KNF | KOMISJA NADZORU FINANSOWEGO

....., ...
(miejscowość, data)

Komisja Nadzoru Finansowego
Plac Powstańców Warszawy 1
00-950 Warszawa

INFORMACJA DO KOMISJI NADZORU FINANSOWEGO W CELU POTWIERDZENIA SPEŁNIANIA PRZEZ KRAJOWĄ INSTYTUCJĘ PŁATNICZĄ WYMOGÓW OKREŚLONYCH W DZIALE IV USTAWY O USŁUGACH PŁATNICZYCH

Działając na podstawie art. 15 ust. 2 ustawy z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw krajowa instytucja płatnicza działająca pod firmą:

……..……..

1) **przedkłada w załączeniu następujące dokumenty i informacje** *(zaznaczyć właściwe)***:**
   - ☐ procedury monitorowania, postępowania i podejmowania działań następczych związanych z incydentami bezpieczeństwa oraz skargami klientów dotyczącymi bezpieczeństwa
   - ☐ procedurę dokumentowania, monitorowania, śledzenia i ograniczania dostępu do danych szczególnie chronionych dotyczących płatności
   - ☐ opis rozwiązań zapewniających ciągłość działania
   - ☐ zasady i definicje mające zastosowanie do gromadzenia danych statystycznych dotyczących wyników, transakcji i oszustw
   - ☐ politykę bezpieczeństwa
   - ☐ opis mechanizmów kontroli wewnętrznej zgodnych z obowiązkami związanymi z zapobieganiem praniu pieniędzy i finansowaniu terroryzmu
   - ☐ dokumenty dotyczące zmian, o których mowa w pkt 2) niniejszej informacji.

2) **oświadcza, że w zakresie pozostałych informacji i dokumentów określonych w art. 61 ust. 1 ustawy o usługach płatniczych, w stosunku do informacji i dokumentów przekazanych Komisji Nadzoru Finansowego wcześniej, w tym w postępowaniu w sprawie zezwolenia na świadczenie usług płatniczych w charakterze krajowej instytucji płatniczej** *(zaznaczyć właściwe)***:**
   - ☐ nie zaszły istotne zmiany
   - ☐ zaszły następujące istotne zmiany:

   proszę opisać zmiany; opis może być przekazany w formie odrębnego załącznika

……
(podpis zgodnie z zasadami reprezentacji)

KNF | KOMISJA NADZORU FINANSOWEGO

Szczegółowa charakterystyka dokumentów niezbędnych do przedłożenia w związku informacją przedkładaną Komisji Nadzoru Finansowego w celu potwierdzenia spełniania przez krajową instytucję płatniczą wymogów określonych w Dziale IV ustawy o usługach płatniczych

Przy opracowywaniu dokumentów należy kierować się wytycznymi wydanymi w przedmiotowym zakresie przez Europejski Urząd Nadzoru Bankowego, tj. *Wytycznymi dotyczącymi informacji, które należy przedstawić w celu uzyskania zezwolenia przez instytucje płatnicze i instytucje elektronicznego oraz zarejestrowania dostawców usługi dostępu do informacji o rachunku zgodnie z art. 5 ust. 5 dyrektywy (UE) 2015/2366* (EBA/GL/2017/09) (link: http://www.eba.europa.eu/documents/Guidelines+on+Authorisations+of+Payment+Institutions/GL/PL)

1. **Procedury monitorowania, postępowania i podejmowania działań następczych związanych z incydentami bezpieczeństwa oraz skargami klientów dotyczącymi bezpieczeństwa** powinny obejmować:
   - opis środków organizacyjnych i narzędzi zapobiegających oszustwom;
   - szczegółowe informacje o osobie fizycznej/osobach fizycznych lub osobach fizycznych i organach odpowiedzialnych za pomoc klientom w przypadku oszustw, problemów technicznych lub zarządzanie roszczeniami;
   - informacje o kanałach, za pośrednictwem których należy zgłaszać przypadki oszustwa;
   - dane punktu kontaktowego dla klientów, w tym imię, nazwisko i adres e-mail;
     - opis procedury zgłaszania incydentów, w tym przekazywania zgłoszeń organom wewnętrznym i zewnętrznym, w tym powiadamiania KNF o poważnych incydentach i oszustwach zgodnie z art. 32g ust. 1 i art. 32h ust. 1 ustawy o usługach płatniczych, z uwzględnieniem wytycznych Europejskiego Urzędu Nadzoru Bankowego w sprawie zgłaszania incydentów zgodnie z art. 96 dyrektywy (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych (link: http://www.eba.europa.eu/Guidelines+on+incident+reporting+under+PSD2/GL/PL);
   - informacje o wykorzystywanych narzędziach monitorowania oraz środkach i procedurach następczych stosowanych w celu ograniczenia ryzyk w zakresie bezpieczeństwa.

   Szczegółowe informacje dotyczące powiadamiania KNF o poważnych incydentach i oszustwach związanych z wykonywaniem usług płatniczych zostaną opublikowane w odrębnym komunikacie KNF.

2. **Procedura dokumentowania, monitorowania, śledzenia i ograniczania dostępu do danych szczególnie chronionych dotyczących płatności** powinna obejmować:
   - opis przepływu danych sklasyfikowanych jako dane szczególnie chronione dotyczące płatności w kontekście modelu działalności instytucji płatniczej;
   - opis procedur wprowadzonych w celu zezwolenia na dostęp do szczególnie chronionych danych dotyczących płatności;
   - opis narzędzi monitorowania;
   - opis polityki w zakresie uzyskiwania praw dostępu do danych szczególnie chronionych, z wyszczególnieniem prawa dostępu do wszystkich stosownych komponentów i systemów infrastruktury, w tym baz danych i kopii zapasowych;
   - opis sposobu przechowywania zgromadzonych danych w dokumentacji;
   - informacje na temat zakładanego wewnętrznego lub zewnętrznego sposobu wykorzystania zgromadzonych danych, w tym również przez podmioty współpracujące z krajową instytucją płatniczą;
   - opis wprowadzonego systemu informatycznego i środków ochrony technicznej, w tym szyfrowania lub tokenizacji;
   - zasady identyfikacji osób fizycznych (imiona i nazwiska), organów lub komisji krajowej instytucji płatniczej posiadających dostęp do szczególnie chronionych danych dotyczących płatności;
   - wyjaśnienia dotyczące sposobu wykrywania naruszeń i radzenia sobie z nimi;
   - informację na temat corocznego programu kontroli wewnętrznej w zakresie bezpieczeństwa systemów informatycznych.

3. **Opis rozwiązań zapewniających ciągłość działania** powinien obejmować:
   - analizę wpływu na działanie (BIA – *Business Impact Analysis*), w tym procesów biznesowych i parametrów odtworzenia krytycznych procesów organizacji w przypadku sytuacji kryzysowej: RTO (*Recovery Time Objective*) – czas, w jakim należy przywrócić procesy po wystąpieniu awarii; oraz RPO (*Recovery Point Objective*) – akceptowalny poziom utraty danych wyrażony w czasie oraz aktywa chronione;
   - określenie zapasowej strony internetowej, dostępu do infrastruktury informatycznej oraz kluczowego oprogramowania i danych, które zostaną odzyskane po awarii lub zakłóceniu funkcjonowania;
   - informacje o działaniach podejmowanych w przypadku poważnego zdarzenia lub zakłócenia funkcjonowania mającego wpływ na ciągłość działania, takiego jak awaria kluczowych systemów, utrata kluczowych danych, brak dostępu do pomieszczeń oraz utrata kluczowych osób;
   - określenie częstotliwości, z jaką krajowa instytucja płatnicza zamierza weryfikować ciągłość działania i plany odtworzeniowe, w tym sposób rejestrowania wyników weryfikacji;
   - opis przyjętych przez krajową instytucję płatniczą środków ograniczających ryzyko w przypadku zakończenia świadczenia usług płatniczych, zapewniających wykonanie niezrealizowanych transakcji płatniczych oraz wygaśnięcie istniejących umów.

4. **Zasady i definicje mające zastosowanie do gromadzenia danych statystycznych dotyczących wyników, transakcji i oszustw** powinny obejmować informacje o:
   - rodzaju gromadzonych danych dotyczących klientów, rodzaju usług płatniczych, kanałów dystrybucji usług, instrumentów płatniczych, obszarów działania i walut, w jakich dokonywane są transakcje płatnicze;
   - zakresie gromadzonych danych w odniesieniu do określonych działań i podmiotów, w tym oddziałów i agentów;
   - środkach lub sposobach gromadzenia danych;
   - celu gromadzenia danych;
   - częstotliwości gromadzenia danych;
   - dokumentach uzupełniających, takich jak instrukcja, dokumenty opisujące sposób działania systemu.

5. **Polityka bezpieczeństwa** powinna obejmować:
   - szczegółową ocenę ryzyka, w tym ryzyka oszustwa, w odniesieniu do usług płatniczych, z uwzględnieniem środków kontroli bezpieczeństwa i ograniczania ryzyka podjętych w celu adekwatnej ochrony użytkowników usług płatniczych przed zidentyfikowanymi rodzajami ryzyka;
   - opis systemów informatycznych, który powinien zawierać:
     – architekturę systemów i elementów ich sieci;
     – biznesowe systemy informatyczne wspierające prowadzoną działalność gospodarczą, takie jak witryny internetowe, portfele, mechanizm płatności, mechanizm zarządzania ryzykiem i przeciwdziałania oszustwom oraz rozliczanie klientów;
     – wspierające systemy informatyczne wykorzystywane w organizacji i administracji krajowej instytucji płatniczej, takie jak księgowe, sprawozdawcze, zarządzania personelem, zarządzania relacjami z klientami, serwerów poczty elektronicznej i serwerów plików wewnętrznych;
     – informacje, czy systemy te są już używane przez krajową instytucję płatniczą lub grupę podmiotów, do której należy, oraz szacunkowy termin ich wdrożenia, jeśli dotyczy;
   - informacje o rodzajach autoryzowanych połączeń (m.in. telekomunikacyjnych/teleinformatycznych/ informatycznych) z zewnątrz, takich jak połączenia z partnerami, dostawcami usług, podmiotami z grupy i pracownikami pracującymi na odległość, w tym powody nawiązywania takich połączeń;
   - dla każdego połączenia określonego w poprzednim punkcie, logiczne środki i mechanizmy bezpieczeństwa , ze wskazaniem zasad kontroli sprawowanej nad dostępem, w tym również charakter i częstotliwość każdej kontroli, np. techniczna czy organizacyjna, prewencyjna czy mająca na celu wykrycie określonych okoliczności, monitorowanie w czasie rzeczywistym, regularną weryfikację, np. wykorzystanie usług active directory (*hierarchiczna baza danych – usługa katalogowa dla systemów Windows*) osobno od grupy, otwieranie/zamykanie linii komunikacyjnych, konfigurację sprzętu bezpieczeństwa, generowanie kluczy lub certyfikatów uwierzytelniania klienta, monitorowanie systemu, uwierzytelnianie, poufność komunikacji, wykrywanie włamań, systemy antywirusowe i dzienniki;

- logiczne środki i mechanizmy bezpieczeństwa w zakresie zarządzania dostępem wewnętrznym do systemów informatycznych, które powinny zawierać:
  - techniczny i organizacyjny charakter oraz częstotliwość stosowania każdego środka, np. czy jest on prewencyjny czy mający na celu wykrycie określonych okoliczności i czy jest wykonywany w czasie rzeczywistym;
  - sposób postępowania w zakresie rozdzielenia środowisk informatycznych klientów w przypadku, gdy ich zasoby informatyczne są wspólne z zasobami krajowej instytucji płatniczej;
- fizyczne środki i mechanizmy bezpieczeństwa pomieszczeń oraz centrum danych krajowej instytucji płatniczej, takie jak kontrole dostępu i bezpieczeństwo środowiskowe;
- rozwiązania w zakresie bezpieczeństwa procesów płatniczych, które powinny zawierać:
  - procedurę uwierzytelniania klienta stosowaną w przypadku dostępu zarówno w celach informacyjnych jak i transakcyjnych oraz wszystkich dostępnych instrumentów płatniczych;
  - opis sposobu zapewnienia bezpiecznego przesyłania środków pieniężnych do właściwego użytkownika usług płatniczych oraz integralności elementów uwierzytelniania, np. tokeny sprzętowe i aplikacje mobilne, zarówno w momencie początkowej rejestracji jak i w przypadku przedłużenia ich ważności (lub ich odnowienia);
  - opis systemów i procedur, które krajowa instytucja płatnicza wprowadziła w celu analizy transakcji i identyfikacji transakcji podejrzanych lub nietypowych;
- wykaz głównych procedur w formie pisemnej w odniesieniu do systemów informatycznych krajowej instytucji płatniczej lub, w przypadku procedur, które nie zostały jeszcze sformalizowane, szacunkowy termin ich finalizacji.

6. **Opis mechanizmów kontroli wewnętrznej zgodnych z obowiązkami związanymi z zapobieganiem praniu pieniędzy i finansowaniu terroryzmu** powinien obejmować:
   - opis procesu oceny ryzyka prania pieniędzy i finansowania terroryzmu, w tym związanego z bazą klientów krajowej instytucji płatniczej, udostępnionymi produktami i świadczonymi usługami, używanymi kanałami dystrybucji oraz geograficznymi obszarami działania;
   - informacje na temat środków, które zostały wprowadzone w celu zmniejszenia ryzyka i wypełnienia obowiązków związanych z zapobieganiem praniu pieniędzy i finansowaniu terroryzmu, w tym stosowanych procedur oceny ryzyka, zasad i procedur w zakresie wymogów należytej staranności w stosunku do klientów oraz zasad i procedur wykrywania i zgłaszania podejrzanych transakcji i czynności/działań;
   - opis systemów i mechanizmów kontrolnych, które zostały wprowadzone w celu zapewnienia, że oddziały i agenci krajowej instytucji płatniczej stosują się do obowiązujących wymagań w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, w tym w przypadku, gdy agent lub oddział są zlokalizowani w innym państwie członkowskim;
   - rozwiązania, które krajowa instytucja płatnicza wprowadziła lub wprowadzi, aby zapewnić, że pracownicy i agenci zostali właściwe przeszkoleni w zakresie spraw związanych z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu;
   - dane pozwalające na ustalenie tożsamości osoby odpowiedzialnej za zapewnienie wypełniania przez krajową instytucję płatniczą obowiązków związanych z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu oraz dowód potwierdzający, że jego kompetencje w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu są wystarczające, aby zapewnić skuteczne wypełnienie tej roli;
   - opis systemów i mechanizmów kontrolnych, które zostały wprowadzone w celu zapewnienia aktualności, skuteczności i stosowności polityki i procedur dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu;
   - opis systemów i mechanizmów kontrolnych, które zostały wprowadzone w celu zapewnienia, że działalność agentów krajowej instytucji płatniczej nie będzie źródłem zwiększonego ryzyka związanego z praniem pieniędzy oraz finansowaniem terroryzmu;
   - wytyczne i informacje dla pracowników krajowej instytucji płatniczej w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu.