RODO – CO OZNACZA DLA ZESPOŁÓW IT?

Tomasz Łużak
Remigiusz Wiśniewski

27.03.2018 r.

LIFE IS FOR SHARING.

AGENDA SPOTKANIA

01 RODO – czy diabeł jest naprawdę taki straszny?

02 Podstawowe wymagania i wyzwania z puntu widzenia IT?

03 W jakim zakresie szefowie IT mogą skorzystać z doświadczeń T-Mobile?

> **RODO MA W ZAŁOŻENIU WPISAĆ OCHRONĘ DANYCH OSOBOWYCH W MODEL OPERACYJNY PRZEDSIĘBIORSTWA.**

RODO

CZY DIABEŁ JEST NAPRAWDĘ TAKI STRASZNY?

LIFE IS FOR SHARING.

GENERAL DATA PROTECTION REGULATION

CO TO JEST?

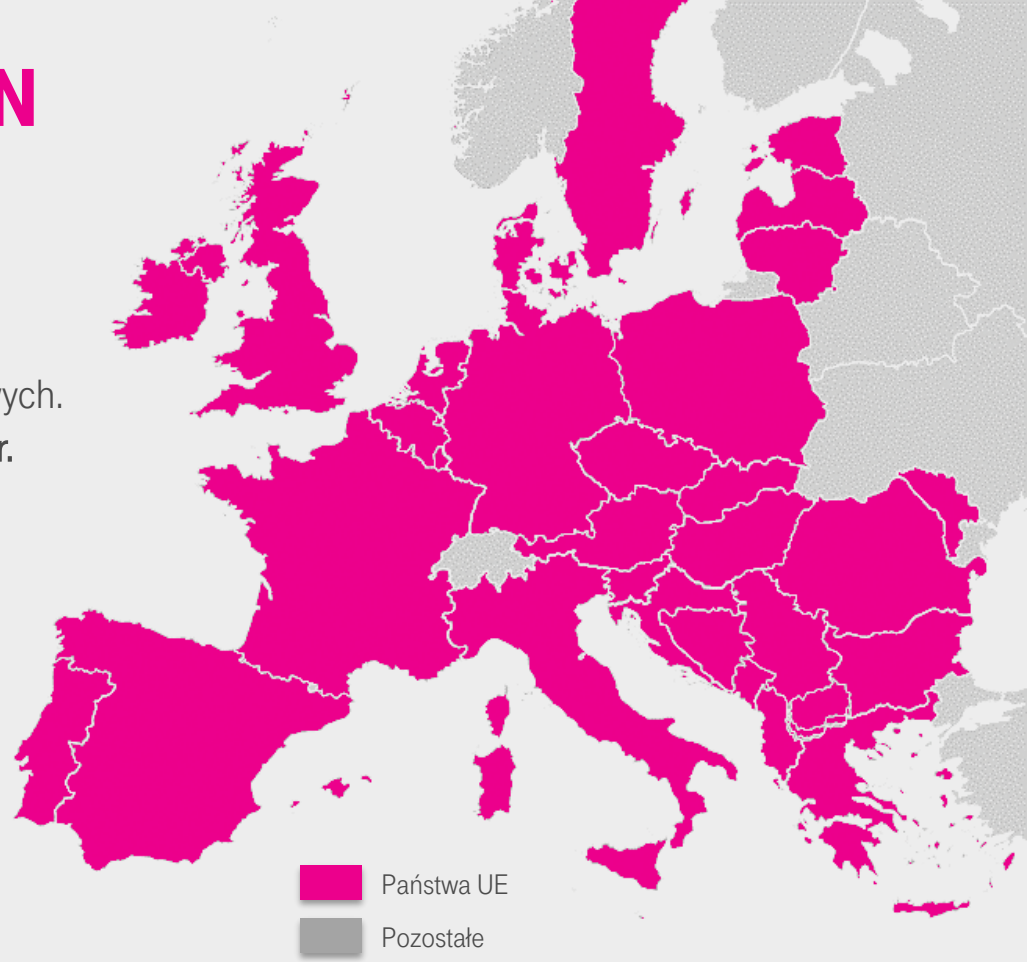
Rozporządzenie ustanawia zasady dotyczące przetwarzania danych osobowych.
Wymogi obowiązują wszystkie instytucje, działające w UE **od 25 maja 2018 r.**

NEW

- Nowe wymagania.
- Nowe prawa osób, których dane osobowe są przetwarzane.
- Nowa terminologia i nowe definicje.

€

Grzywny z tytułu niezgodności mogą wynieść **20 milionów EUR** lub **4% światowego rocznego obrotu**, w zależności od tego, która wartość jest wyższa.



DANE OSOBOWE OZNACZAJĄ WSZELKIE INFORMACJE DOTYCZĄCE ZIDENTYFIKOWANEJ LUB MOŻLIWEJ DO ZIDENTYFIKOWANIA OSOBY FIZYCZNEJ: BEZPOŚREDNIO LUB POŚREDNIO.

GDPR W POLSCE

> **NOWA USTAWA MA ZAPEWNIĆ SKUTECZNE STOSOWANIE W POLSKIM PORZĄDKU PRAWNYM ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679.**

GDPR W POLSCE NAZYWA SIĘ RODO (ROZPORZĄDZENIE O OCHRONIE DANYCH OSOBOWYCH)

- Ministerstwo Cyfryzacji **opublikowało 9 lutego br. nowy** projekt ustawy o ochronie danych osobowych, który ma dostosować polskie regulacje do rozporządzenia EU.
- Projekt ustawy przewiduje m.in..:
  - Bardziej konsultacyjny charakter Prezesa Urzędu Ochrony Danych Osobowych (zastąpi GIODO).
  - **Jednoinstancyjność postępowania, wyłączenie ugody**, wymóg nadawania **rygoru natychmiastowej wykonalności**.
  - Rozszerzenie przepisów **karnych**.
  - **Obostrzone kryteria** dla uzyskania zgody na profilowanie od osób, których dane dotyczą.
  - Zasady **akredytacji podmiotów certyfikujących** uczestniczących w nowej procedurze certyfikacji.
  - Wprowadzone będą nowe **zasady przetwarzania danych biometrycznych**.
  - Potrzebne będzie uzyskanie zgody opiekuna wszystkich osób **poniżej13 lat** których dane osobowe będą przetwarzane.
- Obok projektu nowej ustawy o ochronie danych osobowych jest projekt zmian ponad 130 ustaw sektorowych.

CELEM RODO JEST WPISANIE OCHRONY DANYCH OSOBOWYCH W MODEL OPERACYJNY PRZEDSIĘBIORSTWA

ODPOWIEDZIALNOŚĆ ZA OCHRONĘ DANYCH POWINNA OBEJMOWAĆ CAŁY CYKL ŻYCIA DANYCH

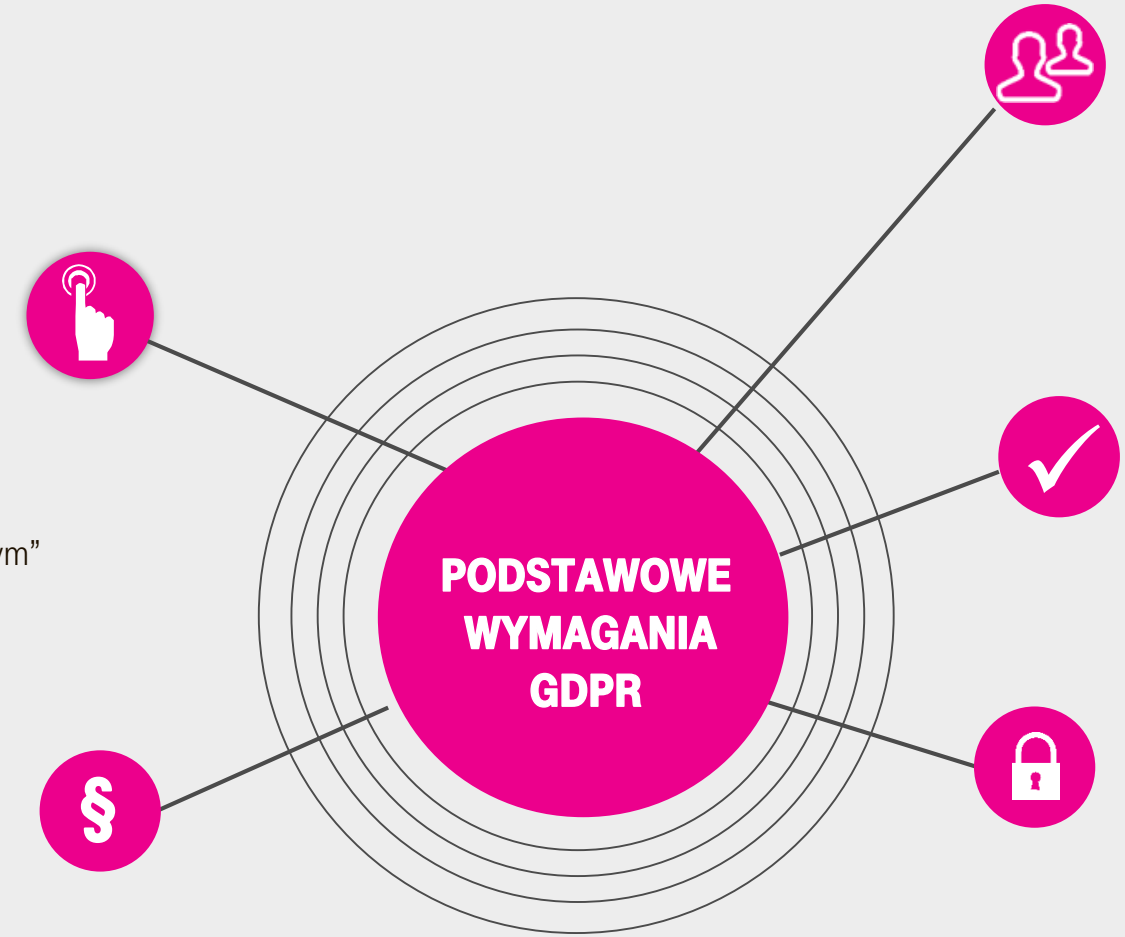
GENERAL DATA PROTECTION REGULATION
PODSTAWOWE WYMAGANIA

ROZSZERZONE PRAWA OSÓB FIZYCZNYCH

- Prawo dostępu do informacji osobistych: Klient może poprosić o modyfikację, usunięcie i „eksport” danych.
- Klient ma prawo do „bycia zapomnianym” i żądać ograniczenia przetwarzania.

WYMAGANIA PRAWNE I ZGODY

- Katalog zasad i warunków przetwarzania danych osobowych.
- „Wyraźna i pozytywna” zgoda.
- Przejrzyste informacje i komunikacja.



ODPOWIEDZIALNOŚĆ

- Administrator i podmiot przetwarzający.
- Konieczność udowodnienia, że zapewniono bezpieczeństwo danych osobowych.
- Udokumentowana metoda analizy ryzyka i oceny wpływu (Privacy Impact Assesment).
- Rejestry przetwarzania danych osobowych.

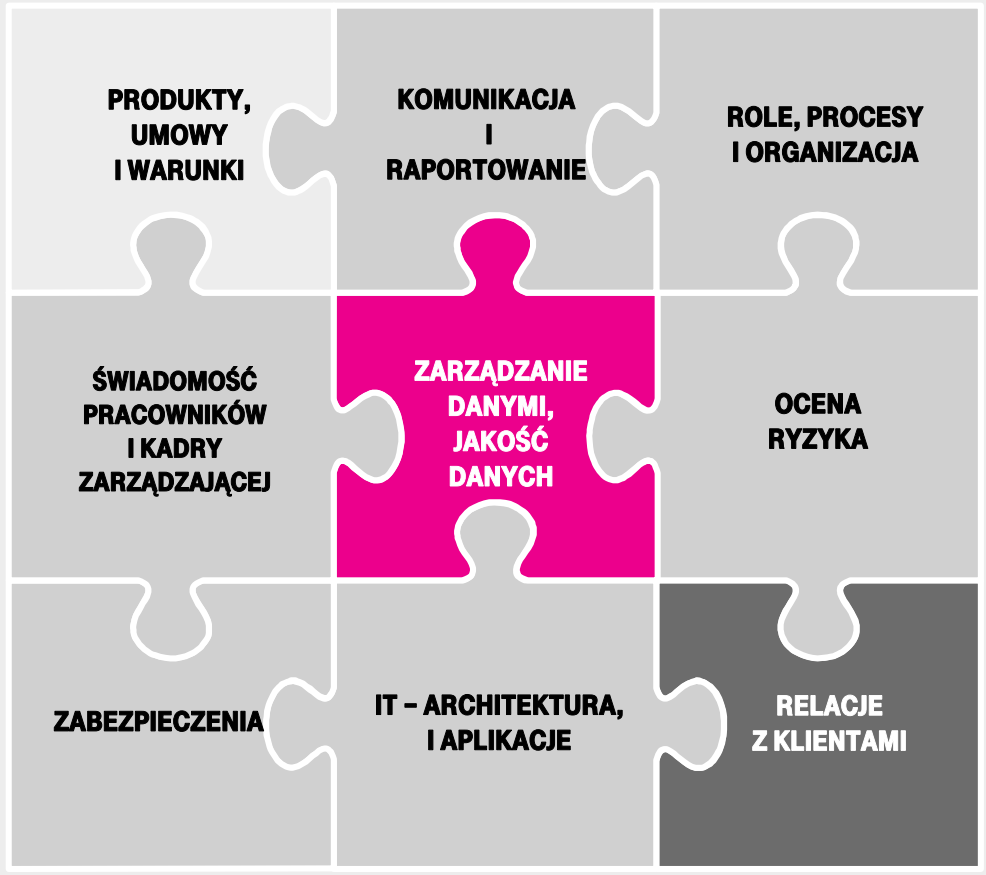
ZGODNOŚĆ Z GDPR

- Zasada prywatności w fazie projektowania (Privacy by Design).
- Zasada prywatności w ustawieniach domyślnych (Privacy by Default).

BEZPIECZEŃSTWO DANYCH

- Poziom bezpieczeństwa dostosowany do ryzyk.
- Konieczność zapewnienia poufności (anonimizacja i szyfrowanie), dostępności oraz regularnego testowania i monitorowania.
- Konieczność informowania o incydentach (do 72 h).

WYMOGI RODO – ASPEKTY WYMAGAJĄCE UWZGLĘDNIENIA WYBRANE PYTANIA, KTÓRE POWINNIŚMY SOBIE ZADAĆ



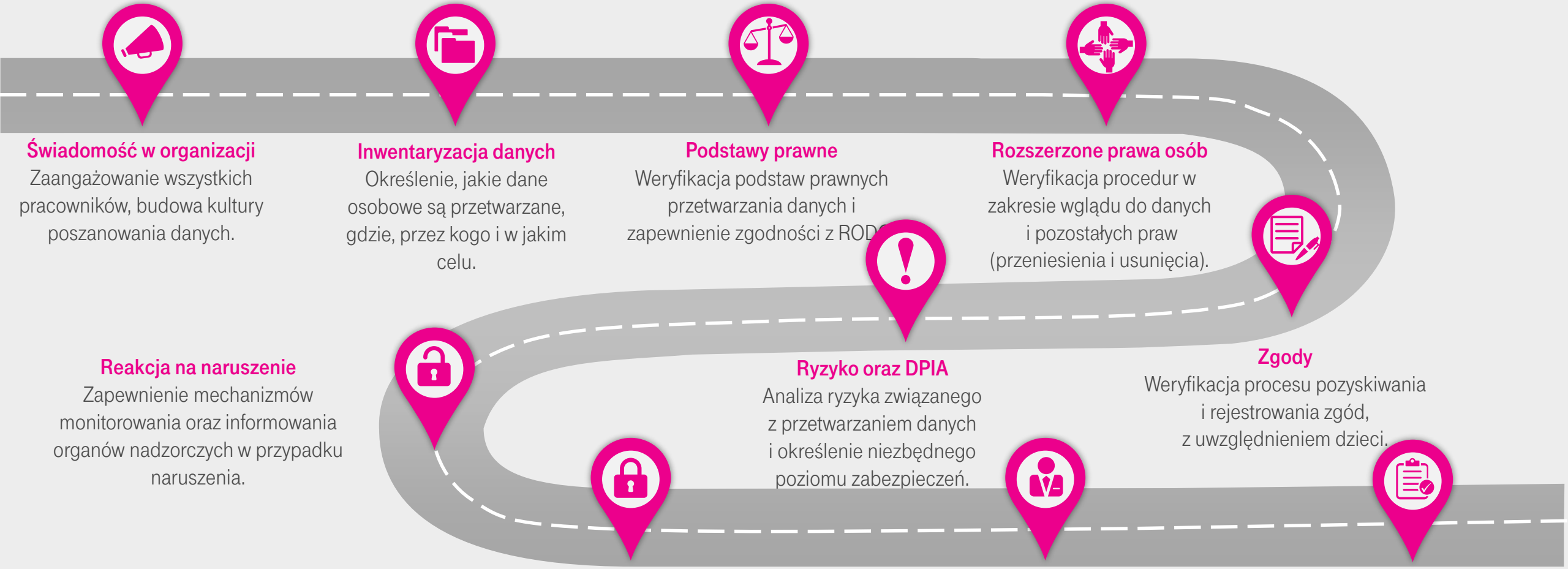
- Jakie dane osobowe posiadamy? Dokładnie gdzie, w jakich procesach i systemach są przechowywane? Czy uwzględniliśmy dane niestrukturalne?
- Kto jest odpowiedzialny za dane w firmie? Kto posiada dostęp do danych?
- Czy możemy zapewnić, że dane są wykorzystywane wyłącznie do faktycznego celu?
- Jaką kontrolę mamy nad danymi zewnętrznymi, czy umowy są kompletne i aktualne?
- Czy wdrożyliśmy zarządzanie ochroną danych dla naszych procesów i systemów informatycznych?
- Czy możemy udokumentować bezpieczeństwo przetwarzania danych osobowych?
- Czy prowadzimy rejestr wszystkich operacji przetwarzania danych?
- Czy możemy monitorować okresy przechowywania?
- Czy możemy zidentyfikować naruszenie ochrony danych osobowych i zgłosić je do właściwego organu regulacyjnego w odpowiednim czasie?
- Co już zautomatyzowaliśmy? Co możemy/chcemy zautomatyzować?
- i wiele innych...

“WYMOGI UNIJNEGO ROZPORZĄDZENIA STWARZAJĄ KONIECZNOŚĆ ZADANIA WIELU PYTAŃ I PODEJŚCIA UWZGLĘDNIAJĄCEGO WIELE ASPEKTÓW”

RODO

GŁÓWNE WYMAGANIA I WYZWANIA Z PUNTU WIDZENIA IT

DROGA DO ZGODNOŚCI Z RODO A ROLA IT



Świadomość w organizacji
Zaangażowanie wszystkich pracowników, budowa kultury poszanowania danych.

Inwentaryzacja danych
Określenie, jakie dane osobowe są przetwarzane, gdzie, przez kogo i w jakim celu.

Podstawy prawne
Weryfikacja podstaw prawnych przetwarzania danych i zapewnienie zgodności z RODO.

Rozszerzone prawa osób
Weryfikacja procedur w zakresie wglądu do danych i pozostałych praw (przeniesienia i usunięcia).

Zgody
Weryfikacja procesu pozyskiwania i rejestrowania zgód, z uwzględnieniem dzieci.

Ryzyko oraz DPIA
Analiza ryzyka związanego z przetwarzaniem danych i określenie niezbędnego poziomu zabezpieczeń.

Reakcja na naruszenie
Zapewnienie mechanizmów monitorowania oraz informowania organów nadzorczych w przypadku naruszenia.

Mechanizmy zabezpieczeń
Weryfikacja istniejących zabezpieczeń oraz ich dostosowanie od określonego ryzyka.

Zarządzanie danymi i ABI
Określenie konieczności powołania IDO, wprowadzenie mechanizmów Data Governance.

Potwierdzenie zgodności
Przygotowanie odpowiedniej dokumentacji potwierdzającej zgodność.

RODO - ISTOTNE ASPEKTY I WYZWANIA

- Wsparcie w realizacji rozszerzonych prawa osób.
- Zapewnienie Bezpieczeństwa danych.
- Wsparcie w spełnieniu wymogów prawnych.
- Wsparcie w realizacji zasady rozliczalności.
- Wsparcie w analizie ryzyka, testowaniu i monitorowaniu.
- Wsparcie narzędziowe.
- Wdrożenie wewnętrznych procesów i procedur i zmian w systemach.

“UNIJNE ROZPORZĄDZENIE NIE ZAWIERA ŻADNYCH KONKRETNYCH WYTYCZNYCH I W WIELU MIEJSCACH JEST MAŁO PRECYZYJNE.”

PUNKTEM WYJŚCIA SĄ ZASADY I WARUNKI PRZETWARZANIA DANYCH OSOBOWYCH OSÓB FIZYCZNYCH

Zasady przetwarzania danych osobowych
(Rozdział II, artykuł 5)

- Zasada rzetelności i prawidłowości.
- Zasada ograniczenia celu.
- Zasada minimalizacji danych.
- Zasady integralności i poufności.
- Zasada rozliczalności.
- Zasada przejrzystości.

Zgodności przetwarzania z prawem
Artykuł 6

- Katalog warunków.

Nowe warunki dotyczące zgód na przetwarzanie danych osobowych
Artykuły 7 i 8.

Zapewnienie zgodności przetwarzania danych z prawem

- Inwentaryzacja danych po stronie systemów IT.
  - Dane strukturalne.
  - Dane niestrukturalne.
- Powiązanie zbiorów danych z celami przetwarzania.
- Wprowadzenie mechanizmów retencji danych.
  - Klasyfikacja zbiorów z uwzględnieniem celów i okresowe przeglądy.
- Jakość danych.
- Aktualizacja polityki ochrony danych.
- Centralne rejestry.
- Automatyzacja.

PRAWA OSÓB FIZYCZNYCH, KTÓRYCH DANE SĄ PRZECHOWYWANE, BĘDĄ ISTOTNIE ROZSZERZONE

Prawo do sprostowania danych
Artykuł 16.

Prawo do usunięcia danych
czyli Prawo do bycia zapomnianym
Artykuł 17.

Prawo do ograniczenia przetwarzania
Artykuł 18.

Prawo do przenoszenia danych
Artykuł 20.

Prawo do sprzeciwu
Artykuł 21.

Prawa właściciela danych

Prawo do usunięcia danych

- Musi być kompletne.
- Również obejmuje przekazanie danych.
- Uwaga na upublicznione dane.
- Działania w celu usuwania mają być racjonalne.

Prawo do ograniczenia przetwarzania

- Nie dotyczy przechowywania.
- Z wyjątkiem ochrony interesów.
- Może być czasowe lub stałe.
- Oznaczenie w bazie, czasowe przesunięcie.

Prawo do przenoszenia danych

- Ustrukturyzowany, powszechnie używany format
- Przesłanie bezpośrednio do innego administratora.
- Brak obowiązku wprowadzenia systemów technicznych.
- Dane rozdzielne, żeby nie powodować uszczerbku praw i wolności innych osób.

Prawo do sprzeciwu

- Profilowanie, marketing bezpośredni...
- Konieczność informowania przy okazji pierwszej komunikacji.

ASPEKTY TECHNICZNE I BEZPIECZEŃSTWO

Privacy by Design
Zaprojektowana zgodność.
Artykuł 25.

Privacy by Default
Prywatność w ustawieniach domyślnych.
Artykuł 25.

Bezpieczeństwo danych
Szyfrowanie oraz anonimizacja/pseudonimizacja danych.
Artykuł 32.

Bezpieczeństwo systemów
Poufność, integralność, dostępność i odporność systemów.
Artykuł 32.

Weryfikacja
Proces regularnego testowania, oceny i oceny skuteczności środków technicznych i organizacyjnych.
Artykuł 32.

Bezpieczeństwo informatyczne

- Ochrona systemów komputerowych.
  - Hardware, software, dane.
- CIA (Confidentality, Integrity, Availability).
  - Poufność.
  - Integralność.
  - Dostępność.
  - Autentyczność, niezaprzeczalność, rozliczalność.
- Ryzyko, podatność, zagrożenie.
- Typy zagrożeń.
  - Zewnętrzne/Wewnętrzne.
  - Technologiczne/Ludzkie/Naturalne.
  - Wrogie/Przypadkowe.

ASPEKTY TECHNICZNE I BEZPIECZEŃSTWO

Privacy by Design
Zaprojektowana zgodność.
Artykuł 25.

Privacy by Default.
Prywatność w ustawieniach domyślnych.
Artykuł 25.

Bezpieczeństwo danych
Szyfrowanie oraz anonimizacja/pseudonimizacja danych.
Artykuł 32.

Bezpieczeństwo systemów
poufność, integralność, dostępność i odporność systemów.
Artykuł 32.

Weryfikacja
Proces regularnego testowania, oceny i oceny skuteczności środków technicznych i organizacyjnych.
Artykuł 32.

Odpowiednie zabezpieczenia

- Co to znaczy „odpowiednie”?
- Spełniający wymagane warunki.
- Warunki finansowe i technologiczne.
- Ważność danych.
- Rozwiązania.
  - Komercyjne/płatne a otwarte/darmowe.
  - Cykliczne i jednorazowe.
  - Ludzkie i technologiczne.
- In-depth security.

ROZWIĄZANIA W ZAKRESIE BEZPIECZEŃSTWA IT WSPIERAJĄCE RODO

Systemy klasy:

- DLP (Data Leakage Prevention)
- Firewall & IPS (Intrusion Prevention System)
- Anty-malware
- WAF (Web Application Firewall)
- DAM/DBF (Database Activity Monitoring/Database Firewall)
- PIM/PAM (Privileged Identity/Access Managament)
- anty-DDoS
- SIEM (Security Information and Event Managament)

Usługi profesjonalne:

- Testy penetracyjne
- Symulowanie ataków cybernetycznych
- Doradztwo w zakresie architektury systemów bezpieczeństwa
- Szkolenia dla pracowników z zakresu cyberbezpieczeństwa

Narzędzia do:

- Skanowania podatności
- Szyfrowania komunikacji elektronicznej
- Szyfrowania nośników danych
- Security baseline

ASPEKTY TECHNICZNE I BEZPIECZEŃSTWO

Privacy by Design
Zaprojektowana zgodność.
Artykuł 25.

Privacy by Default.
Prywatność w ustawieniach domyślnych.
Artykuł 25.

Bezpieczeństwo danych
Szyfrowanie oraz animizacja/pseudonimizacja danych.
Artykuł 32.

Bezpieczeństwo systemów
poufność, integralność, dostępność
i odporność systemów.
Artykuł 32.

Weryfikacja
Proces regularnego testowania, oceny i oceny skuteczności środków technicznych i organizacyjnych.
Artykuł 32.

Analiza ryzyka

- Dowolna metodyka.
  - NIST, ISO, audyt aktywów.
- Ocena aktywów.
- Identyfikacja zagrożeń.
- Prawdopodobieństwo wystąpienia.
- Potencjalny rozmiar strat.
- Ryzyko = Prawdopodobieństwo x Strata.
- Mitygacja ryzyka.

ASPEKTY TECHNICZNE I BEZPIECZEŃSTWO

Privacy by Design
Zaprojektowana zgodność.
Artykuł 25.

Privacy by Default
Prywatność w ustawieniach domyślnych.
Artykuł 25.

Bezpieczeństwo danych
Szyfrowanie oraz animizacja/pseudonimizacja danych.
Artykuł 32.

Bezpieczeństwo systemów
poufność, integralność, dostępność
i odporność systemów.
Artykuł 32.

Weryfikacja
Proces regularnego testowania, oceny i oceny
skuteczności środków technicznych i organizacyjnych.
Artykuł 32.

Privacy by Design

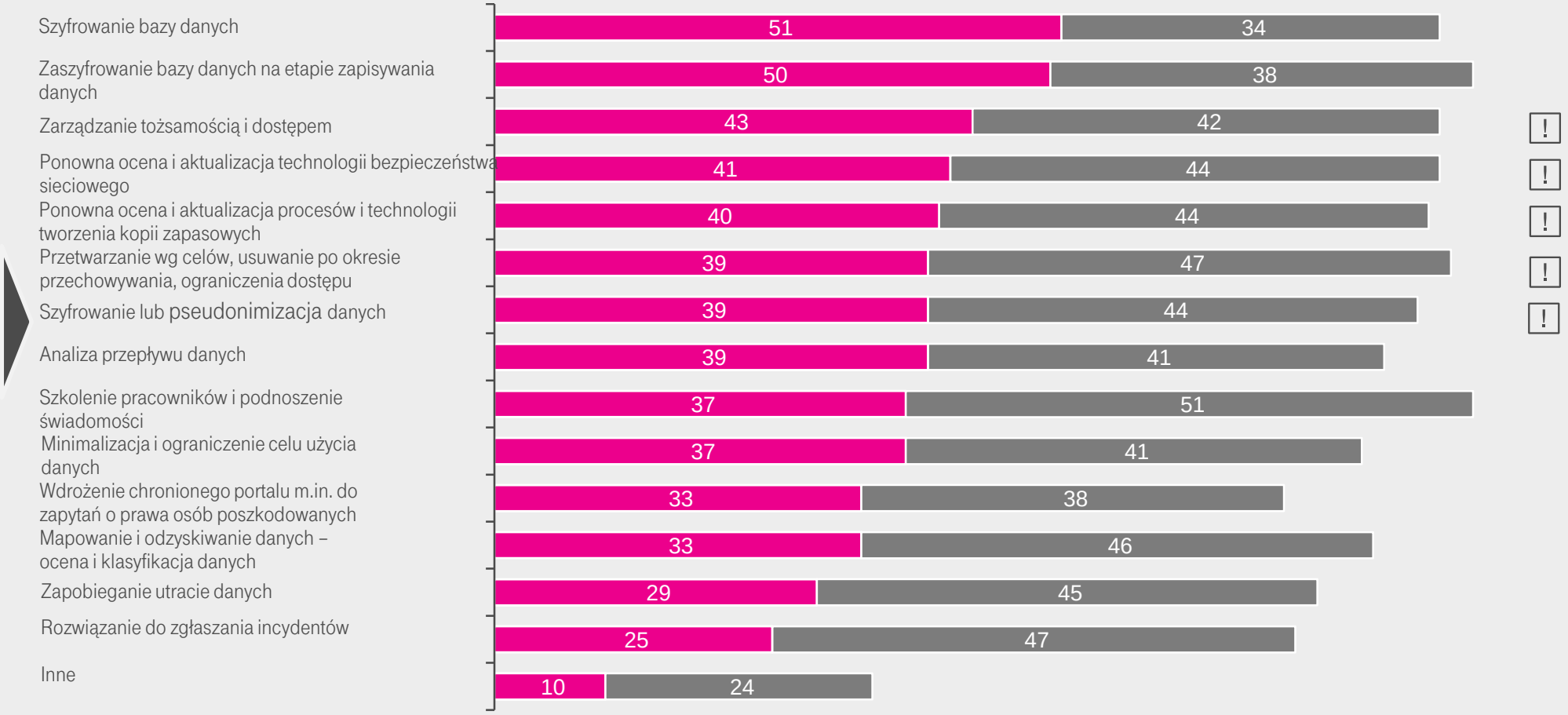
- Pro aktywność - działania profilaktyczne a nie zaradcze.
- Prywatność w ustawieniach domyślnych.
- Zaprojektowana zgodność z ochroną danych.
- Pełna funkcjonalność.
- Bezpieczeństwo End-to-End.
- Widoczność i przejrzystość.
- Koncentracja na użytkowniku.

KONKRETNE DZIAŁANIA

KLUCZOWE OBSZARY

- IT Governance
- Data Governance
- Procesy
- Rozwój systemów
- Interfejsy
- Modele danych
- Bezpieczeństwo IT
- Bezpieczeństwo informacji
- Podnoszenie świadomości

Jakie działania podjęła lub zaplanowała Państwa firma w celu ochrony danych osobowych i spełnienia nowych wymogów RODO?



W JAKIM ZAKRESIE SZEFOWIE IT MOGĄ SKORZYSTAĆ Z DOŚWIADCZEŃ T-MOBILE?

LIFE IS FOR SHARING.

ZAKRES USŁUG T-MOBILE W KONTEKŚCIE RODO

PODSUMOWANIE - KLUCZOWE WNIOSKI

- Do wejścia w życie RODO **pozostało niecałe 60 dni!**
- IT powinno odgrywać **kluczową rolę** we wdrożeniu RODO.
- Trzeba się przygotować na **wystąpienie incydentu – szyfrowanie oraz zarządzanie uprawnieniami.**
- Korzystanie z **doświadczeń i wiedzy innych.**
- ... diabeł **nie jest taki straszny** jak go malują.

ZAPRASZAMY DO KONTAKTU !

Tomasz Łużak
Tomasz.Luzak@t-mobile.pl

LIFE IS FOR SHARING.