

Urząd Gminy Suwałki - Sekretariat <sekretariat@gmina.suwalki.pl>

6.7.2022 08:08

Fwd: Pd: WNIOSEK

Do Kożuchowski <serwis@gmina.suwalki.pl>

--- Treść przekazanej wiadomości ---

Temat: Pd: WNIOSEK

Data: Tue, 05 Jul 2022 23:13:53 +0200

Nadawca: rodo.rod55@wp.pl

WNIOSEK INFORMACJA PUBLICZNA

Na podstawie art. 2 ust. 1 ustawy o dostępie do informacji publicznej z dnia 6 września 2001 r. (Dz. U. Nr 112, poz. 1198) zwracam się z prośbą o udostępnienie informacji publicznej.

Pozwalamy sobie przypomnieć, że ipso iure 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.

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

Celem naszych wniosków jest - sensu largo - usprawnienie, naprawa - na miarę istniejących możliwości - funkcjonowania struktur Administracji Publicznej - głównie w Gminach/Miastach/szkołach - gdzie jak wynika z naszych wniosków - stan faktyczny wymaga wszczęcia procedur sanacyjnych. W takiej sytuacji KPA nie ma zastosowania; więcej na jawność.pl

**

W przypadku braku odpowiedzi na informację publiczną *złożymy wniosek do Wojewódzkiego Sądu Administracyjnego skargę na bezczynność.*

Treść wniosku:

W maju-czerwcu Prezes UODO nałożył już 3 kary pieniężne na administratorów danych. Co je łączy? Każda z nich podyktowana została brakiem właściwej współpracy administratorów z organem nadzorczym, brak odpowiednich kwalifikacji IOD oraz uchybień w zakresie wdrożenia RODO. Czy w najbliższym czasie możemy spodziewać się kolejnych kar? Tak.

My natomiast zwracamy się do Państwa o udzielenie informacji publicznej oraz przesłania odpowiedzi na maila :
rodo.rodo55@wp.pl

1.Czy na stronie www są pełne danych IOD?

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

/2.///Wnosimy o dokumentacjępotwierdzającą realizację zadań przez IOD lub opis jego działań od dnia 25 maja 2018 roku (zadań wynikających z art. 39 rozporządzenia RODO)

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

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

/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).

/6.///Czy został opracowanyRejestr czynności przetwarzania danych osobowych oraz jego zmiany.

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

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

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

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

/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.).

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.

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”.

2. *W Wojewódzkim Sądzie Administracyjnym w Warszawie odbyła się 26 sierpnia 2020 r. rozprawa w sprawie skargi Burmistrza Aleksandrowa Kujawskiego na decyzję Prezesa Urzędu nakładającą administracyjną karę pieniężną. WSA oddalił skargę.*

WSA rozpatrywał skargę Burmistrza Aleksandrowa Kujawskiego na decyzję Prezesa UODO z 18 października 2019 r. w związku z przetwarzaniem przez Burmistrza danych osobowych w Biuletynie Informacji Publicznej.

Przypomnijmy, że jednym z powodów nałożenia kary w wysokości 40 tys. zł na Burmistrza miasta było to, że nie zawarł umowy powierzenia przetwarzania danych osobowych z podmiotami, którym przekazywał dane*. Ponadto, w decyzji Prezes UODO zarzucił brak procedur wewnętrznych dotyczących przeglądu zasobów dostępnych w BIP pod kątem ustalenia okresu ich publikowania.* To spowodowało, że przykładowo w BIP były dostępne m.in. oświadczenia majątkowe z 2010 roku, podczas gdy okres ich przechowywania wynosi 6 lat, co wynika z przepisów sektorowych.

Sąd na rozprawie oddalił skargę Burmistrza. W uzasadnieniu wyroku sąd wskazał, że nie znajduje podstaw do uchylenia zaskarżonej decyzji. Zdaniem sądu Prezes UODO prawidłowo zastosował przepisy ogólnego rozporządzenia o ochronie danych osobowych. Sąd także podkreślił, że RODO ma zastosowanie do danych przetwarzanych w BIP.

Ponadto WSA uznał, że organ nadzorczy w sposób wyczerpujący w wydanej decyzji uzasadnił zajęte stanowisko i wysokość nałożonej kary.

W ocenie sądu nałożona na Burmistrza kara nie stanowi nadmiernego obciążenia dla organu i jest adekwatna do stwierdzonych naruszeń w obszarze przetwarzania danych.

Więcej o decyzji Prezesa UODO o nałożeniu kary w komunikacie

dostępnym pod linkiem: <https://uodo.gov.pl/pl/138/1240>

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

14. PREAMBUŁA WNIOSKU O INFORMACJĘ PUBLICZNĄ W ZAKRESIE KWALIFIKACJI IOD W ZWIĄZKU Z RAPORTEM

<https://www.nik.gov.pl/kontrole/P/19/007/>

GDZIE STWIERDZONO, ŻE W WIELU PODMIOTACH IOD NIE POSIADA ODPOWIEDNICH KWALIFIKACJI ORAZ STWIERDZONO KONFLIKTY INTERESÓW

Art 37 ust. 5 RODO inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań*, * o których mowa w art. 39 RODO.

Według UODO Karami administracyjnymi obwarowane są zatem zarówno poszczególne obowiązki administratorów danych dotyczące także wyznaczania IOD . To na administratorze spoczywa ciężar wyznaczenia IOD zgodnie z kwalifikacjami i wiedzą prawniczą:
<https://uodo.gov.pl/pl/225/637>

Jednakże warto zrealizować rekonesans - w tym obszarze i dokonać stosownej analizy - wykazując troskę o bezpieczeństwo danych oraz wydatkowanie środków publicznych na IOD zgodnie z

kwalifikacjami. Tymczasem często na IOD są wybierani osoby nie mające kwalifikacji, wiedzy prawniczej. Co gorsza często takie funkcje piastują osoby z wykształceniem informatycznym.

Dzięki kontrolom NIK i UODO oraz działaniom sfer Rządowych (w skali makro) w ostatnim czasie sytuacja ulega poprawie, jednakże bez szybkiej sanacji tego obszaru (w skali mikro) również w Gminach i jednostkach oświatowych

- proces ten będzie w dalszym ciągu przebiegał zbyt wolno
-często są to osoby przypadkowe lub informatycy, zewnątrzni IOD nie mający wiedzy prawniczej.

W związku z powyższym:

I Wniosek:

1.1) Na mocy art. 61 Konstytucji RP, w trybie inter alia:
art. 6 ust. 1 pkt 3 lit. f, art. 6 ust. 1 pkt 5 Ustawy z dnia 6 września o dostępie do informacji publicznej (Dz.U.2018.1330 t.j. z 2018.07.10) - wnosimy o udzielenie informacji publicznej w przedmiocie :

Wnosimy o wykazanie kwalifikacji IOD w zakresie wiedzy prawniczej?

Czy IOD jest prawnikiem? Jakiego posiada doświadczenie?

Kto i w jaki sposób weryfikował kwalifikacje IOD?

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.

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.

Nadmieniamy, iż powyższe pytania o informację publiczną - wydają się szczególnie istotne z punktu widzenia interesu publicznego pro publico bono - nawiązując do art. 3 ust. 1 pkt. 1 Ustawy z dnia 6 września o dostępie do informacji publicznej (Dz.U.2018.1330 t.j. z 2018.07.10) - gdyż ten obszar RODO i kwalifikacji IOD a zwłaszcza doświadczenia i wiedzy prawniczej wydaje się (jak wynika z uprzednio uzyskanych przez nas odpowiedzi) - szczególnie wymagać - wdrożenia procedur aby takie „przypadkowe” osoby nie pełniły takich funkcji.

Pozostałe pytania:

1. Czy podmiot prowadzi BIP i pod jakim adresem internetowym

2. Z usług jakiego dostawcy BIP podmiot korzysta. Czy jest to www.nbip.pl lub

www.bip.edu.pl czy inny (podać jaki)?

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.

4. Proszę podać liczbę informacji publicznych opublikowanych w BIP w latach 2017-do czerwca 2022r.

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.

6. Wnosimy o udostępnienie wszystkich wniosków o informację publiczną na stronie BIP

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

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 któreś z tych

osób został lub zostanie wypłacony ekwiwalent za niewykorzystany urlop (jeśli tak w jakiej kwocie i komu)

*Celem zachowania pełnej przejrzystości działań - wnosimy o opublikowanie treści wnioski na stronie internetowej podmiotu wraz z odpowiedziami i uchybieniami na podstawie art. 8 ust. 1 ww. Ustawy o petycjach Chcemy działać w pełni jawnie i transparentnie. *

Każdy Podmiot mający styczność z Urzędem - ma prawo i obowiązek - usprawniać struktury administracji samorządowej

Pozwalamy jeszcze raz przypomnieć, że ipso iure 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 - głównie w Gminach/Miastach/szkołach' jednostkach podległych - gdzie jak wynika z naszych wniosków - stan faktyczny wymaga wszczęcia procedur sanacyjnych.

PYTANIA Z KRAJOWYCH RAM INTEROPERACYJNOŚCI

Zgodnie z Rozporządzeniem R. M. 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 2012r. poz. 526) "każdy podmiot publiczny zobowiązany jest do zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok (§ 20 ust.2 pkt 14). "

Pytania informacja publiczna?

- 1.Kto dokonuje corocznych audytów z KRI?
- 2.Czy IOD realizuje zadania w związku z KRIO?
- 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*.

*Podstawa: *

* rozporządzenie Rady Ministrów z 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 2012 r. poz. 526).

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? CZYIOD
KONTROLUJĘ EWIDENCJĘ

b) oprogramowania (np. licencje)? IOD KONTROLUJĘ EWIDENCJĘ

c) umów serwisowych?

2.

Czy przypisano konkretnym osobom obowiązków 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 ZOSTAŁO PRZEPROWADZONE? CZY IOD
KONTROLUJE W/W

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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

4.

Czy pracownicy mogą używać swojego sprzętu domowego do pracy nad

zadaniami powierzonymi

w ramach obowiązków służbowych? IOD KONTROLUJĘ EWIDENCJĘ

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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

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 ZOSTAŁO

PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

7.

Czy monitoruję połączenia ewentualnych nieautoryzowanych punktów bezprzewodowych do infrastruktury służbowej?/CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO 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/

.

2.

Czy wiem, które systemy są krytyczne dla działania
jednostki?/CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK
KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD
KONTROLUJE W/W/

3.

Czy mam pewność, że każdy krytyczny system jest w stanie

odtworzyć z kopii zapasowych w odpowiednim czasie?/CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

4.

Czy mam opracowane plany działania w 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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

Jeśli TAK proszę o przedłożenie dokumentu.

2.

Czy osoby te posiadają stosowne kompetencje?

Jeśli TAK proszę o potwierdzenie tego faktu.

3.

Czy wszyscy pracownicy zaangażowani w proces przetwarzania informacji posiadają pisemne 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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

5.

Czy identyfikatory i hasła nadawane są po uprzednim pisemnym złożeniu wniosku?

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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

7.

Czy prowadzona jest formalna lista zadań /obowiązków /uprawnień takich osób?/CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

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).

2.

Podstawowe elementy ochrony przed nieautoryzowanymi działaniami związanymi z przetwarzaniem informacji:

a.

ochrona sieci na poziomie portów LAN

b.

BIOS

c.

centralny system kontroli dostępu logicznego do pojedynczych komputerowych stanowisk pracy, serwerów i zasobów sieci - na poziomie domeny Windows

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
ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

e.

system ochrony zewnętrznej klasy firewall

f.

system ochrony zewnętrznego dostępu logicznego (urządzenie sieciowe-serwer VPN); – zabezpieczenie kodem PIN dostępu do wydruków;

g.

stosowanie tokenów z hasłami jednorazowymi

**

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 ZOSTAŁO
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/

.

2.

Czy w umowach zawieranych z podmiotami zewnętrznymi określono
zakres i tryb dostępu do własnych zasobów IT?

Jeśli TAK proszę o udokumentowanie.

3.

Czy w pracy na odległość stosuję bezpieczne metody połączenia?

4.

Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, posiadają aktualne oprogramowanie antywirusowe/są w pełni zaktualizowane?

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.

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 ZOSTAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W/

1.

Czy jednostka posiada zapisy gwarantujące odpowiedni poziom bezpieczeństwa ITw umowach zawieranychz dostawcami sprzętu/oprogramowania?

Jeśli TAK proszę o udokumentowanie.

2.

Czy posiadam krytyczne systemy, dla których nie ma zapisów umownych dotyczących bezpieczeństwa (np. zapewnienie możliwości wgrania aktualizacji komponentów, na których bazuje dany system)?

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 ZOSTAŁO 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.

2.

Czy posiadam mechanizmy uniemożliwiające dostęp do danych na urządzeniu mobilnym po jego utraceniu (np. pin/szyfrowanie przestrzeni dyskowej na urządzeniu)?

3.

Czy istnieją możliwości zdalnego, trwałego usunięcia danych z tego

typu urządzenia?

4.

Czy kontroluję to, co użytkownicy mogą realizować na urządzeniach mobilnych (np. uruchamianie dowolnych aplikacji)?

5.

Czy mam zapewnione bezpieczne połączenie urządzeń mobilnych z moją infrastrukturą (np. tylko protokoły szyfrowane)?

6.

Czy pracownicy mogą podłączać swoje urządzenia mobilne do mojej infrastruktury IT?

Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych./CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTAŁO 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?

2.

Czy aktualizuję oprogramowanie firmware na urządzeniach sieciowych – szczególnie tych, które mają bezpośredni styk z Internetem?

3.

Czy posiadam aktualne sygnatury dla systemu antywirusowego?

4.

Czy mam przygotowaną procedurę odtworzenia danej stacji roboczej
/ serwera po wykryciu na nim wirusa?

5.

Czy mam informacje o systemach, dla których aktualizacja nie
powiodła się?

6.

Czy wiem, które systemy IT są krytyczne dla prawidłowego
działania jednostki?

7.

Czy zapewniono ciągłość działania w przypadku wystąpienia awarii ww. systemów?

8.

Czy użytkownicy sieci przesyłają wrażliwe informacje w formie jawnej (np. za pośrednictwem e-mail lub przenosząc na pendrive / telefonie)?

9.

Czy obowiązuje w jednostce instrukcja reagowania na incydenty bezpieczeństwa IT?

10.

Czy wiem, z jakimi innymi wymaganiami prawnymi muszą być zgodne użytkowane systemy?

11

Czy zapewniam odpowiednio bezpieczny dostęp do poczty elektronicznej (dostęp tylko szyfrowany)?

12.

Czy umożliwiony jest zdalny dostęp do poczty elektronicznej?

13.

Czy dostęp do Internetu w jednostce jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp)?

14.

Czy w odpowiedni sposób zapewnia się ochronę przed fizyczną ingerencją w infrastrukturę IT (np.: odpowiednie zabezpieczenia serwerowni, okablowania)

Zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiające szybkie podjęcie działań korygujących.

1.

Czy istnieją w jednostce procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?

2.

Czy okresowo testuje się procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?

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.

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

Odpowiedzi w ustawowym terminie tj. do 14 dni proszę kierować na adres poczty elektronicznej:

Odpowiedzi proszę przesłać na maila:
rodo.rod55@wp.pl

Anna Mierzejewska

Łódź

- Part_2.html (798 KB)