FORMULARZ ZGŁOSZENIA INCYDENTU PRZEZ DOSTAWCĘ USŁUG ZAUFANIA

INFORMACJE O INCDENCIE:

Data wystąpienia:			Czas trwania (godz.)	Czy w ocenie dostawcy usług zaufania incydent wymaga notyfikowania w ramach art. 19 eIDAS	**T** □ **N** □ **Opinia nadzoru:**	Czy w ocenie dostawcy usług zaufania incydent wymaga poinformowania opinii publicznej.	**T** □ **N** □ **Opinia nadzoru:**
Dzień	Miesiąc	Rok					

Nazwa usługi/usług zaufania objętych incydentem:	Klasyfikacja wpływu: Ciężar incydentu (skala 1-5): ….. Wpływ na aktywa dostawcy: □ – niski □ – średni □ – wysoki
Ogólny opis incydentu: Szczegółowy opis przyczyn: Szkody po stronie dostawcy usług zaufania:	Na co wpłynął incydent? □ – poufność □ – integralność □ – dostępność Przyczyny incydentu: □ – błąd ludzki □ – awaria systemu □ – zdarzenie naturalne □ – czyn przestępczy □ – dysfunkcje podmiotów trzecich
Czy incydent: □ – dotyczy danych osobowych □ – dotyczy bezpieczeństwa sieci teleinformatycznych □ – dotyczy bezpieczeństwa przetwarzania informacji niejawnych □ – posiada skutki transgraniczne	Czy i jak dostawca poinformował subskrybentów usług: ....
Czy skutki transgraniczne dotyczą wszystkich wymienionych usług zaufania: □ Tak □ Nie, tylko: ……	

DODATKOWE INFORMACJE O ZDARZENIU:

Aktywa dotknięte incydentem	Szkody dla odbiorców usług	Pokrycie z ubezpieczenia (TAK/NIE)	Procent dotkniętych użytkowników	Poinformowane organy państwa	Kraje do poinformowania

INFORMACJE O DZIAŁANIACH PODJĘTYCH CELEM ZAŻEGNANIA SKUTKÓW:

A. PODJĘTE DZIAŁANIA:

B. ŚRODKI BEZPIECZEŃSTWA:

C. WNIOSKI NA PRZYSZŁOŚĆ:

DANE ZGŁASZAJĄCEGO:

Dostawca usług zaufania:.....

Imię i nazwisko ..... Stanowisko .....

Telefon:..... Email:.....

Data: …….. Podpis: ……

MINISTER CYFRYZACJI
notyfikowany organ nadzoru nad dostawcami usług zaufania
Adres do zgłaszania incydentów: nccert@nccert.pl
Departament Rozwoju Usług Cyfrowych i Otwartości Danych
Ministerstwo Cyfryzacji
ul. Królewska 27
00-060 Warszawa
tel. 22 245 55 44
e-mail: sekretariat.druciod@mc.gov.pl

PODSTAWA PRAWNA:

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

Artykuł 19 Wymogi w zakresie bezpieczeństwa mające zastosowanie do dostawców usług zaufania 1. Kwalifikowani i niekwalifikowani dostawcy usług zaufania przyjmują odpowiednie środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług zaufania. Przy uwzględnieniu najnowszych osiągnięć w dziedzinie technologii środki te zapewniają poziom bezpieczeństwa współmierny ze stopniem ryzyka. W szczególności należy podjąć środki zapobiegające incydentom związanym z bezpieczeństwem lub minimalizujące ich wpływ oraz należy informować zainteresowane strony o negatywnych skutkach wszelkich takich incydentów.
2. Kwalifikowani i niekwalifikowani dostawcy usług zaufania, bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu zdarzenia, zawiadamiają organ nadzoru i, w stosownych przypadkach, inne właściwe podmioty, takie jak właściwy krajowy organ ds. bezpieczeństwa informacji lub organ ochrony danych, o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe.
W przypadku gdy prawdopodobne jest, że naruszenie bezpieczeństwa lub utrata integralności niekorzystnie wpłyną na osobę fizyczną lub prawną, na rzecz której świadczona była usługa zaufania, dostawca usług zaufania bez zbędnej zwłoki zawiadamia także tę osobę fizyczną lub prawną o tym naruszeniu bezpieczeństwa lub utracie integralności.
W stosownych przypadkach, w szczególności jeżeli naruszenie bezpieczeństwa lub utrata integralności dotyczą dwóch lub większej liczby państw członkowskich, zawiadomiony organ nadzoru powiadamia organy nadzoru w pozostałych zainteresowanych państwach członkowskich oraz ENISA.
Zawiadomiony organ nadzoru podaje zaistniałe fakty do wiadomości publicznej lub nakłada taki obowiązek na dostawcę usług zaufania, w przypadku gdy uzna, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym.

POUCZENIE:

Formularz służy przygotowaniu zgłoszenia do systemu CIRAS-T. Aby to było możliwe, zgłoszenie musi zawierać przynajmniej:

1. Dane identyfikacyjne osoby zgłaszającej
2. Dane kontaktowe umożliwiające weryfikację zgłoszenia
3. Nazwę dostawcy usług zaufania
4. Opis incydentu

Wypełnienie pozostałych pól formularza ułatwi ocenę przypadku.

Dokonanie ww. zgłoszenia może być przeprowadzone wyłącznie przez osoby uprawnione w świetle regulacji wewnętrznych lub procedur dostawcy usług zaufania, którego incydent dotyczy.

Uprzejmie informujemy, że podane we wniosku przez Panią/Pana dane osobowe będą przetwarzane i administrowane zgodnie z ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) przez Ministerstwo Cyfryzacji w celu realizacji art. 19 rozporządzenia eIDAS.

Jednocześnie informujemy, iż Pani/Pana dane mogą być przekazane GIODO lub CERT oraz że ma Pani/Pan prawo dostępu do treści zgłoszenia oraz prawo ich poprawiania i sprzeciwu wobec ich przetwarzania w wyżej opisanym celu do chwili ich wprowadzenia do systemu CIRAS-T.

Celem zachowania integralności zgłoszenia oraz uniknięcia czynności potwierdzających zgłoszenie przez nadzór zaleca się opatrzenie przedmiotowego zgłoszenia kwalifikowanym podpisem elektronicznym.