Zarządzenie Nr KR.120.106.2018

Burmistrza Woźnik

z dnia 18 czerwca 2018 r.

w sprawie zmiany Zarządzenia nr KR.120.91.2018 z dnia 24 maja 2018r. Burmistrza Woźnik w sprawie wprowadzenia dokumentacji dotyczącej ochrony danych osobowych w Urzędzie Miejskim w Woźnikach

Na podstawie art. 33 ust. 1 i ust.3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r., poz. 994 z późn.zm.) oraz 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 zarządzam, co następuje;

§ 1

W załączniku nr 1 do Zarządzenia nr KR.120.91.2018 z dnia 24 maja 2018r. Burmistrza Woźnik w sprawie wprowadzenia dokumentacji dotyczącej ochrony danych osobowych w Urzędzie Miejskim w Woźnikach wprowadza się następujące zmiany;
1.Skreśla się słowa lub zwroty:" ABI', „Administrator bezpieczeństwa Informacji".

2.W Rozdziale II Podstawowe definicje w § 1 ust.1 tiret 12, po słowie "Administrator" dodaje się zapis „ADO".

3.W Rozdziale II Podstawowe definicje w § 1 ust.1 na końcu dodaje się zapis;

- „ Burmistrz – Burmistrz Woźnik"

4.W Rozdziale III Polityka bezpieczeństwa po § 3 dodaje się § 3a i § 3b o treści;

„§ 3a

Obsługa wniosków podmiotów

1.Każda osoba, której dane dotyczą ma możliwość skorzystania ze swoich praw i w tym celu zgłosić się do instytucji.
2. Złożenie wniosku przez podmiot winno być możliwe w każdej formie, przy czym dla celów dowodowych zaleca się utrwalenie wniosku (żądanie, zapytanie, skargi, wnioski, itd.) co najmniej w formie e-maila.
3.Każdy składany wniosek w pierwszej kolejności powinien być zweryfikowany pod względem uprawnienia danej osoby do jego złożenia. Należy zachować szczególną ostrożność w przypadkach, kiedy za osobę, której dane dotyczą, występuje jej reprezentant/pełnomocnik. Wówczas w pierwszej kolejności należy sprawdzić poprawność reprezentacji/pełnomocnictwa.

4.Wnioski rozpatruje się wyłącznie, gdy zostały złożone przez uprawnioną osobę tj. osobę, której dane dotyczą lub osobę właściwie umocowaną.
5.Nigdy nie udziela się odpowiedzi na zapytania ustne, w tym kierowane telefonicznie, o ile instytucja nie ma możliwości potwierdzenia tożsamości rozmówcy.
6.Wnioski rozpatruje się biorąc pod uwagę ich treść, a nie tytuł.
7.Każdy wniosek, którego rozpatrzenie wymaga zastosowanie przedmiotowych zasad, musi być zweryfikowany przez IOD. Osoba otrzymująca wniosek jest zobowiązana przekazać wniosek do konsultacji IOD niezwłocznie, po otrzymaniu takiego wniosku.
8.Odpowiedź na wniosek wymagający konsultacji musi być sporządzony lub zaopiniowany przez IOD, zanim zostanie wysłany.
9.Odpowiedzi na wniosek udziela się bez zbędnej zwłoki – w każdym razie w terminie miesiąca od otrzymania żądania. Odpowiedź zawiera informacje o działaniach podjętych w związku z żądaniami o których mowa w § 3b.
10.W razie potrzeby termin wskazany w pkt.9 może być przedłużony o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania instytucja informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.
11.Jeżeli osoba, której dane dotyczą, przekazała swoje żądanie w formie elektronicznej, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, żąda innej formy. Na wnioski odpowiada się z wykorzystaniem danych adresowych, na które wniosek został skierowany, o ile IOD nie zaleci inaczej (np. w szczególnych sytuacjach).
12.Jeżeli instytucja nie podejmuje działań na żądanie osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz o skorzystaniu ze środków ochrony prawnej przed sądem.
13.Po rozpatrzeniu wniosku i udzieleniu odpowiedzi IOD wydaje dalsze wskazówki, dotyczące postępowania z danymi osobowymi danej osoby.

§ 3b

Rodzaje wniosków

Dostęp do informacji o osobie, której dane dotyczą;
1.Osoba, której dane dotyczą jest uprawniona do uzyskania od ADO potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące.
2.Jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji;

- celu przetwarzania,
- kategorie danych osobowych,
- informacje o odbiorach lub kategorii odbiorców, których dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorach w państwach trzecich lub organizacjach międzynarodowych.,
- w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest ot możliwe, kryteria ustalania tego okresu,

- informacje o prawie żądania od ADO sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczących osoby, której dane dotyczą oraz do wniesienia sprzeciwu wobec takiego przetwarzania,
- informacje o prawie wniesienia skargi do organu nadzorczego,
- jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą- wszelkie dostępne informacje i tym źródle,
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą,
- jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach danych związanych z przetwarzaniem.

3.Instytucja dostarcza osobie, której dane dotyczą, kopie danych osobowych podlegających przetwarzaniu.

4.Jeżeli nie ma to miejsca, osoba występująca z wnioskiem powinna zostać powiadomiona o nie występowaniu danych jej dotyczących. W celu zajęcia takiego stanowiska, instytucja zobowiązana jest do zweryfikowania każdego miesiąca, w którym może następować przetwarzanie danych.

6.Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, ADO może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię danych elektroniczną i nie jest zaznaczony inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

<u>Sprostowanie danych.</u>

1.Osoba, której dane dotyczą, ma prawo żądania od ADO niezwłocznego sprostowania (poprawienia) dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowych oświadczeń (np. do celów uprzedniej weryfikacji prawidłowości i aktualności podanych danych).

2.W związku z tym, że wnioski w tym zakresie nie dotyczą prawa bezwzględnego, w przypadkach spornych wymagana jest konsultacja z IOD w celu weryfikacji, czy złożony wniosek i przedstawione w nim żądanie jest skuteczne.

3.Jeżeli upubliczniono dane osobowe, a na mocy pkt.2 istnieje obowiązek ich usunięcia, to biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje się rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe w wyniku udostępnienia, że osoba które dane dotyczą żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich repliki.

<u>Ograniczenie przetwarzania danych osobowych</u>

1.Osoba, której dane dotyczą ma prawo zażądać ograniczenia przetwarzania jej danych osobowych w przypadkach o których mowa w rozporządzeniu.

2.W związku z tym, że wnioski w tym zakresie nie dotyczą prawa bezwzględnego, w przypadkach spornych wymagana jest uprzednio konsultacja z IOD w celu weryfikacji, czy złożony wniosek i przedstawione w nim żądanie jest skuteczne.

Przenoszenie danych

1.Osoba, której dane dotyczą ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące oraz ma prawo przesłać te dane osobowe innemu administratorowi bez żadnych przeszkód ze strony instytucji.

2.Wykonując prawo do przenoszenia danych na mocy pkt.1 osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez instytucję bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

3.W związku z tym, że wnioski w tym zakresie nie dotyczą prawa bezwzględnego, w przypadkach spornych wymagana jest konsultacja z IOD w celu weryfikacji, czy złożony wniosek i przedstawione w nim żądanie jest skuteczne.

Sprzeciw wobec przetwarzania danych

1.Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych w przypadkach, o których mowa w rozporządzeniu.

2. W związku z tym, że wnioski w tym zakresie nie dotyczą prawa bezwzględnego, w przypadkach spornych wymagana jest konsultacja z IOD w celu weryfikacji, czy złożony wniosek i przedstawione w nim żądanie jest skuteczne.

Odwołanie zgody

1.Każda osoba, która wyrażała zgodę na przetwarzanie jej danych osobowych ma prawo ją odwołać w dowolnym momencie.

2.W takim wypadku instytucja nie ma dłużej prawa przetwarzać danych osobowych w celu objętym oświadczeniem zgody (zgoda jest odwoływana, więc odpada podstawa prawna do przetwarzania danych).

3.W wyniku odwołania zgody dane przetwarzane w celach objętych zgodą powinny zostać bezwzględnie usunięte."

5.W Rozdziale IV Instrukcja zarządzania systemem informatycznym skreśla się § 4 Metody i środki uwierzytelniania w dotychczasowym brzmieniu nadając mu nową treść;

„§ 4

Metody i środki uwierzytelniania

Identyfikator

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora (login) i hasła, jako narzędzi umożliwiających bezpieczne uwierzytelnienie.

2. Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator, którego nazwa składa się z pierwszej litery imienia pisanej z małej litery oraz nazwiska pisanego z małej litery. Między imieniem i nazwiskiem nie ma spacji, ani kropki.

3. W przypadku zbieżności nadawanego identyfikatora z identyfikatorem wcześniej zarejestrowanego użytkownika IOD, nadaje inny identyfikator odstępując od ogólnej zasady.

4. W identyfikatorze stosuje się polskie znaki diakrytyczne.

5.Identyfikator użytkownika winien być tak skonstruowany, by w sposób jednoznaczny można było go przypisać temu użytkownikowi.

6.Każdy identyfikator musi być unikalny tzn. zabrania się tworzenia dwóch lub więcej takich samych identyfikatorów.

7.Niedopuszczalne jest korzystanie z tego samego identyfikatora przez więcej niż jednego użytkownika.

8.Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi.

9.Systemy informatyczne służące do przetwarzania danych muszą umożliwiać automatyczne odnotowywanie identyfikatora użytego do uwierzytelnienia, w ten sposób, by identyfikator ten można było w łatwy sposób powiązać z użytkownikiem, który się nim posłużył podczas uwierzytelniania. Identyfikator ten powinien również być odnotowywany (w sposób automatyczny) za każdym razem, gdy posługujący się nim użytkownik wprowadza po raz pierwszy dane osobowe do systemu informatycznego.

Hasła

1. Użytkownik posiadający upoważnienie do przetwarzania danych osobowych powinien posiadać hasło do systemu operacyjnego oraz osobne do baz danych osobowych i aplikacji.

2.Przekazywanie haseł użytkownikom powinno odbywać się metodą zapewniającą poufność.

3. Hasło składa się, z co najmniej ośmiu znaków, zawiera, co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny.

4. Hasło nie powinno zawierać żadnych informacji, które można skojarzyć z użytkownikiem komputera (imiona najbliższych, daty urodzenia, inicjały itp.) i nie może być sekwencją kolejnych znaków klawiatury.

5.Hasła nie powinny być powszechnie używanymi słowami.

6.Hasło nie może być tożsame z identyfikatorem użytkownika.

7. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do zgłoszenia tego faktu ASI i do natychmiastowej zmiany hasła.

8. Hasła podlegają okresowej zmianie. W miarę możliwości należy dążyć do tego, by zmiana hasła była wymuszana przez system informatyczny w sposób automatyczny. Jeżeli system informatyczny nie daje takich możliwości, obowiązek zmiany hasła spoczywa na użytkowniku. Należy zapewnić zmianę hasła nie rzadziej, niż co 90 dni.

9.Zmiana hasła powinna być wymuszona przy pierwszym logowaniu, chyba, że system informatyczny nie umożliwia wykonanie takiej operacji – wówczas za zmianę hasła odpowiada użytkownik.

10. Należy unikać stosowania tego samego hasła do ochrony różnych zasobów np. to samo hasło do komputera i poszczególnych systemów informatycznych.

11.Hasła wpisane z klawiatury nie mogą pojawiać się na ekranie monitora w formie jawnej.

12.Hasło nie może być ujawnione nawet po utracie przez nie ważności.

13.W przypadku korzystania z komputera podłączonego do sieci publicznej nie wolno zgadzać się na zapamiętywanie hasła w systemie komputerowym lub w przeglądarce.

14.Zakazuje się przechowywać zapisane hasła w łatwo dostępnym miejscu (na monitorach komputera, na klawiaturze, itp.).

15.W przypadku podejrzenia, że hasło poznała osoba nieupoważniona do przetwarzania danych osobowych, użytkownik ma obowiązek niezwłocznego poinformowania ASI. ASI po otrzymaniu takiej informacji zmienia hasło dla tego użytkownika (w przypadku gdy użytkownik nie ma możliwości zmiany hasła własnoręcznie) oraz sprawdza loginy systemowe, czy w międzyczasie nie dokonane zostały nieautoryzowane dostępy do systemu informatycznego.

16. Hasła najwyższego poziomu, którymi dysponuje ASI gromadzone są w zamkniętej kopercie przez IOD".

6.W Rozdziale IV Instrukcja zarządzania systemem informatycznym po § 4 dodaje się § 4a o treści;

„§ 4a

Zasady pracy z pocztą elektroniczną

1. Pracownicy instytucji do kontaktów służbowych mogą wykorzystywać wyłącznie służbowe adresy a-mail nadane przez instytucję.

2.Za służbowe adresy e-mail uznaje się takie, które zostały założone w domenie instytucji i dostępy do zasobów poczty elektronicznej są kontrolowane (nadawane, blokowane, dobierane) przez instytucję.

3.Zabronione jest przesyłanie służbowych wiadomości e-mail na prywatne skrzynki mailowe, jak tez zapisywanie załączników na prywatne nośniki.

4.Zabronione jest przesyłanie na adresy służbowych skrzynek pocztowych wiadomości prywatnych (a zwłaszcza filmów, zdjęć, dokumentów).

5.Każdy użytkownik poczty elektronicznej posiada swoje indywidualne hasło i identyfikator dostępowy do konta.

6.Zabronione jest wymienianie się swoimi danymi logowania.

7.Sytaucja, kiedy kilku użytkowników ma mieć dostęp do zawartości jednego konta jest możliwa wyłącznie wówczas, gdy zapewniona jest rozliczalność wykonywanych operacji (tzn. kiedy instytucja jest w stanie określić, który użytkownik dokonywał operacji w systemie).

8.Użytkowncy mają zakaz otwierania podejrzanych e-maili, co oznacza w szczególności, że;

a/. pochodzą od osoby nieznanej, która nie ma powodu aby przysyłać wiadomości lub załączniki,

b/. załącznik jest przesyłany w pustej wiadomości,

c/.w e-mailu jest wiadomość ale nie ma jakiegokolwiek sensu,

d/.jest wiadomość ale wydaje się mało prawdopodobne aby to ten nadawca ja wysłał,

e/. e-mail zawiera łącza do pornograficznych witryn internetowych, erotyczne obrazy, itd.,

f/.wiadomość nie zawiera żadnych osobistych zwrotów (np. wiadomość w której jest tylko napisane „Musisz na to spojrzeć" lub „Wysyłam to do Ciebie, gdyż potrzebuje twojej porady"),

g/. wiadomość podpisana jest przez nadawcę, którego dane adresowe ze stopki e-mail nie odpowiadają danym domenie, z której e-mail został wysłany,

h/.załącznik ma rozszerzone nazwy, który wskazuje na to, że jest to plik wykonywalny,

i/.załącznik ma nazwę o podwójnym rozszerzeniu np. NAZWA.JPG.vbs lub NAWZA.TXT.scr (podejrzany adresat, temat wiadomości).

9.W przypadku otrzymania podejrzanej wiadomości e-mail lub tez w przypadku gdy system antywirusowy/antyspamowy sugeruje, że wiadomość jest niebezpieczna dla systemu, użytkownik ma obowiązek zgłosić sprawę do ASI".

7. W Rozdziale IV Instrukcja zarządzania systemem informatycznym po §11 dodaje się § 11a i § 11b o treści;

„§11a

Wytyczne dotyczące wewnętrznych okresów przechowywania

1. Każdy pracownik zobowiązany jest do stosowania się do zasady ograniczenia czasowego przetwarzania danych osobowych. Oznacza to, że dane osobowe mogą być przechowywane w formie umożliwiającej identyfikacje osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

2.Wymaga się zapewnienia okresu ograniczenia przechowywania danych do ścisłego minimum.

3.Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, instytucja ustala termin lub kryteria ustalania terminów ich przechowania, po czym dane powinny zostać usunięte lub zanonimizowane.

4.Bez względu na powyższe każdy pracownik zobowiązany jest do okresowego przeglądu danych osobowych, na których pracuje pod kątem ich przydatności dla działalności jednostki. Oznacza to w szczególności przegląd; skrzynek pocztowych, folderów typu „Pobrane", „Usunięte" plików zapisywanych w innych miejscach na dysku (lokalnym lub sieciowym) posiadanych kopii lub oryginałów dokumentów, korespondencji, wydruków, roboczych notatek, itp.

5.W przypadku zidentyfikowania niepotrzebnych plików/dokumentów/wiadomości – powinny one zostać trwale usunięte przez pracownika.

6.Do czasu ich usunięcia dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

7.Wszędzie gdzie mowa o formularzach czy dokumentacji podlegającej przechowaniu, należy przez to rozumieć także elektroniczne formy (scany zapisane na dyskach, e-maile, wpisy w systemie informatycznym).

§ 11b

Procedura zgłaszania naruszeń ochrony danych osobowych

Definicja naruszenia bezpieczeństwa ochrony danych osobowych

1.Przez naruszenie ochrony danych osobowych należy rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

2.Na potrzeby powyższego wprowadza się następujące pojęcia;

a/.atak – próba zniszczenia, ujawnienia, zmiany, uniemożliwienia dostępu, kradzieży lub uzyskania nieautoryzowanego dostępu albo nieautoryzowanego użycia danych osobowych,

b/.zdarzenie związane z bezpieczeństwem danych osobowych – stwierdzone wystąpienie stanu systemu, usługi lub sieci, które wskazuje na możliwe naruszenie procedur bezpieczeństwa instytucji lub błąd zabezpieczenia lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem danych osobowych.

3.Za naruszenie bezpieczeństwa danych osobowych uznawany jest każdy stwierdzony fakt (w tym atak skutkujący wystąpieniem zdarzenia) oraz uzasadnione podejrzenie wystąpienia zdarzenia, a w szczególności;

a/.nieuprawnione ujawnienie danych osobowych,

b/.naruszenie hasła dostępu i identyfikatora (system nie reaguje na hasło lub je ignoruje bądź można przetwarzać informacje bez wprowadzenia hasła),

c/.częściowy lub całkowity brak informacji, w tym danych osobowych albo dostęp do informacji w zakresie szerszym niż wynikający z przyznanych uprawnień,

d/.brak dostępu do właściwej aplikacji lub zmiana zakresu wyznaczonego dostępu do zasobów serwera,

e/. wykrycie wirusa komputerowego,

f/.zauważenie elektronicznych śladów próby włamania do systemu informatycznego,

g/.znaczne spowolnienie działania systemu informatycznego,

h/.podejrzenie kradzieży sprzętu komputerowego lub dokumentów zawierających

chronione informacje,

i/.istotna zmiana położenia sprzętu komputerowego,

j/. zauważenie śladów usiłowania lub dokonania włamania do pomieszczeń lub zamykanych szaf,

k/.zabrania informacji chronionych, w tym danych osobowych przez osobę nieuprawnioną,

l/.uszkodzenie lub zniszczenie informacji lub jakiegokolwiek elementu systemu informatycznego,

ł/.działanie wbrew postanowieniom procedur bezpieczeństwa danych osobowych obowiązujących w instytucji.

Tryb postępowania.

1.Każdy pracownik posiadający informację o ataku, zdarzeniu lub innym naruszeniu albo uzasadnionym podejrzeniu wystąpienia ataku, zdarzenia lub naruszenia bezpieczeństwa danych osobowych, obowiązany jest bezzwłocznie poinformować o tym ASI według wzoru stanowiącego formularz nr 19. Pracownik do czasu przybycia na miejsce ASI podejmuje tylko takie czynności, które zmierzają do;

a/.zabezpieczenia śladów naruszenia,

b/.zapobieżenia dalszym zagrożeniom,

c/.powstrzymywania skutków naruszenia,

d/.ustalenia przyczyn i sprawcy naruszenia,

e/.przygotowanie opisu incydentu.

2.Pracownik nie opuszcza bez uzasadnionej przyczyny miejsca zdarzenia do czasu przybycia ASI lub osoby przez niego wskazanej.

3.ASI po otrzymaniu zawiadomienia o którym mowa powyżej powinien niezwłocznie;

a/.przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności naruszenia bezpieczeństwa danych osobowych,

b/.podjąć działania chroniące system przed ponownym naruszeniem,

c/.w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych odnotować fakt wystąpienia incydentu w ewidencji incydentów stanowiącej formularz nr 20, a następnie niezwłocznie, nie później niż w terminie 48 godzin od wykrycia zdarzenia, przesłać jego opis do Burmistrza oraz do IOD.

4.Burmistrz po zapoznaniu się z opisem zdarzenia, podejmuje decyzję o dalszym trybie postępowania, powiadomieniu właściwych organów oraz podjęciu innych szczególnych czynności zapewniających bezpieczeństwo systemu informatycznego bądź zastosowaniu środków ochrony fizycznej.

5.IOD po zapoznaniu się z opisem zdarzenia, podejmuje – po uzyskaniu akceptacji ze strony Burmistrza – decyzje o ewentualnym powiadomieniu organu nadzorczego oraz,

jeśli to konieczne osoby/osób, których dane dotyczą.

6.Zawiadomienie organu nadzorczego musi nastąpić bez zbędnej zwłoki – w miarę możliwości, nie później jednak niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

7.Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

8.Zgłoszenie do organu nadzorczego musi co najmniej;

a/. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną ilość osób, których dane dotyczą oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,

b/.zawierać imię i nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,

c/.opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

d/.opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

9.Jeżeli informacji o których mowa w pkt.8 lit.c/. nie da się udzielić w tym samym czasie można je udzielić sukcesywnie , bez zbędnej zwłoki.

10. IOD dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja to musi organowi nadzorczemu pozwolić weryfikowanie przestrzegania art. 33 rozporządzenia.

11.Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych IOD we współpracy z ASI bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą o takim naruszeniu. Zawiadomienie to musi zostać sformułowane jasnym i prostym językiem i opisywać charakter naruszenia ochrony danych osobowych oraz zawierać przynajmniej;

a/. imię, nazwisko oraz dane kontaktowe IOD lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,

b/.opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,

c/.opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

12.Zawiadomienie o którym mowa w pkt.11 nie jest wymagane w następujących przypadkach;

a/.administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające osobom nieuprawnionym

do dostępu do tych danych osobowych,

b/.administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą

c/.wymagałoby one niewspółmiernie dużego wysiłku. W takim wypadku zostaje wydany publiczny komunikat lub zostaje zastosowany podobny środek, za pomocą którego osoby, których dane dotyczą zostają poinformowane w równie skuteczny sposób.

13.ASI zobowiązany jest do informowania Burmistrza o awariach systemu informatycznego, zauważalnych przypadkach naruszenia niniejszej procedury przez pracowników, a zwłaszcza o przypadkach posługiwania się przez nich nieautoryzowanymi programami, nieprzestrzegania zasad używania oprogramowania antywirusowego, niewłaściwego wykorzystywania sprzętu komputerowego lub przetwarzania danych w sposób niezgodny z procedurami bezpieczeństwa danych osobowych.

Gromadzenie materiału dowodowego

1.Każdy element materiału dowodowego – dokument papierowy, dokument elektroniczny, kopia zapasowa bazy danych lub plików systemowych i konfiguracyjnych, obraz dysku, dziennik (logów) zdarzeń, dziennik audytu – jest gromadzony i przechowywany w sposób gwarantujący jego poufność, integralność i kompletność.

2.Każdy element materiału dowodowego jest utrwalany z zachowaniem integralności całego procesu przetwarzania, od utworzenia do ewentualnego przedstawienia jako dowodu w postępowaniu sądowym;

a/.dla dokumentu papierowego – oryginał jest bezpiecznie przechowywany wraz z informacją o źródle, czasie i okolicznościach utrwalenia dokumentu,

b/.dla plików utrwalanych na nośnikach komputerowych – sporządzenie kopii zapasowej lub obrazu dysku wraz z udokumentowaniem procesu kopiowania oraz bezpieczne ich przechowywanie.

3.Protokół ze sporządzenia elementu materiału dowodowego lub zabezpieczenia środków przetwarzania informacji jest sporządzany zgodnie ze wzorem zamieszonym w formularzu nr 21.

4.Wszelkie działania w systemie informatycznym, związane z postępowaniem ze zdarzeniem, mogą być prowadzone wyłącznie z wykorzystaniem kopii zapasowych, obrazów dysków, kopii plików konfiguracyjnych i systemowych, rejestrów systemowych i aplikacji, plików dokumentów identycznych ze sporządzonymi uprzednio kopiami przechowywanymi jako materiał dowodowy".

§ 2

W załączniku nr 1 do Zarządzenia nr KR.120.91.2018 z dnia 24 maja 2018r. Burmistrza Woźnik w sprawie wprowadzenia dokumentacji dotyczącej ochrony danych

osobowych w Urzędzie Miejskim w Woźnikach dodaje się po formularzu nr 18 dodaje się formularze nr 19, nr 20 i nr 21".

§ 3

Pozostałe postanowienia Zarządzenia nr KR.120.91.2018 z dnia 24 maja 2018r. Burmistrza Woźnik w sprawie wprowadzenia dokumentacji dotyczącej ochrony danych osobowych w Urzędzie Miejskim w Woźnikach nie ulegają zmianom.

§ 4

Wykonanie Zarządzenia powierza się Inspektorowi ochrony danych (IOD).

§ 5

Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ

Alojzy Cichowski

Formularz nr 19

Instrukcja zgłaszania zdarzeń związanych z naruszeniem ochrony danych osobowych

1.Każdy pracownik w przypadku zaistnienia podejrzenia lub stwierdzenia faktu zagrożenia bezpieczeństwa danych osobowych w obszarze infrastruktury teleinformatycznej, ma obowiązek zgłoszenia naruszenia bezpieczeństwa, używając do tego dostępnych mu w takim przypadku środków.
2.Pracownik zgłasza incydent;
a/. ASI;
- osobiście,
- telefonicznie
- za pośrednictwem e- maila admin@wozniki.pl
b/. IOD;
- telefonicznie
- za pośrednictwem e- maila bip@wozniki.pl
Niezależnie od powyższego należy przedstawić możliwie wyczerpujący opis zdarzenia;
a/. termin/y zdarzenia – data i godzina z podaniem dokładnego czasu,
b/. jeśli występuje i jest znane – cel/e ataku – adres IP/nazwa urządzenia docelowego miejsca ataku, rodzaj narażonej usługi, atakowanego systemu, itp.,
c/.typ zdarzenia (np. spam, złośliwy kod, podszywanie się, wyłudzenie),
d/.opis zdarzenia (obserwacje, spostrzeżenia, uwagi) – opis wykrycia oraz przebiegu incydentu, konsekwencje (rozmiar możliwych do oszacowania szkód), zasięg szkodliwych działań (liczba zaatakowanych systemów), inne źródła (urządzenia/sieci), termin rozpoczęcia, zakończenia i czas trwania ataku (np. czy zdarzenie ma dalej miejsce, itp.),
e/. dowodu zdarzenia (nagłówki pocztowe, kopie ekranu, itp),
f/.w przypadku konieczności zgłoszenia podejrzenia incydentu bezpieczeństwa informatycznego z pominięciem standardowej ścieżki raportowania w sytuacji, gdy ścieżka ta jest nieskuteczna, pracownik upoważniony jest do bezpośredniego kontaktu z Burmistrzem.

BURMISTRZ
Alojzy Cichowski

Formularz nr 20

Ewidencja zdarzeń związanych z naruszeniem ochrony danych osobowych

Data zdarzenia	Nazwa zdarzenia	Kategoria zdarzenia	Rodzaj komponentu, którego dotyczy zdarzenie	Nazwa systemu, którego dotyczy zdarzenie	Środki zaradcze

.....

(podpis ASI)

BURMISTRZ

Alojzy Ci[illegible]owski

Formularz nr 21

Wzór protokołu zabezpieczenia materiału dowodowego

PROTOKÓŁ ZABEZPIECZENIA MATERIAŁU DOWODOWEGO

Sporządzony w dniu ..... o godz..... w obecności;

Świadek
1;.....
Imię, nazwisko, stanowisko, dział

Świadek
2;.....
Imię, nazwisko, stanowisko, dział

Świadek
3;.....
Imię, nazwisko, stanowisko, dział

1.Rodzaj materiału dowodowego

(zaznaczyć właściwe pole i wpisać odpowiednie nazwy i oznaczenia).

Dokument papierowy	Rodzaj i nazwa dokumentu;	
Dokument elektroniczny	Rodzaj i nazwa dokumentu;	
Kopia zapasowa	System operacyjny *Nazwa i wersja systemu*	Aplikacja *Nazwa i wersja aplikacji* .....
Baza danych *nazwa i wersja bazy:*	Oznaczenie nośnika;	
Kopia zawartości Skrzynki pocztowej	Zewnętrzne *Nazwa skrzynki Pocztowej*	Wewnętrzne *za okres do* .....

2.Opis czynności

(opisać kolejne czynności)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

.....
.....

3.Wytwarzany materiał dowodowy

Wykonano kopie materiału dowodowego w 2 egzemplarzach, którym nadano etykiety;

.....egzemplarz nr 1

.....egzemplarz nr 2

4.Zabezpieczenie materiału dowodowego

(opisać sposób zabezpieczenia jednego z egzemplarzy)

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

Protokół sporządził;

.....

Podpisano;

Świadek 1.....

Świadek 2.....

Świadek 3.....

BURMISTRZ

Alojzy [illegible]owski