

**PRAKTYCZNY KOMENTARZ  
DO USTAWY  
Z DNIA 1 GRUDNIA 2022 R.  
O SYSTEMIE  
INFORMACJI  
FINANSOWEJ**

**WIESŁAW MICHAŁ JASIŃSKI  
MACIEJ ALEKSANDER KĘDZIERSKI**

stan prawny na dzień 10 października 2023 r.

**SZCZYTNO 2023**

**Recenzenci**

*dr hab. Wojciech Filipkowski, prof. UwB*

**Redakcja Wydawcy**

*Małgorzata Bukowska*

*Adam Rogala*

**Projekt okładki**

*Agnieszka Kamińska*



© Wszelkie prawa zastrzeżone — Akademia Policji w Szczytnie

**ISBN 978-83-7462-856-3**

**e-ISBN 978-83-7462-857-0**

Druk i oprawa:

Dział Wydawnictw i Poligrafii Akademii Policji w Szczytnie

ul. Marszałka Józefa Piłsudskiego 111, 12-100 Szczytno

tel. 47 733 5410

e-mail: [wwip@apol.edu.pl](mailto:wwip@apol.edu.pl)

Objętość: 18,77 ark. wyd.

# SPIS TREŚCI

Wykaz pojęć i skrótów użytych w treści komentarza .....	6
Wprowadzenie .....	9
<b>Rozdział 1. Przepisy ogólne .....</b>	<b>27</b>
1. Zakres regulacji ustawy o SInF .....	27
2. Określenie celów ustawy o SInF .....	32
3. Objasnienie pojęć wskazanych w ustawie .....	48
4. Zakres informacji rejestrowanej .....	77
<b>Rozdział 2. Organ właściwy w sprawie SInF .....</b>	<b>85</b>
5. Organ właściwy w zakresie wykonywania zadań z ustawy .....	85
6. Administrator danych zgromadzonych w SInF .....	87
7. Zadania organu właściwego .....	89
8. Sprawozdanie z działalności właściwego organu .....	95
9. Obowiązek posiadania kwalifikacji zapewniających bezpieczeństwo systemu teleinformatycznego .....	98
<b>Rozdział 3. Informacje rejestrowane oraz ich przekazywanie do SInF .....</b>	<b>105</b>
10. Obowiązek przekazywania informacji rejestrowanych do systemu ...	105
11. Kryteria przekazywania informacji do systemu .....	107
12. Zakresy informacji rejestrowanych .....	111
13. Przekazywanie informacji do systemu za pośrednictwem STIR .....	125
14. Termin przekazywania informacji rejestrowanej .....	131
15. Możliwość wystąpienia z żądaniem ponownego przekazania informacji rejestrowanej .....	135
16. Czas przetwarzania informacji rejestrowanych .....	139
17. Przekazywanie informacji rejestrowanych w postaci elektronicznej ...	147
<b>Rozdział 4. Wykorzystanie informacji rejestrowanych zgromadzonych w SInF .....</b>	<b>149</b>
18. Niezwłoczne przekazywanie informacji rejestrowanych do Generalnego Inspektora Informacji Finansowej .....	149
19. Podmioty uprawnione do uzyskiwania informacji rejestrowanych z SInF .....	159
20. Cele przetwarzania danych zgromadzonych w systemie .....	172
21. Osoby upoważnione przez podmioty uprawnione do dostępu do systemu .....	176
22. Rejestr osób upoważnionych do dostępu do systemu .....	186
23. Dane potrzebne do uzyskania dostępu do zgromadzonych w systemie informacji rejestrowanych .....	188
24. Termin przekazywania informacji rejestrowanych z systemu .....	192

25. Rejestr działań osób uzyskujących informacje rejestrowane z systemu .....	193
26. Informacje przekazywane sądom i prokuratorom na potrzeby postępowania karnego .....	206
27. Zabezpieczenia zapobiegające nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu .....	209
28. Rozporządzenie określające szczegóły przekazywania informacji rejestrowanych .....	213
<b>Rozdział 5. Ochrona danych i kontrola przekazywania do SIInF informacji rejestrowanych .....</b>	<b>221</b>
29. Niestosowanie przepisów regulujących ograniczenia udostępniania danych objętych tajemnicami ustawowo chronionymi. ....	221
30. Kontrola wykonywania przez instytucje zobowiązane obowiązków w zakresie przekazywania do STIR informacji rejestrowanych .....	226
<b>Rozdział 6. Kary pieniężne .....</b>	<b>231</b>
31. Kary pieniężne wobec instytucji zobowiązanej .....	231
32. Kary pieniężne wobec instytucji rozliczeniowej .....	238
33. Wpływy z kar pieniężnych .....	242
<b>Rozdział 7. Przepisy karne .....</b>	<b>243</b>
34. Przepięstwo ujawnienia osobom nieuprawnionym przetwarzanych w systemie informacji rejestrowanych lub informacji z rejestru .....	243
35. Kary za przetwarzanie informacji rejestrowanych lub informacji z rejestru .....	246
<b>Rozdział 8. Zmiany w przepisach .....</b>	<b>249</b>
36. Zmiany w przepisach Ustawy z dnia 29 sierpnia 1997 r. — Ordynacja podatkowa (Dz.U. z 2023 r., poz. 2383, 2760) .....	250
37. Zmiany w przepisach Ustawy z dnia 29 sierpnia 1997 r. — Prawo bankowe (Dz.U. z 2023 r., poz. 2488) .....	257
38. Zmiany w przepisach Ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz.U. z 2023 r., poz. 646, 825, 1723, 1941) .....	258
39. Zmiany w przepisach Ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym (Dz.U. z 2023 r., poz. 753, 825, 1705, 1723, 1843) .....	260
40. Zmiany w przepisach Ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz.U. z 2023 r., poz. 1278, 1394, 1407, 1723, 1843) .....	262
41. Zmiany w przepisach Ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. z 2023 r., poz. 783) .....	265

42. Zmiany w przepisach Ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz.U. z 2023 r., poz. 615, 556, 588, 641, 658, 760, 996, 1059, 1193, 1195, 1234, 1598).....	269
43. Zmiany w przepisach Ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2023 r., poz. 1124, 1285, 1723, 1843) .....	279
<b>Rozdział 9. Przepisy przejściowe, dostosowujące i końcowe</b> .....	297
44. Przepisy przejściowe, dostosowujące i końcowe .....	297
<b>Rozdział 10. Dalsze prace ustawodawcze nad zmianą dyrektywy 2019/1153.</b>	303
<b>Załączniki (akty prawne i ich projekty)</b> .....	307
Załącznik nr 1. Rozporządzenie Ministra Finansów z dnia ..... w sprawie warunków technicznych dla elektronicznej wymiany danych z Systemu Informacji Finansowej (projekt z dnia 6 lipca 2022 r. wraz z uzasadnieniem) .....	307
Załącznik nr 2. Rozporządzenie Ministra Finansów z dnia ..... w sprawie wyznaczenia organu Krajowej Administracji Skarbowej do wykonywania zadań organu właściwego do prowadzenia Systemu Informacji Finansowej (projekt z dnia 21 kwietnia 2022 r. wraz z uzasadnieniem) .....	315
Załącznik nr 3. Rozporządzenie Ministra Finansów w sprawie wymogów technicznych dla elektronicznej wymiany danych z Systemu Informacji Finansowej (projekt z dnia 16 sierpnia 2023 r. wraz z uzasadnieniem) .....	317
Załącznik nr 4. Rozporządzenie Ministra Finansów z dnia 9 grudnia 2023 r. w sprawie elektronicznej wymiany danych z Systemu Informacji Finansowej .....	325
<b>Bibliografia</b> .....	329
Literatura .....	329
Wyroki/orzeczenia sądów krajowych .....	331
Akty prawa międzynarodowego (dokumenty) .....	331
Akty prawa krajowego (dokumenty) .....	334
Inne .....	337

## Wykaz pojęć i skrótów użytych w treści komentarza

### I. Akty prawne i publikatory

- dyrektywa 2015/849 — Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE. Tekst mający znaczenie dla EOG (Dz. Urz. UE L 141/73 z 5.06.2015)
- dyrektywa 2018/843 — Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE. Tekst mający znaczenie dla EOG (Dz. Urz. UE L 156/43 z 19.06.2018)
- dyrektywa 2019/1153 — Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1153 z dnia 20 czerwca 2019 r. ustanawiająca zasady ułatwiające korzystanie z informacji finansowych i innych informacji w celu zapobiegania niektórym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania oraz uchylająca decyzję Rady 2000/642/WSiSW (Dz. Urz. UE L 186/122 z 11.07.2019)
- dyrektywa 2021/514 — Dyrektywa Rady (UE) 2021/514 z dnia 22 marca 2021 r. zmieniająca dyrektywę 2011/16/UE w sprawie współpracy administracyjnej w dziedzinie opodatkowania (Dz. Urz. UE L 104/1 z 25.03.2021)
- Dz.U. — Dziennik Ustaw
- Dz. Urz. — Dziennik Urzędowy
- k.c. — Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz.U. z 2023 r., poz. 1610, 1615)
- k.k. — Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. z 2022 r., poz. 1138, 1726, 1855, 2339, 2600; z 2023 r., poz. 289, 403, 818, 852, 1234, 1834)
- k.p.a. — Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz.U. z 2023 r., poz. 775)
- M.P. — Monitor Polski
- OP — Ustawa z dnia 29 sierpnia 1997 r. — Ordynacja podatkowa (Dz.U. z 2023 r., poz. 2383, 2760)
- pr. bankowe — Ustawa z dnia 29 sierpnia 1997 r. — Prawo bankowe (Dz.U. z 2022 r., poz. 2324, 2339, 2640, 2707; z 2023 r., poz. 180, 825, 996, 1059, 1394, 1407)
- RODO — rozporządzenie unijne, Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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). Tekst mający znaczenie dla EOG (Dz. Urz. UE L 119/1 z 04.05.2016)

rozporządzenie (UE) nr 883/2013 — Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz uchylające rozporządzenie (WE) nr 1073/1999 Parlamentu Europejskiego i Rady i rozporządzenie Rady (Euratom) nr 1074/1999 (Dz. Urz. UE L 248/1 z 18.09.2013)

t.j. — tekst jednolity

ustawa o SKOK — Ustawa z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz.U. z 2023 r., poz. 1278, 1394, 1407, 1723, 1843)

ustawa o wymianie informacji — Ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (Dz.U. z 2023 r., poz. 783)

ustawa o KAS — Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (Dz.U. z 2023 r., poz. 615, 556, 588, 641, 658, 760, 996, 1059, 1193, 1195, 1234, 1598)

ustawa o p.p.p.ft. — Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2023 r., poz. 1124, 1285, 1723, 1843)

ustawa o SInF — Ustawa z dnia 1 grudnia 2022 r. o Systemie Informacji Finansowej (Dz.U. z 2023 r., poz. 180)

ustawa o CBR — projekt ustawy o Centralnej Bazie Rachunków z 2016 r.

## II. Organy i instytucje

ABW — Agencja Bezpieczeństwa Wewnętrznego

BOM — Biuro Odzyskiwania Mienia

CBA — Centralne Biuro Antykorupcyjne

CRP KEP — Centralny Rejestr Podmiotów Krajowej Ewidencji Podatników

Europol — Agencja Unii Europejskiej ds. Współpracy Organów Ścigania, policyjna agencja Unii Europejskiej z siedzibą w Hadze

GIIF — Generalny Inspektor Informacji Finansowej (Generalny Inspektor)

JAF — jednostka analityki finansowej

KAS — Krajowa Administracja Skarbowa

KGP — Komenda Główna Policji

KIR S.A. — Krajowa Izba Rozliczeniowa

KNF — Komisja Nadzoru Finansowego

MSWiA — Ministerstwo Spraw Wewnętrznych i Administracji

NBP — Narodowy Bank Polski

N-UCS — naczelnik urzędu celno-skarbowego

RCL — Rządowe Centrum Legislacji

RL — Rada Legislacyjna

SKOK — spółdzielcze kasy oszczędnościowo-kredytowe

SKW — Służba Kontrwywiadu Wojskowego

Szef KAS — Szef Krajowej Administracji Skarbowej w rozumieniu ustawy o KAS  
UCS — urząd celno-skarbowy  
UE — Unia Europejska  
ZJAF — zagraniczne jednostki analityki finansowej

### III. Inne

AMLD — dyrektywy w sprawie przeciwdziałania praniu pieniędzy  
AML/CFT — ang. Anti-Money Laundering/Counter Financing of Terrorism (przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu)  
BIF — plik BIF to plik obrazu rastrowego zawierający obraz próbki slajdu. Składa się z wielu obrazów TIFF, które są łączone przez aplikacje do przeglądania slajdów w jeden złożony obraz, <<https://docs.fileformat.com/pl/image/bif/>>  
FT — finansowanie terroryzmu  
NIP — Numer Identyfikacji Podatkowej  
NRB — Numer Rachunku Bankowego  
IBAN — Międzynarodowy Numer Rachunku Bankowego  
JSON (ang. JavaScript Object Notation) — lekki format wymiany danych komputerowych. JSON jest formatem tekstowym, bazującym na podzbiorze języka JavaScript. Typ MIME dla formatu JSON to application/json. Format został opisany w dokumentach RFC 4627 ↓, ISO/IEC 21778:2017 oraz ECMA-404, <<https://pl.wikipedia.org/wiki/JSON>>  
PESEL — Powszechny Elektroniczny System Ewidencji Ludności, centralny zbiór danych prowadzony w Polsce przez ministra właściwego do spraw informatyzacji na mocy ustawy o ewidencji ludności, <<https://pl.wikipedia.org/wiki/PESEL>>  
PZ — przestępczość zorganizowana  
SAR — ang. Suspicious Activity Report (raporty o podejrzanym aktywności)  
STIR — system teleinformatyczny izby rozliczeniowej spełniający minimalne wymagania dla systemów teleinformatycznych określone w przepisach wydanych na podstawie art. 18 Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (art. 119zg pkt 6 OP)  
STR — ang. Suspicious Transaction Report (raport o transakcji podejrzanym)  
TR — terroryzm  
UID — unikalny identyfikator dostępu  
UTF-8 (ang. 8-bit Unicode Transformation Format) — system kodowania Unicode, wykorzystujący od 1 do 4 bajtów do zakodowania pojedynczego znaku, w pełni kompatybilny z ASCII. Jest najczęściej wykorzystywany do przechowywania napisów w plikach i komunikacji sieciowej, <<https://pl.wikipedia.org/wiki/UTF-8>>



## Wprowadzenie

Od ponad trzech dekad (po 1990 r.) dokonują się zmiany prawa w zakresie dostępu do informacji finansowych w związku z realizacją czynności w procesie wykrywania przestępstw. Chodzi tu o zmiany w wielu ustawach określających funkcjonowanie zarówno instytucji finansowych, organów administracji publicznej, jak i organów ścigania. Ich przedmiotem są m.in. zakres informacji finansowych potrzebnych do zwalczania przestępstw, procedury dostępu do tych informacji, zakres czynności organów ścigania, które warunkują taki dostęp, a także zakres i sposób ich wykorzystywania. Materia ta jest o tyle skomplikowana, że chodzi w niej również o ingerencję w ustawową ochronę praw i wolności obywatelskich, którą objęte są niektóre z tych informacji finansowych. Trybunał Konstytucyjny stwierdził, że prawo do prywatności obejmuje też ochronę danych dotyczących sytuacji majątkowej obywatela, a więc odnosi się do posiadanych przez niego rachunków bankowych (i podobnych) oraz dokonywanych przez niego transakcji (Wyrok Trybunału Konstytucyjnego z dnia 24 czerwca 1997 r., K 21/96 OTK 1997, nr 2, poz. 23, <<https://www.saos.org.pl/judgments/205753>>). W takich okolicznościach prawnych wszystkie kategorie podmiotów uczestniczących w przetwarzaniu informacji finansowych na potrzeby wykrywania przestępstw wypracowywały przez lata praktykę stosowania prawa. Było to o tyle trudne, że towarzyszy temu oczywista kolizja interesów podmiotów zaangażowanych w wymianę informacji. Na dodatek przez wiele lat doszło do takiego rozszerzenia katalogu podmiotów uprawnionych do dostępu do informacji finansowych w ramach kompetencji w zakresie zwalczania przestępstw, że zasadą stało się udostępnianie informacji finansowych, a wyjątkiem — ich ochrona przez dysponentów przed podmiotami zewnętrznymi. Poza tym informacje finansowe udostępniane są do coraz większej liczby różnych kategorii postępowań — poczynając od karnego postępowania przygotowawczego, przez postępowania administracyjne, na czynnościach operacyjno-rozpoznawczych organów ścigania kończąc.

Po 2001 r. istotne miejsce w wymianie informacji finansowej zajął Generalny Inspektor Informacji Finansowej (GIIF) w związku ze swoją funkcją przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Nowy podmiot administracji rządowej spowodował też istotne aktywowanie

działań obu stron zainteresowanych wymianą informacji — organów ścigania oraz komercyjnych instytucji finansowych i pozafinansowych.

Organy ścigania tworzyły od tamtego momentu podstawy modelowe śledztwa finansowego rozumianego jako zbieranie, kontrolowanie, kompletowanie, przetwarzanie i analizowanie danych finansowych na rzecz egzekwowania prawa (por. P.C. van Duyne, M. Pheijffer, H.G. Kuijl, A.Th. H. van Dijk, G.J.C.M. Bakker (eds.), *Financial investigation of crime. A Toll of the integral law enforcement approach*, Lelystad 2001, s. 16–19). Jednocześnie rozpoczęła się też budowa instytucjonalnego systemu odzyskiwania mienia z przestępstw. 5 grudnia 2008 r. w strukturach Biura Kryminalnego Komendy Głównej Policji powołano Wydział ds. Odzyskiwania Mienia, pełniący funkcję krajowego Biura ds. Odzyskiwania Mienia (por. art. 145k Ustawy z dnia 6 kwietnia 1990 r. o Policji, Dz.U. z 2023 r., poz. 171; z 2022 r., poz. 2600; z 2023 r., poz. 185, 240, 289, 347, 535, 641, 1088, 1860). Było to też wypełnienie Decyzji Rady Unii Europejskiej 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotyczącej współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w dziedzinie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem (Dz. Urz. UE L 332/103 z 18.12.2007) przyjętej w związku z koniecznością zacieśniania współpracy pomiędzy krajami członkowskimi w zakresie odzyskiwania mienia i pozbawiania sprawców korzyści majątkowych osiągniętych z popełniania przestępstw i zobowiązującej państwa członkowskie Unii Europejskiej do powołania lub desygnowania podmiotu odgrywającego rolę biura ds. odzyskiwania mienia (krajowe punkty kontaktowe). Ostateczny kształt polskiemu systemowi odzyskiwania mienia nadała Ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi (t.j. Dz.U. z 2023 r., poz. 783), która określa zasady i warunki wymiany informacji z organami ścigania w celu wykrywania i ścigania sprawców przestępstw lub przestępstw skarbowych, zapobiegania przestępczości i jej zwalczania oraz przetwarzania informacji, a także podmioty uprawnione w tych sprawach. Precyzuje też zadania i uprawnienia krajowych punktów kontaktowych. Zgodnie z ustawą, podmiotami uprawnionymi do wymiany informacji za pośrednictwem Biura ds. Odzyskiwania Mienia są: Policja, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Żandarmeria Wojskowa, Krajowa Administracja Skarbowa (od 1 marca 2017 r.), Biuro Nadzoru Wewnętrznego (od 27 stycznia 2018 r.), Służba Ochrony Państwa (od 1 lutego 2018 r.), a także prokurator oraz minister właściwy do spraw finansów publicznych.

Podmioty komercyjne natomiast poszukiwały na przestrzeni ostatnich dekad m.in. rozwiązań w zakresie usprawnienia wymiany informacji między sobą, ale też na potrzeby organów ścigania. Ta druga kategoria ma istotne znaczenie historyczne dla Systemu Informacji Finansowej (SInF). Otóż w odpowiedzi na potrzeby organów ścigania Krajowa Izba Rozliczeniowa S.A. (KIR S.A.), działająca jako instytucja infrastrukturalna polskiego sektora bankowego, do istniejącej od 2007 r. aplikacji OGNIVO, której głównym zadaniem jest usprawnienie elektronicznej wymiany informacji pomiędzy bankami, Zakładem Ubezpieczeń Społecznych, Poczta Polska, Krajową Administracją Skarbową (KAS), administracyjnymi organami egzekucyjnymi i komornikami sądowymi, opracowała funkcjonujący od września 2016 r. moduł do obsługi sądów i prokuratur. Jednocześnie 1 lipca 2016 r. weszła w życie nowelizacja Ustawy z dnia 29 stycznia 1997 r. — Prawo bankowe (Dz.U. z 2022 r., poz. 232) wprowadzająca m.in. art. 92bb ust. 1, zgodnie z którym banki zostały zobowiązane prowadzić centralną informację o rachunkach, zwaną „Centralną informacją”. Zgodnie z art. 92bb ust. 2 wymienionej ustawy centralną informację może prowadzić izba rozliczeniowa, o której mowa w art. 67, czyli KIR S.A. Z aplikacji OGNIVO mogą korzystać wyłącznie podmioty uprawnione do uzyskiwania informacji o klientach banków i tylko w zakresie niezbędnym do wykonania czynności, dla których informacja jest pozyskiwana. Pierwotnym celem aplikacji była szybka i bezpieczna wymiana informacji pomiędzy uczestnikami systemów rozliczeniowych, głównie bankami, oraz obsługa reklamacji związanych z rozliczeniami międzybankowymi.

Moduł do obsługi sądów i prokurator stanowi rozwiązanie występującego do 2016 r. problemu związanego z ustalaniem rachunków należących do osoby podejrzanej, podejrzanego i innych osób związanych z przestępstwem. Wprowadzenie aplikacji nie powodowało konieczności zmiany przepisów dotyczących tajemnicy bankowej. Zasada działania aplikacji nie narusza w żaden sposób prawnie chronionych danych objętych tajemnicą bankową, gdyż nie dysponuje ona informacjami banków, a tylko zapewnia możliwość wymiany informacji pomiędzy prokuratorami i bankami. Z tego powodu uzyskanie informacji z wykorzystaniem systemu OGNIVO nie wymaga postanowienia właściwego sądu okręgowego.

Aplikacja OGNIVO składa się z modułów obowiązkowych i opcjonalnych. Do modułów obowiązkowych należą:

- a) moduł reklamacji i zapytań, służący do wymiany informacji pomiędzy przelewami dwóch instytucji;
- b) moduł monitoringu sald systemów rozliczeniowych, umożliwiający sprawdzanie salda konta w banku w ramach systemu rozliczeniowego KIR S.A.;

- c) moduł awaryjnego kopiowania plików BIF;
- d) moduł elektronicznej zgód poleceń zapłaty.

Do modułów opcjonalnych należą:

- a) moduł informacji wyprzedzającej o saldach przychodzących;
- b) moduł do obsługi przenoszenia rachunków i usług płatniczych, który umożliwi terminowe, sprawne i bezpieczne przenoszenie rachunków klientów pomiędzy bankami;
- c) moduł zapytania o rachunki bankowe dłużników, umożliwiający komornikom sądowym i skarbowym elektroniczną komunikację z bankami, co znacząco usprawnia obsługę zajęć;
- d) moduł rozrachunku Izby Rozliczeniowej Giełd Towarowych, który umożliwi przekazywanie danych do rozrachunku pieniężnego transakcji zawieranych na rynkach Towarowej Giełdy Energii;
- e) moduł do obsługi sądów i prokuratur, pozwalający prokuratorom i sądom pozyskiwać dane chronione tajemnicą bankową, które mogą stanowić materiał dowodowy lub umożliwiać realizację zabezpieczenia majątkowego; informacje mogą dotyczyć osób prawnych lub fizycznych, wobec których prowadzone są postępowania przygotowawcze lub powiązanych z przestępstwem.

„Centralna informacja” o rachunkach znacznie wpłynęła na usprawnienie wymiany informacji pomiędzy bankami i spółdzielczymi kasami oszczędnościowo-kredytowymi (SKOK) a uprawnionymi podmiotami, do których należą poza organami ścigania również:

- a) posiadacze rachunków, będący osobami fizycznymi, uprawnieni do odszukania własnych rachunków w bankach i SKOK-ach;
- b) osoby, które uzyskały tytuł prawny do spadku po posiadaczu rachunku lub tytuł prawny do spadku po członku SKOK;
- c) gminy, w zakresie informacji, o których mowa w art. 111c pr. bankowego, czyli o powziętej przez bank informacji w zakresie daty zgonu posiadacza rachunku i posiadanych rachunkach oraz zgromadzonych środkach;
- d) zarządcy sukcesyjni, o których mowa w art. 111c pr. bankowego oraz w art. 13d ust. 1 Ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, w zakresie informacji o rachunkach osób zmarłych.

Do korzyści związanych z wprowadzeniem modułu do obsługi sądów i prokuratur programu OGNIVO zaliczyć można:

- a) łatwy dostęp do informacji o rachunkach w każdym banku i SKOK uczestniczącym w systemie, a tym samym wyeliminowanie konieczności zwracania się z wnioskami o udzielenie informacji do każdej z instytucji osobno; aplikacja OGNIVO umożliwia uzyskanie przez organy ścigania

informacji o rachunkach we wszystkich bankach komercyjnych, bankach spółdzielczych i SKOK-ach, na podstawie jednego wniosku złożonego przez podmiot uprawniony do banku lub SKOK, dla których korzystanie z centralnej informacji jest obligatoryjne;

- b) skrócenie czasu uzyskania informacji przez organy ścigania poprzez zastąpienie pisemnej korespondencji szybką i bezpieczną elektroniczną wymianą informacji.

W toku prowadzonego postępowania przygotowawczego prokurator może z własnej inicjatywy lub na wniosek Policji złożyć wniosek o udzielenie informacji w zakresie rachunków posiadanych przez osoby mające związek z przestępstwem w wybranym przez siebie banku lub SKOK. Preferowane do złożenia wniosku są te banki, które nie pobierają opłaty za udzielenie informacji. Bank lub SKOK, po przyjęciu wniosku, przeprowadza weryfikację podstawy prawnej udzielenia informacji i wprowadza zapytanie do „Centralnej informacji”, która rozsyła je do wszystkich banków i SKOK-ów w systemie. Podmioty objęte „Centralną informacją” są obowiązane do niezwłocznego udzielenia odpowiedzi, nie później jednak niż w terminie 3 dni roboczych. Kolejno generowana jest zbiorcza informacja zawierająca:

- a) wskazanie podmiotów, które prowadzą lub prowadziły rachunek wraz z numerem tego rachunku;
- b) informację, czy rachunek jest nadal prowadzony;
- c) informację, czy jest to rachunek wspólny;
- d) informację o umowach rachunku bankowego rozwiązanych albo wygasłych z powodu śmierci posiadacza rachunku lub braku dyspozycji związanych z rachunkiem w ciągu ostatnich 10 lat.

Zbiorcza informacja jest przekazywana przez „Centralną informację” do banku lub SKOK, który przyjął wniosek, następnie bank lub SKOK przesyła odpowiedź do prokuratora, który wystąpił z wnioskiem. Informacja nie zawiera danych objętych tajemnicą bankową w zakresie zgromadzonych na rachunku środków i historii operacji. Do wydania postanowienia o zabezpieczeniu majątkowym znana musi być kwota podlegająca zabezpieczeniu oraz wskazać należy numer rachunku, rodzaj rachunku, posiadacza i bank lub SKOK prowadzący rachunek. W konsekwencji po zebraniu informacji o istniejących rachunkach, prokurator lub sąd zgodnie z art. 105 ust. 1 pkt 2 lit. b pr. bankowego występują do ustalonego banku z postanowieniem o zwolnieniu z obowiązku zachowania tajemnicy bankowej w zakresie danych o wysokości środków zgromadzonych na rachunku oraz historii wykonanych operacji. Pozyskane tym sposobem informacje mogą być wykorzystane przez prokuratora do wydania postanowienia o zabezpieczeniu majątkowym.

Opisana procedura nie jest skomplikowana, a w postępowaniu przygotowawczym sporządzenie i przesłanie wniosku do podmiotów objętych aplikacją OGNIVO leży w kompetencji prokuratora, który może zainicjować wystąpienie do „Centralnej informacji” samodzielnie albo na pisemny wniosek Policji. Działania zmierzające do ustalenia rachunku osoby podejrzanej, podejrzanego lub osób powiązanych z przestępstwem znajdują szczególne uzasadnienie, gdy:

- a) w postępowaniu nie ustalono rachunku bankowego podejrzanego, a dokonane zabezpieczenie majątkowe jest niewystarczające lub nie wydano postanowienia o zabezpieczeniu majątkowym z uwagi na brak majątku podlegającego zajęciu;
- b) istnieje podejrzenie, że dotąd nieustalony rachunek osoby podejrzanej czy podejrzanego służył do popełnienia przestępstwa albo gromadzono na nim korzyści z przestępstwa;
- c) ustalenie rachunku osoby podejrzanej, podejrzanego lub osoby mającej związek z przestępstwem jest wymagane ze względu na wartość dowodową;
- d) podyktowane jest to koniecznością zapobieżenia, przeciwdziałania popełnieniu przestępstwa lub ograniczenia jego skutków.

Wprowadzenie aplikacji OGNIVO znacznie ułatwiło organom ścigania pozyskiwanie informacji o rachunkach. Nadal jednak przeprowadzenie czynności zmierzających do zabezpieczenia majątkowego środków zgromadzonych na rachunku sprawcy przestępstwa odbywa się w dwóch etapach. Pierwszy etap to ustalenie rachunku otwartego na daną osobę podejrzaną lub podejrzanego, a drugi etap to wystąpienie do określonego banku o udzielenie informacji dotyczących rachunku i zgromadzonych na nim środków oraz historii operacji. W praktyce w pozyskanie danych w dwóch etapach zaangażowana jest prokuratura, która występuje o informacje z własnej inicjatywy lub na wniosek funkcjonariuszy Policji prowadzących postępowanie przygotowawcze lub profilujących majątkowo podejrzanego.

Po 2015 r. rozpoczęto też prace nad rozwiązaniami wspólnymi — organów ścigania i podmiotów komercyjnych — dotyczącymi systemowego udostępniania informacji finansowych, także dla potrzeb zwalczania przestępczości. Pierwszą propozycją ustawodawczą w zakresie uregulowania możliwości pozyskiwania informacji o rachunkach oraz wykorzystywania tej wiedzy przez uprawnione podmioty na potrzeby zwalczania przestępczości była — przygotowana na początku 2016 r. w Departamencie Informacji Finansowej Ministerstwa Finansów — ustawa o Centralnej Bazie Rachunków. Projekt, ze względu na wielość uwag i potrzebę realizacji zadań związanych z ustawą implementującą Dyrektywę Parlamentu Europejskiego

i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającą rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającą dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (tzw. IV Dyrektywa AML), utrzymany został jedynie na poziomie konsultacji międzyresortowych. W tym samym czasie budowano także system oparty na nowej formacji — KAS, co również wymagało dostosowania przepisów do wykonywania zadań przez organy kontroli celno-skarbowej na podstawie m.in. informacji finansowej. Wcześniej, przed 2015 r., bezskutecznie próbę przygotowania podobnej regulacji podjęło Ministerstwo Spraw Wewnętrznych i Administracji. Prace jednak zarzucono na poziomie projektowania przepisów. Tym samym ostatecznie nie zarzucono prac nad przygotowaniem przepisów o centralnym zbiorze rachunków, a przesunięto je w czasie. Powrócono do tego projektu po zakończeniu prac związanych z wdrożeniem kompleksu przepisów o KAS, zmianą ordynacji podatkowej, głównie w zakresie Systemu Teleinformatycznego Izby Rozliczeniowej (STIR), a także ustawą o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (ustawa o p.p.p.f.t.). Należy dodatkowo zaznaczyć, iż w tym czasie to Szef KAS pełnił jednocześnie funkcję GIIF (art. 53 Ustawy z dnia 16 listopada 2016 r. — Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej, Dz.U. z 2016 r., poz. 1948, 2255; z 2017 r., poz. 379, 1537, 1926, 2409; z 2018 r., poz. 2354).

Zgodnie z treścią projektu ustawy o Centralnej Bazie Rachunków (ustawa o CBR) z 2016 r., podstawowym jej celem było ułatwienie uprawnionym organom ścigania i wymiaru sprawiedliwości lokalizowania składników majątkowych pochodzących z przestępstwa. Ponadto istotą przedmiotowego rozwiązania miało być także umożliwienie szybkiego uzyskania przez komorników sądów i organy egzekucyjne pełnej informacji o potencjalnych miejscach przechowywania przez dłużników wartości majątkowych. Informacje z CBR miały być wykorzystywane na potrzeby realizacji zadań ustawowych sądów, prokuratury, właściwych służb, tj. Policji, Centralnego Biura Antykorupcyjnego, Agencji Bezpieczeństwa Wewnętrznego, Służby Kontrwywiadu Wojskowego, Żandarmerii Wojskowej, Straży Granicznej, Generalnego Inspektora Informacji Finansowej, Krajowej Informacji Skarbowej, organów kontroli skarbowej, organów administracji skarbowej, organów skarbowych, organów celno-skarbowych, organów egzekucyjnych prowadzących egzekucję administracyjną należności pieniężnych, Komisji Nadzoru Finansowego (KNF). Projekt przewidywał, że CBR będzie miała formę systemu teleinformatycznego, w którym będą przetwarzane dane z tzw.

instytucji zobowiązanych (art. 2 pkt 1 projektu ustawy o CBR). Organem właściwym w sprawach CBR (w szczególności odpowiedzialnym za prowadzenie CBR, przetwarzanie w niej informacji, zapewnienie bezpieczeństwa informacji i opracowywanie na ich podstawie analiz statystycznych) miał być ustanowiony minister właściwy do spraw finansów publicznych (art. 3–5).

Ustawa o CBR przewidywała także, że w ramach transparentności działania minister właściwy do spraw finansów publicznych będzie przedkładał prezesowi Rady Ministrów roczne sprawozdanie ze swojej działalności w zakresie CBR, w ciągu 3 miesięcy od zakończenia roku, którego będzie ono dotyczyło. Sprawozdanie po jego przekazaniu prezesowi Rady Ministrów miało być publikowane na stronie podmiotowej Biuletynu Informacji Publicznej urzędu obsługującego ministra właściwego do spraw finansów publicznych (art. 6). Ustawa wprowadzała pojęcie instytucji zobowiązanej. Do instytucji zobowiązanych miały zostać zaliczone wszystkie te instytucje, które udostępniają produkty i usługi umożliwiające gromadzenie, przechowywanie i inwestowanie środków finansowych, przede wszystkim instytucje kredytowe i finansowe działające na podstawie przepisów pr. bankowego, a także SKOK-i wraz z Krajową Spółdzielczą Kasą Oszczędnościowo-Kredytową (art. 2 pkt 2). Ze względu na rozwijający się rynek walut wirtualnych uznano za stosowne włączenie do katalogu instytucji zobowiązanych także prowadzących działalność gospodarczą na terytorium Rzeczypospolitej Polskiej podmiotów oferujących produkty i usługi w zakresie przechowywania danych uwierzytelniających, niezbędnych do uzyskania dostępu do walut wirtualnych, takie jak online portfele umożliwiające przechowywanie adresów walut wirtualnych wraz z kluczami prywatnymi (tzw. *hot storage wallets*), które dają ich posiadaczom dostęp do zgromadzonych jednostek walut wirtualnych i możliwość realizowania transakcji. Te instytucje zobowiązane, które są jednocześnie instytucjami obowiązanyymi w myśl przepisów Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. z 2016 r., poz. 299 z późn. zm.) (w czasie przedkładania projektu ustawy o CBR obowiązywała jeszcze Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu), miały przekazywać do CBR nie tylko informacje o rachunkach umożliwiające identyfikację zarówno ich posiadaczy, jak i pełnomocników do nich, lecz także beneficjentów rzeczywistych posiadaczy rachunków. Poza danymi identyfikującymi podmioty powiązane z rachunkiem, instytucje zobowiązane miały przekazywać podstawowe informacje o samym rachunku, tj. dotyczące: rodzaju rachunku, daty jego otwarcia i zamknięcia, okresu, na jaki rachunek został otwarty, a także kodu waluty, w której księgowane są transakcje na rachunku. Projektowane przepisy zakładały,



że informacje o rachunkach będą przekazywane do CBR w ciągu 24 godzin roboczych od otwarcia rachunku, zamknięcia rachunku lub zmiany informacji o rachunku (art. 9). Miało to umożliwić dostęp do relatywnie aktualnych danych, a jednocześnie dać czas instytucjom zobowiązanym na przekazanie tych informacji. Ponadto instytucje zobowiązane miały przekazać do CBR, w terminie 30 dni od dnia wejścia w życie ustawy, informację o rachunkach prowadzonych na dzień poprzedzający wejście w życie ustawy (art. 31).

Zakładano, że informacje o rachunkach będą udostępniane wyłącznie organom i jednostkom wskazanym w ustawie, tzw. podmiotom uprawnionym, w celu wykorzystania do realizacji ich zadań ustawowych (art. 12). Miały one przekazywać udostępnione im informacje o rachunkach także za granicę, lecz jedynie w przypadku, jeśli będzie to konieczne do zapobiegania przestępstwom, do prowadzenia dochodzeń w ich sprawie, do ich wykrywania lub ścigania albo do wykonywania kar, na zasadach określonych w odrębnych ustawach, np. w zakresie, w jakim jest to konieczne do realizacji wniosku o pomoc z zagranicy, czy udzielenia odpowiedzi w związku z realizacją przepisów Ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (Dz.U. poz. 1371 z późn. zm.). Wobec wszystkich podmiotów uprawnionych — z wyjątkiem komorników sądowych i administracyjnych organów egzekucyjnych oraz centralnego biura łącznikowego, o którym mowa w Ustawie z dnia 11 października 2013 r. o wzajemnej pomocy przy dochodzeniu podatków, należności celnych i innych należności pieniężnych — określono, że przekazywany będzie pełny zakres informacji o rachunkach (art. 13). GIIF miała być udostępniana kopia informacji o rachunkach CBR lub ich podzbiór w terminie i formie ustalonych w porozumieniu z organem właściwym (art. 14). Rozwiązanie to miało umożliwić porównanie informacji o rachunkach z informacjami o transakcjach, gromadzonymi przez GIIF, a tym samym poszerzyć możliwości prowadzenia analiz przez GIIF. Niemniej, jak wskazano, wobec znacznej liczby negatywnych opinii otrzymanych w ramach uzgodnień międzyresortowych oraz informacji od podmiotów pozaresortowych, a także podjęcia prac nad nową ustawą o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, zaprzestano dalszych etapów prac legislacyjnych. Jak wykazały inicjatywy podjęte w kolejnych latach przez UE, kierunek tych rozwiązań był jak najbardziej właściwy. Zwłaszcza w tym zakresie istotne okazały się rozwiązania zawarte w dyrektywie UE 2019/1153, w której ustanowiono zasady korzystania z informacji finansowych oraz centralnych baz danych informacji o rachunkach.

W tym czasie sama UE dostrzegła potrzebę wzmocnienia współpracy w zakresie korzystania z informacji finansowych i innych w celu zapobiegania

niektórym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie (Wniosek: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1193 z dnia 20 czerwca 2019 r. ustanawiająca zasady ułatwiające korzystanie z informacji finansowych i innych informacji w celu zapobiegania niektórym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania oraz uchylająca decyzję Rady 2000/642/WSiSW, 17.04.2018, COM(2018) 213 final, Dz. Urz. UE L 186/122 z 11.7.2019). Jednocześnie wskazano, że: aktualnie informacje finansowe są istotne dla prowadzenia dochodzeń w sprawie poważnych przestępstw. Brak informacji finansowych może spowodować, iż niewykorzystane pozostaną możliwości zbadania poważnych przestępstw, przerwania działalności przestępczej, zatrzymania planów ataków terrorystycznych oraz wykrywania i zamrożenia korzyści pochodzących z przestępstwa. Brak informacji na temat wszystkich rachunków należących do podejrzanego może prowadzić do jedynie częściowego zabezpieczenia mienia, stanowiąc ostrzeżenie dla podejrzanego, który może usunąć niewykryte środki z innych rachunków. Wiele postępowań zakończyło się fiaskiem, ponieważ nie udało się zapewnić terminowego, dokładnego i kompleksowego dostępu do odpowiednich danych finansowych. Stało się więc oczywiste, że aby zwiększyć bezpieczeństwo, skuteczniej ścigać przestępstwa finansowe, zwalczać pranie pieniędzy oraz zapobiegać przestępstwom skarbowym w państwach członkowskich i w całej Unii, konieczna jest poprawa dostępu do informacji, jaki mają jednostki analityki finansowej i organy publiczne odpowiedzialne za zapobieganie poważnym przestępstwom, ich wykrywanie, prowadzenie dochodzeń w ich sprawie lub ściganie ich, tak aby zwiększyć ich zdolność do prowadzenia dochodzeń finansowych i poprawić współpracę między nimi (M.W. Płachta, *Ochrona bezpieczeństwa finansowego w Unii Europejskiej: wybrane zagadnienia*, „Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa” 2019, nr 4(45), s. 32).

Ustawa o SIiF ma na celu wykonanie prawa europejskiego. W komunikacie w sprawie planu działania na rzecz skuteczniejszego zwalczania finansowania terroryzmu (Komunikat Komisji do Parlamentu Europejskiego i Rady z dnia 2 lutego 2016 r. w sprawie planu działania na rzecz skuteczniejszego zwalczania finansowania terroryzmu, COM(2016)050 final, EUR-Lex-52016DC0050) Komisja UE zobowiązała się do zbadania możliwości opracowania odrębnego aktu prawnego w celu rozszerzenia dostępu do scentralizowanych rejestrów rachunków bankowych i rachunków płatniczych przez organy państw członkowskich, w tym przez organy odpowiedzialne za zapobieganie przestępstwom, ich wykrywanie, prowadzenie dochodzeń w ich sprawie lub ich ściganie, biura ds. odzyskiwania mienia, organy podatkowe i organy antykorupcyjne. Ponadto w tym planie działań

wezvano również do wskazania przeszkód w dostępie do informacji, wymianie i wykorzystywaniu tych informacji, a także do współpracy operacyjnej między jednostkami analityki finansowej (JAF). Państwa członkowskie UE zobowiązane były do przeniesienia do krajowych systemów prawnych dwóch dyrektyw Parlamentu Europejskiego i Rady Unii Europejskiej. Przedmiotowe dyrektywy to:

- a) Dyrektywa 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz
- b) Dyrektywa 2019/1153 z dnia 20 czerwca 2019 r. ustanawiająca zasady ułatwiające korzystanie z informacji finansowych i innych informacji w celu zapobiegania niektórym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania.

Zgodnie z pierwszym aktem prawnym, każde państwo członkowskie zostało zobowiązane do ustanowienia scentralizowanego rejestru lub systemu wyszukiwania danych, który miał umożliwić szybką identyfikację dowolnej osoby fizycznej lub prawnej, posiadającej lub kontrolującej rachunki płatnicze, rachunki bankowe i skrytki depozytowe. W tym zakresie ustawa o SInF stanowi przede wszystkim efekt wyzwania prawnego mającego na celu implementację art. 1 pkt 19, art. 1 pkt 25 lit. b i art. 1 pkt 42. Natomiast dyrektywa 2019/1153 m.in. zobowiązywała państwa członkowskie UE do wyznaczenia organów krajowych właściwych w sprawach zapobiegania przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania, które powinny mieć dostęp do informacji przechowywanych w takim scentralizowanym rejestrze/systemie wyszukiwania danych. Stosując przepisy dotyczące dostępu, należy wykorzystać istniejące wcześniej mechanizmy, pod warunkiem że JAF będą miały natychmiastowy dostęp do danych, których dotyczy ich zapytanie, z zachowaniem ich pierwotnej formy i treści. Państwa członkowskie powinny rozważyć, w ramach tego ustawodawstwa, możliwość wprowadzenia do takich mechanizmów innych informacji, które zostaną uznane za konieczne i proporcjonalne w celu skuteczniejszego ograniczania zagrożeń związanych z praniem pieniędzy i finansowaniem terroryzmu. Należało zapewnić zachowanie pełnej poufności w odniesieniu do takich zapytań i wniosków o udostępnienie powiązanych informacji kierowanych przez JAF i właściwe organy, inne niż organy ścigania (pkt 20 preambuły dyrektywy 2018/843). W konsekwencji miano zapewnić poszanowanie prywatności i ochronę danych osobowych. W scentralizowanych automatycznych mechanizmach przewidzianych dla rachunków bankowych i płatniczych, takich jak rejestry lub systemy wyszukiwania danych, powinna być przechowywana minimalna ilość danych niezbędnych do prowadzenia

dochodzeń w zakresie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu. Państwa członkowskie powinny więc mieć możliwość określenia danych, których gromadzenie jest przydatne i proporcjonalne w celu umożliwienia miarodajnej identyfikacji beneficjentów rzeczywistych, przy uwzględnieniu istniejących systemów i tradycji prawnych (pkt 21 preambuły dyrektywy 2018/843).

Wobec treści dyrektywy 2019/1153 uznano, że — aby zwiększyć bezpieczeństwo, skuteczniej ścigać przestępstwa finansowe, zwalczać pranie pieniędzy oraz zapobiegać przestępstwom skarbowym w państwach członkowskich i w całej UE — konieczna jest poprawa dostępu do informacji, jaki mają JAF i organy publiczne odpowiedzialne za zapobieganie poważnym przestępstwom, ich wykrywanie, prowadzenie dochodzeń w ich sprawie lub ściganie ich, tak aby zwiększyć ich zdolność do prowadzenia dochodzeń finansowych i poprawić współpracę między nimi (pkt 2 preambuły dyrektywy 2019/1153). Sprawcy przestępstw, w szczególności grupy przestępcze i terroryści, działają w różnych państwach członkowskich, a ich aktywa, w tym rachunki bankowe, znajdują się często w innych państwach członkowskich. Ze względu na transgraniczny wymiar poważnych przestępstw, w tym terroryzmu, oraz związanych z nimi działań finansowych, często konieczne jest, aby właściwe organy prowadzące postępowania przygotowawcze w jednym państwie członkowskim miały dostęp do informacji o rachunkach bankowych prowadzonych w innych państwach członkowskich (pkt 12 preambuły dyrektywy 2019/1153).

Jak wskazano w uzasadnieniu do projektu ustawy o SInF, w aktualnym stanie prawnym (2021) nie istniały przepisy umożliwiające szybkie i sprawne uzyskanie informacji o rachunkach prowadzonych dla osób i podmiotów powiązanych z poważną przestępczością (obszar ten dotyczy m.in. terroryzmu, przestępczości zorganizowanej, działalności związanej z praniem pieniędzy, ale brakuje w tym zakresie „przestępstw skarbowych”). Dlatego organy publiczne w celu pozyskania pełnej informacji na powyższy temat zmuszone były do prowadzenia czasochłonnych i kosztownych działań, w tym korespondencji z licznymi instytucjami funkcjonującymi na rynku finansowym lub korzystania z płatnych rozwiązań komercyjnych, tj. z centralnej informacji o rachunkach działającej przy KIR S.A. Aby ułatwić i przyspieszyć ich działania, powinien zostać utworzony System Informacji Finansowej.

Ustawa o SInF nie definiuje pojęcia „informacji finansowej”, mimo że o ich systemie stanowi. Definiuje natomiast pojęcie „informacji rejestrowanej” jako informacji o rachunkach i niektórych umowach oraz pojęcie „przetwarzania informacji” oznaczające wszelkie operacje wykonywane na informacjach o rachunkach, w szczególności ich zbieranie, utrwalanie,

organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Tym samym zrezygnowano z szerokiej definicji informacji finansowej, a sprecyzowano zakres informacyjny, jaki funkcjonuje w Systemie Informacji Finansowej. Ustawodawca z jednej strony nie chciał wprost zawrzeć definicji, może dlatego, że obawiał się możliwości zbytowego jej ograniczenia. Z drugiej strony mógł zdawać sobie sprawę z tego, że dany rachunek, który tu wydaje się jednak określeniem głównym, podlega w czasie różnym modyfikacjom. Tym samym zakres informacji niejako „podwieszony” został pod dany rachunek i elastycznie będzie ulegał zmianie. Ponadto, jak wskazał projektodawca, w ustawie o SInF zdefiniowano przetwarzanie informacji, który to termin w związku z obowiązującymi przepisami dotyczącymi ochrony danych osobowych wymaga precyzyjnego określenia ustawowego, zwłaszcza w zakresie odpowiedzialności za zarządzanie informacją, ale także na potrzeby określenia pojęcia „informacji finansowej”.

Sam system SInF ma służyć: 1) przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu; 2) wykrywaniu poważnego przestępstwa lub prowadzeniu postępowania karnego w sprawie poważnego przestępstwa, a także w celu identyfikacji, wykrycia lub zabezpieczenia mienia pochodzącego z takiego przestępstwa; 3) innym celom określonym w ustawie. Inne cele, o których mowa w art. 2 ust. 1 pkt 3 ustawy o SInF, to np. przyspieszenie i usprawnienie postępowań sprawdzających i postępowań bezpieczeństwa przemysłowego (cel wskazany w art. 19 ust. 3 ustawy o SInF), przyspieszenie i usprawnienie postępowań kontrolnych dotyczących oświadczeń majątkowych (cel wskazany w art. 19 ust. 4 ustawy o SInF) czy też realizacja zadań ustawowych Szefa KAS w zakresie ujawniania i odzyskiwania mienia zagrożonego przepadkiem, rozpoznawanie, wykrywanie i zwalczanie przestępstw oraz przestępstw skarbowych, zapobieganie tym przestępstwom oraz ściganie ich sprawców (cel wskazany w art. 19 ust. 2 ustawy o SInF). Jest ona więc bardziej ustawą o przetwarzaniu informacji o rachunkach niż informacji finansowych, które posiadają znacznie szerszy zakres i nie sprowadzają się wyłącznie do informacji związanych tylko z rachunkami.

Ponadto należałoby zwrócić uwagę na dość specyficzne podejście do stosowania ustawy wychodzące poza zakres określony w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniającej dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniającej dyrektywy 2009/138/WE i 2013/36/UE (dotyczy to zadań

określonych w art. 2 ust. 1 pkt 2 i 3 oraz w art. 19 ust. 2–4 projektu ustawy o SInF). Wskazanie w ustawie o SInF, iż organem właściwym w sprawach SInF jest Szef KAS, powoduje, że GIIF będzie jedynie jednym z odbiorców informacji nie zaś podmiotem administrującym i nadzorującym, ale także kreującym ten zakres bezpieczeństwa finansowego. Na podstawie art. 18 bowiem informacje o rachunku zgromadzone w SInF będą niezwłocznie, w całości, przekazywane GIIF. Z punktu widzenia analizy informacji finansowej priorytetem pozostaje, aby GIIF otrzymywał te informacje w sposób systematyczny, uporządkowany i z zakresu tych informacji można było wywieść atrybuty umożliwiające dokonanie oceny, czy i w jakim zakresie (przedmiotowym i podmiotowym) prowadzony był proceder prania pieniędzy czy finansowania terroryzmu. Ta odrębność GIIF wynika z potrzeby wdrożenia zapisów z art. 32a dyrektywy 2015/849 w brzmieniu nadanym przez dyrektywę 2018/843, iż informacje rejestrowane mają być dostępne dla JAF „z zachowaniem ich pierwotnej formy i treści”, co należy rozumieć jako dostęp „do całości” danych zgromadzonych w SInF.

Zakres uprawnień GIIF różni się od zakresu uprawnień do uzyskiwania danych zgromadzonych w SInF przez inne podmioty, jako podmioty uprawnione, o których mowa w art. 19 ust. 2 ustawy o SInF. Informacje rejestrowane, które mają być przekazywane i przechowywane w SInF, pozostają nacechowane wieloma atrybutami, które będzie można wykorzystać do kojarzenia podmiotów i zdarzeń w zakresie analiz prowadzonych zarówno na poziomie JAF, jak i jednostek współpracujących w systemie AML/CFT. To kolejne uzupełnienie informacyjne danych, na podstawie których będzie można prowadzić analizy operacyjne czy finansowe w JAF. Ponadto częściowa odmienność instytucji zobowiązanych (ustawa o SInF) wobec instytucji obowiązanych (ustawa o p.p.p.f.t.) poszerza zakres podmiotowy instytucji, od których będzie można te dane pozyskiwać.

Należy zauważyć, że ustawa o SInF zwiększa możliwości samego systemu AML/CFT. Dotychczas funkcjonujące rozwiązania bazują na ocenie ryzyka i analizie realizowanej przez instytucje obowiązane, w wyniku których JAF otrzymuje raporty jako SAR (ang. Suspicious Activity Report). W przypadku polskiego systemu AML/CFT są to raporty dotyczące informacji o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu (art. 74 ustawy o p.p.p.f.t.). Ponadto do GIIF kierowane są zawiadomienia z instytucji obowiązanych o przypadku powzięcia uzasadnionego podejrzenia, że określona transakcja lub określone wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu (art. 86 ustawy o p.p.p.f.t.). Jednocześnie GIIF otrzymuje informacje o tzw. transakcjach ponadprogowych.

Jednakże, jak wskazano w Strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (Uchwała nr 50 Rady Ministrów z dnia 19 kwietnia 2021 r. w sprawie przyjęcia Strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, M.P. z 2021 r., poz. 435) tego rodzaju informacje — z tzw. transakcji ponadprogowych — są niezwykle przydatne przy szybkim opracowywaniu analiz operacyjnych w odniesieniu do powziętych podejrzeń prania pieniędzy lub finansowania terroryzmu w celu podjęcia niezwłocznych decyzji co do zastosowania instrumentów prawnych przewidzianych przepisami ustawy o p.p.p.f.t. czy też prowadzeniu analiz strategicznych.

Sam obowiązek gromadzenia informacji o tzw. transakcjach ponadprogowych nie wynika z przepisów dyrektywy 2015/849. Wysokość progu mającego zastosowanie do raportowania transakcji jest różny w różnych państwach członkowskich. W niektórych krajach progi te są stosunkowo wysokie i w rezultacie utrudnia to skuteczny monitoring transakcji. Ustalenie stosunkowo niskiego progu wysokości transakcji podlegających raportowaniu ma znaczenie zwłaszcza w przypadku transakcji gotówkowych, gdy wysoki próg transakcyjny może być nieskuteczny jako narzędzie przeciwko praniu pieniędzy poprzez dokonywanie przez sprawców mniejszych, podprogowych transakcji rozłożonych w czasie. Wysoki próg transakcyjny może też mieć wpływ na zwiększone ryzyko prania pieniędzy oraz finansowania terroryzmu związane przede wszystkim z anonimowością przeprowadzanych transakcji, realizowanych często właśnie tuż poniżej tego progu. Informacje o transakcjach gotówkowych pozwalają też na pozyskanie wiedzy o środkach wpływających oraz wycofywanych z systemu finansowego (Strategia przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu [w:] Uchwała nr 50 Rady Ministrów z dnia 19 kwietnia 2021 r. w sprawie przyjęcia Strategii przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, s. 17–18). System SInF pozwala więc na zastosowanie alternatywnego, ale i uzupełniającego przeciwdziałania nakierowanego na ustalony podmiot podejrzany poprzez precyzyjne wskazanie gdzie, ile i jakie rodzaje rachunków/umowy skrytek seifowych posiada on w całości bazy wiedzy instytucji zobowiązanych. Takie podejście znacząco uzupełnia dotychczasowe zadania realizowane przez JAF i umożliwia skuteczne i precyzyjne podejmowane działań wobec podejrzewanych podmiotów. W konsekwencji system AML/CFT oparty jest na analizie ryzyka, regułach transakcji ponadprogowych i precyzyjnym budowaniu analizy informacji finansowej przy wykorzystaniu SInF z poziomu JAF i jednostek współpracujących (podmiotów uprawnionych).

Jedną z podstawowych taktyk przeciwdziałania przestępczości, w tym w jej formie zorganizowanej, jest niedopuszczenie do konsumpcji zysku otrzymanego w sposób niezgodny z prawem oraz uzyskania statusu jego

legalizacji. Aktualnie organy ścigania i podmioty AML/CFT musiały wdrażać powielane i skomplikowane procedury ustaleniuowe celem pozyskania wiedzy o rachunkach prowadzonych dla osób i podmiotów mających powiązania z przestępczością zorganizowaną (PZ). W szczególności niezbędne było prowadzenie szerokiej korespondencji z podmiotami, które, świadcząc określonego rodzaju usługi, mogły deponować (nawet nieświadomie) środki finansowe i inne aktywa pochodzące z przestępstw. Taki stan rzeczy znacząco przedłużał prowadzenie czynności służbowych, także w ramach prowadzonych postępowań karnych. SInF, z którego będą mogły korzystać organy ścigania na potrzeby nie tylko krajowe, lecz także wymiany międzynarodowej pozwala na skrócenie procedur oraz bardziej precyzyjne działanie (np. zabezpieczenie środków na potrzeby konfiskaty) wobec aktywów wygenerowanych przez przestępców i deponowanych na rachunkach bankowych czy w skrytkach sejfowych.

Ustawa o SInF przewiduje również wprowadzenie zmian w innych aktach prawnych rangi ustawy. Tym samym zaproponowano wprowadzenie do ustawy o p.p.p.f.t. nowych definicji, w tym definicji informacji finansowej, przez którą rozumie się informacje dotyczące wartości majątkowych, transakcji i stosunków gospodarczych, będące w posiadaniu GIIF, zgromadzone na podstawie ustawy o p.p.p.f.t. W uzasadnieniu do projektu wskazano, że konieczność zdefiniowania „informacji finansowej” wiąże się z potrzebą określenia zakresu informacji podlegających wymianie na podstawie przepisów implementujących dyrektywę 2019/1153. Nieprecyzyjne lub zbyt wąskie określenie zakresu informacji podlegających wymianie na podstawie postanowień dyrektywy 2019/1153 mogłoby się wiązać ze sformułowaniem zarzutów nieprawidłowej implementacji przepisów Unii Europejskiej. Konieczne stało się więc dodanie do ustawy o p.p.p.f.t. definicji informacji finansowej wprost wynikającej z niniejszej dyrektywy.

W konsekwencji można wskazać, że idea powstania i funkcjonowania systemu SInF posiada dwa główne cele: wzmocnienie i uzupełnienie funkcjonowania dotychczasowego systemu AML/CFT oraz zwiększenie skuteczności rozpoznawania, ścigania i karania najpoważniejszych przestępstw, jakie zostały określone w szeroko rozumianym systemie prawa karnego.

Ustawa:

1) w zakresie swojej regulacji wdraża:

- Dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniającą dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniającą dyrektywy 2009/138/WE i 2013/36/UE (Dz. Urz. UE L 156/43 z 19.06.2018),



- Dyrektywę Rady (UE) 2021/514 z dnia 22 marca 2021 r. zmieniającą dyrektywę 2011/16/UE w sprawie współpracy administracyjnej w dziedzinie opodatkowania (Dz. Urz. UE L 104/1 z 25.03.2021);
- 2) wdraża także Dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1153 z dnia 20 czerwca 2019 r. ustanawiającą zasady ułatwiające korzystanie z informacji finansowych i innych informacji w celu zapobiegania niektórym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania oraz uchylającą decyzję Rady 2000/642/WSiSW (Dz. Urz. UE L 186/122 z 11.07.2019);
  - 3) służy stosowaniu Rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczącego dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczenia Nadużyć Finansowych (OLAF) oraz uchylającego rozporządzenie (WE) nr 1073/1999 Parlamentu Europejskiego i Rady i rozporządzenie Rady (Euratom) nr 1074/1999 (Dz. Urz. UE L 248/1 z 18.09.2013; Dz. Urz. UE L 317/1 z 23.11.2016 oraz Dz. Urz. UE L 437/49 z 28.12.2020).

Ponadto zmieniają się następujące ustawy: z dnia 29 sierpnia 1997 r. — Ordynacja podatkowa (OP); z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi; z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym; z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych; z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, państw trzecich, agencjami Unii Europejskiej oraz organizacjami międzynarodowymi; z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej oraz z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Dla zmian wprowadzonych w OP istotne jest to, że izba rozliczeniowa, na której technicznych rozwiązaniach opierał się dotychczasowy system przeciwdziałający przestępczości podatkowej, czyli STIR (System Teleinformatyczny Izby Rozliczeniowej), i która będzie realizowała SInF, uzyskała także dodatkowe możliwości świadczenia usług na rzecz instytucji obowiązanych w zakresie oceny ryzyka AML/CFT, o którym mowa w ustawie o p.p.p.f.t. W celu ustalenia wskaźnika ryzyka izba rozliczeniowa będzie mogła przetwarzać informacje rejestrowane z systemu SInF także w celu: stosowania przez izbę rozliczeniową środków bezpieczeństwa finansowego oraz prowadzenia i dokumentowania wyników bieżącej analizy przeprowadzanych transakcji, o której mowa w art. 43 ust. 3 ustawy o p.p.p.f.t., na podstawie umowy, o której mowa w art. 48 ust. 1 ustawy o p.p.p.f.t., zawartej z bankiem, SKOK lub instytucją zobowiązaną, o której mowa w ustawie o SInF.

Projekt ustawy został przekazany do uzgodnień w lipcu i październiku 2021 r. Komitet ds. Europejskich przyjął projekt ustawy o SInF 6 grudnia

2021 r. Projekt został przyjęty na posiedzeniu Stałego Komitetu Rady Ministrów 23 czerwca 2022 r. Po posiedzeniach Komisji Prawniczej, kolejny, nowy, tekst projektu ustawy o SInF z 16 września 2022 r. został przygotowany w celu zatwierdzenia przez Stały Komitet Rady Ministrów. Zgodnie z Protokołem ustaleń nr 47/2022 z posiedzenia Rady Ministrów w dniu 8 listopada 2022 r. — Rada Ministrów zdecydowała o skierowaniu dokumentu do Sejmu, deklarując, że ma on na celu wykonanie prawa UE, i upoważniła ministra finansów do prezentowania stanowiska rządu w tej sprawie w toku prac parlamentarnych. Projekt ustawy wpłynął do Sejmu 10 listopada 2022 r. (druk sejmowy nr 2771). 1 grudnia 2022 r. Komisja Finansów Publicznych, po rozpatrzeniu poprawek zgłoszonych do projektu ustawy, przyjęła projekt i wniosła o jego uchwalenie przez Sejm w brzmieniu zaproponowanym w dodatkowym sprawozdaniu (druk sejmowy nr 2818–A). Sejm uchwalił ustawę na 67. posiedzeniu 1 grudnia 2022 r.

Ustawa o SInF, po zakończeniu procesu legislacyjnego w Sejmie i Senacie RP (Senat podjął uchwałę o odrzuceniu ustawy na posiedzeniu 15 grudnia 2022 r.), została podpisana przez prezydenta 23 stycznia 2023 r., a jej ogłoszenie nastąpiło 26 stycznia 2023 r. Kolejno dokonano publikacji ustawy o SInF w Dzienniku Ustaw nr 180 z 2023 r. Ustawa o SInF weszła w życie z dniem 10 lutego 2023 r. Akt wykonawczy do przedmiotowej ustawy w postaci rozporządzenia został wydany 9 grudnia 2023 r. — Rozporządzenie Ministra Finansów z dnia 9 grudnia 2023 r. w sprawie elektronicznej wymiany danych z Systemu Informacji Finansowej (Dz.U. z 2023 r., poz. 2774).

# Rozdział 1

## Przepisy ogólne

### 1. Zakres regulacji ustawy o SInF

**Art. 1. Ustawa określa zasady funkcjonowania Systemu Informacji Finansowej, zwanego dalej „SInF”, w tym: 1) instytucje zobowiązane do przekazywania informacji do SInF; 2) organ właściwy w sprawach SInF; 3) zakres informacji przekazywanych do SInF; 4) podmioty uprawnione do uzyskiwania informacji zgromadzonych w SInF; 5) zasady przetwarzania informacji zgromadzonych w SInF; 6) zasady ochrony informacji przetwarzanych w SInF.**

- 1.1. Powołana w ustawie o SInF dyrektywa 2019/1153 ustanowiła środki ułatwiające właściwym organom dostęp do informacji finansowych i informacji o rachunkach bankowych oraz korzystanie z tych informacji w celu zapobiegania poważnym przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania. Przedmiotowa dyrektywa ustanowiła również środki, które mają ułatwiać JAF dostęp do informacji z zakresu egzekwowania prawa do celów zapobiegania praniu pieniędzy, powiązanych z nim przestępstwom źródłowym i finansowaniu terroryzmu oraz zwalczania tych zjawisk, a także środki mające ułatwiać współpracę między JAF (art. 1 ust. 1 dyrektywy 2019/1153). Podobnie ustawa o SInF określiła w swojej treści zasady funkcjonowania Systemu Informacji Finansowej, implementując tym samym postanowienia dyrektywy (art. 1 pkt 1–6 ustawy o SInF).
- 1.2. Zgodnie z definicją słownikową (<<https://www.sjp.pwn.pl/slowniki/zasady.html>>) zasada to: 1. prawo rządzące jakimiś procesami, zjawiskami; też: formuła wyjaśniająca to prawo; 2. norma postępowania; 3. ustalony na mocy jakiegoś przepisu lub zwyczaju sposób postępowania w danych okolicznościach; 4. podstawa

funkcjonowania lub konstrukcji czegoś. Realizacja celów i zadań jest postrzegana poprzez zasady rządzące procesami decyzyjnymi i celami strategicznymi realizowanymi w ramach systemu SInF.

- 1.3. Ustawa o SInF określa więc zasady funkcjonowania tego systemu, w tym określa instytucje zobowiązane, których obowiązkiem jest przekazywanie informacji do SInF, oraz podmioty uprawnione do ich uzyskiwania z systemu. Ponadto określa organ właściwy w sprawach związanych z SInF oraz zakres informacji, jakie mają być przekazywane do systemu. Jednocześnie określa zasady przetwarzania informacji zgromadzonych w przedmiotowym systemie oraz zasady ochrony tych informacji.
- 1.4. Wskazane w pkt 1–6 zasady nie stanowią zamkniętego zbioru zasad, na co wskazuje zapis: „w tym”, który dopuszcza możliwość regulacji w treści ustawy także innych zasad, jakimi ma kierować się SInF.
- 1.5. W toku prac nad projektem ustawy o SInF opinią Rady Legislacyjnej (RL), wskazano, że: „system” pozwala pozyskać dane (wiedzę o rachunku), ale już nie przewiduje metody szybkiego wykorzystania pozyskanych danych, m.in. w celu zabezpieczenia mienia. W trakcie opiniowania projektu ustawy przez RL podniesiono argument, iż taki moduł w „systemie” jest niezbędny, aby w pełni zrealizować cele ustawy. Ostatecznie jednak — po szczegółowym rozważeniu tego zagadnienia — RL podkreśliła, że celem opiniowanego projektu nie jest stworzenie technicznych instrumentów służących do zabezpieczenia mienia, lecz stworzenie optymalnych warunków do tego, aby taka decyzja mogła zostać podjęta w toku postępowania karnego przez uprawniony organ. Do tego niezbędne jest uzyskanie informacji o rachunku w rozumieniu art. 3 pkt 8 projektu ustawy. Dopiero po uzyskaniu takiej informacji możliwe jest podjęcie we właściwym trybie decyzji w przedmiocie zabezpieczenia mienia, np. w ramach zabezpieczenia majątkowego. Rozwiązania przyjęte w projekcie opiniowanej ustawy dostarczyć mają zatem niezbędnych informacji, aby taka decyzja mogła zostać podjęta, nie jest natomiast ich celem tworzenie „modułu”, który mógłby być wykorzystywany do faktycznego zabezpieczania mienia. Taki wniosek jednoznacznie wynika z art. 1 projektu ustawy. Dodatkowo należy podnieść, że z art. 2 projektu ustawy jednoznacznie wynika, że „system” służy nie do „zabezpieczania mienia”, lecz

do „zabezpieczenia mienia”. Tym samym „system” tworzy warunki do tego, aby mienie pochodzące z przestępstwa mogło być zabezpieczone, nie jest natomiast instrumentem zabezpieczającym, tj. nie służy samemu zabezpieczeniu mienia. Samo fizyczne (czy też faktyczne) zabezpieczanie mienia odbywa się na podstawie innych — procesowych — przepisów, przy wykorzystaniu odpowiednich instrumentów prawnych, adekwatnych do charakteru danej instytucji prawnej (Opinia Rady Legislacyjnej przy Prezesie Rady Ministrów z 22 stycznia 2021 r. o projekcie ustawy o Systemie Informacji Finansowej, syg. RL-033-1/21).

- 1.6. **Zasada określenia zakresu podmiotowego SInF** — związana jest z potrzebą ścisłego określenia przez ustawodawcę zakresu podmiotów zobowiązanych do przekazywania informacji do SInF. Zasada ta nie tylko jest ważna dla tego, kto ma realizować ten obowiązek ustawowy, lecz także dla podmiotu, który będzie podlegał kontroli ze względu na nierealizowanie tego obowiązku. W konsekwencji realizowania tej „zasady” instytucja zobowiązana musi stworzyć w ramach swoich rozwiązań organizacyjnych wewnętrzny system przekazywania informacji zgodny z przepisami ustawy o SInF.
- 1.7. Ustawa odnosi się do realizowania obowiązków przez instytucje zobowiązane, których katalog został także określony w niniejszej ustawie (art. 3 pkt 2). Ustawodawca świadomie wprowadził określenie „instytucji zobowiązanej” wobec już funkcjonującej „instytucji obowiązanej”, której zdefiniowanie nastąpiło w ustawie o p.p.p.f.t. Wyróżnienie to jest o tyle istotne, iż zarówno instytucje zobowiązane, jak i obowiązane posiadają część wspólną, a ponadto zarówno ustawa o SInF, jak i ustawa o p.p.p.f.t. za cel przyjmują także przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu. W obu aktach prawnych odmiennie określono też obowiązki tych różnych kategorii podmiotów. Tym samym niezbędne było w ustawie SInF nie tylko wprowadzenie pojęcia „instytucji zobowiązanej”, lecz także wyznaczenie jej zakresu.
- 1.8. **Zasada ustanowienia organu właściwego w sprawach SInF** — zasada ta została rozbudowana w rozdziale 2 ustawy o SInF i posiada kluczowe znaczenie dla funkcjonowania całości SInF, głównie z tego powodu, że jest to system scentralizowany i wymagający administrowania także wobec zarządzania danymi obywateli i ochrony danych osobowych. Jako organ właściwy

został ustanowiony Szef KAS. Należy zauważyć, że wybór ten miał zwłaszcza podstawy w strukturze technicznej przepływu danych, ponieważ do przesyłu danych — informacji rejestrowanych — ma być wykorzystany system STIR, który już jest wykorzystywany na potrzeby Szefa KAS ze względu na przeciwdziałanie przestępczości podatkowej. STIR ma być także przygotowany na potrzeby przekazywania danych rejestrowanych w ramach SInF. Konsekwentnie w ramach tej zasady organ właściwy jest także administratorem danych zgromadzonych w SInF (art. 6 ustawy o SInF). Należy zauważyć, że aby Szef KAS zaistniał jako organ właściwy w SInF, nie jest konieczny dodatkowy „wybór”; organ ten pełni funkcję organu właściwego automatycznie, wykonując zadania z ustawy szczególnej.

- 1.9. **Zasada określenia zakresu informacji, jakie mają być przekazywane do SInF** — zasada odnosi się do obowiązku przekazywania informacji przez instytucje zobowiązane do SInF i stanowi, że zakres tych informacji jest ustawowo określony przez zdefiniowanie informacji rejestrowanej (art. 4, art. 10 ustawy o SInF). Ponadto zasadę tę można wywnioskować ze zdarzeń, które mają być podstawą do przekazania tych informacji (art. 11 ustawy o SInF) oraz ze struktury danych, jakie mają wchodzić w skład informacji rejestrowanej (art. 12 ustawy o SInF).
- 1.10. **Zasada określenia podmiotów uprawnionych do uzyskiwania informacji zgromadzonych w SInF** — zasada ta jest wynikiem określenia celów, jakim służy gromadzenie danych w SInF, wskazanych w art. 2 ustawy o SInF, a w konsekwencji — jak wykorzystywane są informacje zgromadzone w tym systemie (rozdział 4). Określenie podmiotów, ze względu na ich rolę, zadania, obowiązki i realizowane czynności wynikające z przepisów kompetencyjnych, czyni je pretendentami do korzystania z informacji rejestrowanej. Niemniej, co do zasady, ich podmiotowość i zakres możliwości skorzystania z tych informacji został uregulowany w ustawie o SInF. Tym samym można wyróżnić trzy kategorie uprawnionych podmiotów, wobec których zasada wskazana w art. 1 pkt 4 funkcjonuje odpowiednio co do zakresu posiadanego uprawnienia. Te trzy kategorie podmiotów uprawnionych zostały wskazane w art. 18, 19 i 20 ustawy o SInF. W artykułach tych umieszczono generalne zasady uzyskiwania informacji, a uszczegółowiono je w art. 21–28 ustawy o SInF.

- 1.11. **Zasady przetwarzania informacji zgromadzonych w SInF** — zasady te określone są w art. 27–28 ustawy o SInF. Informacje rejestrowane przetwarzane w celach określonych w ustawie podlegają zabezpieczeniu przed nadużyciami lub niezgodnym z prawem dostępem lub przekazywaniem. Jednocześnie w ustawie umieszczono delegację dla przepisu wykonawczego ministra właściwego do spraw finansów publicznych, w którym powinien określić: minimalne wymagania techniczne, których spełnienie jest niezbędne do prowadzenia elektronicznej wymiany informacji, sposób udostępniania danych podmiotom uprawnionym, ich format oraz sposób i tryb przekazywania. Ustawodawca szeroko potraktował przetwarzanie informacji, definiując je jako wszelkie operacje wykonywane na informacjach rejestrowanych, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie przez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (art. 3 pkt 7 ustawy o SInF).
- 1.12. **Zasady ochrony informacji przetwarzanych w SInF** — ochrona danych i kontrola przekazywania do SInF informacji rejestrowanych zostały określone w rozdziale 5. Wskazano w nim m.in., iż do przekazywania informacji rejestrowanych do STIR oraz ze STIR do SInF w trybie i zakresie przewidzianym ustawą o SInF nie stosuje się przepisów regulujących ograniczenia udostępniania danych objętych tajemnicami ustawowo chronionymi. Przepis ten odnosi się do samego przekazywania informacji o rachunkach zgodnie z warunkami określonymi w ustawie. Rozwiązanie takie umożliwi przekazywanie informacji o rachunkach zgodnie z celami wskazanymi w ustawie, zarówno w ramach zasilania SInF informacjami, jak i w zakresie udostępniania informacji podmiotom uprawnionym (uzasadnienie do ustawy o SInF, s. 25). Ponadto do udostępniania z SInF informacji rejestrowanych podmiotom uprawnionym, o których mowa w art. 19 ust. 2, w trybie i zakresie przewidzianych ustawą nie stosuje się przepisów regulujących ograniczenia udostępniania danych objętych tajemnicami ustawowo chronionymi (patrz art. 6 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. z 2019 r., poz. 1781).

## 2. Określenie celów ustawy o SInF

**Art. 2. 1. SInF służy: 1) przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu; 2) rozpoznawaniu i wykrywaniu przestępstwa katalogowego oraz zapobieganiu przestępstwu katalogowemu lub wspomaganie prowadzenia postępowania karnego w sprawie przestępstwa katalogowego, a także w celu identyfikacji, wykrycia lub zabezpieczenia mienia pochodzącego z takiego przestępstwa; 3) innym celem określonym w ustawie.**

**2. SInF jest prowadzony przy użyciu systemu teleinformatycznego.**

- 2.1. Cele SInF określone w art. 2 związane są bezpośrednio z realizacją zobowiązań państwa członkowskiego UE wynikających z dwóch kategorii dyrektyw: po pierwsze — dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, w szczególności przez JAF; po drugie — zwalczania innych niż pranie pieniędzy i finansowanie terroryzmu przestępstw oraz przeciwdziałania im przez inne niż JAF podmioty.
- 2.2. Pierwsza kategoria została wyznaczona przez dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/849, która zobowiązała państwa członkowskie do rozważenia utworzenia scentralizowanych rejestrów rachunków bankowych lub systemów wyszukiwania danych umożliwiających JAF szybką identyfikację osób posiadających rachunki bankowe i płatnicze oraz skrytki depozytowe.
- 2.3. W tym samym obszarze przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu dyrektywa 2018/843 wprost wskazała na potrzebę utworzenia scentralizowanych baz danych o rachunkach. Uznała, że niezbędne jest ustanowienie we wszystkich państwach członkowskich scentralizowanych automatycznych mechanizmów, takich jak rejestry lub systemy wyszukiwania danych, co stanowić ma skuteczny środek pozwalający uzyskać w odpowiednim czasie informacje o tożsamości posiadaczy rachunków bankowych i płatniczych oraz skrytek depozytowych, ich posiadaczy będących pełnomocnikami oraz ich beneficjentów rzeczywistych. Stosując przepisy dotyczące dostępu, należy wykorzystać istniejące wcześniej mechanizmy pod warunkiem, że JAF będą miały natychmiastowy dostęp do danych, których dotyczy ich zapytanie, z zachowaniem ich pierwotnej formy i treści. Państwa członkowskie powinny, w tym kontekście, rozważyć możliwość wprowadzenia do takich mechanizmów



innych informacji, które zostaną uznane za konieczne i proporcjonalne w celu skuteczniejszego ograniczania zagrożeń związanych z praniem pieniędzy i finansowaniem terroryzmu. Należy zapewnić zachowanie pełnej poufności w odniesieniu do takich zapytań i wniosków o udostępnienie powiązanych informacji kierowanych przez JAF i właściwe organy, inne niż organy ścigania (zob. pkt 20 preambuły dyrektywy 2018/843).

- 2.4. Dyrektywa 2018/843 wprowadziła podstawowe przepisy dające podstawy do przygotowania scentralizowanych rejestrów danych o rachunkach.

„Artykuł 32a

1. Państwa członkowskie ustanawiają scentralizowane automatyczne mechanizmy, takie jak centralne rejestry lub centralne systemy wyszukiwania danych elektronicznych, które umożliwiają terminową identyfikację dowolnej osoby fizycznej lub prawnej posiadającej lub kontrolującej rachunki płatnicze oraz rachunki bankowe identyfikowane za pomocą IBAN, zgodnie z definicją zawartą w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 260/2012, a także skrytki depozytowe w instytucji kredytowej na ich terytorium. Państwa członkowskie powiadają Komisję o specyfice tych mechanizmów krajowych.

2. Państwa członkowskie zapewniają, by informacje przechowywane w scentralizowanych mechanizmach, o których mowa w ust. 1 niniejszego artykułu, były bezpośrednio i natychmiastowo dostępne dla krajowych jednostek analityki finansowej z zachowaniem ich pierwotnej formy i treści. Informacje te są również dostępne dla właściwych organów krajowych do celów wykonywania ich obowiązków na mocy niniejszej dyrektywy. Państwa członkowskie zapewniają, by wszystkie jednostki analityki finansowej były w stanie dostarczyć terminowo informacje przechowywane w scentralizowanych mechanizmach, o których mowa w ust. 1 niniejszego artykułu, każdej innej jednostce analityki finansowej, zgodnie z art. 53.

3. Następujące informacje muszą być dostępne oraz musi istnieć także możliwość ich wyszukiwania za pomocą scentralizowanych mechanizmów, o których mowa w ust. 1:

- w przypadku klienta będącego posiadaczem rachunku i dowolnej osoby, która twierdzi, że działa w imieniu klienta: imię i nazwisko lub nazwa, uzupełnione pozostałymi danymi umożliwiającymi ustalenie tożsamości wymaganymi

- na mocy przepisów krajowych transponujących art. 13 ust. 1 lit. a) albo niepowtarzalnym numerem identyfikacyjnym,
- w przypadku beneficjenta rzeczywistego klienta będącego posiadaczem rachunku: imię i nazwisko lub nazwa, uzupełnione pozostałymi danymi umożliwiającymi ustalenie tożsamości wymaganymi na mocy przepisów krajowych transponujących art. 13 ust. 1 lit. b) albo niepowtarzalnym numerem identyfikacyjnym,
  - w przypadku rachunku bankowego lub płatniczego: numer IBAN oraz data otwarcia i zamknięcia rachunku,
  - w przypadku skrytki depozytowej: imię i nazwisko lub nazwa najemcy, uzupełnione pozostałymi danymi umożliwiającymi ustalenie tożsamości wymaganymi na mocy przepisów krajowych transponujących art. 13 ust. 1 albo niepowtarzalnym numerem identyfikacyjnym i czasem trwania najmu.

4. Państwa członkowskie mogą rozważyć objęcie obowiązkiem udostępniania z możliwością wyszukiwania za pomocą scentralizowanych mechanizmów innych informacji uznawanych za mające zasadnicze znaczenie dla jednostek analityki finansowej i właściwych organów do celów wykonywania ich obowiązków na mocy niniejszej dyrektywy.

Artykuł 32b

Państwa członkowskie zapewniają jednostkom analityki finansowej i właściwym organom dostęp do informacji, które umożliwiają terminową identyfikację dowolnej osoby fizycznej lub prawnej będącej właścicielem nieruchomości, w tym za pomocą rejestrów lub systemów wyszukiwania danych elektronicznych, jeżeli takie rejestry lub systemy są dostępne”.

- 2.5. W drugiej kategorii — dotyczącej przeciwdziałania innym niż pranie pieniędzy i finansowanie terroryzmu przestępstwom i ich zwalczania — dyrektywa 2019/1153 wprost wskazała, że oprócz JAF, dostęp do centralnych baz danych gromadzących informacje o rachunkach powinny mieć także inne podmioty. Ze względu na fakt, że w każdym państwie członkowskim istnieje wiele organów lub instytucji właściwych w sprawach zapobiegania przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie lub ich ścigania, a także w celu zapewnienia proporcjonalnego dostępu do informacji finansowych i innych informacji na podstawie tej dyrektywy, na potrzeby niniejszej dyrektywy państwa członkowskie powinny zostać zobowiązane do wy-