Kierownik Jednostki Samorządu Terytorialnego (dalej JST) - w rozumieniu art. 33 ust. 3 Ustawy o samorządzie gminnym (Dz.U.2018.994 t.j. z 2018.05.24)

Dane wnioskodawcy znajdują się poniżej oraz - w załączonym pliku sygnowanym bezpiecznym podpisem elektronicznym, weryfikowanym kwalifikowanym certyfikatem - stosownie do dyspozycji Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U.2019.162 t.j. z dnia 2019.01.28) oraz przepisów art. 4 ust. 5 Ustawy o petycjach (Dz.U.2018.870 t.j. z dnia 2018.05.10) - **Data dostarczenia - zgodna z dyspozycją art. 61 pkt. 2 Ustawy Kodeks Cywilny (Dz.U.2018.1025 t.j. z dnia 2018.05.29)**

Premabuła Wniosku:
Najwyższa Izba Kontroli w protokole pokontrolnym nr kap-4101-002-00/2014 - " (...) negatywnie ocenia działania burmistrzów i prezydentów miast w zakresie zarządzania bezpieczeństwem informacji w urzędach, o którym mowa w § 20 rozporządzenia KRI. NIK stwierdziła nieprawidłowości w tym obszarze w 21 z 24 (87,5%) skontrolowanych urzędów miast, z których sześć oceniła negatywnie. (...)"

W związku z powyższym:

§1) Na mocy art. 61 Konstytucji RP w związku z art. 6 ust. 1 pkt. lit. c Ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U.2018.1330 t.j. z 2018.07.10) - w związku z §20 pkt. 12 lit. a - scilicet "(...) zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: dbałości o aktualizację oprogramowania,(...) " - **wnosimy o udzielnie informacji publicznej w przedmiocie - szacunkowej ilości oprogramowania - użytkowanego w Urzędzie i nieposiadającego obecnie wsparcia producenta - inter alia: Windows XP, Windows Vista, etc,**
Dla ułatwienia in fine wniosku załączamy chronologiczne wyszczególnienie systemów operacyjnych - wraz z informacją statusie wsparcia w zakresie poszczególnego systemu.

Aby nie absorbować niepotrzebnie czasu Urzędników - wnosimy aby opisowe odpowiedzi na poniższe pytania były krótkie, ogólne - maksymalnie kilkuzdaniowe.

§2) Wnosimy o krótki, ogólny opis - **w jaki sposób - Jednostka Samorządu Terytorialnego - zapewnia odpowiedni poziom bezpieczeństwa systemów teleinformatycznych - w związku z dbałością o aktualizację oprogramowania i zapewnieniem bezpieczeństwa plików systemowych stosownie do wytycznych §20 pkt 12 lit. a oraz lit. e ww. Rozporządzenia.**

§2.1) W odniesieniu do ww. przepisu wnosimy również o udzielenie informacji publicznej, w przedmiocie sposobu zabezpieczenia dostępu do wewnętrznej sieci Urzędu z sieci Internet - czy odbywa się to poprzez:
- Urządzenie firewall, czy
- Serwer oparty o linux
W przypadku pierwszej opcji, fakultatywnie - wnosimy o podanie nazwy producenta, oraz modelu wzmiankowanego urządzenia.

§2.3) Czy Urząd dysponuje całościową Polityką Bezpieczeństwa Informacji, wymaganą w §20 ust. 1 i 3 ww. Rozporządzenia?
Jeśli odpowiedź jest twierdząca - wnosimy o krótkie - w kilku ogólnych zdaniach - opisanie przedmiotowej polityki.
§2.4) Kiedy Urząd ostatni raz przeprowadzał wewnętrzny audyt z zakresu bezpieczeństwa informacji - stosownie do wymogów §20 ust. 2 pkt. 14 ww. Rozporządzenia.

§3) Wnosimy o krótki opis polityki tworzenia kopii zapasowych - w kontekście ww. Rozporządzenia.
Fakultatywnie - wnosimy o podanie wersji producenta, wersji oprogramowania oraz zwyczajowego sposobu przechowywania danych - scilicet: czy na dysku sieciowym, dysku USB, nośniku CD/DVD, taśma, pendrive, etc

§4) Na mocy wyżej wzmiankowanych przepisów wnosimy o udzielenie informacji publicznej w przedmiocie, czy Urząd posiada na dzień dostarczenia niniejszego wniosku - bilateralne sygnowaną

umowę (ze strony Urzędu przez upoważnioną osobę) w przedmiocie usług poczty elektronicznej - spełniającą wymogi 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 (...) ?
§4.1) Fakultatywnie wnosimy o podanie ilości zdefiniowanych skrzynek poczty elektronicznej, oraz nazwy dostawcy (własny serwer, nazwa usługodawcy, etc)

§5) Na mocy wyżej wymienionych przepisów wnosimy o podanie danych Pracownika Urzędu, który w zakresie wykonywanych zadań i powierzonych kompetencji odpowiada operacyjnie za wyżej wzmiankowany obszar związany z informatyzacją Urzędu.
Mówiąc o danych Pracownika Urzędu - Wnioskodawca ma na myśli - imię i nazwisko, adres e-mail, nr tel. etc

§6) Na mocy art. 61 Konstytucji RP, w trybie art. 6 ust. 1 pkt. 1 lit c oraz art. 6 ust. 1 pkt. 2 lit. b Ustawy z dnia 6 września o dostępie do informacji publicznej (Dz.U.2018.1330 t.j. z 2018.07.10) - wnosimy o udzielnie informacji publicznej w przedmiocie - ile procent oprogramowania użytkowanego na potrzeby wykonywania zadań publicznych (na terenie Urzędu) - może na dzień złożenia niniejszego wniosku, nie posiadać ważnej licencji użytkowania - wymaganej wg. prawa?
W rozumieniu wnioskodawcy wystarczy w tej mierze aproksymować stan faktyczny poprzez szacunkowe porównanie ilości użytkowanego oprogramowania wymagającego posiadanie licencji w stosunku do zewidencjonowanej dokumentacji licencyjnej.

6a) Pomimo, że nie wnioskujemy o informację przetworzoną w zakresie wymagającym znacznych nakładów pracy, uzasadniamy nasze pytania stosownie do brzmienia art. 3 ust. 1 pkt. 1 Ustawy o dostępie do informacji publicznej – tym, że przedmiotowa informacja oraz ewentualna późniejsza próba optymalizacji tego obszaru wydaje się szczególnie istotna z punktu widzenia Interesu Społecznego.

Osnowa Wniosku:
Kiedy 3 lata temu Wnioskodawca zadawał pytanie Gminom - o ilość oprogramowania użytkowanego przez Urząd, które może nie posiadać ważnej licencji - niektóre odpowiedzi poświadczały - expressis verbis - że nawet 30% oprogramowania użytkowanego przez Urząd może takiej licencji nie posiadać (odpowiedzi tego typu opublikowaliśmy na portalu [redacted] - zatem wydaje się ze ponowne zbadanie stanu faktycznego - jest ze wszech miar uzasadnione.
Zastrzegamy sobie możliwość opublikowania wybranych odpowiedzi w naszym portalu [redacted]

Zdaniem wnioskodawcy obszar ten - stosownie do art. 241 KPA, wymaga optymalizacji.
§6b) Wnosimy o zwrotne potwierdzenie otrzymania niniejszego wniosku w odnośnych przepisów - na adres e-mail [redacted]
§7) Wnosimy o to, aby odpowiedź w przedmiocie powyższych pytań złożonych na mocy art. 61 Konstytucji RP w Ustawy o dostępie do informacji publicznej w związku z art. 221 i 241 KPA, została udzielona - zwrotnie na adres e-mail [redacted]
§8) Wniosek został sygnowany kwalifikowanym podpisem elektronicznym - stosownie do wytycznych Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U.2019.162 t.j. z dnia 2019.01.28)

[redacted]

SEKRETARZ MIASTA
GORZOWA WIELKOPOLSKIEGO

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

T: +48 95 7355 500
F: +48 95 7355 670
E: kancelaria@um.gorzow.pl
I: www.gorzow.pl

Gorzów Wlkp., 29.05.2019 r.

WOR - III.1431.149.2019.KPa

[redacted]

W odpowiedzi na złożony w dniu 15 maja 2019 roku wniosek o udostępnienie informacji publicznej, przekazuję odpowiedzi na zadane pytania:

§1 Systemy operacyjne i status wsparcia:

- Windows XP Home - system nie wspierany 0
- Windows XP Pro. - system nie wspierany 77
- Windows Vista Home (koniec wsparcia rozszerzonego: 11.04.2017 r.) 0
- Windows Vista Business (koniec wsparcia rozszerzonego: 11.04.2017 r.) 0
- Windows 7 Pro (koniec wsparcia rozszerzonego: 14.01.2020 r.) 126
- Windows 7 Home (koniec wsparcia rozszerzonego: 14.01.2020 r.) 0
- Windows 8/8.1 Home 0
- Windows 8/8.1 Pro 0
- Windows 10 Home 0
- Windows 10 Pro 298
- Windows Server 2003/R2 1
- Windows Server 2008/R2 2
- Windows Server 2012/R2 3
- Windows Server 2016 36
- Windows Server 2019 0

§2 Wytyczne opisane w §20 lit. a i e – aktualizacje oprogramowania wykonywane są w sposób automatyczny, zalecany przez producentów oprogramowania. Wdrożenie aktualizacji poprzedzają próby w środowisku testowym.

§2.1 Zabezpieczenie dostępu do sieci wewnętrznej jest zapewnione przez szereg uzupełniających się rozwiązań. Opis przyjętego rozwiązania, podobnie jak podanie nazwy producentów i modeli urządzeń w opinii odpowiadającego nie może być przedmiotem

odpowiedzi z uwagi na potencjalną możliwość wykorzystania znanych lub w przyszłości wykrytych podatności. W związku z powyższym odnośnie tego pytania zostanie wydana decyzja administracyjna o odmowie dostępu do informacji publicznej na podst. art. 5 ust 1 ustawy z dnia 6 września 2001 r o dostępie do informacji publicznej.

§2.3 Polityka Bezpieczeństwa Informacji jest w trakcie opracowania.

§2.4 Ostatni audyt w zakresie bezpieczeństwa informacji na przełomie 2017 i 2018 roku.

Kwestionariusz Kontroli Wewnętrznej WSI 1 KRI	
Nazwa zadania	„Przetwarzanie danych osobowych przez pracowników Urzędu Miasta Gorzowa Wlkp. w systemach informatycznych i w formie papierowej".
Numer zadania	2017/12
Cel badania	Zapewnienie działania zgodnego z prawem. Zapewnienie minimalnych wymagań dla systemu teleinformatycznego.
Kryterium oceny ustaleń stanu faktycznego	1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2017 poz. 570). 2. 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 (t.j. Dz. U. z 2017 poz. 2247), zwane dalej rozporządzeniem w sprawie KRI.
Jednostka audytowana	Urząd Miasta Gorzowa Wlkp., jako podmiot realizujący zadania publiczne (UM). Wydział Zarządzania Systemami Informatycznymi (WSI)

§3 Kopie zapasowe danych z serwerów przechowywane są w lokalizacjach sieciowych (poza miejscem fizycznej lokalizacji serwera). Użytkowane oprogramowanie - Veeam Backup & Replication.

§4 W opinii odpowiadającego Rozporządzenie 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, nie zawiera zapisów dotyczących poczty elektronicznej oraz umów zawieranych z dostawcami tego typu usług.

§5 Zgodnie z utrwalonym orzecznictwem Naczelnego Sądu Administracyjnego nie jest informacją publiczną żądanie dotyczące podania: który wydział lub który konkretnie pracownik tego wydziału jest odpowiedzialny za realizację określonych zadań a w niniejszym przypadku za prowadzenie polityki bezpieczeństwa systemów informatycznych (por. wyrok NSA z dnia 8 lutego 2018 r. sygn. akt I OSK 1828/17). Jest to bowiem informacja niemająca charakteru czy znamion informacji publicznej, jako że dotyczy wewnętrznej organizacji pracy. Wskazanie wydziału, który odpowiada za realizację określonych obowiązków, jako elementu wewnętrznej struktury organizacyjnej Urzędu Miasta, jak również imienia i nazwiska osoby realizującej dane zadanie nie jest informacją publiczną. Są to kwestie związane z wewnętrznym funkcjonowaniem organu administracyjnego, z techniczną realizacją zadań, a nie z jego "zewnętrzną" działalnością skierowaną do podmiotów pozostających poza strukturami

administracji publicznej. Z tych też względów żądane dane nie mogą być udostępnione w trybie dostępu do informacji publicznej.

§6 Urząd Miasta Gorzowa Wlkp. nie korzysta z oprogramowania bez ważnej licencji. Prowadzony jest regularny monitoring używanego oprogramowania i posiadanych licencji. Wszelkie nieprawidłowości usuwane są na bieżąco.

SEKRETARZ MIASTA
Eugeniusz Kurzawski