

# WZMOCNIJ BEZPIECZEŃSTWO

z Najmocniejszymi Niszczarkami Świata™



Wprowadzenie do **RODO** i **NIS-2**.  
Uczyń ochronę danych częścią swojej  
codziennej pracy.

**Fellowes**

# WPROWADZENIE

## Dlaczego ochrona danych jest dziś ważniejsza niż kiedykolwiek

W świecie, w którym wszystko jest coraz bardziej połączone, a zagrożenia cybernetyczne i ryzyko dla prywatności rosną, ochrona danych przestała być wyborem. Dbając o bezpieczeństwo danych swojej firmy i przestrzegając przepisów, chronisz nie tylko informacje, ale też swoją reputację.

Przepisy, takie jak RODO czy zaktualizowana dyrektywa NIS-2, wymagają, by firmy odpowiedzialnie chroniły dane wrażliwe i osobowe – zarówno w wersji fizycznej, jak i cyfrowej. Ich nieprzestrzeganie może skończyć się wysokimi karami, utratą zaufania klientów, a nawet osobistą odpowiedzialnością dla kadry zarządzającej.

Ten przewodnik przybliży oba przepisy i pokazuje, jakie kroki możesz podjąć, by być w zgodzie z prawem i pewnie chronić swoją firmę.

**Wzmocnij bezpieczeństwo.  
Chroń swoją firmę.  
Działaj zgodnie z przepisami.**



## Czym są dane osobowe?

Dane osobowe to wszystkie informacje, które pozwalają zidentyfikować żyjącą osobę, bezpośrednio lub pośrednio. Mogą to być na przykład:



**Imię i nazwisko**



**Adres zamieszkania**



**Numer ubezpieczenia społecznego**



**Nagrania z kamer monitoringu**

**Ochrona danych oznacza ochronę danych cyfrowych, jak i papierowych – ponieważ naruszenie danych może wystąpić w obu formach.**

# Czym jest NIS-2?

## Wzmacnianie cyberbezpieczeństwa w Europie

NIS-2, czyli Dyrektywa o bezpieczeństwie sieci i informacji 2, to najnowsze unijne przepisy, które mają poprawić cyberbezpieczeństwo i odporność kluczowych sektorów. Weszły w życie w 2023 roku, a wszystkie kraje UE muszą je wdrożyć do października 2024.

Dyrektywa NIS-2 pokazuje, jak bardzo nowoczesna gospodarka zależy od infrastruktury cyfrowej. Zakończenia spowodowane cyberatakami mogą mieć poważne skutki, dlatego przepisy dotyczą zarówno podmiotów kluczowych, jak i ważnych dla funkcjonowania społeczeństwa i gospodarki.

## Czy NIS-2 dotyczy Twojej firmy?

Jeśli Twoja organizacja w jakikolwiek sposób odgrywa kluczową rolę w gospodarce lub społeczeństwie, istnieje duże prawdopodobieństwo, że podlega przepisom NIS-2. Dyrektywa obejmuje produkty i usługi zaliczane do sektorów „niezbędnych” lub „ważnych”.

### Podmioty niezbędne:



Energia



Transport



Infrastruktura  
cyfrowa



Bankowość



Infrastruktura  
rynków finansowych



Woda pitna



Zarządzanie ICT



Administracja  
publiczna



Sektor kosmiczny



Oczyszczanie  
ścieków



Ochrona zdrowia

### Podmioty ważne:



Usługi pocztowe  
i kurierskie



Gospodarka  
odpadami



Przemysł  
wytwórczy



Produkcja  
chemiczna



Badania naukowe



Produkcja  
żywności



Dostawcy usług  
cyfrowych

## Dwie podstawowe zasady NIS-2

Dla firm objętych zakresem NIS-2 przepisy wymagają zarówno działań zapobiegawczych, jak i mechanizmów reagowania.



### **Obowiązek dbania o bezpieczeństwo (Duty of Care):**

Pierwsza zasada nakłada na organizacje obowiązek wprowadzenia proporcjonalnych środków technicznych, operacyjnych i organizacyjnych, które zapewnią bezpieczeństwo cyfrowe i ciągłość działania. Może to obejmować zabezpieczenie systemów IT, ocenę podatności, zarządzanie ryzykiem w łańcuchu dostaw oraz zapewnienie odpowiedzialności na poziomie kierownictwa.



### **Obowiązek zgłaszania incydentów (Duty to Report):**

Druga zasada wymaga od organizacji powiadamiania odpowiednich krajowych organów o poważnych incydentach. Istotne zakłócenia usług muszą być zgłoszone w ciągu 24 godzin, pozostałe incydenty w ciągu 72 godzin. Końcowy, szczegółowy raport należy przestać w ciągu miesiąca.

## Kary za nieprzestrzeganie NIS-2

Nieprzestrzeganie przepisów NIS-2 może prowadzić do poważnych konsekwencji finansowych i operacyjnych:

**KARY**  
mogą sięgać  
nawet



**10 mln €**

lub 2% rocznego globalnego obrotu

**KARY**  
mogą sięgać  
nawet



**7 mln €**

lub 1,4% rocznego globalnego obrotu

Kadra zarządzająca może ponosić indywidualną odpowiedzialność za zapewnienie zgodności z NIS-2. Grozi jej także czasowy lub stały zakaz działalności w określonych sektorach.

## Ukryte ryzyko: wycieki danych z dokumentów papierowych

Choć NIS-2 koncentruje się na odporności cyfrowej, wyciek danych nie zawsze oznacza atak cybernetyczny. Firmy nie mogą ignorować fizycznego aspektu ochrony danych. Każdy incydent, w którym dane osobowe zostaną utracone, skradzione lub ujawnione w niewłaściwy sposób (w tym dokumenty papierowe niewłaściwie zniszczone) może stanowić zagrożenie. Pomyśl o sytuacjach takich jak: umowy wyrzucone do zwykłych koszy na śmieci, arkusze kalkulacyjne pozostawione na biurkach, akta pracowników w niezabezpieczonych szafach czy faktury wyrzucone do otwartych pojemników na recykling. Każdy z tych przypadków może narazić Twoją firmę na kary finansowe i utratę reputacji.

# CZYM JEST RODO?

## Ochrona danych osobowych

Ogólne Rozporządzenie o Ochronie Danych (RODO, ang. GDPR) reguluje ochronę danych osobowych w całej UE i Wielkiej Brytanii od 2018 roku. Zapewnia, że dane osobowe są przetwarzane zgodnie z prawem, w sposób przejrzysty i bezpieczny.

## 6 zasad ochrony danych

Te sześć zasad powinno być podstawą każdej strategii ochrony danych. Dane powinny być:

1. Przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty.
2. Zbierane w określonych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób sprzeczny z tymi celami.
3. Adekwatne, stosowne i ograniczone do tego, co niezbędne.
4. Dokładne i aktualne; nieścisłości powinny być niezwłocznie poprawiane lub usuwane.
5. Przechowywane nie dłużej, niż jest to konieczne.
6. Przetwarzane w sposób zapewniający bezpieczeństwo.

## Kiedy należy zgłaszać naruszenia danych?

Naruszenia muszą zostać zgłoszone do organów nadzorczych w ciągu 72 godzin od ich wykrycia, a w niektórych przypadkach należy również poinformować osoby, których dane dotyczą.



## Kary za nieprzestrzeganie przepisów:

Nieprzestrzeganie RODO może prowadzić do poważnych konsekwencji finansowych.

**KARY**  
mogą sięgać  
nawet



**20 mln €**

lub 4% globalnego obrotu, w zależności od tego, która kwota jest wyższa

# NIS-2 vs RODO

## Zrozumienie różnic

Podsumowując, oto jak te dwa odrębne rozporządzenia prezentują się w skrócie:

ASPEKT	NIS-2	RODO
<b>Cel</b>	Cyberbezpieczeństwo i odporność cyfrowa w sektorach kluczowych i ważnych	Ochrona danych osobowych (cyfrowych i papierowych) dla wszystkich organizacji przetwarzających dane obywateli UE/Wielkiej Brytanii
<b>Zakres</b>	Podmioty kluczowe i ważne (energia, transport, bankowość, zdrowie, infrastruktura cyfrowa itp.)	Każda organizacja, która gromadzi, przechowuje lub przetwarza dane osobowe
<b>Zasady kluczowe</b>	Obowiązek należytej staranności i obowiązek raportowania	Sześć zasad ochrony danych (zgodność z prawem, ograniczenie celu, minimalizacja, prawidłowość, ograniczenie przechowywania, integralność i poufność)
<b>Zgłaszanie naruszeń</b>	Zgłoszenie władzom w ciągu 24h w przypadku zakłóceń usług, 72h w innych przypadkach	Zgłoszenie organowi nadzorcemu w ciągu 72h, czasami także osobom fizycznym
<b>Kary</b>	Do 10 mln € lub 2% globalnego obrotu (dla podmiotów kluczowych). Do 7 mln € lub 1,4% globalnego obrotu (dla podmiotów ważnych)	Do 20 mln € lub 4% globalnego obrotu
<b>Odpowiedzialność zarządcza</b>	Kierownictwo może ponosić osobistą odpowiedzialność, w tym zakazy pracy w sektorach	Kara nakładana jest na organizację jako całość, choć odpowiedzialność może dotyczyć także Inspektorów Ochrony Danych (IOD) lub menedżerów

# Praktyczne działania

## Wzmocnij zgodność

Dla większości organizacji spełnianie wymogów NIS-2 i RODO oznacza połączenie solidnych polityk, bezpiecznych technologii oraz codziennej świadomości pracowników. Skorzystaj z tej listy kontrolnej, aby ukierunkować swoje działania:

### 1 Potwierdź swoje obowiązki

Sprawdź, czy Twoja organizacja jest zaklasyfikowana jako podmiot kluczowy lub ważny w ramach NIS2.

Przejrzyj swoje obowiązki wynikające z RODO i upewnij się, że wiesz, jakie dane posiadasz i w jakim celu je przetwarzasz.

### 2 Wzmocnij praktyki bezpieczeństwa

Wdrażaj i regularnie aktualizuj zapory sieciowe, szyfrowanie oraz plany reagowania na incydenty.

Nie pomijaj ryzyk fizycznych — wprowadź kontrolę nad niepilnowanymi wydrukami, archiwizacją i bezpieczną utylizacją.

### 3 Określ procedury zgłaszania

Ustal jasne ścieżki działania w przypadku incydentów.

Wyznacz odpowiedzialnych za zgłaszanie i dokumentowanie naruszeń.

Upewnij się, że Twój zespół jest w stanie dotrzymać rygorystycznych terminów zgłoszeń (24–72 godziny).

### 4 Regularnie szkol pracowników

Uczyn ochronę danych elementem codziennej kultury organizacyjnej, a nie tylko polityką IT.

Obejmij szkoleniami zarówno ryzyka cyfrowe (np. phishing na ekranie, higiena haseł), jak i obsługę dokumentów papierowych (przechowywanie, niszczenie).

### 5 Kontroluj cykl życia dokumentów

Wprowadź politykę niszczenia nieaktualnych dokumentów papierowych.

Przechowuj poufne dokumenty w bezpieczny sposób aż do momentu utylizacji.

Przechowuj tylko to, co jest niezbędne - regularnie przeglądaj archiwa i bezpiecznie niszcz przeterminowane pliki.

# Rozwiązania Fellowes

## Praktyczne narzędzia wspierające zgodność

Od bezpiecznego niszczenia dokumentów, przez uporządkowaną archiwizację, aż po ochronę ekranu – rozwiązania Fellowes pomagają chronić informacje na każdym etapie ich cyklu życia, wspierając Twoje działania w zakresie zgodności z NIS-2 i RODO.

### Wyzwanie

Zapobieganie naruszeniom danych wynikającym z drukowanych dokumentów.

### Twoje rozwiązanie:

**Niszczarki do papieru** - włączenie niszczarek do polityki przechowywania dokumentów pomaga zminimalizować ryzyko naruszenia danych. Niszcz wydruki, które nie muszą być już przechowywane (uniemożliwia to odzyskanie lub niewłaściwe wykorzystanie poufnych informacji). To kluczowy krok w spełnianiu wymagań dotyczących bezpiecznej utylizacji oraz zarządzania cyklem życia informacji.

[Zobacz niszczarki Fellowes.](#)



### Wyzwanie

Bezpieczne i systematyczne przechowywanie dokumentacji papierowej.

### Twoje rozwiązanie:

**Rozwiązania archiwizacyjne** - utrzymuj porządek w archiwach dzięki wyraźnie oznakowanemu i dobrze zorganizowanemu systemowi produktów BANKERS BOX®, zgodnie z polityką zarządzania dokumentami. Pudła archiwizacyjne umożliwiają bezpieczne przenoszenie dokumentów pomiędzy lokalizacjami aż do momentu ich zniszczenia

[Zobacz pudła archiwizacyjne Fellowes.](#)



## Wyzwanie

Ochrona danych wyświetlanych na ekranie przed ciekawskimi spojrzzeniami lub nieuprawnionym dostępem do urządzenia.

## Twoje rozwiązanie:

**Filtry prywatyzujące** - pomagają zapobiegać naruszeniom danych poprzez tzw. „hakowanie wizualne” ekranów pracowników. Idealne dla osób pracujących hybrydowo, w przestrzeniach współdzielonych i w środowiskach, gdzie na ekranach przetwarzane są poufne informacje. Filtry ograniczają ryzyko kradzieży i nieautoryzowanego dostępu do wrażliwych danych biznesowych.

[Zobacz filtry prywatyzujące Fellowes.](#)

## Wyzwanie

Zabezpieczenie urządzeń podczas pracy w podróży i w przestrzeniach współdzielonych.

## Twoje rozwiązanie:

**Ochrona laptopa** - torba Breyta™ typu dwa w jednym, zamykana na klucz, została zaprojektowana, by chronić laptop, ważne dokumenty i akcesoria podczas pracy w przestrzeniach otwartych lub współdzielonych. Torba pełni także funkcję podstawki pod laptop, co czyni ją idealnym rozwiązaniem łączącym bezpieczeństwo i ergonomię w pracy hybrydowej.

[Zobacz torbę na laptop Breyta™ 2 w 1.](#)





Ochrona danych to już nie tylko obowiązek działu IT to zobowiązanie całej organizacji. Dostosowując się do RODO i NIS-2 oraz wdrażając bezpieczne praktyki dotyczące dokumentów i danych w codziennych procesach, Twoja firma może unikać kar, budować zaufanie i pozostawać odporna na zagrożenia.

**Uczyń ochronę danych częścią swojej codziennej pracy.**

**Fellowes**  
Brands™

FIRMA RODZINNA  
OD 1917 ROKU

[www.fellowes.pl](http://www.fellowes.pl)