Ustawy i normy

RODO

- RODO to unijne rozporządzenie o ochronie danych osobowych (tj. Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 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).
- RODO obowiązuje od 25 maja 2018 roku.
- Przepisy RODO stosuje się, kiedy organizacja przetwarza dane osobowe obywateli Unii Europejskiej na całym świecie.
- Nowe rozporządzenie o ochronie danych osobowych chroni prawa osób, których dane dotyczą – zarówno osób fizycznych, jak również prawnych prowadzących działalność gospodarczą (przepisy RODO regulują kwestie związane z ochroną danych osobowych i ich przetwarzaniem przez przedsiębiorców prowadzących działalność gospodarczą na terenie Unii Europejskiej (spółki, osoby fizyczne prowadzące działalność gospodarczą czy oddział zagranicznego przedsiębiorcy), którzy przetwarzają dane osobowe swoich klientów.
- Przepisy RODO nie dotyczą działalności osobistej lub domowej, czyli przetwarzania danych osobowych w celach prywatnych, np. wysyłanie kartek świątecznych do rodziny (dane są przetwarzane w innych celach, niż tych związanych z działalnością handlową, gospodarczą lub zawodową osoby przetwarzającej dane). RODO chroni tylko osoby żyjące, przepisy nie dotyczą zmarłych.
- RODO to przepis prawa obowiązujący w całej Unii Europejskiej. Może on jednak w niektórych obszarach zostać uzupełniony przepisami prawa krajowego. Organizacje spoza Unii Europejskiej również podlegają nowym przepisom – w przypadku, kiedy oferują towary i usługi na terenie Unii Europejskiej lub jeżeli monitorują zachowanie osoby, której dane dotyczą w UE.

Źródło:https://orodo.pl/co-to-jest-rodo/

RODO

- RODO (Rozporządzenie o Ochronie Danych Osobowych) to unijne prawodawstwo regulujące ochronę danych osobowych i prywatności obywateli UE. To przepisy, które wymagają od przedsiębiorstw i organizacji przetwarzających dane osobowe przestrzegania określonych standardów ochrony prywatności. Przepisy RODO mają na celu zapewnienie, że dane osobowe są przetwarzane zgodnie z prawem i w sposób bezpieczny dla osób, których te dane dotyczą.

Ustawa o ochronie informacji niejawnych

Rozdział 1

Przepisy ogólne

Art. 1. 1. Ustawa określa zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania, zwanych dalej „informacjami niejawnymi", to jest zasady:

1) klasyfikowania informacji niejawnych;

2) organizowania ochrony informacji niejawnych;

3) przetwarzania informacji niejawnych;

4) postępowania sprawdzającego prowadzonego w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy, zwanego dalej odpowiednio „postępowaniem sprawdzającym" lub „kontrolnym postępowaniem sprawdzającym";

5) postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych, zwanego dalej „postępowaniem bezpieczeństwa przemysłowego";

6) organizacji kontroli stanu zabezpieczenia informacji niejawnych;

7) ochrony informacji niejawnych w systemach teleinformatycznych;

8) stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.

Ustawa o ochronie informacji niejawnych

Rozdział 2

Klasyfikowanie informacji niejawnych

Art. 5. 1. Informacjom niejawnym nadaje się klauzulę „ściśle tajne", jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;

2) zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;

3) zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;

4) osłabi gotowość obronną Rzeczypospolitej Polskiej;

5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;

6) zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;

7) zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. — Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.[5)]), lub osób dla nich najbliższych.

Ustawa o ochronie informacji niejawnych

2. Informacjom niejawnym nadaje się klauzulę „tajne", jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;

2) pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;

3) zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;

4) utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;

5) w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;

6) przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

Ustawa o ochronie informacji niejawnych

3. Informacjom niejawnym nadaje się klauzulę „poufne", jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że:

1) utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;

2) utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;

3) zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;

4) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;

5) utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;

6) zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;

7) wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

Ustawa o ochronie informacji niejawnych

4. Informacjom niejawnym nadaje się klauzulę „zastrzeżone", jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

5. Informacje niejawne przekazane przez organizacje międzynarodowe lub inne państwa na podstawie umów międzynarodowych oznacza się polskim odpowiednikiem posiadanej klauzuli tajności.

Art. 6. 1. Klauzulę tajności nadaje osoba, która jest uprawniona do podpisania dokumentu lub oznaczenia innego niż dokument materiału.

Ustawa o ochronie informacji niejawnych

Rozdział 3

Organizacja ochrony informacji niejawnych

Art. 10. 1. ABW i SKW, nadzorując funkcjonowanie systemu ochrony informacji niejawnych w jednostkach organizacyjnych pozostających w ich właściwości określonej w ust. 2 i 3:

1) prowadzą kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie;

2) realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych;

3) prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego;

4) zapewniają ochronę informacji niejawnych wymienianych między Rzecząpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi;

5) prowadzą doradztwo i szkolenia w zakresie ochrony informacji niejawnych.

2. SKW realizuje zadania w odniesieniu do:

1) Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych;

2) ataszatów obrony w placówkach zagranicznych;

3) żołnierzy w służbie czynnej wyznaczonych na stanowiska służbowe w innych jednostkach organizacyjnych niż wymienione w pkt 1 i 2.

3. ABW realizuje zadania w odniesieniu do jednostek organizacyjnych i osób podlegających ustawie, niewymienionych w ust. 2.

Art. 11. 1. Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.

2. Krajowa władza bezpieczeństwa jest właściwa do nadzorowania systemu ochrony informacji niejawnych w stosunkach Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi i wydawania dokumentów upoważniających do dostępu do informacji niejawnych Organizacji Traktatu Północnoatlantyckiego, zwanej dalej „NATO", Unii Europejskiej lub innych organizacji międzynarodowych, zwanych dalej „informacjami niejawnymi międzynarodowymi".

Ustawa o ochronie informacji niejawnych

Art. 14. 1. Kierownik jednostki organizacyjnej, w której są przetwarzane informacje niejawne, odpowiada za ich ochronę, w szczególności za zorganizowanie i zapewnienie funkcjonowania tej ochrony.

2. Kierownikowi jednostki organizacyjnej bezpośrednio podlega zatrudniony przez niego pełnomocnik do spraw ochrony informacji niejawnych, zwany dalej „pełnomocnikiem ochrony", który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

3. Pełnomocnikiem ochrony może być osoba, która posiada:

1) obywatelstwo polskie;

2) wykształcenie wyższe;

3) odpowiednie poświadczenie bezpieczeństwa wydane przez ABW albo SKW, a także przez były Urząd Ochrony Państwa lub byłe Wojskowe Służby Informacyjne;

4) zaświadczenie o przeszkoleniu w zakresie ochrony informacji niejawnych przeprowadzonym przez ABW albo SKW, a także przez byłe Wojskowe Służby Informacyjne.

Ustawa o ochronie informacji niejawnych

Rozdział 5

Bezpieczeństwo osobowe

Art. 21. 1. Dopuszczenie do pracy lub pełnienia służby na stanowiskach albo zlecenie prac związanych z dostępem do informacji niejawnych o klauzuli „poufne" lub wyższej może nastąpić, z zastrzeżeniem art. 34, po:

1) uzyskaniu poświadczenia bezpieczeństwa oraz

2) odbyciu szkolenia w zakresie ochrony informacji niejawnych.

Ustawa o ochronie informacji niejawnych

Rozdział 7

Kancelarie tajne. Środki bezpieczeństwa fizycznego

Art. 43. 1. Organizacja pracy kancelarii tajnej zapewnia możliwość ustalenia w każdych okolicznościach, gdzie znajduje się materiał o klauzuli „tajne" lub „ściśle tajne" pozostający w dyspozycji jednostki organizacyjnej oraz kto z tym materiałem się zapoznał.

6. Kancelaria tajna lub komórka, o której mowa w ust. 2, odmawia udostępnienia lub wydania materiału osobie nieuprawnionej.

Art. 45. 1. Jednostki organizacyjne, w których są przetwarzane informacje niejawne, stosują środki bezpieczeństwa fizycznego odpowiednie do poziomu zagrożeń w celu uniemożliwienia osobom nieuprawnionym dostępu do takich informacji, w szczególności chroniące przed:

1) działaniem obcych służb specjalnych;

2) zamachem terrorystycznym lub sabotażem;

3) kradzieżą lub zniszczeniem materiału;

4) próbą wejścia osób nieuprawnionych do pomieszczeń, w których są przetwarzane informacje niejawne;

5) nieuprawnionym dostępem do informacji o wyższej klauzuli tajności niewynikającym z posiadanych uprawnień.

Ustawa o ochronie informacji niejawnych

Rozdział 8

Bezpieczeństwo teleinformatyczne

Art. 48. 1. Systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego.

2. Akredytacji, o której mowa w ust. 1, udziela się na czas określony, nie dłuższy niż 5 lat.

3. ABW albo SKW udziela akredytacji bezpieczeństwa teleinformatycznego dla systemu teleinformatycznego przeznaczonego do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej.

4. ABW albo SKW udziela albo odmawia udzielenia akredytacji, o której mowa w ust. 3, w terminie 6 miesięcy od otrzymania kompletnej dokumentacji bezpieczeństwa systemu teleinformatycznego. W uzasadnionych przypadkach, w szczególności wynikających z rozległości systemu i stopnia jego skomplikowania, termin ten może być przedłużony o kolejne 6 miesięcy. Od odmowy udzielenia akredytacji nie służy odwołanie.

5. Potwierdzeniem udzielenia przez ABW albo SKW akredytacji, o której mowa w ust. 3, jest świadectwo akredytacji bezpieczeństwa systemu teleinformatycznego.

6. Świadectwo, o którym mowa w ust. 5, wydaje się na podstawie:

1) zatwierdzonej przez ABW albo SKW dokumentacji bezpieczeństwa systemu teleinformatycznego;

2) wyników audytu bezpieczeństwa systemu teleinformatycznego przeprowadzonego przez ABW albo SKW.

Ustawa o ochronie informacji niejawnych

Art. 49. 1. Dokument szczególnych wymagań bezpieczeństwa systemu teleinformatycznego powinien zawierać w szczególności wyniki procesu szacowania ryzyka dla bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym oraz określać przyjęte w ramach zarządzania ryzykiem sposoby osiągania i utrzymywania odpowiedniego poziomu bezpieczeństwa systemu, a także opisywać aspekty jego budowy, zasady działania i eksploatacji, które mają związek z bezpieczeństwem systemu lub wpływają na jego bezpieczeństwo. Przebieg i wyniki procesu szacowania ryzyka mogą zostać przedstawione w odrębnym dokumencie niż dokument szczególnych wymagań bezpieczeństwa.

2. Dokument szczególnych wymagań bezpieczeństwa opracowuje się na etapie projektowania, w razie potrzeby konsultuje z ABW albo SKW, bieżąco uzupełnia na etapie wdrażania i modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.

3. Dokument procedur bezpiecznej eksploatacji opracowuje się na etapie wdrażania oraz modyfikuje na etapie eksploatacji przed dokonaniem zmian w systemie teleinformatycznym.

Ustawa o ochronie informacji niejawnych

Art. 50. 1. Środki ochrony elektromagnetycznej przeznaczone do ochrony informacji niejawnych o klauzuli „poufne" lub wyższej podlegają badaniom i ocenie bezpieczeństwa w ramach certyfikacji prowadzonych przez ABW albo SKW.

2. Urządzenia i narzędzia kryptograficzne przeznaczone do ochrony informacji niejawnych podlegają badaniom i ocenie bezpieczeństwa w ramach certyfikacji prowadzonych przez ABW albo SKW.

3. ABW albo SKW, na wniosek zainteresowanego podmiotu, przeprowadza certyfikację urządzenia lub narzędzia służącego do realizacji zabezpieczenia teleinformatycznego, przeznaczonego do ochrony informacji niejawnych.

4. Pozytywne wyniki ocen bezpieczeństwa uzyskane na podstawie wyników badań prowadzonych w ramach certyfikacji, o których mowa w ust. 1—3, stanowią podstawę do wydania przez ABW albo SKW certyfikatu ochrony elektromagnetycznej, certyfikatu ochrony kryptograficznej lub certyfikatu bezpieczeństwa teleinformatycznego. Certyfikaty są wydawane, w zależności od wyników ocen bezpieczeństwa, na okres nie krótszy niż 3 lata. Od odmowy wydania certyfikatu nie służy odwołanie.

https://www.bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/certyfikacja-wyrobow-pr/5110,Certyfikacja-wyrobow-przeznaczonych-do-ochrony-informacji-niejawnych.html

Ustawa o ochronie informacji niejawnych

ANKIETA BEZPIECZEŃSTWA OSOBOWEGO

CZĘŚĆ I: DANE OSOBOWE	
KOLOROWE ZDJĘCIE OSOBY SPRAWDZANEJ (WYS. 5 cm x SZER. 4 cm)	
1. NAZWISKO	
2. PIERWSZE IMIĘ	3. DRUGIE IMIĘ
4. NAZWISKO RODOWE	5. INNE POPRZEDNIE NAZWISKA
6. DATA URODZENIA (DD-MM-RRRR) – –	7. MIEJSCE URODZENIA (MIEJSCOWOŚĆ, PAŃSTWO)
8. POSIADANE OBYWATELSTWA (OD KIEDY?)	
9. WCZEŚNIEJ POSIADANE OBYWATELSTWA (OD KIEDY – DO KIEDY?)	
10. NR PESEL	11. NIP
12.1. NR DOWODU OSOBISTEGO	12.2. DATA WAŻNOŚCI DOWODU OSOBISTEGO

Ustawa o krajowym systemie cyberbezpieczeństwa

Przedmiotem ustawy jest organizacja krajowego systemu cyberbezpieczeństwa i określenie zadań oraz obowiązków podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa. Ustawa reguluje również kwestie sprawowania nadzoru i kontroli przestrzegania jej przepisów oraz tryb ustanawiania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Treść ustawy określa zarówno podmioty będące uczestnikami krajowego systemy cyberbezpieczeństwa w Polsce oraz ich obowiązki.

Ustawa o krajowym systemie cyberbezpieczeństwa

Art. 2. Użyte w ustawie określenia oznaczają:

1) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;

2) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;

3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;

Ustawa o krajowym systemie cyberbezpieczeństwa

NASK powstała wiosną 1992 r. przy Uniwersytecie Warszawskim jako zespół koordynacyjny ds. rozwoju akademickich sieci komputerowych (dokładna nazwa: Zespół Koordynacyjny Naukowej i Akademickiej Sieci Komputerowej przy Uniwersytecie Warszawskim). Zespół ten odegrał istotną rolę w podłączeniu Polski do Internetu: nawiązanie po raz pierwszy łączności przy użyciu protokołu IP pomiędzy Instytutem Fizyki Uniwersytetu Warszawskiego a Centrum Komputerowym Uniwersytetu w Kopenhadze nastąpiło 17 sierpnia 1991 r.

Od 1993 r. NASK działa jako jednostka badawczo-rozwojowa prowadząca badania naukowe i prace rozwojowe w zakresie telekomunikacji, teleinformatyki, sieci i usług teleinformatycznych; od dnia 1 października 2010 r. NASK jest instytutem badawczym. NASK jest jednocześnie operatorem telekomunikacyjnym oferującym dostęp do szerokopasmowego Internetu, budowę i utrzymanie sieci korporacyjnych, telefonię klasyczną i telefonię IP, kolokację, hosting, usługi wideokonferencji. Wśród klientów NASK znajdują się instytucje akademickie i naukowe, urzędy administracji państwowej oraz sektor biznesowy.

PS. https://www.rmf24.pl/fakty/news-gumisie-czyli-hakerstwo-po-polsku,nId,109314#crp_state=1

Normy i zalecenia zarządzania bezpieczeństwem

ISO 27001 to norma międzynarodowa, która określa wymagania dla Systemów Zarządzania Bezpieczeństwem Informacji (ISMS). ISO 27001 to standard, który pomaga organizacjom zapewnić, że ich systemy i procesy dotyczące bezpieczeństwa informacji są skuteczne i odpowiadające wymaganiom międzynarodowym.

PN-ISO/IEC 27000:2012 „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia”

PN-ISO/IEC 27001:2014-12 „Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania”

PN-ISO/IEC 27005 „Technika informatyczna – Techniki bezpieczeństwa – Zarządzanie ryzykiem w bezpieczeństwie informacji”

Normy i zalecenia zarządzania bezpieczeństwem

ISO 27001 to międzynarodowy standard dotyczący zarządzania bezpieczeństwem informacji. Standard ten określa wymagania dla systemu zarządzania bezpieczeństwem informacji (ISMS - ang. Information Security Management System), które są niezbędne do zapewnienia odpowiedniego poziomu bezpieczeństwa informacji w organizacji. ISO 27001 obejmuje wiele aspektów, takich jak zarządzanie ryzykiem, polityki bezpieczeństwa, zarządzanie zasobami ludzkimi, zarządzanie systemami informatycznymi i audyty bezpieczeństwa informacji. Standard ten jest powszechnie stosowany przez organizacje na całym świecie, aby zapewnić ochronę swoich informacji przed nieautoryzowanym dostępem, zniszczeniem lub utratą.

Normy i zalecenia zarządzania bezpieczeństwem

Pozyskanie certyfikatu ISO 27001 wymaga od firmy przeprowadzenia procesu wdrożenia standardu. Proces ten obejmuje kilka etapów:

Ocena początkowa - wstępna ocena, która pozwala na określenie poziomu zgodności firmy z wymaganiami ISO 27001 oraz identyfikację obszarów wymagających poprawy.

Planowanie wdrożenia - na podstawie wyników oceny początkowej firma opracowuje plan wdrożenia standardu, który określa cele, zadania, harmonogram oraz budżet procesu wdrożenia.

Wdrożenie - w tym etapie firma podejmuje działania mające na celu dostosowanie swojej działalności do wymagań ISO 27001. Wdrożenie może obejmować m.in. opracowanie polityk bezpieczeństwa informacji, szkolenie pracowników, wdrażanie technicznych środków ochrony informacji.

Audyt wewnętrzny - wewnętrzna ocena zgodności firmy z wymaganiami ISO 27001, którą przeprowadza zespół audytowy składający się z pracowników firmy.

Audyt zewnętrzny - przeprowadzony przez niezależną firmę certyfikującą, który ma na celu potwierdzenie zgodności firmy z wymaganiami ISO 27001.

Po pomyślnym przejściu audytów wewnętrznego i zewnętrznego, firma może otrzymać certyfikat ISO 27001, który potwierdza zgodność z wymaganiami standardu i zobowiązuje firmę do systematycznej poprawy swojego systemu zarządzania bezpieczeństwem informacji.

ISO 27001 i RODO

RODO i ISO 27001 to dwa różne, ale ze sobą powiązane tematy, ponieważ oba dotyczą ochrony danych osobowych i prywatności. ISO 27001 może pomóc organizacjom w spełnieniu wymagań RODO i zapewnieniu skutecznego zarządzania bezpieczeństwem informacji, co jest kluczowe dla zapewnienia bezpieczeństwa danych osobowych i prywatności.
Wdrożenie i certyfikacja systemu zgodnego z ISO 27001 może stanowić dowód dla organów nadzorczych i klientów, że organizacja spełnia wymagania RODO w zakresie ochrony danych osobowych.

Literatura

https://bip.abw.gov.pl/bip/informacje-niejawne-1/bezpieczenstwo-teleinf/154,BEZPIECZENSTWO-TELEINFORMATYCZNE.html

ISO 27001 a RODO:
https://www.youtube.com/watch?v=YM2KmArGSW4