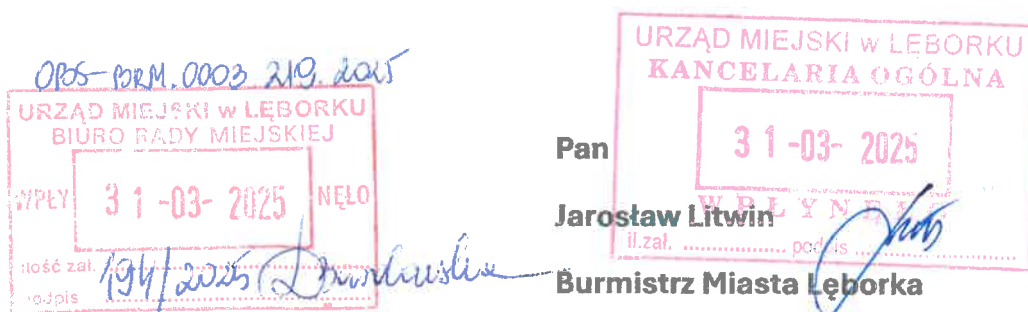


Lębork dnia 31 marca 2025 roku



## ZAPYTANIE

### dotyczące wycieku danych osobowych na stronie BIP Lębork

Według doniesień prasowych w dniu 21.03.2025 roku zamieszczono w BIP Lębork w Zakładce Rada Miejska oraz w zakładce projekty uchwał, projekt uchwały nr.4a. W zakładce Rada Miejska umieszczono 1056 stron uproszczonych wpisów z rejestru gruntów zawierających dane osobowe właścicieli oraz współwłaścicieli obejmujące imiona i nazwiska, imiona rodziców, numer pesel oraz adresy zamieszkania. Natomiast w zakładce projekty uchwał powyższe dokumenty zostały umieszczone w załączniku 1,9,2 pdf. Uproszczone wypisy z rejestru zostały usunięte z BIP w dniu 25.03.2025 roku, co jest skandalem i złamaniem wszelkich procedur oraz może stanowić przestępstwo. W tym przypadku jest mi podwójnie przykro z uwagi, iż zespół kontrolny komisji rewizyjnej w 2022 roku zakończył kontrolę nr. 2 udostępniania informacji publicznej w 2021 roku, która zakończyła się bardzo dużą ilością wniosków, a sam protokół z kontroli liczył ponad 200 stron i opisano w nim całość materii z związanej z tą problematyką, wnioski zostały przyjęte w formie uchwały przez radę miejską, natomiast w dniu 20 grudnia 2024 roku wystąpiłem z interpelacją do Burmistrza Miasta Lęborka o wdrożenie wniosków z kontroli dotyczącej BIP. Jak widać nie przyniosło to żadnego rezultatu. Pojęcie administratora danych zdefiniowane zostało w art. 7 pkt 4 ustawy o ochronie danych osobowych. Zgodnie z tym przepisem jest to organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych. Zgodnie z klauzulą informacyjną dotyczącą przetwarzania danych osobowych i zapisami art. 13 oraz art. 14 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) (Dz. Urz. UE L 119 z dnia 04.05.2016) informujemy, że Administratorem Państwa danych osobowych

przetwarzanych w Urzędzie Miejskim w Lęborku jest Burmistrz Miasta Lęborka. Administrator - Burmistrz Miasta Lęborka wyznaczył inspektora ochrony danych (IOD), W Zarządzeniu nr 19/2022 Burmistrza Miasta Lęborka z dnia 10 lutego 2022 r. , w sprawie wyznaczenia pracowników odpowiedzialnych za przekazywanie ministrowi właściwemu do spraw informatyzacji informacji niezbędnych do zamieszczania na stronie głównej BIP oraz wprowadzanie zmian w treści informacji publicznej udostępnianych na stronie podmiotowej Biuletynu Informacji Publicznej Gminy Miasta Lęborka, na podstawie art. 33 ust. 5 ustawy z dnia 8 marca 1990 roku o samorządzie gminnym (t.j. Dz. U. z 2021 roku poz. 1372 z późn. zm.) oraz § 15 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 roku w sprawie Biuletynu Informacji Publicznej (Dz. U. Nr 10): Wyznacza się na członka Zespołu ds. BIP, odpowiedzialnego za weryfikowanie informacji publicznej przeznaczonej do zamieszczenia na stronie podmiotowej BIP w zakresie ochrony danych osobowych oraz powierza się jej funkcje Koordynatora Zespołu ds. BIP. Koordynator Zespołu ds. BIP, o którym mowa w ust. 1, odpowiedzialny jest za przyjmowanie informacji publicznych, przeznaczonych do zamieszczenia na stronie podmiotowej BIP, od wyznaczonych do tego osób oraz z poszczególnych komórek organizacyjnych Urzędu Miejskiego w Lęborku. Koordynator Zespołu ds. BIP poleca odpowiednim członkom Zespołu ds. BIP weryfikację dostarczonych informacji publicznych w zakresie ochrony informacji niejawnych lub tajemnicy skarbowej, a następnie poleca edytorowi systemu zamieszczenie informacji publicznych na stronie podmiotowej BIP. Zarządzenie Nr 55/2018 Burmistrza Miasta Lęborka z dnia 5 czerwca 2018 r. w sprawie zmiany zarządzenia Nr 68/2014 Burmistrza Miasta Lęborka z dnia 1 lipca 2014 roku w sprawie zasad i trybu postępowania z dokumentami wynikającymi z wykonywania zadań publicznych organów gminy przed ich przekazaniem do wglądu dla mieszkańców . Na podstawie: art. 30 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym t.j. Dz. U. z 2018 r. poz. 994 ze zm. oraz § 71 Statutu Miasta Lęborka, zarządza się, co następuje: § 1. W zarządzeniu Nr 68/2014 Burmistrza Miasta Lęborka z dnia 1 lipca 2014 r. w sprawie zasad i trybu postępowania z dokumentami wynikającymi z wykonywania zadań publicznych organów gminy przed ich przekazaniem do wglądu dla mieszkańców, wprowadza się następujące zmiany: 1) § 1 otrzymuje brzmienie: „§ 1. Biuro Rady Miejskiej przekazuje Inspektorowi Ochrony Danych uwierzytelnione kserokopie protokołów z sesji Rady Miejskiej oraz posiedzeń komisji Rady.”; 2) § 2 otrzymuje brzmienie: „§ 2. Inspektor Ochrony Danych we współpracy z Pełnomocnikiem do spraw ochrony informacji niejawnych i osobą upoważnioną przez Skarbnika Miasta dokonuje sprawdzenia jawności udostępnianych dokumentów, biorąc pod uwagę ustawy ograniczające jawność działania organów gminy, a w szczególności: ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych, Rozporządzenie Parlamentu Europejskiego i Rady UE z dnia 27 kwietnia 2016 r., w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych . Starosta udostępnia informacje zawarte w operacie ewidencyjnym w szczególności w formie: wypisów z rejestrów, kartotek i wykazów tego operatu; wyrysów z mapy

ewidencyjnej; kopii dokumentów uzasadniających wpisy do bazy danych operatu ewidencyjnego, a także plików komputerowych sformatowanych zgodnie z obowiązującym standardem wymiany danych ewidencyjnych. Każdy może żądać udostępnienia informacji zawartych w operacie ewidencyjnym. Jednak starosta udostępnia dane z ewidencji gruntów i budynków w zakresie, w jakim zawierają one dane właścicieli nieruchomości (tzw. dane podmiotowe) oraz wydaje wypisy z operatu ewidencyjnego, zawierające takie dane, tylko na żądanie: właścicieli oraz osób i jednostek organizacyjnych władających gruntami, budynkami lub lokalami, których dotyczy udostępniany zbiór danych lub wypis; organów administracji publicznej; operatorów sieci i systemu przesyłowego, a także innych podmiotów, które mają w tym interes prawny. W celu uzyskania wypisu i /albo wyciągu z ewidencji gruntów i budynków należy złożyć w urzędzie gminy odpowiedni wniosek, sporządzony na urzędowym formularzu. Zgodnie z przepisami ustawy „przetwarzaniem” danych osobowych są jakiegokolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

### **Artykuł 33 – Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu**

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorcemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorcemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

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

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych 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.

4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorcemu weryfikowanie przestrzegania niniejszego artykułu.

#### **Art. 34. Ustawy o ochronie danych osobowych**

1.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

2.

Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w **art. 33** *zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu*.

3.

Zawiadomienie, o którym mowa w ust. 1, 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 odczyt 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 ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

4.

Jeżeli administrator nie zawiadomił jeszcze osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, organ nadzorczy – biorąc pod uwagę prawdopodobieństwo, że to naruszenie ochrony danych osobowych spowoduje wysokie ryzyko – może od niego tego zażądać lub może stwierdzić, że spełniony został jeden z warunków, o których mowa w ust. 3.

Administrator danych powinien zawiadomić o naruszeniu osobę, której dotyczy naruszenie, jeśli stwierdzi, że naruszenie to może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. W tym miejscu, z praktycznego punktu widzenia, warto jedynie dodatkowo odnotować dotychczasowe szczególne podejście UODO

do naruszeń, które dotyczą numeru PESEL. Jeśli naruszenie dotyczy numeru PESEL, można zakładać, że w ocenie UODO będzie ono się zapewne wiązać z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, które powoduje konieczność zawiadomienia o naruszeniu podmiotów danych. Jeśli administrator zgłosi naruszenie do UODO i jednocześnie oceni, że o naruszeniu nie trzeba zawiadomić podmiotów danych, może okazać się, że UODO zakwestionuje taką ocenę i nakaże administratorowi dokonać zawiadomienia (zazwyczaj po uprzednim wezwaniu administratora do okazania dokumentu potwierdzającego dokonanie oceny ryzyka związanego z naruszeniem wraz z informacją o wykorzystanej metodologii oceny). W takiej sytuacji nie można wykluczyć ryzyka, że organ dojdzie do wniosku, że brak zawiadomienia lub nieprawidłowe przeprowadzenie oceny ryzyka związanego z naruszeniem stanowi złamanie przepisów RODO, co może narazić administratora na odpowiedzialność administracyjnoprawną.

*W myśl art. 82 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę (ust. 1). Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. W przypadku rozpowszechniania danych osobowych w sposób bezprawny osobie, której dane udostępniono przysługuje odszkodowanie. Co do zasady odszkodowanie za udostępnienie danych osobowych bez zgody, a tym samym naruszenie RODO należy się zawsze, kiedy do niego dochodzi. Osoby, których dane osobowe zostały nielegalnie ujawnione, mogą mieć prawo do dochodzenia roszczeń odszkodowawczych za poniesione szkody.*

#### 1. Odszkodowanie za straty materialne:

Osoba poszkodowana może domagać się odszkodowania finansowego za poniesione straty materialne wynikające bezpośrednio z nielegalnego ujawnienia danych osobowych. Mogą to być np. koszty poniesione na skutek kradzieży tożsamości, utraty środków pieniężnych z konta bankowego lub koszty związane z koniecznością zmiany dokumentów tożsamości.

#### 2. Odszkodowanie za cierpienie emocjonalne i moralne:

Osoba poszkodowana może dochodzić odszkodowania za cierpienie emocjonalne i moralne wynikające z naruszenia prywatności. Obejmuje to stres, niepokój, utratę poczucia bezpieczeństwa oraz inne negatywne skutki emocjonalne, jakie mogą wynikać z ujawnienia jej danych.

#### 3. Odszkodowanie za utratę reputacji:

Jeśli ujawnienie danych osobowych prowadzi do uszczerbku na reputacji osoby poszkodowanej, ta może domagać się odszkodowania za jej utratę. Obejmuje to negatywne skutki społeczne i zawodowe wynikające z nielegalnego ujawnienia informacji osobistych.

#### 4. Odszkodowanie za naruszenie praw osobistych:

Osoba dotknięta naruszeniem prywatności może dochodzić odszkodowania za naruszenie jej praw osobistych, takich jak prawo do prywatności, godności czy autonomii. Odszkodowanie ma na celu zrehabilitowanie utraconych wartości osobistych i moralnych.

#### 5. Odszkodowanie za poniesione koszty procesowe:

Osoba poszkodowana może również domagać się zwrotu poniesionych kosztów związanych z dochodzeniem roszczeń odszkodowawczych, takich jak koszty zatrudnienia prawnika czy opłaty sądowe.

Rodzaje odszkodowania, na które osoba poszkodowana może mieć prawo, mogą różnić się, w zależności od konkretnych okoliczności oraz od obowiązujących przepisów prawa. Wysokość odszkodowania za ujawnienie danych osobowych nie jest ściśle określona i ustala ją sąd po przeprowadzonym postępowaniu dowodowym. W konsekwencji, wysokość odszkodowania w każdym przypadku jest inna i zależy będzie od poniesionej szkody, która co do zasady stanowi równoznaczność odszkodowania. Dodatkowo oprócz odszkodowania, osoba, której dane osobowe bezprawnie ujawniono i po jej stronie powstała szkoda niemajątkowa, może domagać się zadośćuczynienia. Zgodnie z zasadą rozliczalności, o której mowa w art. 5 ust. 2 RODO, na administratorze (lub na podmiocie przetwarzającym) ciąży obowiązek wykazania zgodności przetwarzania danych z przepisami RODO lub konieczność wykazania, że nie ponosi on winy za wyrządzoną szkodę. Kluczowa, z punktu widzenia RODO, zasada rozliczalności jest faktycznie przeciwieństwem zasady domniemania niewinności, wynikającym z art. 5 § 1 kodeksu karnego (dalej kk). W zakresie odpowiedzialności karnej za niezgodne z prawem przetwarzanie danych osobowych nie pozostaje ona jednak bez wpływu na ewentualną odpowiedzialność karną sprawcy naruszenia. Zasada rozliczalności pomaga również wykazać umyślność popełnienia przestępstwa, szczególnie jeżeli sprawca działał w zamiarze ewentualnym.

Jak już wcześniej wspomniałem nielegalne przetwarzanie danych osobowych może wiązać się z dokonaniem przestępstwa i tak zgodnie z **Art. 304. § 2 kpk**. Instytucje państwowe i samorządowe, które w związku ze swą działalnością dowiedziały się o popełnieniu przestępstwa ściganego z urzędu, są obowiązane niezwłocznie zawiadomić o tym prokuratora lub Policję oraz przedsięwziąć niezbędne czynności do czasu przybycia organu powołanego do ścigania przestępstw lub do czasu wydania przez ten organ stosownego zarządzenia, aby nie dopuścić do zatarcia śladów i dowodów przestępstwa.

Obowiązujący kodeks karny w art. **115 § 13** postanawia, że „Funkcjonariuszem publicznym jest: 1) Prezydent Rzeczypospolitej Polskiej, 2) poseł, senator, radny, 2a) poseł do Parlamentu Europejskiego, 3) sędzia, ławnik, prokurator, funkcjonariusz finansowego organu postępowania przygotowawczego lub organu nadrzędnego nad finansowym

organem postępowania przygotowawczego, notariusz, komornik, kurator sądowy, syndyk, nadzorca sądowy i zarządca, osoba orzekająca w organach dyscyplinarnych działających na podstawie ustawy, 4) osoba będąca pracownikiem administracji rządowej, innego organu państwowego lub **samorządu terytorialnego**, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wydawania decyzji administracyjnych, 5) osoba będąca pracownikiem organu kontroli państwowej lub organu kontroli samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, 6) osoba zajmująca kierownicze stanowisko w innej instytucji państwowej, 7) funkcjonariusz organu powołanego do ochrony bezpieczeństwa publicznego albo funkcjonariusz Służby Więziennej, 8) osoba pełniąca czynną służbę wojskową . Reasumując powyższy przepis każdy z pracowników samorządowych zatrudnionych na stanowiskach urzędniczych może być zaliczany do funkcjonariuszy publicznych . Natomiast nie można zaliczyć do tego katalogu osób zatrudnionych na stanowiskach pomocniczych i obsługi .Według Wojewódzkiego Sadu Administracyjnego nawet wąski zakres kompetencji decyzyjnej to przesłanka o tym , że pracownik administracji samorządowej staje się funkcjonariuszem publicznym

#### **Art. 231. KK**

##### § 1.

Funkcjonariusz publiczny, który, przekraczając swoje uprawnienia lub nie dopełniając obowiązków, działa na szkodę interesu publicznego lub prywatnego, podlega karze pozbawienia wolności do lat 3.

##### § 2.

Jeżeli sprawca dopuszcza się czynu określonego w § 1 w celu osiągnięcia korzyści majątkowej lub osobistej, podlega karze pozbawienia wolności od roku do lat 10.

##### § 3.

Jeżeli sprawca czynu określonego w § 1 działa **nieumyślnie** i wyrządza istotną szkodę, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

##### § 4.

Przepisu § 2 nie stosuje się, jeżeli czyn wyczerpuje znamiona czynu zabronionego określonego w **art. 228 sprzedajność pełniącego funkcję publiczną**.

#### **Art. 107. Ustawy o ochronie danych osobowych**

##### §1.

Kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

Czynnością sprawczą jest więc samo przetwarzanie danych, niezależnie od tego, czy dla osoby, której takie dane dotyczą, wiąże się to z jakimikolwiek niekorzystnymi skutkami (przestępstwo formalne, bez skutkowe). Możliwe jest nawet, że osoba, której dane dotyczą, nie wie o tym, że jej dane są przetwarzane przez określoną osobę/określony podmiot pomimo braku podstawy prawnej albo przetwarzane są przez osobę, która nie legitymuje się właściwym upoważnieniem.

**Zastosowana sankcja finansowa jest wysoka, bowiem limit kar za naruszenie RODO dla organów administracji samorządowej wynosi 100.000 zł**

**W związku z przedstawionym materiałem proszę o udzielenie odpowiedzi na poszczególne pytania :**

- kto wydał polecenie wprowadzenia uproszczonych wpisów rejestru gruntów wraz z danymi osobowymi do BIP,
- kto podejmował w tej sprawie jakiegokolwiek decyzje i na jakiej podstawie prawnej , czy posiadał takie umocowanie zgodnie z zakresem swoich obowiązków służbowych
- czy projekt uchwały przed wprowadzeniem do BIP wraz z załącznikami został sprawdzony przez zespół radców prawnych ,
- kto podpisał się pod projektem wraz z załącznikami ,
- czy projekt przed wprowadzeniem do BIP w jakikolwiek sposób był sprawdzany i kto posiada taki obowiązek służbowy ,  
pod kątem ochrony danych osobowych
- kto podejmuje decyzje o anonimizacji dokumentów i dlaczego tego nie zrobiono , jakie obowiązują procedury w tym zakresie ,
- jakie podjęto kroki w związku ze złożoną interpelacją w tej sprawie
- czy zostali zapoznani z protokołem kontroli oraz wnioskami z kontroli pracownicy Urzędu Miasta Lęborka , jakie w związku z tym wprowadzono zmiany
- czy projekt uchwały zgodnie z obowiązującymi przepisami był sprawdzony przez członka Zespołu ds. BIP, odpowiedzialnego za weryfikowanie informacji publicznej przeznaczonej do zamieszczenia na stronie podmiotowej BIP w zakresie ochrony danych osobowych tj. Koordynatora Zespołu ds. BIP. Koordynator Zespołu ds. BIP, o którym mowa w ust. 1, odpowiedzialny jest za przyjmowanie informacji publicznych, przeznaczonych do zamieszczenia na stronie podmiotowej BIP
- czy z projektem uchwały zapoznawał się Inspektor Ochrony Danych Osobowych pod kątem ochrony danych osobowych , i jakie obowiązują w tym zakresie procedury ,



- czy powiadomiono Prezesa UODO i po jakim czasie ,
- dlaczego ograniczono się tylko do ogłoszenia na stronie Urzędu Miasta informacji o wycieku danych a nie wysłano odrębnych pism do każdej osoby której nielegalnie ujawniono dane w praktyce ujawnienie numeru pesel Prezes UODO traktuje jako wysokie naruszenie prawa ,
- kto pokryje koszty nałożonych kar przez Prezesa UODO oraz odszkodowań cywilnych - **chyba nie mieszkańcy czyli podatnicy,**
- jakie są możliwości prawne dochodzenia roszczeń finansowych w ramach regresu od urzędników odpowiedzialnych za wyciek danych osobowych ,
- jakie wszczęto dotychczas postępowania dyscyplinarne w związku z zaistniałą sytuacją
- czy o tym fakcie zostały powiadomione organy ścigania w związku z uzasadnionym podejrzeniem popełnienia przestępstwa z art.231 par. 1 KK , art.107 ustawy o ochronie danych osobowych , prezes UODO nie posiada kompetencji do prowadzenia postępowań przygotowawczych , a burmistrz na podstawie art.304 par.2 kpk ma obowiązek prawny do powiadomienia o możliwości popełnienia przestępstwa . Tylko Policja i Prokuratora posiadają kompetencje do wyjaśnienia czy przestępstwo zaistniało czy nie .
- czy z zakresu udostępniania informacji publicznej kiedykolwiek w Urzędzie Miasta w Lęborku były prowadzone szkolenia ,
- jakie podjęto działania żeby w przyszłości nie dopuścić do zaistniałej sytuacji
- proszę o przekazanie kserokopii zgłoszenia naruszenia danych osobowych jakie wysłano do UODO

**z poważaniem**

Krzysztof Świętczak

**Wykonano w 2 egzemplarzach**

Egz. Nr. 1 – adresat

Egz. Nr. 2 – a/a