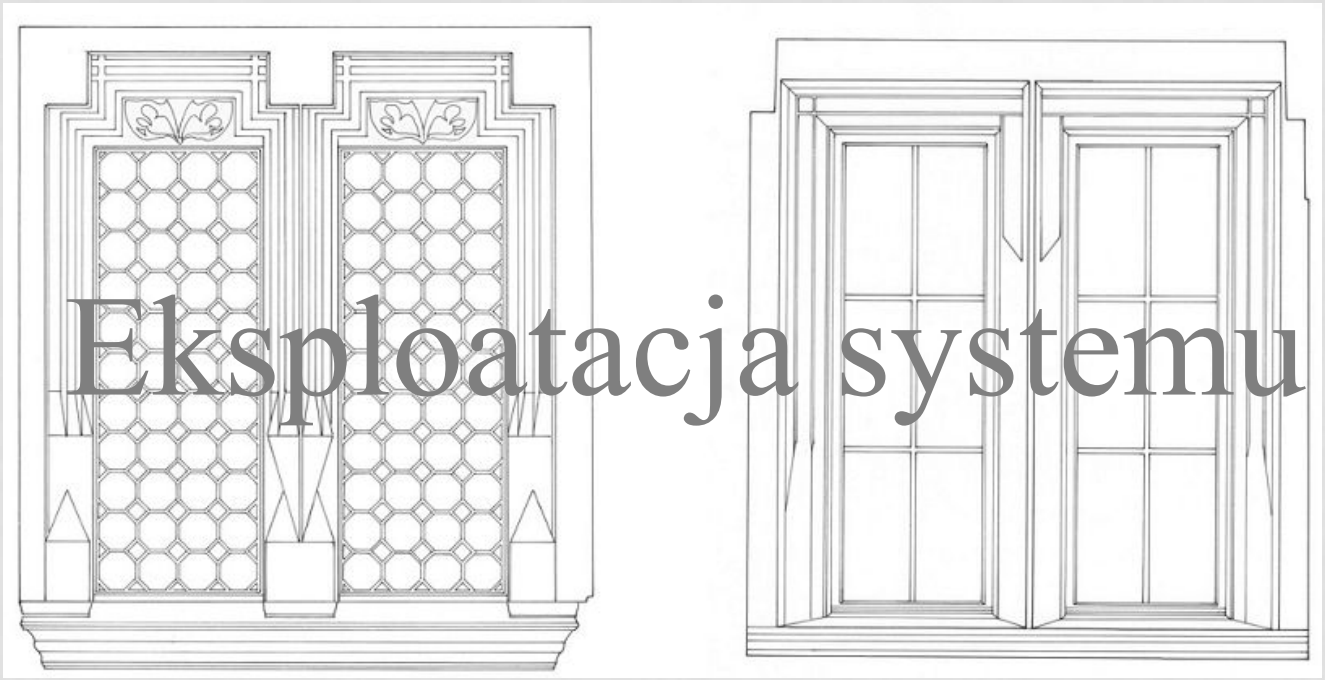


Eksploatacja systemu

Eksploatacja systemu informatycznego obejmuje dwa równolegle przebiegające procesy:

· użytkowanie (uzyskiwanie określonych informacji w żądanej formie i czasie),

· obsługiwanie (konserwacja, modernizacja, rozwój).

Podczas eksploatacji systemu wszystkie zadania użytkowe systemu powinny być wykonywane przy możliwie najniższych kosztach własnych i z zachowaniem wymienionych poniżej parametrów eksploatacyjnych systemu.

- *czas uzyskiwania informacji*
  (czas odpowiedzi systemu, czas obsługi transakcji, itp.),

- *wiarygodność informacji*
  (mierzona odsetkiem błędów na wyjściu systemu – błędy mogą być spowodowane awariami sprzętu i oprogramowania, nieuwagą lub niedbałością personelu – muszą być usuwane zarówno błędy jak ich przyczyny),

- *poziom ochrony danych*
  (ochrona integralności danych, ochrona dostępu do danych),

- *diagnostyczność systemu*
  (łatwość i szybkość ustalania przyczyny uszkodzenia systemu),

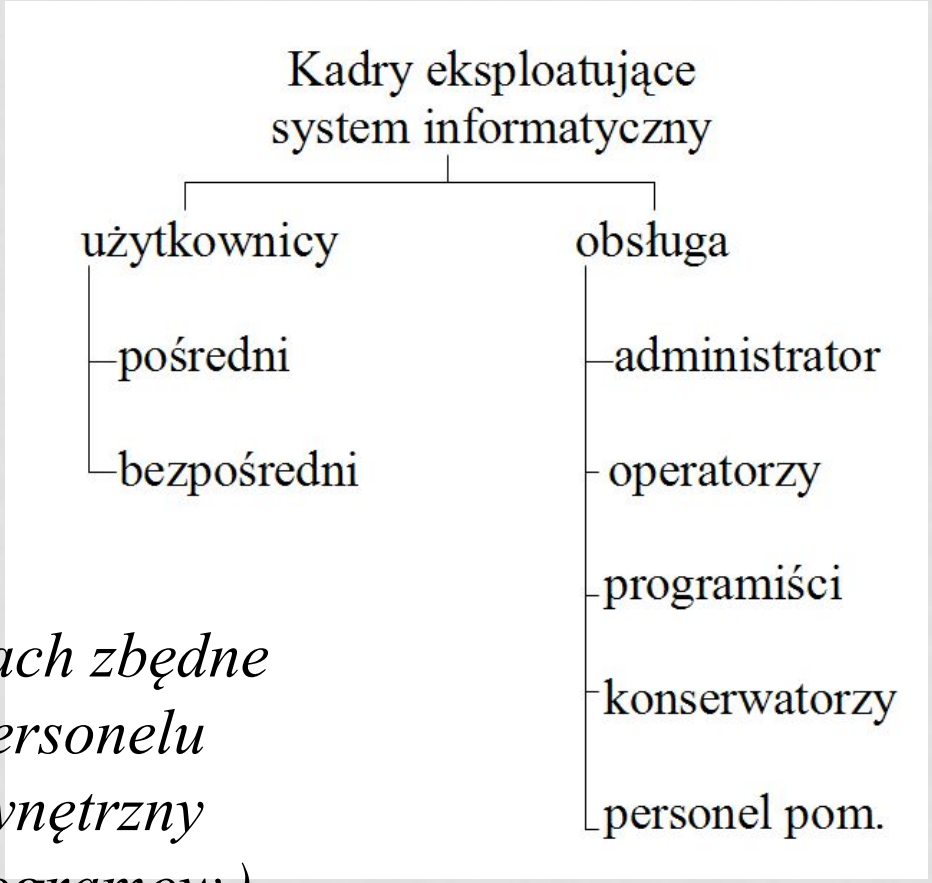
- *elastyczność systemu*
  (stopień swobody przy dostosowywaniu systemu do zmieniających się warunków eksploatacji),

- *niezawodność system*u
  (techniczna, oprogramowania, odporność na błędy użytkownika),

- *koszty eksploatacji*.

Organizacja eksploatacji

1. Struktura kadr



W prostych systemach zbędne jest zatrudnianie personelu obsługującego (zewnętrzny serwis techn. i oprogramow.)

Organizacja eksploatacji

2. Główny cel obsługi systemu

a) konserwacja,
b) modernizacja,
c) rozwój.

b) i c) wymagają znacznie większych sił i środków (nakładów) niż a).

Organizacja eksploatacji

3. Dobór strategii obsługi systemu

Jeśli idzie o czas reakcji:

a) wg stanu

działania naprawcze podejmuje się w razie stwierdzenia uszkodzenia bądź realnego zagrożenia systemu (np. powtórne indeksowanie bazy),

Organizacja eksploatacji

b) wg resursu

wykonywanie czynności obsługi po określonych (w uzasadniony sposób) okresach użytkowania (np. cotygodniowe przeglądy i testowanie poprawności działania modułów komputerów, elementów sieci, modułów oprogramowania – testy integralności bazy).

Organizacja eksploatacji

Jeśli idzie o ocenę całego systemu:

a) wg niezawodności

(działania podejmowane na podstawie wyników okresowej kontroli poziomu niezawodności)

Organizacja eksploatacji

b) wg efektywności

(działania mające na celu usunięcie skutków moralnego starzenia się systemu - system a potrzeby informacyjne użytkowników, ergonomiczność systemu).

Monitory programowe – programy rejestrujące odpowiednie dane eksploatacyjne systemu (są zawarte w systemie operacyjnym bądź w oprogramowaniu użytkowym).

Monitorowanie procesu przetwarzania danych przebiega w trakcie przetwarzania i może dotyczyć:

- pracy poszczególnych elementów systemu komputerowego lub sieci,

-przebiegu wykonania aplikacji,

- statyki i dynamiki plików/baz danych.

Administrator systemu

Główne zadania administratora w trakcie eksploatacji systemu to:

- reagowanie na reklamacje użytkowników,

- rozpoznawanie przyczyn uszkodzeń,

- uruchamianie procedur ich likwidacji.

Administrator systemu

Inne zadania administratora:

- rutynowe działania w celu utrzymania sprawnego działania systemu (reorganizacja baz, kontrola integralności baz, zmiana kluczy ochrony),

- przywracanie normalnego stanu systemu za pomoca standardowych procedur (odtwarzanie baz, odłączanie urządzeń generujących błędy, etc.).

Administrator systemu

- zabezpieczanie systemu przed skutkami uszkodzeń (backup, archiwizacja, etc.),

- uruchamianie diagnostyki systemu,

- udostępnianie systemu nowym użytkownikom, analiza naruszeń praw dostępu

- ochrona systemu przed wirusami komputerowymi.

Ochrona danych w systemie informatycznym

A. Ochrona integralności danych

zapewnienie poprawności, kompletności i dostępności danych

B. Ochrona dostępu do danych

uzyskanie odpowiedniego poziomu tajności i poufności danych

Ochrona danych w systemie informatycznym

Środki ochrony danych:

·prawne,
·administracyjno-organizacyjne,
·sprzętowe,
·programowe (w systemie operac. i aplikacji).

Ochrona danych w systemie informatycznym

Zagrożenia integralności danych:

1. przekłamanie pojedynczej danej w trakcie wprowadzania do systemu,
2. zagubienie rekordu lub powiązania między rekordami,
3. zniszczenie pliku lub części bazy danych,
4. utrata wszystkich plików lub całej bazy danych.

Ochrona danych w systemie informatycznym

Przeciwdziałanie:

1. kontrola danych podczas wprowadzania,
2. redundancja informacyjna (cyfry i sumy kontrolne),
3. backup i archiwizacja danych,
4. specjalizowane rozwiązania sprzętowe i programistyczne (system transakcji, miroring, dupleksing, macierze dyskowe),
5. programy diagnostyki danych,
6. programy antywirusowe.

Ochrona danych w systemie informatycznym

Zagrożenia ochrony dostępu do danych:

1. wykonywanie zadań przez nieuprawnionych użytkowników,

2. odczytanie i/lub zniszczenie danych tajnych lub poufnych.

Ochrona danych w systemie informatycznym

Przeciwdziałanie:

1. fizyczna kontrola dostępu do pomieszczeń lub stanowisk,

2. karty identyfikacyjne uprawniające do pracy,

3. indywidualne hasła dostępu do zasobów systemu,

Ochrona danych w systemie informatycznym

4. nadawanie użytkownikom systemu uprawnień do wykonywania określonych zadań i kontrola ich wykorzystania,

5. prowadzenie dziennika ochrony systemu,

6. szyfrowanie zawartości plików i przesyłanych komunikatów.

Akty prawne bezpośrednio związane z użytkowaniem oprogramowania komputerowego wspomagającego zarządzanie

·*„Ustawa o prawie autorskim i prawach pokrewnych” z 4.02.1994r.*

1) Prawnoautorskie ujęcie oprogramowania komputerowego
2) Oprogramowanie komputerowe w obrocie gospodarczym

- *„Ustawa o ochronie danych osobowych” z 29.08.1997r.*

- *RODO (ang. General Data Protection Regulation, GDPR) - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*

http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32016R0679& from=EN

- *„Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych”*

GIODO UODO i PUODO

RODO podlega każdy przedsiębiorca, który prowadzi działalność w Unii Europejskiej.

Może to być działalność w jakiejkolwiek formie prawnej: spółka, jednoosobowa działalność gospodarcza, czy nawet oddział w Unii Europejskiej przedsiębiorcy mającego siedzibę poza Unią.

Nie ma znaczenia narodowość osób, których dane osobowe są przetwarzane. Nie ma znaczenia to, gdzie są przetwarzane dane osobowe (gdzie znajdują się serwery).

Przykłady:

• korzystanie przez polską spółkę z o. o. z usług przetwarzania danych w chmurze nie zwalnia tej spółki z konieczności
stosowania RODO,

• polski podmiot oferujący swoje usługi obywatelom Ukrainy podlega przepisom RODO,

• oddział w Polsce przedsiębiorcy z USA podlega przepisom RODO.

RODO znajdzie zastosowanie nawet wtedy, gdy podmioty spoza Unii Europejskiej oferują swoje towary i usług osobom przebywający w Unii.

RODO nie znajduje zastosowania do działalności osobistej lub domowej.

To oznacza, że osoba fizyczna prowadząca działalność gospodarczą musi stosować RODO do danych osobowych swoich klientów, czy pracowników, ale nie stosuje RODO do danych przetwarzanych w celach czysto prywatnych, np. do danych adresatów wysyłanych corocznie kartek świątecznych.

RODO stosuje się do przetwarzania danych osobowych. Przetwarzaniem danych osobowych są jakiekolwiek operacje wykonywane na danych osobowych, takie jak:

- zbieranie danych,
- przechowywanie danych (zgoda 10 lat, umowa 3 lata, inne)
- usuwanie danych,
- opracowywanie danych,
- udostępnianie danych.

Dane osobowe to wszelkie informacje **odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.**

Osobą zidentyfikowaną jest taka osoba, której tożsamość znamy, którą możemy wskazać spośród innych osób.

Osobą możliwą do zidentyfikowania jest taka osoba, której tożsamości nie znamy, ale możemy poznać, korzystając z tych środków, które mamy.

Przykłady:

• osoba zidentyfikowana: pracownik, którego dane osobowe przetwarza pracodawca; klient sklepu internetowego, który podał swoje dane osobowe do wysyłki zamówienia; osoba, która w formularzu kontaktowym podaje swoje imię, nazwisko i adres e-mail,

• osoba możliwa do zidentyfikowania: potencjalny kontrahent, którego posiadamy tylko numer ewidencyjny w CEIDG; nadawca listu poleconego na podstawie numeru przesyłki;

Wyróżnia się dwie kategorie danych osobowych:

a)tzw. dane osobowe zwykłe,

b) dane osobowe zaliczające się do szczególnych kategorii danych (dawniej zwane danymi wrażliwymi).

Do szczególnych kategorii danych osobowych zaliczamy dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

Dane osobowe, które nie należą do żadnej z tych kategorii, to dane zwykłe. Zgodnie z RODO, do kategorii danych osobowych zwykłych należą także dane osobowe dotyczące wyroków skazujących.

Jeżeli jakiś przedsiębiorca przetwarza dane osobowe, to może to robić jako jeden z dwóch kategorii podmiotów:

- administrator danych,
- podmiot przetwarzający dane.

Administrator danych to taki podmiot, który decyduje o celach i sposobach przetwarzania danych. Innymi słowy, decyduje o tym, po co (cele) i jak (sposoby) wykorzystać dane osobowe.

Przykłady:

- pracodawca w stosunku do danych osobowych swoich pracowników,

- sprzedawca w sklepie internetowym w stosunku do danych osobowych swoich klientów,

- właściciel strony internetowej w stosunku do danych osobowych osób, które zaprenumerowały newsletter.

Administratorem danych jest zawsze określony podmiot – np. spółka, a **nie jego pracownik**.

Przykłady:

• administratorem danych jest spółka z o.o., a nie jej prezes zarządu, czy dyrektor marketingu,

• administratorem danych jest Jan Kowalski prowadzący jednoosobową działalność gospodarczą.

Podmiot przetwarzający dane osobowe nie decyduje o celach i środkach przetwarzania danych – działa na podstawie umowy z administratorem danych.

Administrator danych może bowiem albo sam przetwarzać dane, albo skorzystać z usług zewnętrznego podmiotu, który te dane będzie przetwarzał dla niego.

Przykłady:

• biuro rachunkowe przetwarza na zlecenie dane osobowe przekazane mu w tym celu przez klientów,

• podmiot utrzymujący na zlecenie swoich klientów konta poczty elektronicznej przetwarza na zlecenie dane osobowe,

• podmiot zajmujący się profesjonalnie niszczeniem danych osobowych przetwarza w tym zakresie dane osobowe na zlecenie swoich klientów.

Podmiot przetwarzający dane na zlecenie powinien zawrzeć z administratorem danych odpowiednią umowę, tzw. **umowę powierzenia**, w której określone zostaną zasady przetwarzania danych.

W danej organizacji, dane osobowe faktycznie przetwarzają konkretne osoby fizyczne – pracownicy lub współpracownicy administratora lub podmiotu przetwarzającego dane.

Takie osoby powinny posiadać upoważnienie do przetwarzania danych osobowych (uprawnienia w systemie informatycznym!).

Dane osobowe można przetwarzać wyłącznie wtedy, gdy istnieje tzw. podstawa prawna przetwarzania danych.

W przypadku przedsiębiorców, typowymi podstawami przetwarzania danych zwykłych są:

a) zgoda osoby, której dane dotyczą,
b) przetwarzanie danych jest niezbędne do wykonania umowy z osobą, której dane dotyczą lub do podjęcia działań poprzedzających zawarcie umowy, na żądanie tej osoby,
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
d) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią.

W przypadku szczególnych kategorii danych, typowe podstawy przetwarzania danych to:

a)wyraźna zgoda osoby, której dane dotyczą,

b) przetwarzanie danych jest niezbędne do wykonania zadań związanych z zatrudnieniem, ubezpieczeniem społecznym pracowników,

c) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika
do pracy,

d) przetwarzanie danych jest niezbędne w celu dochodzenia praw przed sądem.

Zawsze to administrator danych powinien móc wykazać, że dysponuje odpowiednią podstawą przetwarzania danych.

Jest to prawny obowiązek administratora danych wynikający z tzw. **zasady rozliczalności**.

RODO wprowadza tzw. **zasadę minimalizacji** danych osobowych. Zgodnie z nią, można przetwarzać wyłącznie takie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania danych.

Przetwarzanie danych powinno więc zostać ograniczone do takich danych, bez których nie można osiągnąć celu przetwarzania danych.

Przykład – jeżeli celem przetwarzania danych jest realizacja zamówienia w sklepie internetowym, przetwarzanie danych o sytuacji rodzinnej, czy finansowej klienta, nie będzie dopuszczalne.

Przetwarzanie takich danych byłoby dopuszczalne, ale w innym celu, np. w celu marketingowym, na innej podstawie prawnej.

Użyte powyżej definicje i przykłady pochodzą z: „Przewodnik po RODO dla małych i średnich przedsiębiorców”, Autor: dr Paweł Litwiński, Min. Przeds. i Technologii

·„*Ustawa o rachunkowości”*
z 29.09.1994r.

Komputer w prowadzeniu księgowości
(Ust. z dn. 29.09.1994 r., Dz.U.Nr 121, poz. 591)
Wg art. 10 ustawy jednostka powinna posiadać dokumentację systemu przetwarzania danych przy użyciu komputera, która zawiera co najmniej:

1. Wykaz i opis zbiorów danych tworzących system
2. Opis funkcji modułów - programów wchodzących w skład systemu
3. Opis sposobów ochrony danych (trwałość, nienaruszalność)
4. Opis sposobów zapewnienia właściwego stosowania programów
5. Opis zasad ewidencji przebiegu przetwarzania danych

- *„Ustawa z 18 września 2001 r. o podpisie elektronicznym”*

- *„Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE”*

https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32014R0910

- *„Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej”*

Zgodnie z art. 10 ustawy o usługach zaufania oraz identyfikacji elektronicznej, Narodowe Centrum Certyfikacji wykonuje następujące zadania:

- *tworzy i wydaje kwalifikowanym dostawcom usług zaufania certyfikaty służące do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych,*
- *publikuje certyfikaty,*
- *publikuje listy unieważnionych certyfikatów,*
- *tworzy dane do opatrywania pieczęcią elektroniczną wydanych certyfikatów, oraz certyfikatów do weryfikacji tych pieczęci (tzw. certyfikaty narodowego centrum certyfikacji).*

Narodowe Centrum Certyfikacji nie świadczy kwalifikowanych usług zaufania w rozumieniu ustawy o usługach zaufania i identyfikacji elektronicznej (w szczególności nie wydaje kwalifikowanych certyfikatów) – zajmują się tym inne podmioty zwane ***kwalifikowanymi dostawcami usług zaufania****. Według stanu na dzień 17 listopada 2016 r. w Polsce działa pięciu kwalifikowanych dostawców usług zaufania. Są to:*

Asseco Data Systems S.A. (Certum)
Enigma Systemy Ochrony Informacji Sp. z o.o. (Cencert)
Eurocert Sp. z o.o. (Eurocert)
Krajowa Izba Rozliczeniowa S.A. (KIR)
Polska Wytwórnia Papierów Wartościowych SA (PWPW)

Elementy niezbędne do podpisania dokumentu:

- certyfikat zawierający informacje o właścicielu Certyfikatu
- klucz publiczny, który służy do weryfikacji podpisu
- klucz prywatny, który w przypadku certyfikatu kwalifikowanego znajduje się na karcie kryptograficznej
- urządzenie do odczytu kart
- aplikacja podpisująca

Zastosowanie:

- kontakty drogą elektroniczną, kontakty prawne oraz podpisywanie deklaracji z ZUS,
- składanie e-deklaracji do Urzędu Skarbowego,
- pozyskiwanie wypisów elektronicznych z KRS,
- składanie formularzy do KIO,
- zawieranie umów cywilno-prawnych drogą elektroniczną,
- wystawianie faktur w formie elektronicznej,
- branie udziału w aukcjach i przetargach,
- podpisywanie raportów do GIIF,
- przesyłanie e-deklaracji do UFG,
- przesyłanie drogą elektroniczną zbiorów danych osobowych do GIODO,
- składanie droga elektroniczną wniosków o dotacje unijne do PARP,
- podpisywanie wniosków do GUS RG-1, RG-2.

- *„USTAWA z dnia 27 lipca 2001 r. o ochronie baz danych”*

- *„USTAWA z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną”*