



Regulamin

Dostępu Klientów Zewnętrznych do Zasobów Teleinformatycznych Operatora Gazociągów Przesyłowych Gaz-System S.A.

Spis treści

1. Cel dokumentu.....	3
2. Definicje	4
3. Zgłoszenie zapotrzebowania na uzyskanie, zmianę lub anulowanie prawa dostępu.....	6
4. Zasady przyznania lub odmowy	7
5. Realizacja decyzji	8

1. CEL DOKUMENTU

§ 1

1. Niniejszy Regulamin jest dokumentem regulującym zasady przyznawania, zmiany oraz odbierania Prawa dostępu Użytkownikom Zewnętrznym do Zasobów Teleinformatycznych OGP Gaz-System S.A oraz do Informacji podlegających w nich Przetwarzaniu
2. Celem wprowadzenia jest zapewnienie czytelnych zasad przyznawania zmiany oraz odbierania Prawa dostępu do Zasobów Teleinformatycznych OGP Gaz-System S.A. oraz do Informacji podlegających w nich Przetwarzaniu, dla Klientów Zewnętrznych.
3. Niniejsza dokument precyzuje ogólne zasady, w zakresie zasad przyznawania, zmiany oraz odbierania Praw dostępu Użytkownikom, zawarte w dokumentach „Polityka Bezpieczeństwa Teleinformatycznego” oraz „Regulamin dla Użytkowników zasobów teleinformatycznych w OGP GAZ-SYSTEM S.A.”
4. W zakresie nieuregulowanym w niniejszym Regulaminie, stosuje się odpowiednio postanowienia Polityki Bezpieczeństwa Teleinformatycznego oraz Regulamin dla Użytkowników zasobów teleinformatycznych w OGP GAZ-SYSTEM S.A.

2. DEFINICJE

§ 2

Występujące w niniejszym dokumencie zwroty oznaczają:

- 1) **OGP GAZ-SYSTEM S.A. – Operator Gazociągów Przesyłowych GAZ-SYSTEM S.A.;**
- 2) **Administrator systemu** – osoba odpowiedzialna za sprawne funkcjonowanie Systemów teleinformatycznych i przestrzeganie zasad i wymagań bezpieczeństwa Systemu teleinformatycznego i Sieci teleinformatycznej;
- 3) **Aplikacja** – oprogramowanie używane do wykonywania określonych zadań;
- 4) **Pion Informatyki** – Pion Informatyki w spółce w rozumieniu Regulaminu Organizacyjnego OGP GAZ-SYSTEM S.A.;
- 5) **Hasło dostępu** – ciąg znaków literowych, cyfrowych lub innych umożliwiający uwierzytelnienie Użytkownika;
- 6) **Identyfikator (LOGIN)** – logiczna nazwa jednoznacznie identyfikująca Użytkownika w wielodostępowym Systemie teleinformatycznym;
- 7) **Informacja** – każda informacja występująca w postaci danych elektronicznych przetwarzanych w Systemach teleinformatycznych, w tym zbiory danych, w szczególności każdy przekaz elektroniczny takich informacji, danych,
- 8) **Jednostka organizacyjna** - Pion lub Oddział stanowiący zgrupowanie komórek organizacyjnych (działów, terenowych jednostek eksploatacji lub samodzielnych stanowisk) podległych kierownikowi jednostki organizacyjnej i realizujących wyznaczone zadania w jednym lub kilku obszarach powiązanych merytorycznie albo realizujących jedną z funkcji OGP GAZ-SYSTEM S.A.
- 9) **Klient wewnętrzny** - Dyrektor Pionu lub osoba przez niego upoważniona oraz inne osoby upoważnione do podejmowania decyzji, w szczególności finansowych w zakresie określonym regulacjami wewnętrznymi OGP GAZ-System S.A. i odpowiadające za pewien zakres czynności na zajmowanym stanowisku.
- 10) **Klient zewnętrzny** - Użytkownik nie będący pracownikiem OGP GAZ-SYSTEM S.A., którego łączy lub którego pracodawcę/zleceniodawcę łączy z OGP GAZ-SYSTEM S.A. umowa
- 11) **Komórka organizacyjna** – komórka organizacyjna w rozumieniu Regulaminu Organizacyjnego OGP GAZ-SYSTEM S.A.
- 12) **Pion Audytu i Bezpieczeństwa** – Pion Audytu i Bezpieczeństwa w rozumieniu Regulaminu Organizacyjnego OGP GAZ-SYSTEM S.A..
- 13) **Polityka Bezpieczeństwa Teleinformatycznego** – dokument, stanowiący element składowy Polityki Bezpieczeństwa Informacji, określający szczegółowo wymagania, które należy spełnić, aby zapewnić bezpieczeństwo Systemów i Sieci teleinformatycznych w OGP GAZ-SYSTEM S.A. oraz regulujący



zasady zarządzania bezpieczeństwem Systemów teleinformatycznych, obowiązujący OGP GAZ-SYSTEM S.A.;

- 14) **Prawa dostępu** – lista określająca zakres działań, jakie Użytkownik może wykonać na w Zasobie teleinformatycznym w Systemie teleinformatycznym;
- 15) **Program destrukcyjny** – kod, który dokonuje zaprogramowanych przez jego autora niepożądanych zmian w środowisku systemowym uszkadzając dane i programy, w szczególności zmieniając sposób działania sprzętu, jak i Sieci teleinformatycznej;
- 16) **Przetwarzanie** – procesy związane z wytwarzaniem, zbieraniem, przeglądaniem, utrwalaniem, modyfikacją, przesyłaniem, przechowywaniem, opracowywaniem, przekazywaniem, przetwarzaniem, udostępnianiem lub usuwaniem Informacji;
- 17) **ServiceDesk** - punkt kontaktowy do komunikacji na styku służb informatyki, działających w Pionie Informatyki i Użytkowników;
- 18) **Sieć teleinformatyczna** – organizacyjne i techniczne połączenie systemów teleinformatycznych;
- 19) **System teleinformatyczny** – system, który tworzą urządzenia, narzędzia, Aplikacje, metody postępowania i procedury stosowane w sposób zapewniający Przetwarzanie Informacji w OGP GAZ-SYSTEM S.A.;
- 20) **Usługi teleinformatyczne** – zespół czynności podejmowanych przez służby informatyczne Spółki w odniesieniu do elementów Systemu teleinformatycznego, w celu zaspokojenia potrzeb Użytkowników, w zakresie wsparcia informatycznego realizowanych przez nich zadań;
- 21) **Użytkownik** - jest to każda osoba fizyczna, a w szczególności pracownik Spółki korzystający z Informacji oraz Systemów Teleinformatycznych oraz infrastruktury teleinformatycznej, na zasadach określonych w Polityce Bezpieczeństwa Teleinformatycznego;
- 22) **Właściciel biznesowy** – Klient wewnętrzny będący kierownikiem jednostki organizacyjnej odpowiedzialny merytorycznie za określony zakres zadań OGP Gaz-System S.A. dla wsparcia którego świadczona jest Usługa teleinformatyczna
- 23) **Zasoby informacyjne** – Informacje, w tym informacje dotyczące działalności Spółki i jej pracowników, w tym dane osobowe i tajemnice przedsiębiorstwa, w rozumieniu Regulaminu organizacyjnego Spółki, bez względu na sposób ich utrwalania, zawarte w Zasobie teleinformatycznym
- 24) **Zasób teleinformatyczny** – elementy sprzętowe oraz programowe Systemu teleinformatycznego, zapewniające podstawowe możliwości Przetwarzania Informacji (procesor, pamięć, urządzenia wejścia/wyjścia), elementy softwarowe oraz Informacje niezbędne do prawidłowego funkcjonowania Usług teleinformatycznych;

3. ZGŁOSZENIE ZAPOTRZEBOWANIA NA UZYSKANIE, ZMIANĘ LUB ANULOWANIE PRAWA DOSTĘPU

§ 3

1. Klient Wewnętrzny lub Właściciel biznesowy, który przewiduje konieczność nadania, zmiany lub anulowania Prawa dostępu dla Klienta Zewnętrznego, obejmującego dostęp do Zasobów Informacyjnych zobowiązany jest uzyskać pisemna lub w formie elektronicznej, akceptację Dyrektora Pionu Audytu i Bezpieczeństwa na dostęp do Zasobów Informacyjnych i w tym celu przekazać do Pionu Audytu i Bezpieczeństwa zgłoszenie zawierające wskazanie podstawy nadania, zmiany lub anulowania Prawa dostępu dla Klienta Zewnętrznego, w szczególności wynikające z umowy łączącej Klienta Zewnętrznego z OGP Gaz-SYSTEM S.A., z której wynika konieczność udostępnienia Zasobów Klientowi Zewnętrznemu, w tym osobom przez niego upoważnionym. Decyzja o akceptacji lub jej braku, jest podejmowana nie później niż w terminie 3 dni roboczych liczonych od daty dokonania zgłoszenia. W przypadku braku akceptacji Dyrektora Pionu Audytu i Bezpieczeństwa, w ww. terminie, do wnioskującego przekazywane jest dodatkowo uzasadnienie braku tej akceptacji.
2. Klient Wewnętrzny lub Właściciel biznesowy dokonuje zgłoszenia zapotrzebowania na uzyskanie, zmianę lub anulowanie Prawa dostępu do Pionu Informatyki, zgodnie z ust 3-5 oraz §4. przy czym dokonując zgłoszenia przekazuje również akceptację Dyrektora Pionu Audytu i Bezpieczeństwa na dostęp do Zasobów Informacyjnych
3. Zgłoszenia zapotrzebowania na uzyskanie, zmianę lub anulowanie Prawa dostępu dla Klienta Zewnętrznego dokonuje się za pośrednictwem:
 - a. **poczty korporacyjnej (e-mail) – bezpośrednio na adres SerwisDesku (preferowana forma kontaktu)**
 - b. telefonicznie – bezpośrednio do SerwisDesku.
4. Zgłoszenie zapotrzebowania na uzyskanie Prawa dostępu lub jego zmianę winno zawierać:
 - a. Imię Nazwisko Klienta Wewnętrznego dokonującego zgłoszenia
 - b. Dane identyfikujące Klienta Zewnętrznego oraz jego pracodawcy, wraz z danymi kontaktowymi;
 - c. cel przyznania Prawa dostępu oraz rodzaj wnioskowanego Zasobu oraz zakres Prawa dostępu, niezbędny do realizacji umowy łączącej OGP Gaz-System S.A. z Klientem Zewnętrznym lub jego pracodawcą.
 - d. określenie ram czasowych Prawa dostępu;
 - e. akceptacja zgoda Dyrektora Pionu Audytu i Bezpieczeństwa na dostęp do Zasobów Informacyjnych, w przypadku o którym mowa w ust 1
5. Zgłoszenie o anulowanie Prawa dostępu winno zawierać:
 - a. Imię Nazwisko Klienta Wewnętrznego dokonującego zgłoszenia,

- b. Dane identyfikujące Klienta Zewnętrznego oraz jego pracodawcy, wraz z danymi kontaktowymi;
- c. rodzaj Zasobu oraz zakres Prawa dostępu,
- d. datę utraty Prawa dostępu,

4. ZASADY PRYZNANIA LUB ODMOWY

§ 4

1. Z zastrzeżeniem ust 8, decyzję o przyznaniu lub odmowie przyznania Prawa dostępu, zmianie Prawa dostępu lub anulowaniu Prawa dostępu, podejmuje Dyrektor Pionu Informatyki lub inna osoba przez niego upoważniona, przy czym w przypadku gdy dane zgłoszenie, o którym mowa w §3 ust 2 dotyczy również dostępu do Zasobów Informacyjnych, podejmuje odpowiednie ww. decyzje o ile Dyrektor Pionu Audytu i Bezpieczeństwa dokonał akceptacji o której mowa w §3 ust 1, .
2. Decyzja, o której mowa w ust 1, jest podejmowana nie później niż w terminie 3 dni roboczych liczonych od daty dokonania zgłoszenia, o którym mowa w §3 ust.2.
3. W przypadku decyzji przyznającej/zmieniającej/ Prawo dostępu dla Klienta Zewnętrznego, z zastrzeżeniem ust 4-5, jest ona realizowana poprzez środowisko terminalowe funkcjonujące w OGP Gaz-System S.A., a wszelkie działania podejmowane w Systemie teleinformatycznym przez Klienta Zewnętrznego są monitorowane i mogą być nagrywane. Login nadawany jest zgodnie z Polityką Bezpieczeństwa Teleinformatycznego. Weryfikacja Klienta Zewnętrznego następuje poprzez login jednoznacznie go określający oraz hasło dostępu utworzone zgodnie z Polityką Bezpieczeństwa Teleinformatycznego.
4. W szczególnie uzasadnionych przypadkach w których zagrożone jest bezpieczeństwo Systemu teleinformatycznego lub bezpieczeństwo Zasobów Informacyjnych Spółki lub gdy przemawiają za tym względy techniczne, w sytuacji wydania decyzji przyznającej/zmieniającej/ Prawo dostępu dla Klienta Zewnętrznego, jest ona realizowana z wyłączeniem środowiska terminalowego funkcjonującego w OGP Gaz-System S.A., w tym z wyłączeniem urządzeń pośredniczących, przy czym wyłącznie wówczas gdy taką decyzję wydali łącznie Dyrektor Pionu Informatyki i Dyrektor Pionu Audytu i Bezpieczeństwa w formie pisemnej. Działający łącznie Dyrektor Pionu Informatyki i Dyrektor Pionu Audytu i Bezpieczeństwa są uprawnieni do wydania pisemnej decyzji o realizowaniu decyzji przyznającej/zmieniającej/ Prawo dostępu dla Klienta Zewnętrznego z wyłączeniem środowiska terminalowego funkcjonującego w OGP Gaz-System S.A., w sytuacjach o których mowa w zdaniu pierwszym niniejszego ustępu.
5. W przypadku decyzji przyznającej/zmieniającej Prawo dostępu dla Klienta Zewnętrznego do zdalnego Prawa dostępu, autoryzacja Klienta Zewnętrznego odbywa się poprzez login jednoznacznie go określający oraz hasło składającego się z pinu oraz zestawu haseł jednorazowych.
6. W przypadku decyzji odmawiającej przyznania/zmiany/ anulowania Prawa dostępu, Dyrektor Pionu Informatyki lub inna osoba przez niego upoważniona obowiązany jest przekazać w formie pisemnej lub w formie e-mail Klientowi wewnętrznemu lub Właścicielowi Biznesowemu, dokonującemu zgłoszenia, o

którym mowa w §3 ust 2 oraz do Pionu Audytu i Bezpieczeństwa, uzasadnienie tej decyzji ze wskazaniem przyczyny odmowy, a osobą uprawnioną do ponownego przeanalizowania możliwości wydania decyzji o której mowa w ust 1 i jej wydania jest wówczas Prezes Zarządu, po przedstawieniu opinii Dyrektora Pionu Informatyki oraz Dyrektora Pionu Audytu i Bezpieczeństwa.

7. Klient zewnętrzny musi przed realizacją decyzji o przyznaniu Prawa dostępu zostać zapoznany z podstawowymi zasadami bezpieczeństwa Systemu teleinformatycznego, przez pracowników Pionu Informatyki.
8. Klient zewnętrzny, który ma podjąć czynności związane z koniecznością Przetwarzania Danych osobowych powinien przed przystąpieniem do pracy:
 - 1) posiadać upoważnienie do Przetwarzania Danych osobowych stosownie do Regulaminu Ochrony danych osobowych w Spółce Operator Gazociągów Przesyłowych Gaz-System S.A.,
 - 2) odbyć szkolenie zapoznające go z obowiązkami i przepisami regulującymi Przetwarzanie Danych osobowych,
9. Klient Wewnętrzny lub Właściciel biznesowy, który występował ze zgłoszeniem o którym mowa w §3 ust 2, wobec Klienta zewnętrznego, z którym lub z którego pracodawcą/zleceniodawcą ma nastąpić rozwiązanie/wygaśnięcie umowy łączącej go z OGP Gaz-System S.A., powinien rozważyć potrzebę ograniczenia temu Klientowi Zewnętrznemu przydzielonego Prawa dostępu i :
 - 1) wystąpić o zmianę zakresu Prawa dostępu Klienta zewnętrznego do Zasobu, wraz z podaniem daty od której ma obowiązywać ta zmiana, nie później niż na dwa dni przed planowaną zmianą, z pominięciem dni ustawowo wolnych od pracy, jak i dodatkowych dni wolnych ustalonych w OGP GAZ-SYSTEM S.A.,
 - 2) wystąpić o anulowanie Prawa dostępu Klienta zewnętrznego do Zasobów z podaniem daty anulowania tego prawa odpowiadającej dacie rozwiązania/wygaśnięcia danej umowy, chyba że decyzja o przyznaniu Prawa dostępu była na czas określony odpowiadający terminowi obowiązywania danej umowy pomiędzy Klientem zewnętrznym lub jego pracodawcą a OGP GAZ-SYSTEM S.A..

5. REALIZACJA DECYZJI

§ 5

1. Decyzję przyznającą/zmieniającą/anulującą Prawo dostępu dla Klienta Zewnętrznego, realizuje wyznaczony przez Dyrektora Pionu Informatyki pracownik Pionu Informatyki, z zastrzeżeniem ust 4.
2. Decyzja, o której mowa w ust 1, jest przekazywana dokonującemu zgłoszenia Klientowi wewnętrznemu lub Właścicielowi biznesowemu, bezpośrednio przez Dyrektora Pionu Informatyki lub poprzez pracownika Pionu Informatyki, o którym mowa w ust 1.
3. W przypadku decyzji przyznającej/zmieniającej Prawo dostępu dla Klienta Zewnętrznego, pracownik Pionu Informatyki, o którym mowa w ust 1, przed dokonaniem aktywacji Prawa dostępu, przekazuje Klientowi Zewnętrznemu oświadczenie, którego wzór stanowi Załącznik nr 1, wraz z wyciągami z ustaw

regulujących zagadnienie odpowiedzialności za naruszenie przepisów o ochronie zasobów informacyjnych, w celach informacyjnych. Warunkiem aktywacji Prawa dostępu jest podpisanie przez Klienta Zewnętrznego oświadczenie, którego wzór stanowi Załącznik nr 1.

4. Aktywacji Prawa dostępu dokonuje Administrator systemu na wniosek pracownika Pionu Informatyki, o którym mowa w ust 1. Pracownik Pionu Informatyki, o którym mowa w ust 1, koordynuje działania Administratora systemu, w zakresie aktywacji Prawa dostępu.
5. Pracownik Pionu Informatyki, o którym mowa w ust 1 przechowuje oświadczenia Klientów zewnętrznych, o których mowa w ust 3 oraz prowadzi rejestr wydanych Klientom zewnętrznym tokenów RSA SecureID. Kopia oświadczeń Klientów zewnętrznych, o których mowa w ust 3, w formie elektronicznej jest przechowywana w Centrum Przetwarzania Danych, przez Administratora systemu, uwierzytelniającego Klientów zewnętrznych.
6. W przypadku decyzji o anulowaniu Prawa dostępu dla Klienta Zewnętrznego, czynności realizujące tą decyzję wykonywane są niezwłocznie. Pracownik Pionu Informatyki, o którym mowa w ust 1, powiadamia Dyrektora Pionu Informatyki oraz SerwisDesk o podjętych działaniach.
7. W szczególnych uzasadnionych przypadkach, w których zagrożone jest bezpieczeństwo Systemu teleinformatycznego lub bezpieczeństwo Zasobów Informacyjnych Spółki, niezależnie od decyzji o której mowa w §4 ust 1, polecenie zablokowania dostępu do Zasobów Teleinformatycznych, do których Prawo dostępu przyznano Klientowi zewnętrznemu, może wydać Dyrektor Pionu Audytu i Bezpieczeństwa, z jednoczesnym powiadomieniem Dyrektora Pionu Informatyki. Postanowienia ust 1-6 stosuje się odpowiednio. W takiej sytuacji Dyrektor Pionu Audytu i Bezpieczeństwa, informuje o zaistniałej sytuacji Klienta wewnętrznego lub Właściciela biznesowego, który dokonał zgłoszenia o przyznanie/zmianę Prawa dostępu dla Klienta zewnętrznego, któremu zablokowano dostęp. Dyrektor Pionu Audytu i Bezpieczeństwa lub osoba przez niego wskazana zobowiązany jest wówczas wystąpić ze zgłoszeniem o anulowanie przedmiotowego Prawa dostępu.
8. Proces realizacji decyzji o przyznaniu/zmianie/anulowaniu Praw dostępu dla Klientów zewnętrznych koordynuje wyznaczony przez Dyrektora Pionu Informatyki pracownik Pionu Informatyki.
9. Niezależnie od decyzji o której mowa w §4 ust 1, w przypadku stwierdzenia niezgodnego z przeznaczeniem użycia Prawa dostępu, wykonania/ wprowadzenia do Systemu teleinformatycznego Programu destrukcyjnego, świadomie czy nieświadomie przez Klienta zewnętrznego dostęp do Zasobów, do których Prawo dostępu przyznano Klientowi zewnętrznemu jest czasowo blokowany przez Administratora systemu, do wyjaśnienia zaistniałego incydentu. Wraz z dokonaniem blokady, Administrator systemu powiadamia o tym fakcie i o przyczynie blokady SerwisDesk, Dyrektora Pionu Informatyki, Dyrektora Pionu Audytu i Bezpieczeństwa oraz pracownika koordynującego proces realizacji decyzji o przyznaniu/zmianie/anulowaniu Praw dostępu dla Klientów zewnętrznych. O zdarzeniu informowany jest również Klient Wewnętrzny lub Właściciel biznesowy wnioskujący o dany dostęp.

9.06.11.

mgr inż. Sławomir Kozłowski
RADCA PRAWNY





.....,dn.....

.....
Imię i nazwisko

.....
Nazwa przedsiębiorcy będącego Klientem Zewnętrznym lub jego pracodawca

Oświadczenie

W związku z przyznaniem mi Prawa dostępu do Zasobów teleinformatycznych Operatora Gazociągów Przesyłowych GAZ-SYSTEM S.A. oświadczam iż zapoznałem się z regulacjami wewnętrznymi Operatora Gazociągów Przesyłowych GAZ-SYSTEM S.A. (wyciągiem z Polityki Bezpieczeństwa Teleinformatycznego, Regulaminem dla Użytkowników zasobów teleinformatycznych w OGP GAZ-SYSTEM S.A, Regulaminem Dostępu Klientów zewnętrznych do Zasobów teleinformatycznych Operatora Gazociągów Przesyłowych Gaz-System S.A, Regulaminem Ochrony Danych Osobowych w Spółce Operator Gazociągów Przesyłowych Gaz-System S.A.) i zobowiązuję się niniejszym do przestrzegania ich postanowień oraz do dołożenia należytej staranności w zakresie ochrony tych Zasobów teleinformatycznych, a w szczególności do:

- właściwego zabezpieczania sprzętu,
- właściwego zabezpieczania narzędzi i innych elementów służących do uzyskania dostępu do Zasobów teleinformatycznych (np. nie udostępniania haseł, PIN'u oraz klucza RSA osobom nieupoważnionym),

W przypadkach niebezpieczeństwa lub naruszenia ochrony w/w. Zasobów teleinformatycznych (np. kradzież/zagubienie komputera/tokena (klucza)/możliwość wykorzystania hasła przez osobę nieuprawnioną) zobowiązuję się niniejszym do niezwłocznego poinformowania jednej z wymienionych poniżej osób:

1. SerwisDesk (tel..... E-mail:)
2.(imię i nazwisko) – Pracownika Pionu Informatyki do którego zadań należy bezpieczeństwo zasobów teleinformatycznych OGP Gaz-System S.A.
3.(imię i nazwisko) – Dyrektora Pionu Informatyki
4.(imię i nazwisko) - Dyrektora Pionu Audytu i Bezpieczeństwa) Dział Bezpieczeństwa E-mail: security@gaz-system.pl , tel.

Zostałem poinformowany, iż każde naruszenie przeze mnie postanowień obowiązujących w Spółce Polityki Bezpieczeństwa Teleinformatycznego będzie skutkowało odebraniem przyznanych mi uprawnień.

Jednocześnie potwierdzam, że zapoznałem się z wyciągiem z ustaw regulujących zagadnienia odpowiedzialności za naruszenie przepisów o ochronie zasobów informatycznych, załączonym do niniejszego oświadczenia i są mi znane moje prawa i obowiązki w tym zakresie. Zostałem poinformowany o możliwości rejestrowania moich działań w Zasobach teleinformatycznych Operatora Gazociągów Przesyłowych Gaz-System S.A.

.....
Pieczęć i podpis przyjmującego oświadczenie

.....
Podpis składającego oświadczenie

Wyciągi z ustaw regulujących zagadnienie odpowiedzialności za naruszenie przepisów o ochronie zasobów informacyjnych:

✓ **USTAWA z dnia 6 czerwca 1997 r. KODEKS KARNY**
(Dz. U. z 1997 nr 88 poz. 553 z późn. zm.)

Rozdział XXXIII

Przestępstwa przeciwko ochronie informacji

Art. 265. § 1. Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli "tajne" lub "ściśle tajne", podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Jeżeli informację określoną w § 1 ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 3. Kto nieumyślnie ujawnia informację określoną w § 1, z którą zapoznał się w związku z pełnieniem funkcji publicznej lub otrzymanym upoważnieniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 266. § 1. Kto, wbrew przepisom ustawy lub przyjętemu na siebie zobowiązaniu, ujawnia lub wykorzystuje informację, z którą zapoznał się w związku z pełnioną funkcją, wykonywaną pracą, działalnością publiczną, społeczną, gospodarczą lub naukową, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Funkcjonariusz publiczny, który ujawnia osobie nieuprawnionej informację niejawną o klauzuli "zastrzeżone" lub "poufne" lub informację, którą uzyskał w związku z wykonywaniem czynności służbowych, a której ujawnienie może narazić na szkodę prawnie chroniony interes, podlega karze pozbawienia wolności do lat 3.

§ 3. Ściganie przestępstwa określonego w § 1 następuje na wniosek pokrzywdzonego.

Art. 267. § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przetwarzając albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1-3 ujawnia innej osobie.

§ 5. Ściganie przestępstwa określonego w § 1-4 następuje na wniosek pokrzywdzonego.

Art. 268. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268a. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Art. 269. § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.

Art. 269a. Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Art. 269b. § 1. ⁽¹⁵¹⁾ Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3.

§ 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

✓ **USTAWA z dnia 16 kwietnia 1993 r. O ZWALCZANIU NIEUCZLIWEJ KONKURENCJI**
(tj. z 2003r. Dz. U. nr 153, poz. 1503 z późn. zm.)

Rozdział 4
Przepisy karne

Art. 23.

1. Kto, wbrew ciężącemu na nim obowiązкови w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informację stanowiącą tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy,

podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Tej samej karze podlega, kto, uzyskawszy bezprawnie informację stanowiącą tajemnicę przedsiębiorstwa, ujawnia ją innej osobie lub wykorzystuje we własnej działalności gospodarczej.

...

✓ **USTAWA z dnia 29 sierpnia 1997 r. O OCHRONIE DANYCH OSOBOWYCH**
(Dz. U. tj. z 2002, nr 101, poz. 926 z późn. zm.)

Rozdział 5
Zabezpieczenie danych osobowych

...

Art. 39.

1. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać:

- 1) imię i nazwisko osoby upoważnionej,
- 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych,
- 3) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

2. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.

...

Rozdział 8
Przepisy karne

Art. 49.

1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

Art. 51.

1. Kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku

Art. 52.

Kto administrując danymi narusza choćby nieumyślnie obowiązek zabezpieczenia ich przed zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 53.

Kto będąc do tego obowiązany nie zgłasza do rejestracji zbioru danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Art. 54.

Kto administrując zbiorem danych nie dopełnia obowiązku poinformowania osoby, której dane dotyczą, o jej prawach lub przekazania tej osobie informacji umożliwiających korzystanie z praw przyznanych jej w niniejszej ustawie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku

Art. 54a.

Kto inspektorowi udaremnia lub utrudnia wykonanie czynności kontrolnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

✓ **USTAWA z dnia 14 lipca 1983 r. O NARODOWYM ZASOBIE ARCHIWALNYM I ARCHIWACH**
(Dz. U. t.j. z 2006, nr 97, poz. 673 z późn. zm.)

Rozdział 5
Przepisy karne

Art. 52.

1. Kto, posiadając szczególny obowiązek ochrony materiałów archiwalnych, uszkadza je lub niszczy, podlega karze pozbawienia wolności do lat 3.
2. Jeżeli sprawca działa nieumyślnie, podlega grzywnie albo karze ograniczenia wolności (...)