**Informacja dotycząca przetwarzania danych osobowych w ramach zadań realizowanych przez sektorowy zespół cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych (CSIRT KNF), pozyskanych w związku z incydentami i zagrożeniami cyberbezpieczeństwa**

Zgodnie z art. 39 ust. 9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 z późn. zm.) (dalej: uksc) informuje się, że:

1. Administratorem danych osobowych jest Komisji Nadzoru Finansowego („Administrator") z siedzibą w Warszawie (kod pocztowy: 00-549), przy ul. Pięknej 20. Z Administratorem można się kontaktować pisemnie, kierując korespondencję na adres: ul. Piękna 20, skr. poczt. nr 419, kod pocztowy: 00-549 Warszawa lub pocztą elektroniczną na adres: knf@knf.gov.pl.
2. Administrator zapewnia kontakt z inspektorem ochrony danych za pośrednictwem poczty elektronicznej pod adresem: iod@knf.gov.pl lub drogą pocztową na adres korespondencyjny Administratora. Z IOD można się kontaktować we wszystkich sprawach dotyczących przetwarzania danych osobowych, w szczególności w zakresie korzystania z praw związanych z ich przetwarzaniem.
3. Podstawą prawną przetwarzania danych osobowych jest:
    a. art. 6 ust. 1 lit. c) 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 - „RODO") w związku z art. 44 uksc, tj. niezbędność przetwarzania do wypełnienia obowiązku prawnego ciążącego na Administratorze,
    b. art. 6 ust. 1 lit. e) RODO, tj. niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi,
    c. art. 6 ust. 1 lit c) RODO, tj. niezbędność przetwarzania do wypełnienia obowiązku prawnego ciążącego na Administratorze, wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz.U. z 2020 r. poz. 164 z późn. zm.) w związku z koniecznością archiwizacji dokumentacji.
4. Dane osobowe będą przetwarzane w celu realizacji zadań sektorowego zespołu cyberbezpieczeństwa, w tym w szczególności:
    a. przyjmowania zgłoszeń o incydentach poważnych oraz wsparcia w obsłudze tych incydentów,
    b. wspierania operatorów usług kluczowych w wykonywaniu obowiązków w zakresie określonym przepisami uksc,
    c. analizowania incydentów poważnych, wyszukiwania powiązań pomiędzy incydentami oraz opracowywania wniosków z obsługi incydentu,
    d. współpracy z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych,

    oraz archiwizacji dokumentacji.
5. Dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa mogą być przekazywane:
    a. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowym zespołom cyberbezpieczeństwa, w celu i zakresie niezbędnym do realizacji zadań określonych w uksc,
    b. innym organom administracji publicznej lub innym podmiotom upoważnionym na podstawie przepisów prawa, wykonującym zadania realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej,

c. podmiotom świadczącym usługi pocztowe oraz podmiotom zapewniającym usługi doręczeń przy użyciu środków komunikacji elektronicznej, którym dane mogą być przekazywane w przypadku konieczności prowadzenia korespondencji,
d. podmioty, z którymi Administrator zawarł umowę świadczenia usług w związku z wykorzystywanymi systemami informatycznymi.

6. Administrator będzie pozyskiwał w szczególności: imię i nazwisko, stanowisko służbowe, miejsce zatrudnienia, adres służbowy, służbowy adres e-mail, służbowy nr telefonu oraz inne dane niezbędne do realizacji celów określonych w pkt. 4 powyżej.
7. Administrator przetwarzać będzie dane w celach opisanych w pkt 4 powyżej, przez okres niezbędny dla realizacji celu, w którym dane te są przetwarzane, ale nie dłużej niż przez okres 5 lat od zakończenia obsługi incydentu, którego dane dotyczą.
8. Przetwarzanie danych, o których mowa w pkt. 6 powyżej, nie wymaga realizacji obowiązków wynikających z art. 15, art. 16, art. 18 ust. 1 lit. a i d oraz art. 19 zdanie drugie RODO, jeżeli:
    a. uniemożliwiłoby to Administratorowi realizację zadań określonych w uksc,
    b. administrator prowadzi analizę ryzyka, stosuje środki ochrony przed złośliwym oprogramowaniem oraz mechanizmy kontroli dostępu do danych, a także opracowuje procedury bezpiecznej wymiany informacji.
9. W przypadku uznania, że przetwarzanie danych osobowych narusza przepisy prawa, przysługuje prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.
10. Administrator będzie pozyskiwał dane osobowe w szczególności od operatorów usług kluczowych, CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowych zespołów cyberbezpieczeństwa, a także bezpośrednio od osób zgłaszających incydenty.