, nie dotyczyła organu lub organ nie był w posiadaniu żądanych informacji/dokumentów.

Liczba wniosków, które wpłynęły do Urzędu Gminy Kuźnica w 2020 r. wynosi 91. Liczba wniosków, na które udzielono odpowiedzi wraz z wnioskowaną informacją w roku 2020 wyniosła 69, 1 wniosek został złożony, po czym został wycofany przez wnioskodawcę, natomiast na pozostałe 20 odpowiedzi zostały udzielone częściowo, ponieważ część pytań nie stanowiła informacji publicznej, nie dotyczyła organu lub organ nie był w posiadaniu żądanych informacji/dokumentów. Na 1 wniosek mimo udzielenia odpowiedzi przez Urząd wnioskodawca złożył skargę, którą sąd odrzucił.

Liczba wniosków, które wpłynęły do Urzędu Gminy Kuźnica w 2021 r. wynosi 74. Liczba wniosków, na które udzielono odpowiedzi wraz z wnioskowaną informacją w roku 2021 wyniosła 64, 1 wniosek został najpierw złożony, a następnie wycofany przez wnioskodawcę, 1 wniosek został złożony, lecz nie zawierał treści pytań, na które należałoby odpowiedzieć, a wnioskodawca został poproszony o ponowne przesłanie wniosku, lecz wniosek nie został dosłany, natomiast na pozostałe 8 odpowiedzi zostały udzielone częściowo, ponieważ część pytań nie stanowiła informacji publicznej, nie dotyczyła organu lub organ nie był w posiadaniu żądanych informacji/dokumentów.

We wskazanych latach nie było wniosków, na które nie udzielono odpowiedzi.

Odpowiedź dotyczy pytania zawartego we wniosku o następującej treści - cyt. pytanie:
„6.Wnosimy o udostępnienie wszystkich wniosków o informację publiczną na stronie BIP.

Odpowiadając na powyższe żądanie informuję, że przepisy ustawy o dostępie do informacji publicznej nie dają podstawy do składania wniosków co do sposobu prowadzenia Biuletynu Informacji Publicznej jak również publikowania w nim określonych treści. Zgodnie z utrwaloną linią orzeczniczą sądów administracyjnych – sama czynność utworzenia Biuletynu Informacji Publicznej czy też czynność zamieszczania tam określonej informacji publicznej nie dotyczy uprawnień lub obowiązków obywateli. Nie istnieje bowiem przepis prawa, który uprawniałby do żądania zamieszczenia lub usunięcia z BIP informacji publicznej. Sam wynikający z przepisów ustawy o dostępie do informacji publicznej obowiązek utworzenia Biuletynu nie rodzi po stronie indywidualnego podmiotu uprawnień (por. postanowienie NSA z dnia 21 grudnia 2005 r. sygn. akt I OSK 1210/05, postanowienie WSA w Łodzi z dnia 16 października 2008 r. sygn. akt II SAB/Łd 40/08). Wobec powyższego wniosek w przedmiotowym zakresie, nie może być uwzględniony.

7. Wnosimy o udostępnienie wszystkich wniosków o informację publiczną jako informację publiczną w latach 2016 do dnia wpłynięcia wniosku.”.

Informacją publiczną co do zasady są tylko dokumenty urzędowe, a więc wytworzone przez organ w ramach realizacji powierzonych mu zadań. Nie wszystkie pisma będące w posiadaniu urzędu mają ten walor. *Dokument prywatny*, który trafia do organu, nie staje się z tego tytułu dokumentem urzędowym.

Przepisy u.d.i.p. nie definiują pojęcia *dokumentu prywatnego*. Według Sądu Najwyższego, *dokumentem prywatnym* jest każde pismo będące dokumentem, jeśli nie jest ono dokumentem urzędowym (zob. wyrok SN z 3 października 2000 r., I CKN 804/98). Niewątpliwie **wniosek (pismo) osoby fizycznej jest *dokumentem prywatnym*. A zatem wszelkiego rodzaju *dokumenty prywatne*, które podmiot prywatny kieruje do organu administracji publicznej, bez względu na to, jakiego rodzaju postępowanie wszczyna *dokument prywatny* lub też jakiej czynności oczekuje podmiot, składając ten dokument, nie stanowią informacji publicznej.** *Dokument prywatny*, niezależnie od tego, czy inicjuje postępowanie w konkretnej sprawie przed organem administracji publicznej, czy też nie, współtworzy wespół z innymi dokumentami całość akt prowadzonej przed nim sprawy. Okoliczność, że *dokument prywatny* trafia do organu i służy realizacji powierzonych prawem zadań organu, nie oznacza, że przez to nabiera on cech dokumentu urzędowego. Dokument skierowany do organu administracji publicznej przez podmiot prywatny nigdy nie stanie się dokumentem urzędowym tylko dlatego, że został doń zaadresowany i znajduje się w jego posiadaniu. Nie nabierze zatem cech dokumentu urzędowego w rozumieniu przepisów u.d.i.p. nawet wówczas, jeśli jego forma będzie miała postać oficjalnego wzoru (por. wyroki WSA: w Warszawie z 4 czerwca 2012 r., II SAB/Wa 102/12; z 24 marca 2014 r., II SA/Wa 10/14; z 24 lutego 2014 r., II SAB/Wa 450/13 i w Gdańsku z 20 marca 2013 r., II SAB/Gd 92/12). Organ nie może go więc udostępnić osobom trzecim w ramach wniosku o dostęp do informacji publicznej (por. wyrok NSA z 13 czerwca 2014 r., I OSK 3070/13).

Dokumentem prywatnym jest każde pismo będące dokumentem, o ile nie jest ono dokumentem urzędowym (art. 245 k.p.c.). - wyrok Sądu Najwyższego z dnia 3 października 2000 r. I CKN 804/98

8. Kierownikowi jednostki – Wójtowi Gminy na dzień udzielenia odpowiedzi pozostało 22 dni urlopu wypoczynkowego do wykorzystania, natomiast Skarbnik Gminy ma do wykorzystania 20 dni urlopu wypoczynkowego. Ekwiwalent za niewykorzystany urlop w tym roku żadnej z wymienionych osób nie zostanie wypłacony.

„1. Kto dokonuje corocznych audytów z KRI?"

Informuję, iż okresowy audyt z zakresu bezpieczeństwa informacji wykonywany m.in. w oparciu o 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 (Dz.U. z 2017 poz. 2247) zrealizowany został przez zewnętrzny podmiot.

„2. Czy IOD realizuje zadania w związku z KRIO?".
Informuję, że inspektor ochrony danych wypełnia swoją funkcję w ramach monitorowania zgodności przetwarzania danych osobowych, a także informowania i doradzania administratorowi danych, w tym również podczas realizowanych w Urzędzie zadań wynikających z Krajowych Ram Interoperacyjności.

„3. Kto przeprowadza audyt bezpieczeństwa?"
Informuję, iż audyt z zakresu bezpieczeństwa informacji w Urzędzie przeprowadził zewnętrzny podmiot.

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	Tak	Nie	
	b) oprogramowania (np. licencje)? IOD KONTROLUJĘ EWIDENCJĘ	Tak	 Nie	
	c) umów serwisowych?	Tak		
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	Tak	 Nie	Wszelka dokumentacja zawierająca rozwiązania organizacyjno-techniczne mające na celu ochronę dóbr w podmiocie, stanowi dokumentację wewnętrzną. Zgodnie z wyrokiem NSA z 4.04.2019 r., I OSK 1709/17 uznać należy, że dokument wewnętrzny to dokument wytworzony na potrzeby danego podmiotu i zawiera tylko dane związane z jego funkcjonowaniem, a więc nie wykorzystywane w stosunku do podmiotów zewnętrznych. Zarówno jej treść jak informacje jej dotyczące nie

				podlegają udostępnieniu w trybie i na zasadach określonych w ustawie o dostępie do informacji publicznej.
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*	Tak	Nie	Odpowiedź jak wyżej.
4.	Czy pracownicy mogą używać swojego sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych? IOD KONTROLUJĘ EWIDENCJĘ	Nie	Nie	Odpowiedź jak wyżej.
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*		Nie Nie	
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*	Tak	Nie	

7.	Czy monitoruję podłączenia ewentualnych nieautoryzowanych punktów bezprzewodowych do infrastruktury służbowej? *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	Tak	Nie	
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		
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	Nie	
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*	Tak	Nie	
4.	Czy mam opracowane plany działania w	Tak		

	momencie naruszenia bezpieczeństwa IT w mojej organizacji (np. procedury reagowania na incydenty IT)?			
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	Nie	

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* Jeśli TAK proszę o przedłożenie dokumentu.	Tak	Nie	Wszelka dokumentacja zawierająca rozwiązania organizacyjno-techniczne mające na celu ochronę dóbr w podmiocie, stanowi dokumentację wewnętrzną. Zgodnie z wyrokiem NSA z 4.04.2019 r., I OSK 1709/17 uznać należy, że dokument wewnętrzny to dokument wytworzony na potrzeby danego podmiotu i zawiera tylko dane związane z jego funkcjonowaniem, a więc nie wykorzystywane w stosunku do podmiotów zewnętrznych. Zarówno jej treść jak informacje jej dotyczące nie podlegają udostępnieniu w trybie i na zasadach określonych w ustawie o

				dostępie do informacji publicznej.
2.	Czy osoby te posiadają stosowne kompetencje? Jeśli TAK proszę o potwierdzenie tego faktu.	Tak		Kompetencje ASI, poprzez ich wyznaczenie w formie udokumentowanej. W pozostałym zakresie odpowiedź jak wyżej.
3.	Czy wszyscy pracownicy zaangażowani w proces przetwarzania informacji posiadają pisemne uprawnienia?	Tak		Pracownicy posiadają upoważnienia i nadane uprawnienia.
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*	tak	Nie	W pozostałym zakresie odpowiedź jak wyżej.
5.	Czy identyfikatory i hasła nadawane są po uprzednim pisemnym złożeniu wniosku?	Tak		
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*	Tak	Nie	W pozostałym zakresie odpowiedź jak wyżej.

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*	Tak		Zakres obowiązków.
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*	X	X	

	KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W			
e.	system ochrony zewnętrznej klasy firewall		X	
f.	system ochrony zewnętrznego dostępu logicznego (urządzanie sieciowe-serwer VPN); – zabezpieczenie kodem PIN dostępu do wydruków;	X		
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		Dokument wewnętrzny administratora. Wszelka dokumentacja zawierająca rozwiązania organizacyjno-techniczne mające na celu ochronę dóbr w podmiocie stanowi dokumentację wewnętrzną. Zgodnie z wyrokiem NSA z 4.04.2019 r., I OSK 1709/17 uznać należy, że dokument wewnętrzny to dokument wytworzony na potrzeby danego podmiotu i zawiera tylko dane związane z jego funkcjonowaniem, a więc nie wykorzystywane w stosunku do podmiotów zewnętrznych. Zarówno jej treść jak informacje jej dotyczące nie

				podlegają udostępnieniu w trybie i na zasadach określonych w ustawie o dostępie do informacji publicznej.
2.	Czy w umowach zawieranych z podmiotami zewnętrznymi określono zakres i tryb dostępu do własnych zasobów IT? Jeśli TAK proszę o udokumentowanie.	X		Nie ma takich klauzul.
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		Wszelka dokumentacja zawierająca rozwiązania organizacyjno-techniczne mające na celu ochronę dóbr w podmiocie, stanowi dokumentację wewnętrzną. Zgodnie z wyrokiem NSA z 4.04.2019 r., I OSK 1709/17 uznać należy, że dokument wewnętrzny to dokument wytworzony na potrzeby danego podmiotu i zawiera tylko dane związane z jego funkcjonowaniem, a więc nie wykorzystywane w stosunku do podmiotów zewnętrznych. Zarówno jej treść jak informacje

				jej dotyczące nie podlegają udostępnieniu w trybie i na zasadach określonych w ustawie o dostępie do informacji publicznej.
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		Wzór umowy powierzenia przetwarzania danych
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	Wszelka dokumentacja zawierająca rozwiązania organizacyjno-techniczne mające na celu ochronę dóbr w podmiocie stanowi dokumentację wewnętrzną. Zgodnie z wyrokiem NSA z 4.04.2019 r., I OSK 1709/17 uznać należy, że dokument wewnętrzny to dokument wytworzony na potrzeby danego podmiotu i zawiera tylko dane związane z jego funkcjonowaniem, a więc nie wykorzystywane w stosunku do podmiotów zewnętrznych. Zarówno jej treść jak informacje jej dotyczące nie podlegają udostępnieniu w trybie i na zasadach określonych w ustawie o dostępie do informacji publicznej.

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? Tak*				
1.	Czy obowiązują odpowiednie regulacje dotyczące zapisu danych na nośnikach przenośnych? Jeśli TAK proszę o przedłożenie.		X	Wszelka dokumentacja zawierająca rozwiązania organizacyjno-techniczne mające na celu ochronę dóbr w podmiocie stanowi dokumentację wewnętrzną. Zgodnie z wyrokiem NSA z 4.04.2019 r., I OSK 1709/17 uznać należy, że dokument wewnętrzny to dokument wytworzony na potrzeby danego podmiotu i zawiera tylko dane związane z jego funkcjonowaniem, a więc nie wykorzystywane w stosunku do podmiotów zewnętrznych. Zarówno jej treść jak informacje jej dotyczące nie podlegają udostępnieniu w trybie i na zasadach określonych w ustawie o dostępie do informacji publicznej.
2.	Czy posiadam mechanizmy uniemożliwiające dostęp do danych na urządzeniu mobilnym po jego utraceniu (np. pin/szyfrowanie przestrzeni dyskowej na urządzeniu)?	X		
3.	Czy istniej 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."

Wnioskowana informacja nie odnosi się do sfery faktów. Nie posiada waloru informacji publicznej i nie podlega udostępnieniu w trybie ustawy o dostępie do informacji publicznej.

Na gruncie przepisów ustawy o dostępie do informacji publicznej podmiot jest zobowiązany do udzielenia informacji, ale tylko takiej, która znajduje się w jego posiadaniu i której używa do zrealizowania powierzonych prawem działań. W sytuacji, gdy wnioskodawca żąda udzielenia informacji (co ma miejsce w niniejszym przypadku), które nie są informacjami publicznymi, podmiot nie ma obowiązku wydawania decyzji o odmowie udzielenia informacji, lecz zawiadamia jedynie wnoszącego, iż żądane dane nie mieszczą się w pojęciu objętym przedmiotową ustawą, co niniejszym czynię.

„Czy Państwa jednostka organizacyjna wdrożyła wewnętrzną procedurę schematów podatkowych (MDR – Mandatory Disclosure Rules), zgodnie z wymaganiami ustawy ordynacja podatkowa?".

Wewnętrzna procedura schematów podatkowych nie została wdrożona.

WÓJT
mgr inż. Paweł Miklasz

Załączniki:

1. Klauzula informacyjna o przetwarzaniu danych osobowych w niniejszej sprawie.

Informacja o przetwarzaniu danych osobowych

1. Administratorem Pana/Pani danych osobowych jest Urząd Gminy Kuźnica (dalej: „ADMINISTRATOR"), z siedzibą: pl. 1000-lecia Państwa Polskiego 1, 16-123 Kuźnica. Z Administratorem można się kontaktować pisemnie, za pomocą poczty tradycyjnej na adres: pl. 1000-lecia Państwa Polskiego 1, 16-123 Kuźnica lub drogą e-mailową pod adresem: sekretariat@kuznica.ug.gov.pl.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można się skontaktować pod adresem mailowym: iod@kuznica.ug.gov.pl.
3. Pana/Pani dane osobowe są przetwarzane na podstawie 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), w celu prowadzenia postępowania o udostępnienie informacji publicznej.
4. Pana/Pani dane osobowe nie będą przekazywane do państwa trzeciego.
5. Nie przewiduje się udostępniania danych poza sytuacjami opisanymi przepisami prawa.
6. Pozyskane dane będą przechowywane przez okres niezbędny do prowadzenia postępowania o udostępnienie informacji publicznej a następnie na czas niezbędny do celów archiwalnych (przez 5 lat poczynając od 1 stycznia roku następnego po roku, w którym nastąpiło przekazanie dokumentacji do archiwum zakładowego).

7. Przysługuje Panu/Pani prawo do sprostowania, usunięcia, ograniczenia przetwarzania lub wniesienia sprzeciwu wobec przetwarzania.
8. Przysługuje Panu/Pani prawo do żądania dostępu do swoich danych, wniesienia skargi do organu nadzorczego, którym jest Urząd Ochrony Danych Osobowych.
9. Podanie danych osobowych jest nieobowiązkowe. Dane mogą zostać wykorzystane w celach kontaktowych w prowadzonej sprawie, co może usprawnić jej realizację. Podając dane wnioskodawca wyraża zgodę na włączenie ich do akt sprawy prowadzonej przez Urząd Gminy Kuźnica.
10. Pana/Pani dane osobowe nie będą podlegały zautomatyzowanym procesom podejmowania decyzji, w tym profilowaniu.