

Zarządzenie nr 3/2025
Starosty Sokołowskiego
z dnia 24 stycznia 2025 r.

zmieniające zarządzenie w sprawie dokumentacji z zakresu ochrony danych osobowych
w Starostwie Powiatowym w Sokołowie Podlaskim

Na podstawie art. 34 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2024 r. poz. 107 ze zm.) oraz art. 24 ust. 1 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. 2016.119.1) zarządzam, co następuje:

§1

W Polityce Bezpieczeństwa Przetwarzania Danych Osobowych w Starostwie Powiatowym w Sokołowie Podlaskim stanowiącej załącznik do zarządzenia Nr 42/2020 Starosty Sokołowskiego z dnia 7 września 2020 r. wprowadza się następujące zmiany:

- 1) w rozdziale 6 ust. 6.1 pkt 1 otrzymuje brzmienie:
„1. Obszarem przetwarzania danych osobowych w Starostwie Powiatowym w Sokołowie Podlaskim są pomieszczenia biurowe, w których odbywa się praca na danych osobowych, miejsca przechowywania nośników informacji zawierających dane osobowe oraz pomieszczenia, w których znajduje się sprzęt służący do ich przetwarzania zlokalizowane w dwóch budynkach Starostwa Powiatowego w Sokołowie Podlaskim znajdujących się pod adresem: 08-300 Sokołów Podlaski, ul. Wolności 23 oraz 08-300 Sokołów Podlaski, ul. Armii Krajowej 4.”;
- 2) w rozdziale 6 ust. 6.2.3. otrzymuje brzmienie:
„1. W Starostwie Powiatowym w Sokołowie Podlaskim został zainstalowany monitoring wizyjny obejmujący teren wokół budynku znajdującego się pod adresem: ul. Wolności 23, 08-300 Sokołów Podlaski oraz ul. Armii Krajowej 4, 08-300 Sokołów Podlaski.
2. Celem zastosowania monitoringu wizyjnego w Starostwie Powiatowym w Sokołowie Podlaskim jest zapewnienie bezpieczeństwa oraz ochrona mienia.
3. System monitoringu wizyjnego obejmuje w szczególności: kamery, rejestrator, okablowanie i oprogramowanie monitoringu, a ponadto stanowisko umożliwiające podgląd obrazu z kamer.
4. Monitoring funkcjonuje całodobowo.
5. Rejestracji i zapisowi na nośniku danych podlega tylko obraz z kamer systemu monitoringu wizyjnego, bez rejestracji dźwięku. Rejestrator będący częścią monitoringu znajduje się w serwerowni.
6. Dane pochodzące z nagrań umożliwiające identyfikację osoby, zarejestrowane i przechowywane uważane są za dane osobowe, w rozumieniu art. 4 pkt 1 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. Rejestracja obrazu zdarzeń, prowadzona jest z poszanowaniem godności człowieka.
7. Nagrania obrazu przetwarzane są wyłącznie do celów, dla których zostały zebrane i przechowywane są przez okres nie dłuższy niż 30 dni – do nadpisania danych. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub Administrator powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin ten ulega przedłużeniu do czasu

- prawomocnego zakończenia postępowania.
8. Obszar objęty monitoringiem został oznaczony za pomocą piktogramu z symbolem kamery. Obowiązek informacyjny został wypełniony poprzez zamieszczenie klauzuli informacyjnej dotyczącej przetwarzania danych osobowych.
 9. Przeglądanie i kopiowanie materiału archiwalnego odbywa się na prośbę organu prowadzącego czynności służbowe w danej sprawie oraz w uzasadnionych przypadkach osoby fizycznej będącej obiektem zdarzenia zarejestrowanego przez monitoring wizyjny, po uprzednim złożeniu do Administratora pisemnego wniosku.
 10. Udostępnienie następuje po wyrażeniu zgody przez Starostę lub Wicestarostę.
 11. Dane zapisane na nośnikach nie stanowią informacji publicznej i nie podlegają udostępnieniu w oparciu o przepisy ustawy o dostępie do informacji publicznej.”,
- 3) w rozdziale 6 ust. 6.2.9 pkt 1 otrzymuje brzmienie:
- „1. Na podstawie umowy outsourcingowej zawartej z firmą „Advocatus” Doradztwo Prawne Paulina Skrouba, został wyznaczony Inspektor Ochrony Danych – Pani Paulina Skrouba.”,
- 4) w rozdziale 6 ust. 6.2.9 pkt 10 i 11 otrzymują brzmienie:
- „10. Funkcję Administratora Systemów Informatycznych Starostwa Powiatowego w Sokołowie Podlaskim pełni informatyk, który jest zatrudniony na pełen etat. ASI wykonuje prace związane z konfiguracją sieci, systemów operacyjnych, programów narzędziowych, wykonywaniem kopii zapasowych oraz prace związane z konfiguracją systemów dziedzinowych, za wyjątkiem programów dziedzinowych administrowanych przez firmy zewnętrzne.
11. Serwisantami systemów dziedzinowych w Starostwie Powiatowym w Sokołowie Podlaskim są firmy:
- 1) QNT Systemy Informatyczne Sp. z o.o., ul. Knurowska 19, 41-800 Zabrze,
 - 2) INKOM Komputery, Oprogramowanie, ul. Skłodowskiej- Curie 12, 08-300 Sokołów Podlaski,
 - 3) GEOBID Sp. Z o.o., ul. Kossutha 11, 40-844 Katowice,
 - 4) Nefeni Sp. z o.o. z siedzibą w Poznaniu, przy ulicy Głogowskiej 216, 60-104 Poznań,
 - 5) MWC Sp. z o.o. z siedzibą w Poznaniu przy ul. Kowalewickiej 12.”,

5) w rozdziale 6 ust. 6.2.10 otrzymuje oznaczenie 6.2.13,

6) w rozdziale 6 po ust. 6.2.9. dodaje się ust. 6.2.10 - 6.2.12 w brzmieniu:

„ 6.2.10 Zasady korzystania z portali internetowych oraz poczty elektronicznej

1. Na służbowych komputerach, a także na innych urządzeniach dopuszczonych do pracy w sieci teleinformatycznej Administrator, zabrania się korzystania ze stron internetowych do celów prywatnych, w tym do korzystania z portali społecznościowych i rozrywkowych.
2. Administrator zapewnia dostęp do kont poczty elektronicznej w domenie, którą zarządza lub u dostawcy usług, który zapewnia możliwość zawarcia umowy powierzenia przetwarzania danych.
3. Niedopuszczalne jest:
 - 1) rejestrowanie kont służących realizacji zadań w publicznie dostępnych domenach;
 - 2) wykorzystywanie do celów służbowych prywatnych kont poczty elektronicznej osób upoważnionych;
 - 3) wykorzystywanie do celów prywatnych służbowych kont poczty elektronicznej osób upoważnionych.

4. Osoba upoważniona odpowiedzialna jest za korzystanie z poczty elektronicznej, w tym każdorazowe weryfikowanie nadawcy i nieotwieranie załączników pochodzących z nieznanego źródła.
5. W przypadku przesyłania drogą mailową, pomiędzy osobami upoważnionymi lub przesyłanie odbiorcom danych, danych osobowych konieczne jest ich skompresowanie i zaszyfrowanie zaufanym oprogramowaniem i nadanie skompresowanemu plikowi bezpiecznego hasła (hasło nie krótsze niż 8 znaków, które zawiera małe i wielkie litery, cyfry i znaki specjalne). Hasło powinno zostać przekazane adresatowi innym środkiem komunikacji niż droga mailowa.

6.2.11. Zasady prowadzenia podmiotowej strony Biuletynu Informacji Publicznej Starostwa Powiatowego w Sokolowie Podlaskim

1. Za prowadzenie strony BIP odpowiada redaktor, który został wyznaczony przez Administratora.
2. Informacja publiczna na stronach BIP pochodzi bezpośrednio od użytkowników, którzy odpowiadają za przygotowanie i sprawdzenie informacji przekazanej do zamieszczenia na stronie BIP.
3. Użytkownik sporządzający dokumenty, które mają zostać umieszczone w Biuletynie Informacji Publicznej zobowiązany jest do wstępnej oceny przedmiotowego dokumentu pod względem dopuszczalności publikacji danych osobowych osób fizycznych niepełniących funkcji publicznych lub kierowniczych.
4. W sytuacji stwierdzenia obecności danych osobowych osób fizycznych w dokumentach, które mają być przekazane do publikacji w BIP, pracownik zobowiązany jest do dokonania analizy legalności publikacji danych osobowych, a jeśli przepisy prawa na to nie pozwalają, do dokonania anonimizacji zawartych w nich danych osobowych osób fizycznych, tj. imion, nazwisk, adresu, nr PESEL, wieku, numeru telefonu, stanu zdrowia itp.
5. Publikowanie informacji na stronie BIP następuje w drodze wprowadzenia przez redaktora informacji do właściwych formularzy dostępnych w panelu administracyjnym, zapisaniu ich w bazie danych systemu.
6. Czas wyświetlania informacji na stronie BIP (czas jej aktualności) powinien być zgodny z okresami zawartymi w niniejszym rozdziale. Jeśli czas aktualności informacji zawierających dane osobowe nie został wskazany organizacja stosuje przepisy obowiązującej Instrukcji kancelaryjnej.
7. Dane osobowe najwyższego kierownictwa, osób wchodzących w skład Rady Powiatu, kierowników jednostek organizacyjnych, członków poszczególnych komisji, informacje o pracownikach Starostwa przechowywane są przez okres pełnienia funkcji lub przez czas zatrudnienia.
8. Oświadczenia majątkowe osób zobowiązanych do ich złożenia upubliczniane są w Biuletynie Informacji Publicznej przez okres 6 lat licząc od końca roku kalendarzowego, w którym zostały one złożone.
9. Zarządzenia Starosty, uchwały Rady Powiatu, statut, regulaminy umieszczone są w Biuletynie Informacji Publicznej bezterminowo.
10. Protokoły z sesji Rady Powiatu, zaproszenia na sesje Rady Powiatu publikowane są w BIP-ie przez czas trwania kadencji.
11. Informacje dot. wyników naboru na wolne stanowiska pracy przechowywane są przez okres 3 lat, od końca roku kalendarzowego, w którym dane te zostały udostępnione.

12. Redaktor zobowiązany jest do dokonywania przeglądu informacji zawartych w BIP w celu weryfikacji ich aktualności.

6.2.13 Zasady nagrywania i transmisji sesji Rady Powiatu

1. W celu wypełnienia obowiązków wynikających z przepisów prawa obrady Rady Powiatu są transmitowane i utrwalane za pomocą urządzeń rejestrujących obraz i dźwięk.
2. Nagrania są udostępnione w Biuletynie Informacji Publicznej, na stronie internetowej, a także na wyodrębnionym kanale na portalu eSesja.tv.
3. Przetwarzanie danych osobowych podczas sesji Rady Powiatu Sokołowskiego odbywa się zgodnie z zasadą minimalizacji danych wynikającą z art. 5 ust. 1 lit c RODO oraz poszanowaniem prywatności osób fizycznych. Pozyskiwane podczas transmisji dane powinny być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.
4. W przypadku konieczności przetwarzania w ramach prac organów danych osobowych należących do szczególnych kategorii, tj. np. dotyczących stanu zdrowia lub danych o karalności, sprawy takie rozpatrywane są na posiedzeniach kolegialnych organów pomocniczych, chyba że obowiązek ich rozpatrywania podczas sesji Rady Miejskiej wynika z przepisów prawa.
5. Przewodniczący Rady Powiatu planując przebieg obrad powinien ocenić, czy informacje i tematyka obrad będą wymagały ujawnienia danych osobowych osób fizycznych ze szczególnym uwzględnieniem kategorii danych wskazanych w art. 9 i 10 RODO.
6. Podczas planowania sposobu transmitowania obrad Rady Powiatu należy uwzględnić odpowiednie ustawienie kamer, tak aby obejmowały one swoim zasięgiem przede wszystkim osoby publiczne lub osoby realizujące zadania publiczne biorące udział w obradach. Zminimalizowanie zakresu danych pozyskiwanych w związku z transmisją dokonywane jest także poprzez jej wstrzymanie w przerwach obrad.
7. Ze względu na specyfikę przetwarzania danych w ramach transmisji i udostępniania nagrań z posiedzeń rady powiatu, osoby w nich uczestniczące, przed rozpoczęciem tych obrad powinny zostać poinformowane o samym fakcie i miejscu trwania transmisji wraz ze wskazaniem okresu przechowywania znajdujących się w nagraniach danych osobowych.
8. W przypadku danych osobowych zarówno zwykłych, szczególnej kategorii wskazanych w art. 9 oraz danych określonych w art. 10 RODO, Administrator, przed publikacją nagrania w sieci (pamiętając o zachowaniu oryginału nagrania jako dokumentu podlegającego archiwizacji), powinien dokonać oceny niezbędności ich ujawnienia z punktu widzenia celu informacyjnego, któremu ta informacja ma służyć.
9. W razie konieczności dokonuje się anonimizacji danych zgodnie z zasadą minimalizacji wskazaną w art. 5 ust 1 lit. c RODO.
10. Administrator realizując zasadę integralności i poufności wskazaną w art. 5 ust 1 lit. f RODO zapewnia bezpieczeństwo znajdujących się na nagraniach danych osobowych celem wyeliminowania ryzyka nieuprawnionej ingerencji w ich treść, ich zmiany czy nawet zamiany całego pliku.
11. Administrator danych w przypadku korzystania z usług podmiotów zewnętrznych przy nagrywaniu obrad sesji Rady Powiatu zawiera z nimi umowę powierzenia przetwarzania danych, o której mowa w art. 28 RODO.”,

7) w rozdziale 7 ust. 7.7. otrzymuje brzmienie:

7.7. „Procedura Zarządzania Incydentami (PZI)

7.7.1. Cel i zakres stosowania Procedury Zarządzania Incydentami

1. Procedura Zarządzania Incydentami określa procedurę identyfikacji naruszenia lub uchybienia, które spowodowało bądź mogło spowodować ingerencję w prawa podstawowe osób fizycznych w związku z przetwarzaniem ich danych osobowych. Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji oraz cyberbezpieczeństwem ma na celu zapewnienie ciągłości operacyjnej oraz ograniczenie wpływu przypadków naruszeń bezpieczeństwa zasobów informacyjnych na działalność organizacji.
2. PZI jest stworzona w celu monitorowania procesów związanych z koniecznością zapewnienia bezpieczeństwa informacji.
3. Aby metoda monitorowania Systemu Zarządzania Bezpieczeństwem Informacji poprzez notyfikację incydentów była skuteczna, należy określić: kiedy należy monitorować, kto powinien to robić, kiedy należy analizować zidentyfikowane naruszenia lub uchybienia oraz kto powinien to analizować.
4. Inspektor Ochrony Danych oraz Administrator Systemu Informatycznego:
 - 1) na bieżąco monitoruje, czy w organizacji doszło do uchybienia lub naruszenia i podejmuje w związku z tym określone stosownymi procedurami czynności,
 - 2) cyklicznie, jednak nie rzadziej niż raz na rok, Inspektor Ochrony Danych analizuje zidentyfikowane naruszenia bądź uchybienia, ocenia je pod względem istotności w zakresie bezpieczeństwa informacji, wyciąga wnioski, a także podejmuje działania naprawcze względem zidentyfikowanych incydentów,
 - 3) przeprowadza audyt doraźny, jeśli uzna to za stosowne,
 - 4) podejmuje decyzje w zakresie kwalifikacji incydentu jako zdarzenia, którego wystąpienie skutkuje koniecznością zgłoszenia tego faktu do organu nadzorczego lub CSIRT NASK lub jako zdarzenia, którego wystąpienie nie spowoduje konieczności zgłoszenia,
 - 5) podejmuje decyzje w zakresie kwalifikacji incydentu jako zdarzenia, którego wystąpienie skutkuje koniecznością zawiadomienia osób, których dane dotyczą o fakcie ich naruszenia lub jako zdarzenia, które takich skutków nie wywoła,
 - 6) o każdej kwalifikacji incydentu Inspektor Ochrony Danych oraz Administrator Systemu Informatycznego zawiadamia Administratora, a także informuje Administratora na bieżąco w zakresie prowadzonej przez siebie PZI.
5. Zakres PZI opiewa o procedurę:
 - 1) reagowania na incydenty,
 - 2) zgłoszenia naruszenia ochrony danych osobowych organowi nadzorzemu,
 - 3) zgłoszenia incydentu do CSIRT NASK,
 - 4) zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.
6. Każdy pracownik Starostwa Powiatowego w Sokołowie Podlaskim jest zobowiązany do zgłoszenia swojego podejrzenia bezpośredniemu przełożonemu, który niezwłocznie informuje drogą e-mail lub telefoniczną Inspektora Ochrony Danych lub Administratora Systemu Informatycznego, w przypadku jego braku, Staroście, Wicestaroście lub Sekretarzowi.
7. Względem pracownika, który nie podejmuje czynności, o których mowa w ust. 6 powyżej i bagatelizuje zdarzenie, co do którego można mieć podejrzenie, iż wystąpił incydent, może zostać zastosowane postępowanie dyscyplinarne w trybie art. 52 ustawy z dnia 26 czerwca 1974 r. kodeks pracy.

8. W przypadku zidentyfikowania incydentu w formie uchybienia bądź naruszenia, Inspektor Ochrony Danych sporządza „Protokół uchybienia/naruszenia”.

7.7.2. Kategorie incydentów:

1. Incydent bezpieczeństwa informacji oraz cyberbezpieczeństwa to zdarzenie, którego skutkiem jest lub może być naruszenie bezpieczeństwa aktywów informacyjnych oraz który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny. Jego przyczyną może być:
 - 1) zdarzenie losowe zewnętrzne (np. klęski żywiołowe, pożary, zakłócenia w dostawie energii elektrycznej itp.), którego wystąpienie może spowodować zniszczenie lub uszkodzenie infrastruktury informatycznej albo dokumentacji papierowej oraz zakłócenie ciągłości pracy systemów nie powodując naruszenia poufności danych;
 - 2) zdarzenie losowe wewnętrzne (np. błędy w oprogramowaniu, awarie sprzętu itp.), które mogą powodować zakłócenia ciągłości pracy systemów a także prowadzić do zniszczenia lub utraty danych;
 - 3) świadome i celowe działania mające na celu naruszenie poufności zasobów informacyjnych, w tym poufności danych.
2. Incydentami bezpieczeństwa informacji w szczególności są:
 - 1) naruszenie poufności, to jest ujawnienie informacji niepowołanym osobom;
 - 2) naruszenie integralności, to jest zniszczenie, uszkodzenie lub przekłamanie informacji;
 - 3) naruszenie dostępności, to jest braku dostępu do danych przez uprawnionych użytkowników.
3. Przyczyny incydentów bezpieczeństwa informacji oraz cyberbezpieczeństwa mogą dotyczyć:
 - 1) niewłaściwego wykorzystywania zasobów informatycznych lub niewłaściwe postępowanie z dokumentacją papierową;
 - 2) działania szkodliwego oprogramowania;
 - 3) próby omijania systemów zabezpieczeń;
 - 4) nieautoryzowanego dostępu do systemów, aplikacji i dokumentów;
 - 5) zniszczenia lub kradzieży urządzeń wykorzystywanych do przetwarzania i przechowywania informacji;
 - 6) zniszczenia lub kradzieży nośników danych;
 - 7) próby wyłudzeń informacji;
 - 8) ataków socjotechnicznych, ataków z wykorzystaniem technik zagrażających poufności, integralności lub dostępności informacji;
 - 9) nieprawidłowości w zakresie zabezpieczenia przechowywania danych, w tym danych osobowych;
 - 10) naruszenia zasad obowiązujących w organizacji dotyczących bezpieczeństwa informacji, w tym danych osobowych.

7.7.3. Procedura zgłaszania naruszenia ochrony danych osobowych organowi nadzorcemu:

1. Jeśli w Starostwie Powiatowym w Sokołowie Podlaskim zostanie zidentyfikowane zdarzenie, które spowoduje naruszenie ochrony danych osobowych, Administrator jest w obowiązku zgłosić ten fakt organowi nadzorcemu w terminie 72 godzin, chyba, że jest

mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

2. Zgłoszenie, o którym mowa w ust. 1 powyżej opisuje co najmniej: charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie; imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji; możliwe konsekwencje naruszenia ochrony danych osobowych; 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.
3. Administrator oraz Inspektor Ochrony Danych jest w obowiązku dokumentować cały przebieg podejmowanych czynności począwszy od notyfikacji naruszenia po zgłoszenie tego faktu do organu nadzorczego.
4. W celu zgłoszenia naruszenia Administrator korzysta ze wzoru udostępnionego przez Urząd Ochrony danych Osobowych tj.: „Zgłoszenie naruszenia ochrony danych osobowych”.
5. Administrator Danych prowadzi Rejestr naruszeń ochrony danych – Załącznik nr 11.

7.7.4. Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych:

1. Jeżeli w Starostwie Powiatowym w Sokołowie Podlaskim dojdzie do naruszenia ochrony danych osobowych i zdarzenie to może spowodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, Administrator powiadamia o tym fakcie te osoby.
2. Administrator informuje osoby fizyczne, których naruszenie dotyczy mając jednocześnie na uwadze zasadę przejrzystości – komunikat powinien być jasny, prosty, zrozumiały dla jego odbiorców.
3. Komunikat zawiera:
 - 1) oznaczenie Administratora uwzględniając dane kontaktowe,
 - 2) opis konsekwencji, jakie naruszenie mogło spowodować,
 - 3) działania zaradcze, jakie Administrator podejmie w związku z incydem.
4. Komunikat, o którym mowa powyżej nie będzie konieczny, jeśli:
 - 1) Administrator wdrożył i zastosował takie środki techniczne i organizacyjne względem danych osobowych, których dotyczy naruszenie, że dostęp osób nieuprawnionych jest niemożliwy np.: szyfrowanie,
 - 2) Administrator zastosował również środki eliminujące prawdopodobieństwo wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
 - 3) Wymaga niewspółmiernie dużego wysiłku po stronie Administratora – wtedy Administrator wydaje komunikat publiczny lub stosuje inny równie skuteczny środek, za pomocą którego osoby zostaną w sposób skuteczny poinformowane o fakcie zaistnienia incydentu.

7.7.5. Procedura zgłoszenia incydentu związanego z bezpieczeństwem informacji oraz cyberbezpieczeństwem:

1. Jeśli w organizacji zostanie zidentyfikowany incydent, który ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo Starostwa Powiatowego w Sokołowie

Podlaskim, Administrator za pośrednictwem wyznaczonej osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa ma obowiązek zgłosić incydent niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do CSIRT NASK.

2. Zgłoszenia do CSIRT NASK przekazywane są w sposób elektroniczny. Procedura zgłoszeń opisana jest pod adresem internetowym <https://incydent.cert.pl> . W przypadku braku możliwości przekazania go w sposób elektroniczny można zgłaszać przy użyciu innych dostępnych środków komunikacji (np. na numer telefonu (22) 380 82 74).
3. W zgłoszeniu przekazuje się informacje zgodnie z formularzem oraz zgodnie z treścią art. 23 ust. 1 Ustawy o krajowym systemie cyberbezpieczeństwa z dnia 05 lipca 2018 r.
4. Zgłoszenie incydentu rejestrowane jest przez Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego oraz odnotowywane w dokumentacji.
5. Osoba zgłaszająca incydent powinna w miarę możliwości zabezpieczyć materiał dowodowy (np. zrzut ekranu monitora, zdjęcie niezabezpieczonych materiałów zawierających dane osobowe itp.).
6. Działania związane z obsługą zdarzenia w pierwszej kolejności dotyczą rozpoznania i kwalifikacji zgłoszenia. W przypadku, kiedy zgłoszenie zakwalifikowane zostało jako incydent bezpieczeństwa informacji lub cyberbezpieczeństwa, dokonywana jest jego ocena istotności.
7. Powyższe działania wykonuje Inspektor Ochrony Danych w porozumieniu z Administratorem Systemu Informatycznego.
8. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:
 - 1) powstałe szkody będące wynikiem incydentu;
 - 2) wpływ incydentu na działanie systemów;
 - 3) wpływ incydentu na ciągłość działania Starostwa Powiatowego w Sokołowie Podlaskim;
 - 4) koszty usunięcia skutków incydentu;
 - 5) szacowany czas naprawy skutków wywołanych incydemtem;
 - 6) oszacowanie zasobów koniecznych do przywrócenia ciągłości działania systemów.
9. Zakwalifikowanie zgłoszenia incydentu jako „fałszywy alarm” kończy postępowanie, o czym Inspektor Ochrony Danych informuje zgłaszającego.
10. W przypadku zakwalifikowania zdarzenia jako incydentu związanego z bezpieczeństwem informacji lub cyberbezpieczeństwem, Inspektor Ochrony Danych wspólnie z Administratorem Systemu Informatycznego podejmuje działania zabezpieczające i naprawcze zmierzające do zniwelowania szkód powstałych w wyniku incydentu.
11. Poinformowany o wynikach analizy incydentu oraz podjętych działaniach naprawczych Inspektor Ochrony Danych informuje Administratora.
12. W przypadku stwierdzenia działań zamierzonych, przy jednoczesnym zidentyfikowaniu sprawcy incydentu dotyczącego naruszenia bezpieczeństwa informacji oraz cyberbezpieczeństwa Administrator podejmuje decyzję dotyczącą wyciągnięcia ewentualnych konsekwencji dyscyplinarnych wobec sprawcy incydentu. Jednocześnie, w zależności od wagi incydentu mogą być powiadomione organy ścigania.”

§2

Zobowiązuje się wszystkich Kierowników Wydziałów i pozostałych pracowników Starostwa do zapoznania się z niniejszym zarządzeniem

§3

Wykonanie zarządzenia powierza się Sekretarzowi Powiatu i Kierownikowi Wydziału Organizacyjnego.

§4

Zarządzenie wchodzi w życie z dniem podpisania.

STAROSTA SOKOŁOWSKI

/-/ ADAM GÓRAL