Zarząd
Nieruchomości
Komunalnych
w Lublinie

ul. Grodzka 12, 20-112 Lublin, tel.:+48-81-537-12-00, fax.:+48-81-537-12-01
e-mail: znk@znk-lublin.pl , ePUAP: /znk_lublin/SkrytkaESP , www.znk-lublin.pl

LUBLIN 2023
EUROPEJSKA STOLICA MŁODZIEŻY

DL/11/07/2022

Lublin, dnia 13.07.2022 r.

Dzień dobry. W związku z pytaniami o udzielenie informacji publicznej przesłanymi w dniu 05.07.2022 r. ze skrzynki email: ZNK w Lublinie odpowiada:

I. Pytania IOD

1. IOD ma ukończone studia prawnicze i uprawnienia audytora wewnętrznego oraz jest pracownikiem od 2006 roku.
2. IOD w ramach swoich obowiązków przeprowadza szkolenia dla nowo przyjmowanych pracowników, które kończą się informacją o przebiegu szkolenia w czasie odbywania służby przygotowawczej i testem z wiedzy z zakresu ochrony danych osobowych. IOD na bieżąco współpracuje ze wszystkimi komórkami organizacyjnymi ZNK w zakresie poprawności działania w obszarze ochrony danych osobowych.
3. Zarząd Nieruchomości Komunalnych w Lublinie w ramach art. 24 ust. 1 RODO wdrożył następujące środki techniczne i organizacyjne: zreorganizowano system obsługi klienta, powołano Inspektora Ochrony Danych – zarządzenie Dyrektora z dnia. 25.05.2018 r., wdrożono i uaktualniono politykę bezpieczeństwa informacji w zakresie ochrony danych osobowych, wprowadzono rejestr czynności przetwarzania, rejestr kategorii czynności przetwarzania, rejestr naruszeń ochrony danych osobowych.
4. Wszyscy pracownicy mają dostęp do tzw. dysku wspólnego, w którym znajdują się wszelkie potrzebne informacje związane z bieżąca działalnością ZNK, wśród nich są uregulowania wewnętrzne oraz zewnętrzne.
5. Szkolenie pracowników dotyczące RODO przeprowadzone przy współpracy inspektora danych osobowych i administratora systemów informatycznych w maju 2018 r. IOD w ramach swoich obowiązków przeprowadza szkolenia dla nowo przyjmowanych pracowników, które kończą się informacją o przebiegu szkolenia w czasie odbywania służby przygotowawczej i testem z wiedzy z zakresu ochrony danych osobowych.
6. Tak, rejestr czynności przetwarzania danych osobowych jest na bieżąco uaktualniany.
7. Tak, rejestr kategorii czynności przetwarzania danych osobowych jest na bieżąco uaktualniany.
8. https://znk-lublin.home.pl/znk/dokumenty/RODO_2018.pdf
9. https://znk-lublin.home.pl/znk/dokumenty/RODO_2018.pdf
10. W ZNK nie ma monitoringu wizyjnego.
11. IOD w ramach monitorowania w zakresie prawidłowości przetwarzania danych osobowych co roku przeprowadza ankiety samooceny dla wszystkich pracowników, przeprowadza szkolenia nowo przyjmowanych pracowników, dokonuje analizy zmieniających się przepisów w odniesieniu do ochrony danych osobowych. Co roku w ZNK jest ustalana w formie zarządzenia Dyrektora identyfikacja, analiza oraz ocena

ryzyka w ramach systemu kontroli zarządczej, z której wynika jakie obszary są poddawane badaniu.
12. W ZNK nie ma monitoringu wizyjnego.
13. Do dnia wypełniania odpowiedzi w ZNK nie została opacowana odrębnym dokumentem polityka retencji danych.

II. Pytania ogólne

1. https://biuletyn.lublin.eu/znk/zarzad-nieruchomosci-komunalnych-w-lublinie,1,12298,1.html
2. BIP jest dostarczany przez Urząd Miasta Lublin.
3. BIP jest dostarczany przez Urząd Miasta Lublin.
4. Na stronie internetowej udostępnionych jest 47 informacji publicznych z lat 2017-2022.
5. Liczba wszystkich udostępnionych wniosków – 53, z czego jeden odmowny. ZNK uczestniczyło w jednym postępowaniu sądowym dotyczącym informacji publicznej.
6. https://www.znk-lublin.pl/udost_inf_publ.php
7. https://www.znk-lublin.pl/udost_inf_publ.php
8. Prawo do urlopu jest stosunkiem prawnym między pracownikiem i pracodawcą i do momentu rozwiązania stosunku pracy nie można przewidzieć czy i w jakiej wysokości ekwiwalent będzie wypłacony. Według stanu na dzień odpowiedzi ZNK nie wypłacało żadnemu pracownikowi ekwiwalentu za niewykorzystany urlop w 2022 roku.
9. IOD jest zatrudniony na podstawie umowy o pracę.
10. ZNK nie wdrażała procedury schematów podatkowych (MDR).

III. Pytania KRI

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		
	b) oprogramowania (np. licencje)? IOD KONTROLUJĘ EWIDENCJĘ	Tak		
	c) umów serwisowych?			Serwis wykonywany

				samodzielnie
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		Osobą odpowiedzialną jest Zastępca Kierownika Działu DO ds. informatycznych, zgodnie z Zarządzeniem nr 10 Dyrektora ZNK z dnia 28.03.2022 r.
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		Inwentaryzacja przeprowadzana w ZNK zgodnie z Zarządzeniem nr 15 Dyrektora ZNK z dnia 6.10.2020 r.
4.	Czy pracownicy mogą używać swojego sprzętu domowego do pracy nad zadaniami powierzonymi w ramach obowiązków służbowych? IOD KONTROLUJĘ EWIDENCJĘ		Nie	
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	
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*		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*		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		- awaria zasilania, - włamanie do systemu, - nieuprawniony dostęp, - destrukcja danych.
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		

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		
4.	Czy mam opracowane plany działania w momencie naruszenia bezpieczeństwa IT w mojej organizacji (np. procedury reagowania na incydenty IT)?	Tak		
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		
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		

2.	Czy osoby te posiadają stosowne kompetencje? Jeśli TAK proszę o potwierdzenie tego faktu.	Tak		
3.	Czy wszyscy pracownicy zaangażowani w proces przetwarzania informacji posiadają pisemne uprawnienia?	Tak		
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		
5.	Czy identyfikatory i hasła nadawane są po uprzednim pisemnym złożeniu wniosku?			Automatycznie, bez 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 ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	Tak		
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*	Tak		

	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).	Tak		
2.	Podstawowe elementy ochrony przed nieautoryzowanymi działaniami związanymi z przetwarzaniem informacji:			
a.	ochrona sieci na poziomie portów LAN	Tak		
b.	BIOS	Tak		
c.	centralny system kontroli dostępu logicznego do pojedynczych komputerowych stanowisk pracy, serwerów i zasobów sieci - na poziomie domeny Windows			Tak do serwerów
d.	niezależne od domenowych systemy kontroli dostępu logicznego do kluczowych systemów informatycznych; *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W*	Tak		
e.	system ochrony zewnętrznej klasy firewall	Tak		
f.	system ochrony zewnętrznego dostępu logicznego (urządzanie sieciowe-serwer VPN); – zabezpieczenie kodem PIN dostępu do	Tak		

	wydruków;			
g.	stosowanie tokenów z hasłami jednorazowymi	Tak		

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* .		Nie	
2.	Czy w umowach zawieranych z podmiotami zewnętrznymi określono zakres i tryb dostępu do własnych zasobów IT? Jeśli TAK proszę o udokumentowanie.		Nie	
3.	Czy w pracy na odległość stosuję bezpieczne metody połączenia?			Nie dotyczy
4.	Czy systemy (np. laptopy), które mają zdalny dostęp do infrastruktury jednostki, posiadają aktualne oprogramowanie antywirusowe/są w			Nie dotyczy

	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.			Nie dotyczy
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.	Tak		
2.	Czy posiadam krytyczne systemy, dla których nie ma zapisów umownych dotyczących bezpieczeństwa (np. zapewnienie możliwości wgrania aktualizacji komponentów, na których bazuje dany system)?		Nie	
Zasady postępowania z informacjami, zapewniające minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych. *CZY IOD W TYM ZAKRESIE PRZEPROWADZIŁ AUDYT. JEŚLI TAK KIEDY TAKIE SPRAWOZDANIE Z KRIO ZOSTRAŁO PRZEPROWADZONE? CZY IOD KONTROLUJE W/W. CZY IOD PRZEPROWADZIŁ ANALIZĘ RYZYKA I OCENĘ SKUTKÓW DLA PRZETWARZANIA DANYCH W URZĄDZENIACH MOBILNYCH?*				

1.	Czy obowiązują odpowiednie regulacje dotyczące zapisu danych na nośnikach przenośnych? Jeśli TAK proszę o przedłożenie.			Nie dotyczy
2.	Czy posiadam mechanizmy uniemożliwiające dostęp do danych na urządzeniu mobilnym po jego utraceniu (np. pin/szyfrowanie przestrzeni dyskowej na urządzeniu)?			Nie dotyczy
3.	Czy istniej możliwość zdalnego, trwałego usunięcia danych z tego typu urządzenia?			Nie dotyczy
4.	Czy kontroluję to, co użytkownicy mogą realizować na urządzeniach mobilnych (np. uruchamianie dowolnych aplikacji)?			Nie dotyczy
5.	Czy mam zapewnione bezpieczne połączenie urządzeń mobilnych z moją infrastrukturą (np. tylko protokoły szyfrowane)?			Nie dotyczy
6.	Czy pracownicy mogą podłączać swoje urządzenia mobilne do mojej infrastruktury IT?		Nie	

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	Tak		Nie wszystkie wymienione, tylko

	reader / flash itp.), jak i serwerach?			kluczowe
2.	Czy aktualizuję oprogramowanie firmware na urządzeniach sieciowych – szczególnie tych, które mają bezpośredni styk z Internetem?	Tak		
3.	Czy posiadam aktualne sygnatury dla systemu antywirusowego?	Tak		
4.	Czy mam przygotowaną procedurę odtworzenia danej stacji roboczej / serwera po wykryciu na nim wirusa?	Tak		
5.	Czy mam informacje o systemach, dla których aktualizacja nie powiodła się?			Nie dotyczy
6.	Czy wiem, które systemy IT są krytyczne dla prawidłowego działania jednostki?	Tak		
7.	Czy zapewniono ciągłość działania w przypadku wystąpienia awarii ww. systemów?			Nie było takiego przypadku
8.	Czy użytkownicy sieci przesyłają wrażliwe informacje w formie jawnej (np. za pośrednictwem e-mail lub przenosząc na pendrive / telefonie)?		Nie	
9.	Czy obowiązuje w jednostce instrukcja reagowania na incydenty bezpieczeństwa IT?	Tak		
10.	Czy wiem, z jakimi innymi wymaganiami prawnymi muszą być zgodne użytkowane systemy?	Tak		
11	Czy zapewniam odpowiednio bezpieczny dostęp do poczty elektronicznej (dostęp tylko szyfrowany)?	Tak		

12.	Czy umożliwiony jest zdalny dostęp do poczty elektronicznej?	Tak		
13.	Czy dostęp do Internetu w jednostce jest ograniczany (np. poprzez wykorzystanie serwera proxy i umożliwienie dostępu tylko do kilku usług – np. http, ftp)?	Tak		
14.	Czy w odpowiedni sposób zapewnia się ochronę przed fizyczną ingerencją w infrastrukturę IT (np.: odpowiednie zabezpieczenia serwerowni, okablowania)	Tak		
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?	Tak		
2.	Czy okresowo testuje się procedury zgłaszania incydentów naruszenia bezpieczeństwa informacji?	Tak		

Z up. Dyrektora ZNK
Z-ca DYREKTORA
ds. Eksploatacji

mgr inż. Marek Pastusiak