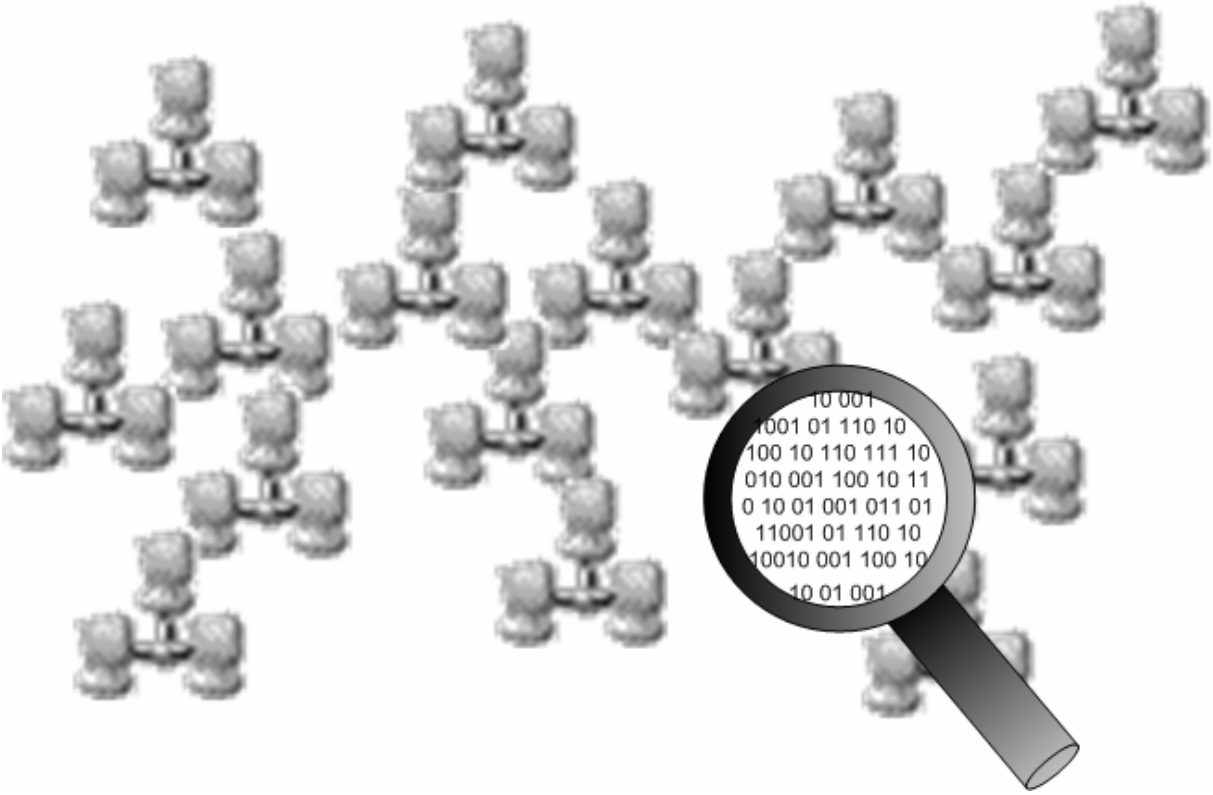


Wytyczna

zarządzania i nadzoru nad systemami informatycznymi pod kątem zgodności z Ustawą o ochronie danych osobowych

czyli

UODO Survival Kit

Zespół ODOSI
Mirosław Błaszczak
Piotr Dzwonkowski
Joanna Karczewska
Sebastian Łataś

Wersja 2.1
Październik 2007

Zastrzeżenie:

Zespół ODOSI nie twierdzi, że jakiekolwiek korzystanie z tego opracowania zapewni pozytywne wyniki. Opracowania nie należy traktować jako zawierającego właściwe informacje, procedury i testy bądź nie zawierającego innych informacji, procedur i testów, które mają na celu osiągnięcie tych samych wyników. W ustalaniu właściwości jakiejkolwiek informacji, procedury lub testu, osoba zajmująca się zawodowo audytem lub kontrolą systemów informatycznych powinna polegać na swoim zawodowym osądzie określonych okoliczności zaistniałych w danym środowisku systemów lub technologii informatycznych.

Wersja wytycznej

Dotychczas ukazały się następujące wersje Wytycznej:

wersja 1.0 PL - w marcu 2005,
wersja 1.1 PL i EN - w kwietniu 2005,
wersja 2.0 PL - w grudniu 2006.

Najważniejsze zmiany w niniejszej wersji dotyczą dostosowania Wytycznej do najnowszej wersji 4.1 schematu COBIT® oraz uwzględniają uwagi zgłoszone przez użytkowników Wytycznej.

Wytyczna zawiera tłumaczenia własne fragmentów COBIT 4.1. Po opublikowaniu oficjalnego tłumaczenia schematu COBIT 4.1 na język polski, autorzy Wytycznej dokonają aktualizacji cytatów zawartych w tym opracowaniu.

Komentarze i uwagi:

Zespół ODOSI zaprasza do zgłaszania wszelkich uwag i komentarzy dotyczących tego opracowania. Listy elektroniczne prosimy kierować na adresy członków zespołu:

Mirosław Błaszczak m.blaszczak@vip.wp.pl
Piotr Dzwonkowski piotr.dzwonkowski@gmail.com
Joanna Karczewska j.karczewska@poczta.onet.pl
Sebastian Łataś latas.s@pg.com

SPIS TREŚCI

Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym

Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym

Konstytucja Rzeczypospolitej Polskiej

1. WPROWADZENIE

1.1. Wstęp

W dzisiejszym mocno sformalizowanym i zinformatyzowanym świecie nasze dane osobowe są gromadzone w niezliczonych firmach i instytucjach. Nasze dane osobowe są przechowywane w postaci elektronicznej, co znacznie ułatwia ich przetwarzanie i dystrybucję. Nie jesteśmy w stanie osobiście przypilnować naszych danych osobowych i zapobiec wykorzystaniu ich wbrew ich przeznaczeniu. Dlatego mamy prawo wymagać zabezpieczenia naszych danych osobowych od tych, którzy mają naszą zgodę na ich gromadzenie i przetwarzanie. Powinniśmy także zadawać sobie pytanie:

„Czy nasze dane osobowe są odpowiednio chronione?"

Z kolei kierownictwa firm i instytucji powinny wiedzieć, że posiadane dane osobowe są przetwarzane w trudnych do policzenia formach, postaciach i miejscach, a dostęp do nich ma wielu pracowników. Dane osobowe są przechowywane w postaci elektronicznej, co ułatwia ich masowe przetwarzanie i dystrybucję. Stwarza to jednak określone zagrożenia i wymusza wprowadzenie dodatkowych systemów kontroli, by gromadzenie i przetwarzanie danych osobowych było zgodne z przepisami polskiego prawa. Firmy, organizacje, zrzeszenia i stowarzyszenia (praktycznie nie ma firmy, która nie przetwarzałaby danych osobowych) powinny zadawać sobie pytania:

„Czy przetwarzając dane osobowe robimy to z zachowaniem wszystkich wymogów prawa?"

„Czy przetwarzane przez nas dane osobowe są odpowiednio chronione?"

1.2. Przepisy prawne

Podstawowymi przepisami prawnymi, które definiują prawne zasady ochrony danych osobowych, są:

- Konstytucja Rzeczypospolitej Polskiej
- Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (t.j. Dz.U. z 2002r. Nr 101, poz.926 i Nr 153, poz.1271 oraz z 2004r. Nr 25, poz.219 i Nr 33, poz.285) – zwana dalej „Ustawą" lub „UODO",
- Rozporządzenie MSWiA z dnia 29 kwietnia 2004r. (t.j. Dz.U. z 2004r. Nr 100, poz.1024) w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych – zwane dalej „Rozporządzeniem". Rozporządzenie weszło w życie 1 listopada 2004r.,

oraz:

- Dyrektywa Parlamentu Europejskiego i Rady 95/46/WE z dnia 24 października 1995r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych,
- Konwencja 108 Rady Europy sporządzona z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych.

W określonych przypadkach mogą również mieć zastosowanie liczne przepisy odrębnych ustaw oraz umów międzynarodowych.

1.3. Potrzeba Wytycznej

Dyrektywa 95/46/WE w punkcie 61 Preambuły zawiera następujący zapis:
"Państwa Członkowskie i Komisja, w zakresie posiadanych kompetencji, mają obowiązek zachęcać stowarzyszenia handlowe i inne zainteresowane organizacje przedstawicielskie do sporządzania kodeksów postępowania w celu ułatwienia wdrażania w życie niniejszej Dyrektywy, uwzględniając różny charakter procesu przetwarzania danych w różnych sektorach i przestrzegając postanowień państwowych dotyczących jego wdrażania."

W księgarniach i Internecie dostępnych jest wiele publikacji opracowanych przez różne podmioty i organizacje, prezentujących kwestie prawne dotyczące ochrony danych osobowych. Natomiast brakuje dokumentów poświęconych zagadnieniom związanym z ochroną danych osobowych w systemach informatycznych. Dlatego członkowie zespołu ODOSI postanowili opracować „Wytyczną zarządzania i nadzoru", która pomoże w zapewnieniu zgodności i bezpieczeństwa, audycie oraz przetwarzaniu danych osobowych w systemach informatycznych.

W Wytycznej nie zostały uwzględnione zagadnienia ściśle związane z ochroną informacji niejawnych (zdefiniowanych w Ustawie o ochronie informacji niejawnych Dz.U. z 2001r. Nr 22, poz.241).

1.4. Adresaci Wytycznej

Wytyczna jest przeznaczona dla wszystkich osób zainteresowanych zapewnieniem zgodności działania systemów informatycznych firmy z Ustawą o Ochronie Danych Osobowych. Poniższa tabelka przedstawia grupy adresatów wraz z ich rolą:

	Adresat Wytycznej	Rola
1.	Administrator Danych Osobowych / kierownictwo firmy lub organizacji	odpowiada za ochronę danych osobowych. Zgodnie z art. 7 Ustawy, jest to organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydująca o celach i środkach przetwarzania danych osobowych.
2.	Administrator Bezpieczeństwa Informacji (ABI)	nadzoruje przestrzeganie zasad ochrony, wyznaczony przez Administratora Danych Osobowych, chyba że on sam wykonuje te czynności (zgodnie z art. 36 Ustawy).
3.	Administrator Zarządzający	odpowiada za przetwarzanie danych osobowych w powierzonym obszarze.
4.	Administrator Wykonawczy (np. administrator systemu/ aplikacji/serwera danych) – Informatyk	wykonuje bieżące czynności związane z realizacją ochrony danych osobowych w danym systemie / aplikacji.
5.	Osoba, której dane dotyczą	może kontrolować przetwarzanie danych, które jej dotyczą, zawartych w zbiorach danych (zgodnie z rozdz. 4 Ustawy).
6.	Podmiot, któremu powierzono przetwarzanie danych (outsourcing)	przed rozpoczęciem przetwarzania danych, jest zobowiązany podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36–39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a Ustawy.

	Adresat Wytycznej	Rola
7.	Audytor systemów informatycznych	weryfikuje zgodność przetwarzania danych osobowych z Ustawą.
8.	Inspektor GIODO	przeprowadza oględziny urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych (zgodnie z art. 14 Ustawy).

1.5. Odniesienie do ISACA® i COBIT®

ISACA® jest wiodącą organizacją na świecie zrzeszającą osoby zajmujące się zawodowo ładem informatycznym oraz nadzorem, bezpieczeństwem i audytem systemów informatycznych. Powstała w 1969 roku. Obecnie należy do niej ponad 65 tysięcy członków, zrzeszonych w oddziałach zlokalizowanych w ponad 140 krajach świata. Członkowie zespołu ODOSI, autorzy Wytycznej, są członkami stowarzyszenia ISACA.

IT Governance Institute® (ITGI) został powołany przez ISACA w 1998 roku. Istnieje, by pomagać liderom firm dopasować IT do biznesu w celu dostarczania mierzalnych korzyści przy optymalnych środkach i właściwym ryzyku działania. ITGI prowadzi unikalne badania nad koncepcjami i stosowaniem ładu informatycznego. Opracowuje materiały skierowane do profesjonalistów funkcjonujących w ciągle zmieniającym się środowisku informatycznym.

COBIT® (Control Objectives for Information and Related Technology), opracowany i aktualizowany przez ISACA® i ITGI®, to schemat ładu informatycznego, który pozwala kierownictwu uzupełnić lukę pomiędzy wymaganiami nadzoru i kontroli, kwestiami technicznymi i ryzykami biznesowymi. Umożliwia opracowanie jednoznacznej polityki i dobrych praktyk nadzoru nad IT w całej firmie. Najnowsza wersja COBIT 4.1 kładzie nacisk na zgodność z regulacjami prawnymi, pomaga firmom zwiększyć wartość osiąganą z IT, umożliwia dopasowanie IT do biznesu oraz upraszcza wdrożenie schematu COBIT.

Prace we wspólnych projektach ISACA i ITGI są prowadzone z zaangażowaniem specjalistów z firm i organizacji z całego świata, również z Polski.

1.5.1 Kryteria informacji

W celu spełnienia celów biznesowych, informacje muszą odpowiadać pewnym kryteriom kontrolnym, które schemat COBIT określa jako biznesowe wymogi informacji. Są to: efektywność, wydajność, poufność, integralność, dostępność, zgodność i rzetelność. W zakresie bezpieczeństwa informacji podstawowe znaczenie mają kryteria poufności i integralności. **Rozliczalność** w dokumentach ISACA® oznacza możliwość prześledzenia, kto odpowiada za daną czynność lub zdarzenie.

Zgodnie z Rozporządzeniem, przy przetwarzaniu danych osobowych obowiązują kryteria poufności, integralności i rozliczalności przetwarzanych danych. **Rozliczalność** oznacza właściwość urządzeń i systemów informatycznych służących do przetwarzania danych osobowych zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.

1.6. Odniesienie do innych standardów i wytycznych

W kwestiach dotyczących bezpieczeństwa informacji i systemów informatycznych polecamy również zastosowanie zasad i rekomendacji zawartych w niżej wymienionych opracowaniach.

1.6.1 Inne dokumenty COBIT

IT Governance Institute® opublikował różne opracowania dotyczące standardów ochrony danych, m.in.:

- COBIT Security Baseline – An Information Security Survival Kit, 2nd Edition [5] – przedstawia problematykę bezpieczeństwa IT w sposób zrozumiały zarówno dla użytkownika w domu, pracownika małej czy średniej firmy jak i dla zarządu i rady nadzorczej dużego przedsiębiorstwa,
- COBIT Mapping Overview of International IT Guidance, 2nd Edition [6] – zawiera porównanie 14 różnych wytycznych opublikowanych na całym świecie, dotyczących konkretnych kwestii związanych z ładem i bezpieczeństwem informatycznym,
- COBIT Mapping: Mapping of ISO/IEC 17799:2005 With COBIT 4.0 [7] – przedstawia relacje pomiędzy procesami i celami kontrolnymi zdefiniowanymi w schemacie COBIT i zapisami znanego standardu międzynarodowego.

1.6.2 Normy bezpieczeństwa informacji

W zakresie zabezpieczenia poufności, integralności i dostępności informacji powszechnie znane i stosowane są:

- norma ISO/IEC 27001:2005,
- norma ISO/IEC 27002:2005,
- norma ISO/IEC 17799:2005,
- polska norma PN-ISO/IEC 17799:2007,
- polska norma PN-ISO/IEC-27001:2007.

1.6.3 Wskazówki GIODO

Na swojej stronie internetowej GIODO opublikowało dokumenty zawierające praktyczne wskazówki dla administratorów danych, opracowane przez Departament Informatyki Biura Generalnego Inspektora:

- Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa [10],
- Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji [11],
- Wymagania dotyczące struktur baz danych osobowych oraz funkcjonalności zarządzających nimi aplikacji [12].

1.7. Odniesienie do prywatności

Prywatność według „Komputerowego Słownika Języka Polskiego PWN" oznacza:

„Życie, sprawy prywatne, osobiste; poczucie bezpieczeństwa we własnym domu; prawo do życia intymnego, chronionego przed ingerencją obcych."

Do prywatności odnosi się Konstytucja Rzeczypospolitej Polskiej w Artykule 47:

„Każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym."

Encyklopedia Britannica definiuje prywatność w sposób zbieżny z wyżej przedstawionym:

"Right of a person to be free from intrusion into matters of a personal nature.
A person's right to privacy may be overcome by a compelling state interest. In tort law, privacy is a right not to have one's intimate life and affairs exposed to public view or otherwise invaded. Less broad protections of privacy are afforded public officials and others defined by law as "public figures" (e.g., movie stars)."

Wikipedia definiuje prywatność w sposób najbardziej chyba intuicyjny:

> *„możliwość jednostki lub grupy osób do utrzymania swych osobistych zwyczajów i zachowań z dala od widoku publicznego."*

Uważa się, że prawo do ochrony informacji dotyczącej osoby fizycznej wypływa z prawa do prywatności. Stosowne zapisy zostały zawarte w Artykule 51 Konstytucji RP:

> *„1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.*
> *2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.*
> *3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.*
> *4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.*
> *5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa."*

Rozwinięciem tego Artykułu jest Ustawa o ochronie danych osobowych.

Zwróćmy uwagę, że we współczesnym świecie ściśle związanym z informatyką często zawęża się znaczenie słowa „prywatność" do spraw związanych z informacją na temat osoby. Przykładem może być wytyczna audytu ISACA dot. prywatności [9], która określa „data privacy" słowem „privacy":

> *"1.6.1 Privacy means adherence to trust and obligation in relation to any information relating to an identified or identifiable individual (data subject). Management is responsible to comply with privacy in accordance with its privacy policy or applicable privacy laws and regulations."*
> (tłum. wł. Prywatność oznacza przestrzeganie zasad zaufania i obowiązku w stosunku do jakichkolwiek danych dotyczących osoby fizycznej, która jest lub może zostać zidentyfikowana na ich podstawie (osoba, której dane dotyczą). Kierownictwo odpowiada za zgodność z wymogami dotyczącymi prywatności zawartymi w polityce prywatności firmy lub odpowiednich przepisach prawa.)

1.8. Zespół ODOSI

Prace zespołu ODOSI zostały zainspirowane opublikowaniem przez ISACA w 2004r. projektu międzynarodowej wytycznej audytu systemów informatycznych pod kątem prywatności [9].

W skład zespołu ODOSI wchodzą członkowie ISACA Warsaw Chapter:

- Mirosław Błaszczak, CISA,
- Piotr Dzwonkowski, CISA, CISM,
- Joanna Karczewska, CISA,
- Sebastian Łataś, CISA, CISM.

Wersja 1.0 Wytycznej została udostępniona wszystkim zainteresowanym w marcu 2005r. w celu konsultacji. Zebrane komentarze i uzupełnienia zostały wprowadzone do wersji 1.1 oraz wersji 2.0. Obecna wersja 2.1 uwzględnia uwagi zebrane przez 2 lata oraz wersję 4.1 schematu COBIT.

1.9. Odniesienie do europejskiego projektu e-PRODAT

Wersja 1.1 Wytycznej została zakwalifikowana do „Trzeciej Edycji Konkursu Na Najlepsze Praktyki Dotyczące Ochrony Danych Osobowych W Sektorze Administracji Publicznej" zorganizowanego przez Agencję Ochrony Danych Osobowych Regionu Madrytu (hiszp. Agencia de Protección de Datos de la Comunidad de Madrid czyli APDCM). Prezentacja Wytycznej odbyła się w trakcie międzynarodowego seminarium zorganizowanego 12 grudnia 2006r. w Madrycie.

APDCM jest także liderem europejskiego projektu "e-PRODAT: e-Government i Ochrona Danych Osobowych w regionach i miastach europejskich", współfinansowanego przez Unię Europejską w ramach inicjatywy INTERREG IIIC. Podstawowe cele projektu to:

- wymiana wiedzy i doświadczeń w zakresie ochrony danych osobowych w instytucjach publicznych należących do różnych państw europejskich.
- stworzenie internetowego europejskiego Obserwatorium ochrony danych w ramach e-Government w celu ustawicznego szacowania zgodności z europejskimi przepisami dotyczącymi ochrony danych oraz podnoszenia świadomości obywateli Europy w kwestiach związanych z ochroną danych,
- identyfikowanie najlepszych praktyk ochrony danych już wdrożonych w ramach e-Government lub innych działań instytucji publicznych, oraz opracowywanie zaleceń dotyczących zwiększenia ochrony danych w sektorze publicznym.

Wszelkie informacje o projekcie e-PRODAT i stworzonym Obserwatorium można uzyskać pod adresem:

www.eprodat.org

Zapraszamy także na strony serwisu:

www.dataprotectionreview.eu

przygotowanego przez APDCM i poświęconego ochronie danych osobowych w Unii Europejskiej.

2. WYTYCZNA

2.1. Jak korzystać z Wytycznej?

Wytyczną mogą stosować osoby zainteresowane ochroną danych osobowych niezależnie od zaawansowania prac oraz własnego przygotowania.

	Stopień przygotowania	Zalecane czynności:
1.	Osoby, które dopiero zaczynają zajmować się ochroną danych osobowych w systemach informatycznych	I. Uważnie zapoznać się z Ustawą i Rozporządzeniem (najlepiej uzupełnione komentarzem) II. Zadać pytania kontrolne (zgodnie z rolą, jaka osoba pełni w firmie) z listy (rozdział 2.2) w celu ustalenia stopnia obowiązywania Ustawy i Rozporządzenia w firmie III. Wykorzystać mapowanie i stosowne Praktyki Kontrolne schematu COBIT, by ustalić co, dlaczego i jak należy wdrożyć w systemach informatycznych dla zapewnienia zgodności z UODO
2.	Osoby, które już wdrożyły mechanizmy ochrony danych osobowych w systemach informatycznych (zwykle Administrator Bezpieczeństwa Informacji)	I. Sprawdzić, czy Ustawa i/lub Rozporządzenie były nowelizowane i uważnie zapoznać się z ewentualnymi zmianami II. Zadać wszystkie pytania kontrolne w celu ustalenia stopnia zastosowania się do Ustawy i Rozporządzenia III. Wykorzystać mapowanie i stosowne Wytyczne Zarządzania schemat COBIT do ustalenia: • kluczowych mechanizmów kontrolnych, • kluczowych mierników, • rodzaju odpowiedzialności (RACI) za wyznaczone czynności, • celów czynności, celów procesu i celów IT dla wyznaczonych procesów IT.
3.	Osoby zarządzające firmami czy organizacjami (Administratorzy Danych Osobowych)	I. Zapoznać się z Ustawą i Rozporządzeniem (najlepiej uzupełnione komentarzem) II. Uzyskać odpowiedzi na pytania kontrolne zawarte w pierwszej kolumnie listy III. Wykorzystać mapowanie i Wytyczne Zarządzania schematu COBIT do oceny poziomu dojrzałości wyznaczonych procesów IT
4.	Osoby, które chcą zweryfikować zgodność z Ustawą / przeprowadzić audyt	I. Uważnie zapoznać się z Ustawą i Rozporządzeniem (najlepiej uzupełnione komentarzem) II. Zadać pytania kontrolne osobom odpowiedzialnym według kompetencji określonych w nagłówku każdej kolumny listy w celu ustalenia stopnia zastosowania się do Ustawy i Rozporządzenia III. Wykorzystać mapowanie i Wytyczne Audytu schematu COBIT do weryfikacji systemów informatycznych pod kątem zgodności z UODO

2.2. Listy pytań kontrolnych

Niniejsze listy zawierają pytania kontrolne. Odpowiedzi na te pytania mogą ułatwić identyfikowanie i w razie potrzeby wprowadzanie lub ulepszanie mechanizmów kontrolnych zapobiegających naruszenie bezpieczeństwa danych osobowych, a także weryfikację zgodności przetwarzania danych osobowych z Ustawą. Pytania są ogólne, to znaczy nie wszystkie będą adekwatne dla każdej organizacji. Zainteresowani muszą sami ocenić przydatność każdego pytania w zależności od wielkości, sposobu działania, zorganizowania i poziomu dojrzałości konkretnej firmy.

Wyróżnione zostały trzy grupy adresatów pytań:

1. **Administrator Danych Osobowych (ADO)** – odpowiada za ochronę danych osobowych. Zgodnie z art.7 Ustawy, jest to organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych.

   Zespół ODOSI uznał, że w odniesieniu do dużych i średnich firm celowe jest wyróżnienie osoby odpowiedzialnej za przetwarzanie danych osobowych w powierzonym jej obszarze (np. dyrektor do spraw marketingu, finansów, kadr czy płac). Osobę tę nazwaliśmy **Administratorem Zarządzającym**.
2. **Administrator Bezpieczeństwa Informacji (ABI)** – zgodnie z art.36 Ustawy jest to osoba nadzorująca przestrzeganie zasad ochrony, wyznaczona przez Administratora Danych Osobowych, chyba że on sam wykonuje te czynności,
3. **Administrator Wykonawczy** (np. systemu/aplikacji/serwera/danych) – wykonuje bieżące czynności związane z realizacją ochrony danych osobowych w danym systemie / aplikacji.

Pytania związane z kontrolą wewnętrzną i audytami zewnętrznymi zostały dopisane jako dodatkowe czynności rekomendowane na podstawie własnych doświadczeń autorów Wytycznej i dobrych praktyk stosowanych w wielu firmach. Nie są to wymogi wynikające z zapisów Ustawy.

Tytuły grup pytań zawierają także odniesienie do artykułów/rozdziałów Ustawy oraz Rozporządzenia.

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
ZBIORY DANYCH OSOBOWYCH			
Zakres stosowania (art. 2, 3, 3a, 6, 40)			
1	Czy Ustawę stosuje się do naszej firmy/organizacji?	W jakim zakresie Ustawę stosuje się do naszej firmy/organizacji. Czy są jakieś wyłączenia?	Czy zostałem poinformowany o tym, że do zbiorów administrowanych przeze mnie stosuję się Ustawę?
2	Jakie dane osobowe w rozumieniu Ustawy są przetwarzane przez firmę?	Jakie dane osobowe w rozumieniu Ustawy są przetwarzane przez firmę w zbiorach/ systemach/ kartotekach?	Jakie dane osobowe w rozumieniu Ustawy są przetwarzane w zbiorach/systemach administrowanych przeze mnie?
3	Czy posiadamy/przetwarzamy również (tylko) dane doraźne?	Które ze zbiorów danych mają charakter zbiorów doraźnych?	Czy zbiory administrowane przeze mnie mają charakter doraźny, techniczny lub związany ze szkoleniami?
4	Które zbiory danych zawierają dane osobowe?	Które zbiory danych zawierające dane osobowe w rozumieniu Ustawy są w posiadaniu firmy?	Czy w zbiorach/systemach przeze mnie administrowanych są przetwarzane dane osobowe?
5	Czy zbiory danych zawierają dane wrażliwe?	W których zborach są przechowywane dane wrażliwe?	Czy w zbiorach/systemach przeze mnie administrowanych są dane wrażliwe?
6	Czy istnieje lista tych zbiorów danych i gdzie jest przechowywana?	Jaką postać ma lista zbiorów danych osobowych? Gdzie jest przechowywana i jak zabezpieczana?	Czy sporządzam i uaktualniam listę zbiorów danych osobowych administrowanych przeze mnie?
7	Skąd wiadomo, że ta lista jest kompletna i aktualna?	W jaki sposób zapewnia się, że wyżej wymieniona lista jest kompletna i aktualna? Czy stosowane są mechanizmy dokumentowania zapisów?	Kiedy ostatnio aktualizowałem informacje na liście opisów zbiorów?
8	Czy zbiory danych podlegają rejestracji w GIODO?	Które zbiory danych osobowych podlegają rejestracji w GIODO? Jak jest procedura przygotowania wniosków do GIODO?	Czy zbiory danych administrowane przeze mnie podlegają rejestracji w GIODO?
9	Czy zbiory danych, które podlegają rejestracji, zostały zarejestrowane?	Jak prowadzona jest dokumentacji potwierdzająca rejestrację w GIODO?	Czy zbiory danych administrowane przeze mnie zostały zarejestrowane w GIODO?
10	Czy w systemach informatycznych firmy przetwarzane są dane osobowe?	Czy i w których systemach informatycznych firmy przetwarzane są dane osobowe? Czy są to dane osobowe w rozumieniu Ustawy?	Czy w moim systemie przetwarzane są dane osobowe?
Role i odpowiedzialności (art. 7, 36, 37, 33, 34)			
11	Kto z członków kierownictwa jest odpowiedzialny za ochronę danych osobowych?	Kto z członków kierownictwa nadzoruje moją pracę jako ABI?	Kto z członków kierownictwa i jest odpowiedzialny za ochronę danych osobowych?

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
12	Kto odpowiada za przetwarzanie danych osobowych w jednostce nadrzędnej?	Czy znam osobę kontaktową odpowiedzialną za przetwarzanie danych osobowych w jednostce nadrzędnej?	Czy osoba (z jednostki nadrzędnej) posiadająca prawa administratora jest identyfikowalna i została formalnie autoryzowana do przetwarzania danych osobowych?
13	Kto odpowiada za przetwarzanie danych osobowych w jednostkach podrzędnych?	Czy odpowiadam również za przetwarzanie danych w jednostkach podrzędnych?	Czy prawa administracyjne administratorów z jednostek podrzędnych są znane i kontrolowane?
14	Kto jest formalnie wyznaczony jako Administrator Bezpieczeństwa Informacji?	Od kiedy pełnię funkcję ABI?	Kto w firmie/organizacji pełni funkcję ABI?
15	Czy jest formalnie ustalony zakres obowiązków ABI?	Czy otrzymałem i potwierdziłem zakres swoich obowiązków jako ABI?	Czy znany mi jest zakres obowiązków i uprawnień ABI w kwestiach dotyczących administrowanych przeze mnie zbiorów/systemów?
16	W jaki sposób ABI nadzoruje przestrzeganie zasad ochrony przetwarzania danych osobowych?	W jaki sposób nadzoruję środki techniczne i organizacyjne chroniące dane osobowe przed osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.?	W jaki sposób zastosowane środki techniczne i organizacyjne chronią dane osobowe przed nieupoważnionym, zabraniem przez osobę nieuprawnioną, zmianą, utratą, uszkodzeniem lub zniszczeniem?
17	Czy są wyznaczeni administratorzy systemów/aplikacji przetwarzających dane osobowe?	Czy lista administratorów zbiorów/systemów jest tworzona i aktualna? Czy jest kompletna?	Czy jest mi znany mój zakres obowiązków jako administratora systemów/aplikacji zawierających bądź przetwarzających dane osobowe?
18	Kto jest upoważniony do przetwarzania danych osobowych?	W jaki sposób dokonuje się upoważniania osób do przetwarzania danych? Kto przygotowuje i przechowuje dokumentację?	Czy osoby mające dostęp/przetwarzające dane osobowe w administrowanych przeze mnie zbiorach/systemach otrzymały upoważnienia?
19	Kto jest upoważniony do udzielania informacji o przetwarzanych danych osobowych?	W jaki sposób i kto jest upoważniony do udzielania informacji o danych osobowych przetwarzanych w firmie/organizacji?	W jaki sposób i kto jest upoważniony do udzielania informacji o danych osobowych przetwarzanych w moich zbiorach/systemach?
PRZETWARZANIE DANYCH OSOBOWYCH			
Podstawy przetwarzania (rozdz. 3)			
20	Jaki jest cel przetwarzania danych?	Jaki jest powód przetwarzania danych, kto go akceptował? Czy powody ulegają zmianom?	Czy zostałem powiadomiony o celach przetwarzania danych w poszczególnych zbiorach danych, będących pod moją administracją?
21	Jaki jest zakres przetwarzania danych?	Jakie są zakresy przetwarzania dla poszczególnych zbiorów danych?	Jakie są zakresy przetwarzania dla poszczególnych zbiorów danych, będących pod moją administracją?

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
22	Czy wymagane są zgody na przetwarzanie danych od osób, których dane dotyczą?	Dla których zbiorów danych wymagane są zgody osób, których dane dotyczą?	Czy dla zbiorów danych, będących pod moją administracją wymagane są zgody osób, których dane dotyczą?
23	Czy mamy zgodę na przetwarzanie danych osoby, której dane dotyczą?	W jakiej postaci i gdzie są przechowywane zgody na przetwarzanie? Czy są one zgodne z ustalonym i rzeczywistym zakresem i celem?	
24	W jakiej formie i gdzie przechowywane są zgody na przetwarzanie?	Czy wymagane zgody na przetwarzanie danych osobowych są odpowiednio zabezpieczone i zarchiwizowane w sposób umożliwiający ich sprawne odnalezienie?	Czy w stosunku do administrowanych przeze mnie zbiorów danych wymagane jest potwierdzenie zgody na przetwarzanie?
25	Czy dane osobowe, jakie przetwarzamy otrzymaliśmy na zasadzie przekazania od firmy trzeciej?	Które zbiory danych przetwarzamy na zasadzie przekazania od firm trzecich?	Czy zbiory, które administruję zostały przekazane od firm trzecich?
26	Czy jest dopełniony obowiązek informacyjny wobec osoby, której dane dotyczą?	W jaki sposób dopełniono obowiązku informacyjnego wobec osób, której dane dotyczą?	
27	Czy zbiory danych są prawidłowo zabezpieczone?	Czy spełnione są wymagane w Ustawie kryteria bezpieczeństwa w stosunku do przetwarzanych zbiorów danych?	Czy spełnione są wymagane kryteria bezpieczeństwa w stosunku do administrowanych przeze mnie zbiorów danych?
Zasady przetwarzania (rozdz. 3)			
28	Czy dane osobowe są kompletne i zgodne ze zgłoszonym stanem faktycznym?	W jaki sposób zapewnia się, że dane osobowe przetwarzane przez firmę są kompletne i zgodne ze zgłoszonym stanem faktycznym?	Czy dane osobowe przetwarzane w zbiorach/systemach będących pod moją administracją są kompletne i zgodne ze zgłoszonym stanem faktycznym?
29	Czy przetwarzanie danych jest zgodne ze zgłoszonym celem i zakresem?	W jaki sposób zapewnia się, że przetwarzanie danych jest zgodne ze zgłoszonym celem i zakresem?	Czy przetwarzanie danych w zbiorach/systemach administrowanych przeze mnie jest zgodne ze zgłoszonym celem i zakresem?
30	Czy jest pewność, że ostateczne rozstrzygnięcie sprawy osoby, której dane dotyczą, nie jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym?	Czy nie posiadamy systemów informatycznych, w których ostateczne rozstrzygnięcie sprawy osoby, której dane dotyczą, jest wyłącznie wynikiem operacji na danych osobowych?	Czy jestem pewien, że w systemach będących pod moją administracją, ostateczne rozstrzygnięcie sprawy osoby, której dane dotyczą, nie jest wyłącznie wynikiem operacji na danych osobowych?
31	W przypadku przetwarzania danych wrażliwych, czy są spełnione warunki dopuszczalności z art.27.2	Czy i w jaki sposób jest weryfikowane spełnianie szczególnych warunków przetwarzania danych wrażliwych? Jakie są to warunki?	Czy w zbiorach/systemach administrowanych przeze mnie są przetwarzane dane wrażliwe?

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
32	Czy stosowane numery porządkowe nie zawierają ukrytych znaczeń (Art. 28)?	Czy we wszystkich zbiorach stosowane numery porządkowe nie zawierają ukrytych znaczeń?	Czy w zbiorach danych administrowanych przeze mnie stosowane numery porządkowe nie zawierają ukrytych znaczeń?
Udostępnianie danych (art.29, 30, 35)			
33	Czy są ustalone procedury udostępniania danych osobowych (nie do zbioru)?	Jakie są procedury udostępniania danych osobowych?	Czy w administrowanym przeze mnie zbiorze/systemie są wdrożone mechanizmy udostępniania danych?
34	Czy jest weryfikowane stosowanie procedur udostępniania danych?	W jaki sposób jest weryfikowane stosowanie procedur udostępniania danych?	Czy w administrowanym przeze mnie zbiorze/systemie są wdrożone mechanizmy rejestracji udostępniania danych?
35	Czy są ustalone procedury odmowy udostępnienia danych (nie do zbioru)?	Jakie są procedury odmowy udostępnienia danych?	
Przekazywanie danych (art. 38)			
36	Czy przekazujemy administrowane zbiory danych osobowych innym podmiotom?	Które zbiory danych osobowych przekazujemy innym podmiotom? Czy są ustalone procedury przekazywania? Czy są zdefiniowane zakresy danych?	Czy zbiory, którymi administruję są przekazywane innym podmiotom? Czy są ustalone formaty przekazywania? Czy są zdefiniowane zakresy danych?
37	Czy prowadzimy dzienniki przekazywania?	Czy dzienniki przekazywania zawierają zakresy, zbiory przekazywane, daty, odbiorcę?	Czy uczestniczę w procesie przekazywania danych i prowadzę dziennik przekazywania?
38	Czy do przekazania danych mamy zgodę osoby, której dane dotyczą?	W jakiej formie przechowywane są zgody osób na przekazywanie danych?	
Powierzenie przetwarzania danych (art. 31)			
39	Czy dane osobowe administrowane przez naszą firmę są przetwarzane przez inny podmiot?	Które zbiory (elementy zbiorów) danych osobowe są przetwarzane przez inne podmioty?	Czy zbiory administrowane przeze mnie są powierzane innym podmiotom?
40	Czy jest podpisana umowa na powierzanie danych?	Czy dla wszystkich powierzonych do przetwarzania zbiorów danych są podpisane umowy?	Czy są mi znane fragmenty umów definiujące metody powierzania danych dotyczących administrowanych przeze mnie?
41	Czy są ustalone procedury powierzania przetwarzania danych innemu podmiotowi?	Czy procedury powierzania przetwarzania są adekwatne do administrowanych zbiorów danych?	Czy znane mi są procedury powierzania danych przeze mnie administrowanych?
42	Czy w umowie powierzenia przetwarzania określony jest cel i zakres przetwarzania?	Czy cel i zakres przetwarzania określony w umowie powierzenia jest zgodny z celami i zakresem naszego przetwarzania?	

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
43	Czy w umowie zawarte są klauzule o możliwości dalszego powierzenia?	Czy klauzule dotyczące dalszego powierzania są zgodne z naszym zakresem i zewnętrznymi uwarunkowaniami prawnymi?	
44	Czy podmiot, któremu powierzono przetwarzanie, stosuje wymagane zabezpieczenia?	W jaki sposób podmiot otrzymujący powierzane dane zapewnia o zachowaniu bezpieczeństwa?	
45	Czy jest weryfikowane bezpieczeństwo powierzanych danych?	W jaki sposób jest weryfikowane bezpieczeństwo przekazywanych danych?	Czy biorę udział w weryfikacji zabezpieczania danych powierzanych?
46	Czy sposób przekazywania danych powierzanych spełnia wymogi bezpieczeństwa?	W jaki sposób jest zapewnione bezpieczeństwo przekazywania danych?	Czy dane przekazuję w sposób bezpieczny?
47	Czy naszej firmie powierzono dane do przetwarzania?	Jakie zbiory danych powierzono nam do przetwarzania? Kto nam powierzył dane?	Czy w moim systemie/aplikacji przetwarzane są dane powierzone?
48	Czy jest określony cel i zakres przetwarzania powierzonych nam danych?	Jaki jest cel i zakres przetwarzania powierzanych danych?	Czy znany mi jest cel i zakres przetwarzania powierzanych danych?
49	Czy są określone procedury przekazywania nam powierzonych danych?	Jakie są procedury przekazywania powierzonych danych?	Czy znane mi są procedury powierzania danych do moich systemów?
50	Czy powierzane dane wymagają szczególnych metod ochrony?	Jakie są wymagane szczególne metody ochrony i jakich danych (zakresów danych) one dotyczą?	Czy znane mi są szczególne procedury ochrony powierzonych danych w moich systemach?
Państwa trzecie (art. 31a, rozdz. 7)			
51	Czy dane przez nas administrowane są przetwarzane w państwie trzecim?	Jakie dane są przetwarzane w państwie trzecim?	Czy dane administrowane przeze mnie są przetwarzane w państwie trzecim?
52		Kto jest przedstawicielem podmiotu z państwa trzeciego w RP?	
53	Czy zbiory są przekazywane do państwa trzeciego?	Jakie są procedury przekazywania zbiorów do państwa trzeciego?	Czy przekazuję zbiory do państwa trzeciego?
54		Czy państwo trzecie, w którym przetwarzane są dane, jest na liście autoryzowanej przez UE?	
55	Czy są spełnione szczególne warunki przekazywania do państwa trzeciego?	Jakie szczególne warunki są spełnione, aby umożliwić przekazanie danych do państwa trzeciego?	Do których zbiorów (zakresów) odnoszą się szczególne warunki przekazania do państwa trzeciego?

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
ZABEZPIECZENIE DANYCH OSOBOWYCH			
Zabezpieczenie organizacyjne (art.31, rozdz. 5) i Rozporządzenie			
56	Czy jest dokonywana regularna analiza ryzyka informacyjnego?	Jaka jest stosowana metodyka analizy ryzyka informacyjnego?	Czy uczestniczę w procesach analizy ryzyka dotyczących administrowanych przeze mnie systemów/aplikacji?
57	Czy i jakie rozpoznano zagrożenia dotyczące ochrony danych?	Jakie zagrożenia dotyczą określonych kategorii danych?	Czy i jakie zagrożenia dotyczą moich systemów?
58	Czy zidentyfikowano właściwy poziom bezpieczeństwa danych przetwarzanych w systemach?	Czy dla każdego zbioru danych określono wymagany poziom bezpieczeństwa?	Jaki poziom bezpieczeństwa jest wymagany dla każdego zbioru w moich systemach?
59	Czy jest prowadzona wymagana dokumentacja?	Jaka dokumentacja jest prowadzona opisującą sposób przetwarzania danych i środki techniczne i organizacyjne zapewniające ochronę danych?	Jaką prowadzę dokumentację opisującą sposoby przetwarzania danych i środki techniczne i organizacyjne zapewniające ochronę danych w moich systemach?
60	Czy pracownicy wyznaczeni do dostępu do danych osobowych podpisują zobowiązania do ochrony danych osobowych.	Gdzie są przechowywane zobowiązania pracowników do ochrony danych osobowych? Czy są weryfikowane?	
61	Czy do przetwarzania danych dopuszczone są wyłącznie osoby upoważnione?	W jaki sposób dokonywane jest upoważnianie osób? Czy osoby przetwarzające dane osobowe otrzymały upoważnienia? Czy potwierdzone kopie upoważnienia są zarchiwizowane?	Jakie osoby są upoważnione do dostępu i przetwarzania danych w moich systemach? Czy ja dostałem takie upoważnienie?
62	Czy jest prowadzona ewidencja osób upoważnionych? W jakiej formie jest prowadzona ewidencja osób upoważnionych?	Czy prowadzona ewidencja osób upoważnionych zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia oraz identyfikator w systemach informatycznych?	Czy mam możliwość weryfikacji upoważnień do moich systemów?
63	Czy zostały wprowadzone mechanizmy rozliczalności przetwarzania danych?	Jakie są stosowane mechanizmy kontroli nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone lub zmodyfikowane i komu są przekazywane?	Czy w moich systemach są zaimplementowane i stosowane mechanizmy rozliczalności przetwarzania danych?
64	Czy upoważnione osoby są zobowiązywane do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia?	W jaki sposób są gromadzone potwierdzenia zobowiązania do zachowania tajemnicy?	

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
Dokumentacja i szkolenia (art.39a oraz Rozporządzenie)			
65	Czy organizacja posiada Politykę Bezpieczeństwa Informacji (w sensie ISO 27001/17799)?	Czy uczestniczę w tworzeniu i aktualizowaniu Polityki Bezpieczeństwa Informacji?	Czy znam Politykę Bezpieczeństwa Informacji?
66	Czy w Polityce Bezpieczeństwa Informacji zawarta jest polityka bezpieczeństwa danych osobowych?	Jakie elementy ogólnej Polityki Bezpieczeństwa Informacji dotyczą ochrony danych osobowych?	Czy procedury i instrukcje ogólnej Polityki Bezpieczeństwa informacji odnoszą się do ochrony danych osobowych?
67	Czy jest opracowana i zatwierdzona polityka bezpieczeństwa ochrony danych osobowych?	Czy polityka bezpieczeństwa zawiera wymagane Rozporządzeniem informacje? (zgodnie z par.4)	Czy uczestniczę w procesie opracowywania polityki bezpieczeństwa?
68	Czy polityka bezpieczeństwa ochrony danych osobowych jest aktualna?	Kiedy i w jaki sposób była weryfikowana ostatnio polityka bezpieczeństwa?	Czy uczestniczę w procesie aktualizacji i weryfikacji polityki bezpieczeństwa?
69	Czy dokumentacja opisująca sposób przetwarzania i zabezpieczenia danych jest prowadzona prawidłowo?	Czy istniejąca dokumentacja jest aktualna? Czy jest formalnie zatwierdzona? Czy zawiera okres ważności/weryfikacji?	Czy mam dostęp do aktualnej dokumentacji?
70	Czy jest opracowana i zatwierdzona instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych?	Czy "Instrukcja" zawiera wymagane Rozporządzeniem informacje? (zgodnie z par.5)	Czy uczestniczę w procesie opracowywania "Instrukcji"?
71	Czy "Instrukcja" jest aktualna?	Kiedy i w jaki sposób była weryfikowana ostatnio "Instrukcja"?	Czy uczestniczę w procesie aktualizacji i weryfikacji "Instrukcji"?
72	Czy dokumentacja została wdrożona?	W jaki sposób została wdrożona polityka bezpieczeństwa oraz "Instrukcja"?	Czy znana jest mi polityka bezpieczeństwa oraz "Instrukcja"?
73	Czy osoby upoważnione zostały zapoznane z dokumentacją przetwarzania?	Jakie jest potwierdzenie zapoznania się z dokumentacją przez osoby upoważnione?	Czy zapoznałem się z dokumentacją?
74		Czy jest prowadzona dodatkowa dokumentacja opisująca zasady przetwarzania i zabezpieczania danych?	Czy znana jest mi dodatkowa dokumentacja?
75	Czy są dostępne szkolenia z zakresu ochrony danych osobowych dla pracowników?	Czy jestem odpowiedzialny za szkolenia?	Czy uczestniczyłem w szkoleniach dotyczących ochrony danych w naszej firmie/organizacji?
Zabezpieczenie techniczne – poufność (art. 39a oraz Rozporządzenie)			
76	Czy są wyznaczone obszary przetwarzania danych osobowych?	Czy są wyznaczone obszary przetwarzania danych osobowych?	Czy znam obszary przetwarzania danych osobowych?

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
77		Czy dostęp do obszarów przetwarzania danych jest zabezpieczony i kontrolowany?	Czy moje systemy/aplikacje są w chronionych obszarach?
78		Jakie są fizyczne zabezpieczenia instalacji informatycznych, baz danych i nośników zawierających dane osobowe?	Jakie zabezpieczenia fizyczne stosuje się bezpośrednio do moich systemów?
79		Kto jest odpowiedzialny za fizyczne bezpieczeństwo instalacji informatycznych, baz danych i nośników zawierających dane osobowe?	Kto jest odpowiedzialny za fizyczne bezpieczeństwo moich systemów?
80		Czy osoby nieupoważnione przebywające w obszarach przetwarzania danych osobowych zawsze są pod nadzorem osób upoważnionych?	Czy w „moim" obszarze przetwarzania danych osobowych osoby nieupoważnione są pod nadzorem?
81		Czy systemy informatyczne mają kontrolę dostępu zapewniającą jednoznaczną identyfikację i uwierzytelnianie?	Czy administrowane przeze mnie systemy mają kontrolę dostępu zapewniającą jednoznaczną identyfikację i uwierzytelnianie?
82		W jaki sposób są weryfikowane nadane uprawnienia dostępu do systemów?	Czy w moim systemie są weryfikowane uprawnienia dostępu?
83		Czy do uwierzytelniania użytkowników stosowane są zasady dotyczące długości i składni haseł oraz okresu ich ważności stosownie do poziomu bezpieczeństwa?	Jakie zasady uwierzytelniania użytkowników stosuję w moich systemach?
84		Czy nośniki danych osobowych przed ich likwidacją, naprawą bądź przekazaniem osobom nieuprawnionym są pozbawione zapisów?	Czy nośniki danych z moich systemów przed ich likwidacją, naprawą bądź przekazaniem osobom nieuprawnionym są pozbawione zapisów?
85		Czy do przesyłania danych musimy stosować metody kryptograficzne?	Jakie metody kryptograficzne są używane do przesyłania danych z/do moich systemów?
86		Czy w dostępie do/z sieci publicznej stosowane są zabezpieczenia fizyczne i logiczne?	Jakie zabezpieczenia fizyczne i logiczne w dostępie do/z sieci publicznej są stosowane do zabezpieczenia moich systemów?
87		Czy dla urządzeń przenośnych (np. laptopów) zawierających dane osobowe stosowane są szczególne metody zabezpieczeń?	Czy dane z moich systemów są przetwarzane na urządzeniach przenośnych? Na czym polegają szczególne metody zabezpieczeń urządzeń przenośnych?

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
88		Jakie są stosowane dodatkowe zabezpieczenia poufności danych?	Jakie dodatkowe zabezpieczenia poufności stosowane są dla moich systemów?
Zabezpieczenie techniczne – integralność (art. 39a oraz Rozporządzenie)			
89		Czy w systemach są rejestrowane informacje dotyczące daty wprowadzenia do systemu i identyfikator użytkownika wprowadzającego?	Czy w moim systemie informatycznym są rejestrowane informacje dotyczące daty wprowadzenia do systemu i identyfikator użytkownika wprowadzającego?
90		Czy informacje o dostępie i zmianach są automatycznie rejestrowane?	Czy informacje o dostępie i zmianach w moim systemie są automatycznie rejestrowane?
91		Czy w systemach są rejestrowane informacje dotyczące źródła danych, nie od osoby, której one dotyczą?	Czy w moim systemie są rejestrowane informacje dotyczące źródła danych, nie od osoby, której one dotyczą?
92		Czy w dostępie do/z sieci publicznej stosowane są zabezpieczenia fizyczne i logiczne?	Jakie zabezpieczenia fizyczne i logiczne w dostępie do/z sieci publicznej są stosowane do zabezpieczenia moich systemów?
93		Jakie są stosowane dodatkowe zabezpieczenia integralności danych?	Jakie dodatkowe zabezpieczenia integralności stosowane są dla moich systemów?
Zabezpieczenie techniczne – dostępność (art.39a oraz Rozporządzenie)			
94		Jakie są stosowane systemy bezpieczeństwa (alarmy, system gaszenia) i systemy środowiskowe (temperatura, wilgotność) dotyczące pomieszczeń, w których znajdują się instalacje informatyczne, bazy danych lub nośniki zawierających dane osobowe?	Jakie są stosowane systemy bezpieczeństwa środowiskowego w pomieszczeniach gdzie zlokalizowane są moje systemy?
95		Kto jest odpowiedzialny za systemy bezpieczeństwa i systemy środowiskowe?	Kto jest odpowiedzialny za bezpieczeństwo środowiskowe moich systemów?
96		Czy są wykonywane kopie zapasowe oraz czy mają zapewnioną fizyczną ochronę nie gorszą niż dane źródłowe?	Czy są wykonywane kopie zapasowe z moich systemów i gdzie są przechowywane?
97		W jaki sposób zapewnia się, że dostęp do kopii zapasowych jest ograniczony i ściśle kontrolowany?	W jaki sposób ograniczamy i kontrolujemy dostęp do kopii zapasowych?
98	Kto odpowiada za wyznaczenie okresów retencji przechowywania danych?	Kto wyznaczył okresy retencji danych oraz kto i w jaki sposób zapewnia realizację tego wymogu?	Jaki jest okres retencji powierzonych mi danych i w jaki sposób go zapewniam?

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
99		Czy dla zapewnienia ciągłości pracy systemów stosowane są systemy awaryjnego zasilania?	Czy moje systemy mają zabezpieczenia przed skutkami braku lub zakłóceń zasilania?
100		Czy zabezpieczenia dostępności do danych są częścią planów BCP/DRP firmy/organizacji?	
101		Jakie są stosowane dodatkowe zabezpieczenia dostępności do danych?	Jakie dodatkowe zabezpieczenia dostępności stosowane są dla moich systemów?
Monitorowanie bezpieczeństwa (art.39a oraz Rozporządzenie)			
102	Czy są monitorowane wdrożone zabezpieczenia?	W jaki sposób dokonywane jest monitorowanie wdrożonych zabezpieczeń?	Czy i w jaki sposób są monitorowane zabezpieczenia dotyczące moich systemów?
103		W jaki sposób są rejestrowane wyniki monitorowania wdrożonych zabezpieczeń?	Czy negatywne zapisy z monitorowania zabezpieczeń dotyczyły moich systemów?
104		W jaki sposób są realizowane zalecenia z monitorowania?	Czy są zalecenia dotyczące moich systemów?
Kontrola wewnętrzna			
105	Czy kontrola wewnętrzna dotyczy zagadnień ochrony przetwarzania danych osobowych?	Kiedy była przeprowadzana ostatnia kontrola wewnętrzna?	Czy kontrola wewnętrzna dotyczyła moich systemów?
106		Jakie zostały przedstawione wnioski i rekomendacje z kontroli?	Czy wnioski i rekomendacje dotyczyły moich systemów?
107		Czy opracowano plan wdrożenia rekomendacji z kontroli?	Czy został opracowany plan wdrożenia rekomendacji dotyczący moich systemów?
108	Czy wszystkie rekomendacje zostały wdrożone?	Czy rekomendacje zostały wprowadzone?	Czy wdrożyłem rekomendacje?
Anonimizacja (art. 2)			
109	Czy zbiory, które nie powinny być dalej przetwarzane, są niszczone bądź poddawane anonimizacji?	W jaki sposób zbiory są niszczone lub poddawane anonimizacji? Jakie są procedury i dowody na wykonanie tych czynności?	W jaki sposób są niszczone bądź poddawane anonimizacji zbiory administrowane przeze mnie? W jaki sposób dokumentowane są te czynności?
KOMUNIKACJA ZEWNĘTRZNA			
GIODO (rozdz. 2)			
110	Czy zostały opracowane procedury współpracy z GIODO w czasie kontroli?	Jakie są procedury współpracy z GIODO w czasie kontroli?	Czy biorę udział w kontroli GIODO?
111	Czy zostały opracowane procedury rejestracji zbiorów w GIODO?	Jakie są procedury rejestracji zbiorów?	Czy zbiory przetwarzane w moich systemach zostały zarejestrowane w GIODO?

Lp.	Administrator Danych Osobowych lub Administrator Zarządzający	Administrator Bezpieczeństwa Informacji (ABI)	Administrator Wykonawczy (np. systemu/aplikacji /serwera/danych)
112		Czy stosujemy platformę elektronicznej rejestracji zbiorów E-GIODO?	
Osoba, której dane dotyczą (rozdz. 4)			
113	Czy osoby, których dane gromadzimy, są o tym fakcie informowane?	W jaki sposób Administrator Danych Osobowych informuje o gromadzeniu danych?	
114	Czy są opracowane procedury realizacji praw osoby, której dane dotyczą?	Jakie są procedury realizacji praw osoby, której dane dotyczą (roz.4)?	Czy system / aplikacja ma możliwość wydruku w formie zrozumiałej danych osoby, której dane dotyczą?
115	Czy są procedury zaprzestania przetwarzania danych w razie sprzeciwu?	Jakie są procedury zaprzestania przetwarzania danych w razie sprzeciwu?	
Inne przepisy (art. 4, 5)			
116	Czy przetwarzanie danych osobowych w firmie podlega przepisom odrębnych ustaw i/lub umów międzynarodowych?	Jakim przepisom odrębnych ustaw i/lub umów międzynarodowych podlega przetwarzanie danych osobowych w firmie/organizacji?	Czy dane w moich systemach podlegają pod specjalne ustawy i/lub umowy międzynarodowe?
Audyty zewnętrzne			
117	Czy audyty zewnętrzne dotyczyły zagadnień przetwarzania danych osobowych?	Kiedy był przeprowadzony ostatni audyt?	Czy audyt dotyczył moich systemów?
118		Jakie zostały przedstawione wnioski i rekomendacje?	Czy wnioski i rekomendacje dotyczyły moich systemów?
119		Czy zostały one wprowadzone w życie?	Czy wdrożyłem rekomendacje?

2.3. Mapowanie

2.3.1 Schemat COBIT – krótki opis

COBIT® (Control Objectives for Information and Related Technology) to schemat ładu informatycznego, który umożliwia kierownictwu firmy opracowanie dobrych praktyk nadzoru i kontroli IT w całej firmie i zorganizowanie czynności IT w ramach domen i procesów IT. Najnowsza wersja COBIT 4.1 kładzie nacisk na zgodność z regulacjami prawnymi, pomaga firmom zwiększyć wartość osiąganą z IT, umożliwia dopasowanie IT do biznesu oraz upraszcza wdrożenie schematu COBIT.

Możliwość zastosowania schematu COBIT w odniesieniu do zarządzania i nadzoru nad systemami informatycznymi pod kątem zgodności z Ustawą o ochronie danych osobowych może pomóc w ocenie i osiągnięciu tej zgodności.

Schemat COBIT 4.1 identyfikuje:

- 4 domeny informatyczne oznaczone:
  - **PO** - Planowanie i organizacja,
  - **AI** - Nabywanie i wdrażanie,
  - **DS** - Dostarczanie i obsługa,
  - **ME** - Monitorowanie i ocena.
- 34 procesy IT,
- 210 celów kontrolnych przypisanych poszczególnym procesom,
- 7 kryteriów informacji: efektywność, wydajność, poufność, integralność, dostępność, zgodność, rzetelność,
- 4 rodzaje zasobów: aplikacje, informacje, infrastruktura, ludzie,
- mechanizmy kontrolne w aplikacji (AC), zdefiniowane jako zautomatyzowane mechanizmy kontrolne zakodowane w aplikacji biznesowej,
- macierze odpowiedzialności (RACI), zawierające wskazówki dotyczące ról i odpowiedzialności na poszczególnych stanowiskach, czyli kto będzie rozliczany (A), odpowiedzialny (R), konsultowany (C) bądź informowany (I),
- mierniki wyznaczone dla procesów IT - pokazują jak te procesy spełniają cele biznesowe i IT; obejmują: kluczowe wskaźniki wydajności (KPI), kluczowe wskaźniki celu procesu i kluczowe wskaźniki celu IT (KGI),
- poziomy dojrzałości procesów: nieistniejący (0), początkujący (1), powtarzalny (2), zdefiniowany (3), zarządzany (4) lub zoptymalizowany (5).

W celu zastosowania schematu COBIT do zarządzania, nadzoru, kontroli i audytu systemów informatycznych pod kątem zgodności z UODO, należy skorzystać z następujących opracowań IT Governance Institute®:

- COBIT 4.1 [1], zawiera Wytyczne Zarządzania,
- COBIT® Control Practices [2], zawiera Praktyki Kontrolne,
- IT Assurance Guide using COBIT® [3], zawiera Wytyczne Zapewnienia.

Poniższe tabele zawierają mapowanie artykułów Ustawy i paragrafów Rozporządzenia na cele kontrolne schematu COBIT 4.1. Dla porządku w obecnej wersji Wytycznej pozostawiliśmy także mapowanie na cele kontrolne zdefiniowane w metodyce COBIT 3rd Edition [4].

2.3.2 Ustawa/COBIT

Ustawa	Cele kontrolne COBIT 4.1	Cele kontrolne COBIT 3rd Edition
ROZDZIAŁ 1 Przepisy ogólne		
Artykuł 1	ME3.1-4	PO8.1, PO8.2
Artykuł 2	ME3.1-4, PO2.2	PO8.1, PO8.2, PO2.2
Artykuł 3	ME3.1-4	PO8.1, PO8.2
Artykuł 3a	ME3.1-4	PO8.1, PO8.2
Artykuł 4	ME3.1-4	PO8.1, PO8.2
Artykuł 5	ME3.1-4	PO8.1, PO8.2
Artykuł 6	ME3.1-4	PO8.1, PO8.2, PO2.2
Artykuł 7	ME3.1-4, PO2.2	PO8.1, PO8.2
ROZDZIAŁ 2 Organ ochrony danych osobowych		
Artykuł 8, 9, 10, 11, 12, 12a, 13 - nie dotyczy		
Artykuł 14	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 15	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 16	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 17	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 18	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 19, 20, 21, 22, 22a - nie dotyczy		
ROZDZIAŁ 3 Zasady przetwarzania danych osobowych		
Artykuł 23	ME3.1-4, PO4.9, PO6.3	PO8.1, PO8.2, PO4.7, PO4.8, PO6.2
Artykuł 24	ME3.1-4, PO4.8-9, PO4.15, PO6.3	PO8.1, PO8.2, PO4.6, PO4.7, PO4.15, PO6.2
Artykuł 25	ME3.1-4, PO4.8-9, PO4.15, PO6.3	PO8.1, PO8.2, PO4.6, PO4.7, PO4.15, PO6.2
Artykuł 26	ME3.1-4, PO2.3, PO4.8-9, PO6.3, DS11.2, DS11.4	PO8.1, PO8.2, PO2.2, PO4.7, PO4.8, PO6.2, DS11.19-22
Artykuł 26a	ME3.1-4, PO6.3, AI2.3, AC5	PO8.1, PO8.2, PO6.2, DS11.12
Artykuł 27	ME3.1-4, PO2.3, PO6.3, AC1	PO8.1, PO8.2, PO2.2, PO6.2, DS11.1
Artykuł 28	ME3.1-4, PO2.3, PO6.3	PO8.1, PO8.2, PO2.2, PO6.2
Artykuł 29	ME3.1-4, PO2.3, PO6.3, AC5, AC6	PO8.1, PO8.2, PO6.2, DS2.7, DS5.8, DS11.12-13, DS11.16
Artykuł 30	ME3.1-4, PO6.3, AC5, AC6	PO8.1, PO8.2, PO6.2, DS11.12-13, DS11.16
Artykuł 31	ME3.1-4, PO2.3, PO4.15, PO6.3, AI5.2, DS2.3-4, DS5.11, AC5, AC6	PO8.1, PO8.2, PO4.15, PO6.2, DS2.3, DS2.5, DS2.7-8, DS5.8, DS11.17
Artykuł 31a	ME3.1-4, PO6.3	PO8.1, PO8.2, PO8.4, PO6.2
ROZDZIAŁ 4 Prawa osoby, której dane dotyczą		
Artykuł 32	ME3.1-4, PO4.15, DS8.1-4	PO8.1, PO8.2, PO4.15, DS10.1
Artykuł 33	ME3.1-4, PO4.15, DS8.1-4	PO8.1, PO8.2, PO4.15, DS10.1

Ustawa	Cele kontrolne COBIT 4.1	Cele kontrolne COBIT 3rd Edition
Artykuł 34	ME3.1-4, PO4.15, DS8.1-4	PO8.1, PO8.2, PO4.15, DS10.1
Artykuł 35	ME3.1-4, PO4.15, PO6.3, DS8.1-4	PO8.1, PO8.2, PO4.15, PO6.2, DS10.1
ROZDZIAŁ 5 Zabezpieczenie danych osobowych		
Artykuł 36	ME3.1-4, PO2.3, PO4.6, PO4.8, PO4.15, PO6.1-3, DS5.1-2, DS5.5	PO8.1, PO8.2, PO4.4, PO4.6, PO6.8, PO6.11, DS5.1-11, DS7.3
Artykuł 37	ME3.1-4, PO4.8-9, DS5.4	PO8.1, PO8.2, PO4.7, PO4.8
Artykuł 38	ME3.1-4, DS11.6, AC1, AC2, AC5	PO8.1, PO8.2, DS11.6, DS11.12, DS11.13, DS11.16
Artykuł 39	ME3.1-4, PO4.15, DS5.3-4	PO8.1, PO8.2, PO4.15, PO6.8, PO6.11, DS5.4, DS7.3
Artykuł 39a – oddzielnie		
ROZDZIAŁ 6 Rejestracja zbiorów danych osobowych		
Artykuł 40	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 41	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 42	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 43	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 44	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 44a	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 45 - (uchylony)		
Artykuł 46	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
Artykuł 46a	ME3.1-4, PO6.3	PO8.1, PO8.2, PO6.2
ROZDZIAŁ 7 Przekazywanie danych osobowych do państwa trzeciego		
Artykuł 47	ME3.1-4, AC6	PO8.1, PO8.2, PO8.4, DS11.17
Artykuł 48	ME3.1-4, AC6	PO8.1, PO8.2, PO8.4, DS11.17

2.3.3 Rozporządzenie/COBIT

Rozporządzenie	Cele kontrolne COBIT 4.1	Cele kontrolne COBIT 3rd Edition
§ 1.	ME3.1-4, PO6.2	PO8.1, PO8.2, PO6.8
§ 2.	ME3.1-4	PO8.1, PO8.2
§ 3.	PO4.8, DS5.2	PO4.6, DS5.1
§ 4.	PO2.2-3, DS5.2, DS5.7, DS5.10, DS12.1-2	PO2.2, PO6.8, DS5.1, DS12.1
§ 5.	PO6.2	PO6.8
pkt 1)	DS5.3-4	DS5.2-6, DS5.9
pkt 2)	AI2.3-4, DS5.3-4	DS5.2-6, DS5.9
pkt 3)	PO7.8	DS5.2-6, DS5.9
pkt 4)	DS11.5	DS11.19-22, DS11.26
pkt 5)	DS11.2-5	DS11.19-22, DS11.26
pkt 6)	DS5.9	DS5.19
pkt 7)	PO2.3, AC5	DS2.7, DS5.8, DS11.16
pkt 8)	AI1.1, AI2.10, DS5.2	DS5.1
§ 6.	PO2.3, DS5.1-4, DS5.7-8, DS5.10-11	PO2.2, PO2.4, DS5.8
poziom bezp.A	DS5.3-4, DS5.8-9, DS11.2-6, DS12.3, DS12.5	
poziom bezp.B	jak dla poziomu A + DS5.11	
poziom bezp.C	jak dla poziomu A + DS5.10-11	
§ 7.	PO2.2, DS5.3	PO2.2, DS5.2, DS5.4
§ 8.	ME3.1-4	PO8.1, PO8.2
§ 9.	ME3.1-4	PO8.1, PO8.2
§ 10.	ME3.1-4	PO8.1, PO8.2

2.4. Zastosowanie COBIT 4.1 do badania zgodności z UODO

Znając cele kontrolne IT[1] wyznaczone dla systemów informatycznych przetwarzających dane osobowe możemy zastosować schemat COBIT do ustalenia mechanizmów[2] i praktyk[3] kontrolnych odpowiednich dla tych systemów w celu zapewnienia zgodności z UODO. COBIT pomoże również ustalić mierniki oraz poziomy dojrzałości procesów informatycznych pod kątem zgodności z Ustawą.

2.4.1 Przykład

Niniejsza tabela zawiera wskazówki dotyczące zastosowania metodyki COBIT na przykładzie art.26 Ustawy i celu kontrolnego DS11.2.

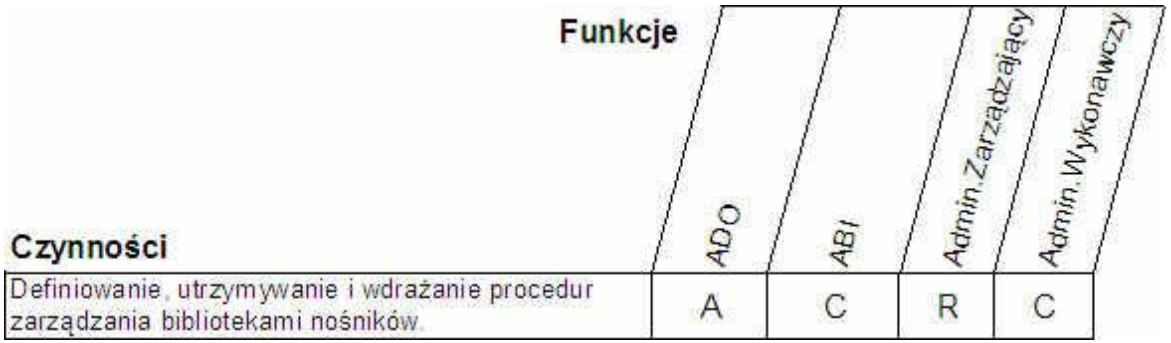
MAPOWANIE		
UODO	**Cele kontrolne COBIT 4.1**	**Cele kontrolne COBIT 3rd Edition**
Artykuł 26 Ustawy: 1. Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były: 1)… 3)... 4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. 2.	ME3.1-4, PO2.3, PO4.8-9, PO6.3, **DS11.2** DS11.4	PO8.1, PO8.2, PO2.2, PO4.7, PO4.8, PO6.2, DS11.19-22

1 Cel kontrolny (ang. control objective) - deklaracja pożądanego wyniku lub celu, który powinien zostać osiągnięty poprzez wdrożenie procedur kontrolnych dla poszczególnych czynności IT. Cele kontrolne określone w schemacie COBIT stanowią minimalne wymagania dla efektywności mechanizmów kontrolnych poszczególnych procesów IT. Każdy proces IT ma zdefiniowany kilka celów kontrolnych.

2 Mechanizm kontrolny (ang. control) - polityki, procedury, praktyki i struktury organizacyjne, które mają dostarczyć racjonalne zapewnienie osiągnięcia celów biznesowych oraz zabezpieczyć struktury przed niepożądanymi zdarzeniami lub je wykryć i naprawić.

3 Praktyki kontrolne (ang. control practices) - dostarczają wskazówek jak, dlaczego i co należy wdrożyć dla każdego celu kontrolnego, by ulepszyć sprawność IT i/lub zająć się ryzykami związanymi z dostarczaniem rozwiązań i usług IT.

<table>
<tr><th colspan="3">COBIT Cel kontrolny: DS11.2 Ustalenia dotyczące przechowywania i składowania</th></tr>
<tr><td colspan="3">Opis: Należy zdefiniować i wdrożyć procedury dla efektywnego i wydajnego przechowywania, składowania i archiwizowania danych w celu osiągania celów biznesowych oraz spełniania polityki bezpieczeństwa firmy i wymagań prawnych.</td></tr>
<tr><th>Publikacja COBIT 4.1</th><th>Wykorzystanie</th><th>Przykład</th></tr>
<tr><td rowspan="4">COBIT 4.1

Schemat
Cele kontrolne
Wytyczne zarządzania
Modele dojrzałości</td><td rowspan="4">Można wykorzystać do:
- powiązania celów IT z celami biznesowymi,
- zmierzenia stopnia osiągnięcia celów za pomocą zdefiniowanych mierników i modeli dojrzałości,
- zidentyfikowania związanych z tym odpowiedzialności właścicieli procesów biznesowych i IT,
- zdefiniowania celów kontrolnych, które kierownictwo powinno uwzględniać,
- zidentyfikowania najważniejszych zasobów IT, na które należy oddziaływać</td><td>Kluczowa czynność:
Definiowanie, utrzymywanie i wdrażanie procedur zarządzania bibliotekami nośników</td></tr>
<tr><td>Kluczowy cel czynności:
Zarządzanie przechowywaniem danych na miejscu i na zewnątrz</td></tr>
<tr><td>Kluczowe mierniki:
- Liczba incydentów związanych z odzyskaniem danych wrażliwych po likwidacji nośników
- Liczba incydentów spowodowanych nieprzestrzeganiem przepisów prawnych dotyczących zarządzania przechowywaniem danych</td></tr>
<tr><td>Tabela RACI:
 
</td></tr>
<tr><td>Praktyki kontrolne COBIT

COBIT Control Practices: Guidance to</td><td>Dostarczają wskazówek jak, dlaczego i co należy wdrożyć dla każdego celu kontrolnego, by ulepszyć sprawność IT i/lub zająć się ryzykami związanymi z dostarczaniem rozwiązań i</td><td>Praktyka kontrolna:
2. Należy ustalić zasady przechowywania i składowania dokumentów, danych, archiwów, programów, raportów i komunikatów (przychodzących i wychodzących) w celu spełnienia wymagań prawnych i biznesowych</td></tr>
</table>

Achieve Control Objectives for Successful IT Governance, 2nd Edition	usług IT. Wspierają zapobieganie, wykrywanie i naprawianie niepożądanych zdarzeń poprzez odpowiedzialne wykorzystanie zasobów, odpowiednie zarządzanie ryzykiem i dostarczanie wartości dla biznesu.	
	Obejmują deklaracje wartości i ryzyk pomocne w wyrażeniu, dlaczego warto wdrożyć dany cel kontrolny	**Wyznacznik ryzyka:** *Brak zgodności z przepisami prawa*
Wytyczne zapewnienia IT Assurance Guide: Using COBIT®	Można wykorzystać w celu dostarczenia wiarygodnego zapewnienia dotyczącego wewnętrznych mechanizmów kontrolnych, ulepszeń procesów, itp. oraz poświadczenia opinii i rekomendacji dotyczących proponowanych ulepszeń	**Testowanie projektu mechanizmów kontrolnych dla celu kontrolnego:** *Należy dokonać przeglądu okresów składowania danych, by upewnić się, że są zgodne z wymaganiami kontraktowymi i prawnymi*
		Testowanie wyniku celu kontrolnego: *Należy zbadać narzędzia do zarządzania danymi, by upewnić się, że są używane zgodnie z opisem*
		Dokumentowanie skutków słabości mechanizmu kontrolnego: *Należy sprawdzić, czy uwzględniono poufność, integralność i dostępność danych, jak również stosowne przepisy*

3. DODATKI

3.1. Bibliografia

3.1.1 Wydane przez IT Governance Institute®

Dostępne na stronach www.itgi.org oraz www.isaca.org.
Opracowania oznaczone 🔓 można pobrać po zarejestrowania się na stronie.
Opracowania oznaczone 🔒 są zastrzeżone dla członków ISACA.

[1] COBIT 4.1 🔓
[2] COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition (dostępne tylko w księgarni ISACA)
[3] IT Assurance Guide using COBIT® 🔒
[4] COBIT® 3rd Edition Control Objectives (wycofane)
[5] COBIT Security Baseline™: An Information Security Survival Kit, 2nd Edition 🔒
[6] COBIT Mapping Overview of International IT Guidance, 2nd Edition
[7] COBIT Mapping: Mapping of ISO/IEC 17799: 2005 With COBIT 4.0 🔒
[8] Aligning COBIT®, ITIL® and ISO 17799 for Business Benefit

3.1.2 Wydane przez ISACA®

[9] G31 IS Auditing Guideline: Privacy

3.1.3 Wydane przez GIODO

Opracowane przez Departament Informatyki Biura Generalnego Inspektora Ochrony Danych Osobowych (dostępne na stronach www.giodo.gov.pl)

[10] Wytyczne w zakresie opracowania i wdrożenia polityki bezpieczeństwa
[11] Wskazówki dotyczące sposobu opracowania instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem wymogów bezpieczeństwa informacji
[12] Wymagania dotyczące struktur baz danych osobowych oraz funkcjonalności zarządzających nimi aplikacji

3.1.4 Wydane przez APDCM

[13] e-PRODAT: e-Government and Data Protection in European Regions and Cities

3.1.5 Dostępne w księgarniach

[14] Janusz Barta, Paweł Fajgielski, Ryszard Markiewicz – “Ochrona danych osobowych – komentarz”, wyd.3, 2004, Kantor Wydawniczy ZAKAMYCZE

3.2. Słownik

Niniejszy słownik zawiera pojęcia związane z ochroną danych osobowych w systemach informatycznych. Został opracowany w celu ułatwienia korzystania z dokumentów w języku angielskim.

Objaśnienie:

- kol.1 - pojęcie związane z ochroną danych osobowych,
- kol.2 - opis pojęcia zawarty w Ustawie lub Rozporządzeniu,
- kol.3 - numer artykułu Ustawy lub paragrafu Rozporządzenia zawierającego opis pojęcia,
- kol.4 - angielski odpowiednik pojęcia podany w oficjalnym tłumaczeniu Ustawy,
- kol.5 - odpowiednik pojęcia występujący w dokumentacji COBIT,
- kol.6 - odpowiednik pojęcia występujący w projekcie wytycznej ISACA dot. prywatności,
- kol.7 - odpowiednik pojęcia występujący w ustawach innych państw.

Pojęcie	Opis pojęcia z Ustawy	Art.	Pojęcie-EN	COBIT	IS Audit Guideline - Privacy	Ustawy innych państw[x]
1	2	3	4	5	6	7
Administrator Bezpieczeństwa Informacji ABI	nadzorujący przestrzegania zasad ochrony	art. 36	administrator of information security	information security manager	privacy officer	internal data protection officer (HU)
Administrator Danych Osobowych	organ, jednostka organizacyjna, podmiot lub osoba decydujące o celach i środkach przetwarzania danych osobowych	art. 7 (art. 3)	controller	management	data controller	chief processor (EE)
administrator systemu, bazy danych, aplikacji		-		data custodian	data custodian	
anonimizacja danych		art. 2	data rendered anonymous			data rendered unidentifiable (AU)
dane doraźne	sporządzane wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji	art. 2	data files prepared ad hoc			
dane osobowe	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej	art. 6	personal data		- personal data / information - personally identifiable information	
dane wrażliwe		-		sensitive information	sensitive data	sensitive data
firma trzecia	podmiot, któremu powierzono przetwarzanie danych	art. 31	another subject	third-party	external partner	processor (AU,CZ,GR) authorised processor (EE)
gromadzenie danych		-			data collection	collection of data (AU)
hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym	§ 2		password		

[x] Inne państwa: AU-Austria, CZ- Czechy, D- Niemcy, EE- Estonia, GR- Grecja, HU- Węgry

Pojęcie	Opis pojęcia z Ustawy	Art.	Pojęcie-EN	COBIT	IS Audit Guideline - Privacy	Ustawy innych państw[x]
1	2	3	4	5	6	7
identyfikator użytkownika	ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym	§ 2		user ID	user ID	
instrukcja	zawartość określona w par.5 Rozporządzenia	§ 5		security plan	security plan	
integralność	właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany	§ 2		integrity	integrity	
kategoria danych		art. 36		data classification		
kontrola dostępu	dotyczy dostępu do danych osobowych	zał.II		access control	access control	
kopia zapasowa	dotyczy zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania	§ 5		back-up	data back-up	
likwidacja	pozbawienie nośnika zapisu danych, a w przypadku gdy nie jest to możliwe, uszkodzenie go w sposób uniemożliwiający ich odczytanie;	zał.VI		disposal		
odbiorca danych	każdy, komu udostępnia się dane osobowe (z wyjątkami)	art. 7	data recipient	user	third party	third person (EE)
	oprogramowanie, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego	zał.III		malicious software	malicious software	
osoba, której dane dotyczą	osoba fizyczna, której dane osobowe są lub mogą być przetwarzane w zbiorach danych	art. 2	data subject		data subject	
państwo trzecie	państwo nie należące do Europejskiego Obszaru Gospodarczego	art. 7	third country			
polityka bezpieczeństwa	zawartość określona w par.4 Rozporządzenia	§ 4		security policy	security policy	
poufność	właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom	§ 2		confidentiality	confidentiality	

Pojęcie	Opis pojęcia z Ustawy	Art.	Pojęcie-EN	COBIT	IS Audit Guideline - Privacy	Ustawy innych państw[x]
1	2	3	4	5	6	7
powierzenie przetwarzania danych		art. 31	authorise another subject to carry out the processing	outsourcing	outsourcing	committing of data (AU)
przekazanie danych	przekazanie danych osobowych innemu Administratorowi Danych Osobowych	art. 38	transfer of data		transfer of data	
przekazanie danych za granicę	Przekazanie danych osobowych do państwa trzeciego	rozdz.7	transfer of data to a third country	transborder data flow	transborder flow of personal data	transfer abroad (D) transmission to foreign states (EE) transboundary flow (GR)
przetwarzanie danych	jakiekolwiek operacje wykonywane na danych osobowych	art. 7	processing of data	processing of data	treatment of personal information	
raport	przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych	§ 2		output		
rejestracja zbiorów danych	zgłoszenie zbioru danych do GIODO	rozdz. 6	registration of personal data filing systems			registration in the Data Processing Register (AU)
rozliczalność	właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi	§ 2	ability to map a given activity or event back to the responsible party	accountability	accountability	
sieć publiczna	sieć telekomunikacyjna nie będąca siecią wewnętrzną, służąca do świadczenia usług telekomunikacyjnych	§ 2		public network		

Pojęcie	Opis pojęcia z Ustawy	Art.	Pojęcie-EN	COBIT	IS Audit Guideline - Privacy	Ustawy innych państw[x]
1	2	3	4	5	6	7
sieć telekomunikacyjna	urządzenia telekomunikacyjne i linie telekomunikacyjne, zestawione i połączone w sposób umożliwiający przekaz sygnałów pomiędzy określonymi zakończeniami sieci, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną	§ 2		telecommunications		
środki bezpieczeństwa	środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną	§ 6		security measures	security measures / safeguards	
teletransmisja	przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej	§ 2		transmission		
udostępnienie danych	udostępnienie posiadanych w zbiorze danych innym osobom lub podmiotom	art.29,30	disclosure of data	disclosure	disclosure	
uprawnienia	dotyczy przetwarzania danych	§ 5		user authorisation	access privileges	
usuwanie danych	zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą	art.7	data erasure	deletion	data erasure / deletion / destruction	personal data liquidation (CZ)
uwierzytelnianie	działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu	§ 2		user authentication		
właściciel danych		-		data owner	information owner	
zabezpieczenie danych	w systemie informatycznym	art. 7 rozdz. 5	- security of data - protection of personal data	data security	- personal information protection / security - privacy controls	
zbiór danych osobowych	każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów	art. 7	data filing system	database	personal database	data file (CZ) file (GR)

3.3. Tablice mapowań

3.3.1 Ustawa/COBIT 4.1 - domeny PO, AI i ME

COBIT 4.1	ME3				PO2		PO4				PO6			AI2	AI5
Ustawa	3.1	3.2	3.3	3.4	2.2	2.3	4.6	4.8	4.9	4.15	6.1	6.2	6.3	2.3	5.2
1	X	X	X	X											
2	X	X	X	X	X										
3	X	X	X	X											
3a	X	X	X	X											
4	X	X	X	X											
5	X	X	X	X											
6	X	X	X	X											
7	X	X	X	X	X										
14	X	X	X	X									X		
15	X	X	X	X									X		
16	X	X	X	X									X		
17	X	X	X	X									X		
18	X	X	X	X									X		
23	X	X	X	X					X				X		
24	X	X	X	X				X	X	X			X		
25	X	X	X	X				X	X	X			X		
26	X	X	X	X		X		X	X				X		
26a	X	X	X	X									X	X	
27	X	X	X	X		X							X		
28	X	X	X	X		X							X		
29	X	X	X	X		X							X		
30	X	X	X	X									X		
31	X	X	X	X		X				X			X		X
31a	X	X	X	X									X		
32	X	X	X	X						X					
33	X	X	X	X						X					
34	X	X	X	X						X					
35	X	X	X	X						X			X		

COBIT 4.1	ME3				PO2		PO4				PO6			AI2	AI5
Ustawa	3.1	3.2	3.3	3.4	2.2	2.3	4.6	4.8	4.9	4.15	6.1	6.2	6.3	2.3	5.2
36	X	X	X	X		X	X	X		X	X	X	X		
37	X	X	X	X				X	X						
38	X	X	X	X											
39	X	X	X	X						X					
40	X	X	X	X									X		
41	X	X	X	X									X		
42	X	X	X	X									X		
43	X	X	X	X									X		
44	X	X	X	X									X		
44a	X	X	X	X									X		
46	X	X	X	X									X		
46a	X	X	X	X									X		
47	X	X	X	X											
48	X	X	X	X											

3.3.2 Ustawa/COBIT 4.1 - domena DS oraz AC

COBIT 4.1	DS2		DS5						DS8				DS11			AC					
Ustawa	2.3	2.4	5.1	5.2	5.3	5.4	5.5	5.11	8.1	8.2	8.3	8.4	11.2	11.4	11.6	1	2	3	4	5	6
23																					
24																					
25																					
26													X	X							
26a																				X	
27																X					
28																					
29																				X	X
30																				X	X
31	X	X						X												X	X
31a																					
32									X	X	X	X									
33									X	X	X	X									
34									X	X	X	X									
35									X	X	X	X									
36			X	X			X														
37						X															
38															X	X	X			X	
39					X	X															
47																					X
48																					X

3.3.3 Rozporządzenie/COBIT 4.1

COBIT 4.1	ME3				PO2		PO4	PO6	PO7	AI1	AI2			AC
Rozp.	3.1	3.2	3.3	3.4	2.2	2.3	4.8	6.2	7.8	1.1	2.3	2.4	2.10	5
§ 1	X	X	X	X				X						
§ 2	X	X	X	X										
§ 3							X							
§ 4					X	X								
§ 5								X						
pkt.1														
2											X	X		
3									X					
4														
5														
6														
7						X								X
8										X			X	
§ 6						X								
§ 7					X									
§ 8	X	X	X	X										
§ 9	X	X	X	X										
§ 10	X	X	X	X										

Rozporządzenie/COBIT 4.1 c.d.

COBIT 4.1	DS5									DS11					DS12			
Rozp.	5.1	5.2	5.3	5.4	5.7	5.8	5.9	5.10	5.11	11.2	11.3	11.4	11.5	11.6	12.1	12.2	12.3	12.5
§ 1																		
§ 2																		
§ 3		X																
§ 4		X			X			X							X	X		
§ 5																		
pkt.1			X	X														
2			X	X														
3																		
4													X					
5										X	X	X	X					
6							X											
7																		
8		X																
§ 6	X	X	X	X	X	X		X	X									
A			X	X		X	X			X	X	X	X	X			X	X
B			X	X		X	X		X	X	X	X	X	X			X	X
C			X	X		X	X	X	X	X	X	X	X	X			X	X
§ 7			X															
§ 8																		
§ 9																		
§ 10																		

3.4. Procesy i cele kontrolne CobiT 4.1 występujące w mapowaniu

Numer	Nazwa angielska	Nazwa polska
ME	**Monitor and Evaluate**	**Monitorowanie i ocena**
Proces **ME3**	ENSURE COMPLIANCE WITH EXTERNAL REQUIREMENTS	ZAPEWNIANIE ZGODNOŚCI Z WYMAGANIAMI ZEWNĘTRZNYMI
ME3.1	Identification of External Legal, Regulatory and Contractual Compliance Requirements	Identyfikacja zewnętrznych wymagań prawnych i umownych
ME3.2	Optimisation of Response to External Requirements	Optymalizacja reakcji na wymagania zewnętrzne
ME3.3	Evaluation of Compliance With External Requirements	Ocena zgodności z wymaganiami zewnętrznymi
ME3.4	Positive Assurance of Compliance	Pozytywne zapewnienie zgodności
PO	**Plan and Organise**	**Planowanie i organizacja**
Proces **PO2**	DEFINE THE INFORMATION ARCHITECTURE	WYZNACZANIE ARCHITEKTURY INFORMATYCZNEJ
PO2.2	Enterprise Data Dictionary and Data Syntax Rules	Firmowy słownik danych i reguły składni danych
PO2.3	Data Classification Scheme	Schemat klasyfikacji danych
Proces **PO4**	DEFINE THE IT PROCESSES, ORGANISATION AND RELATIONSHIPS	OKREŚLANIE PROCESÓW, ORGANIZACJI I POWIĄZAŃ IT
PO4.6	Establishment of Roles and Responsibilities	Ustanowienie ról i odpowiedzialności
PO4.8	Responsibility for Risk, Security and Compliance	Odpowiedzialność za ryzyko, bezpieczeństwo i zgodność
PO4.9	Data and System Ownership	Określenie własności danych i systemów
PO4.15	Relationships	Określenie relacji
Proces **PO6**	COMMUNICATE MANAGEMENT AIMS AND DIRECTION	KOMUNIKOWANIE CELÓW I KIERUNKÓW WYZNACZONYCH PRZEZ KIEROWNICTWO
PO6.1	IT Policy and Control Environment	środowisko kontrolne i polityki IT
PO6.2	Enterprise IT Risk and Control Framework	Schemat ryzyk i kontroli IT firmy
PO6.3	IT Policies Management	Zarządzanie politykami IT
PO6.4	Policy, Standard and Procedures Rollout	Dystrybucja polityk, standardów i procedur
PO6.5	Communication of IT Objectives and Direction	Komunikowanie celów i kierunków IT
Proces **PO7**	MANAGE IT HUMAN RESOURCES	ZARZĄDZANIE ZASOBAMI LUDZKIMI IT
PO7.8	Job Change and Termination	Zmiana pracy i zwolnienie z pracy
AI	**Acquire and Implement**	**Nabywanie i wdrażanie**
Proces **AI1**	IDENTIFY AUTOMATED SOLUTIONS	IDENTYFIKOWANIE ROZWIĄZAŃ ZAUTOMATYZOWANYCH
AI1.1	Definition and Maintenance of Business Functional and Technical Requirements	Definiowanie i utrzymanie biznesowych wymagań funkcjonalnych i technicznych
Proces **AI2**	ACQUIRE AND MAINTAIN APPLICATION SOFTWARE	NABYWANIE I UTRZYMYWANIE OPROGRAMOWANIA

Numer	Nazwa angielska	Nazwa polska
		APLIKACYJNEGO
AI2.3	Application Control and Auditability	Mechanizmy kontrolne i możliwości audytowe w aplikacjach
AI2.4	Application Security and Availability	Bezpieczeństwo i dostępność aplikacji
AI2.10	Application Software Maintenance	Konserwacja aplikacji
Proces **AI5**	PROCURE IT RESOURCES	POZYSKANIE ZASOBÓW IT
AI5.2	Supplier Contract Management	Zarządzanie umowami z dostawcami
DS	**Deliver and Support**	**Dostarczanie i obsługa**
Proces **DS2**	MANAGE THIRD-PARTY SERVICES	ZARZĄDZANIE USŁUGAMI ZEWNĘTRZNYMI
DS2.3	Supplier Risk Management	Zarządzanie ryzykiem związanym z dostawcami
DS2.4	Supplier Performance Monitoring	Monitorowanie sprawności dostawców
Proces **DS5**	ENSURE SYSTEMS SECURITY	ZAPEWNIANIE BEZPIECZEŃSTWA SYSTEMÓW
DS5.1	Management of IT Security	Zarządzanie bezpieczeństwem IT
DS5.2	IT Security Plan	Plan bezpieczeństwa IT
DS5.3	Identity Management	Zarządzanie tożsamością
DS5.4	User Account Management	Zarządzanie kontami użytkowników
DS5.5	Security Testing, Surveillance and Monitoring	Testowanie, nadzorowanie i monitorowanie bezpieczeństwa
DS5.7	Protection of Security Technology	Ochrona technologii IT
DS5.8	Cryptographic Key Management	Zarządzanie kluczami kryptograficznymi
DS5.9	Malicious Software Prevention, Detection and Correction	Zapobieganie, wykrywanie i usuwanie złośliwego oprogramowania
DS5.10	Network Security	Bezpieczeństwo sieci
DS5.11	Exchange of Sensitive Data	Wymiana danych wrażliwych
Proces **DS8**	MANAGE SERVICE DESK AND INCIDENTS	ZARZĄDZANIE WSPARCIEM I INCYDENTAMI
DS8.1	Service Desk	Biuro obsługi
DS8.2	Registration of Customer Queries	Rejestracja zapytań klientów
DS8.3	Incident Escalation	Eskalacja incydentów
DS8.4	Incident Closure	Zamknięcie incydentu
Proces **DS11**	MANAGE DATA	ZARZĄDZANIE DANYMI
DS11.2	Storage and Retention Arrangements	Ustalenia dotyczące przechowywania i składowania
DS11.3	Media Library Management System	System zarządzania biblioteką nośników
DS11.4	Disposal	Likwidacja
DS11.5	Backup and Restoration	Kopie zapasowe i ich przywracanie
DS11.6	Security Requirements for Data Management	Wymagania bezpieczeństwa dla zarządzania danymi
Proces **DS12**	MANAGE THE PHYSICAL ENVIRONMENT	ZARZĄDZANIE ŚRODOWISKIEM FIZYCZNYM
DS12.1	Site Selection and Layout	Wybór i plan obiektu

Numer	Nazwa angielska	Nazwa polska
DS12.2	Physical Security Measures	Środki bezpieczeństwa fizycznego
AC	**Application Controls**	**Mechanizmy kontrolne w aplikacjach**
AC1	Source Data Preparation and Authorisation	Procedury przygotowania i autoryzacji danych źródłowych
AC2	Source Data Collection and Entry	Zbieranie i wprowadzanie danych źródłowych
AC3	Accuracy, Completeness and Authenticity Checks	Weryfikacja dokładności, kompletności i autentyczności
AC4	Processing Integrity and Validity	Integralność i ważność przetwarzania
AC5	Output Review, Reconciliation and Error Handling	Przeglądanie i uzgadnianie wyników oraz obsługa błędów
AC6	Transaction Authentication and Integrity	Uwierzytelnianie i integralność transakcji