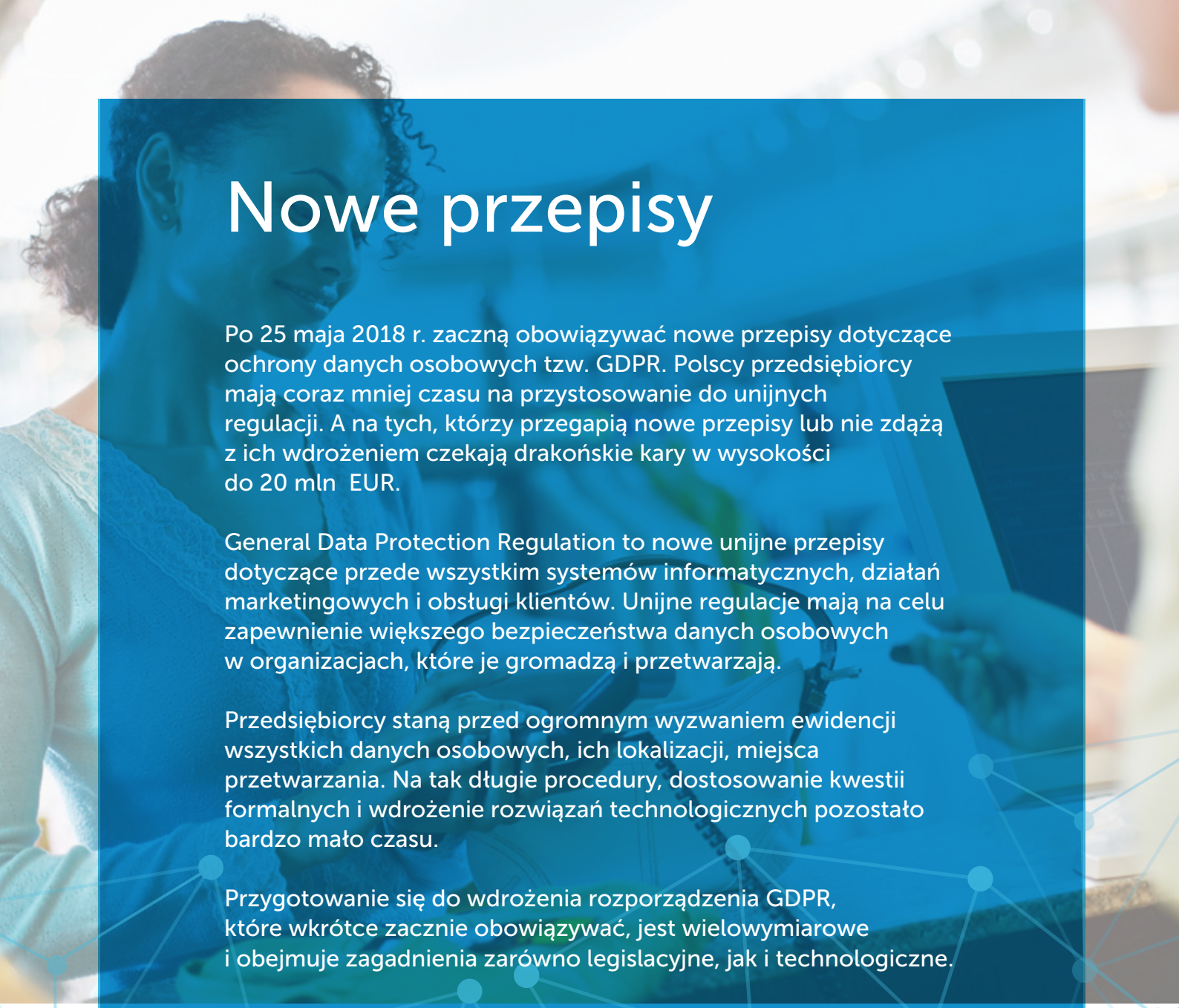
GDPR

Zmiany w prawie o ochronie danych osobowych

K3 system it solutions

Partner
Godny Zaufania



Nowe przepisy

Po 25 maja 2018 r. zaczną obowiązywać nowe przepisy dotyczące ochrony danych osobowych tzw. GDPR. Polscy przedsiębiorcy mają coraz mniej czasu na przystosowanie do unijnych regulacji. A na tych, którzy przegapią nowe przepisy lub nie zdążą z ich wdrożeniem czekają drakońskie kary w wysokości do 20 mln EUR.

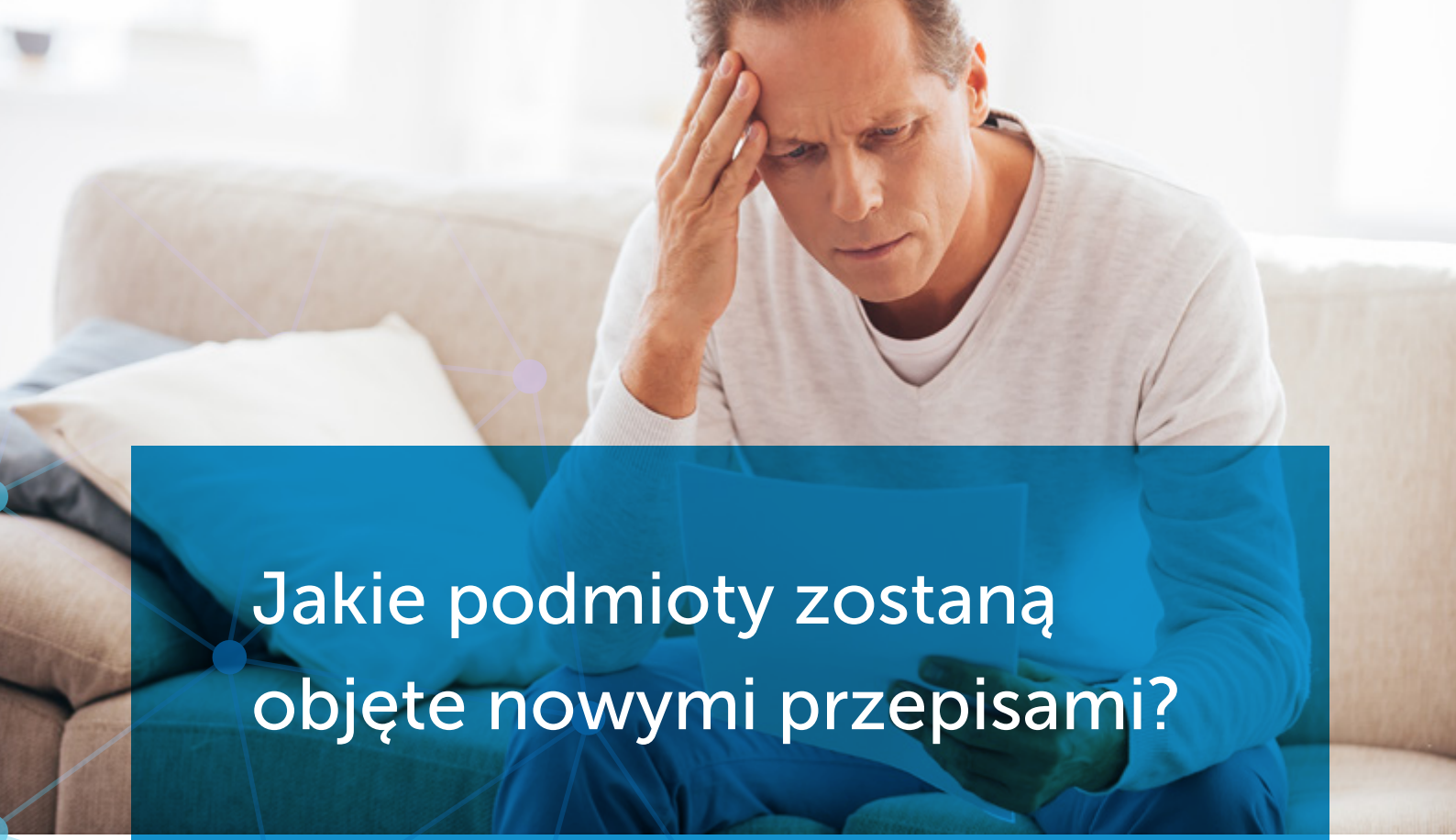
General Data Protection Regulation to nowe unijne przepisy dotyczące przede wszystkim systemów informatycznych, działań marketingowych i obsługi klientów. Unijne regulacje mają na celu zapewnienie większego bezpieczeństwa danych osobowych w organizacjach, które je gromadzą i przetwarzają.

Przedsiębiorcy staną przed ogromnym wyzwaniem ewidencji wszystkich danych osobowych, ich lokalizacji, miejsca przetwarzania. Na tak długie procedury, dostosowanie kwestii formalnych i wdrożenie rozwiązań technologicznych pozostało bardzo mało czasu.

Przygotowanie się do wdrożenia rozporządzenia GDPR, które wkrótce zacznie obowiązywać, jest wielowymiarowe i obejmuje zagadnienia zarówno legislacyjne, jak i technologiczne.

Nowe przepisy wprowadzą m.in. zasadę ochrony „by default”. Oznacza to, że firmy i przedsiębiorcy mogą wykorzystywać dane osobowe klientów tylko i wyłącznie w celu, w którym zostały one pobrane. Przedsiębiorstwa muszą zbudować mechanizmy, które udowodnią, że pozyskane przez nie informacje nie były przetwarzane ani wykorzystywane niezgodnie z przeznaczeniem.

Rozporządzenie wymusi również na przedsiębiorstwach, aby zadbały o ochronę danych osobowych już na etapie projektowania swoich systemów informatycznych. W przypadku naruszenia baz danych albo wycieku informacji administratorzy będą zmuszeni każdorazowo zgłaszać taki incydent do organów nadzorujących.



Jakie podmioty zostaną objęte nowymi przepisami?

- Firmy zatrudniające ponad 250 pracowników
- Każda firma, która przetwarza dane osobowe m.in.: pochodzenie rasowe, etniczne, poglądy polityczne, przekonania religijne, światopoglądowe, dane genetyczne, biometryczne, dane zdrowotne
- Administracja państwowa (za wyjątkiem sądów), służba zdrowia, sektor finansowy (banki), ubezpieczyciele, związki wyznaniowe

Do kogo kierowana jest Unijna Reforma GDPR?

- Dyrektorów i Kierowników ds. CRM
- Dyrektorów i Kierowników ds. baz danych
- Dyrektorów i Kierowników ds. IT
- Dyrektorów i Kierowników Działu Obsługi Klienta
- Administratorów Bezpieczeństwa Informacji (ABI)
- Dyrektorów Działów Prawnych
- Dyrektorów Działów Marketingu
- Dyrektorów ds. Planowania Strategii i Rozwoju
- Osoby kierujące projektami związanymi związanymi z przetwarzaniem danych (informacji)

Nowe obowiązki i wysokie kary

Zgodnie z nowym prawem każda firma, która przetwarza dane osobowe będzie zobowiązana do:

- Wdrożenia właściwych rozwiązań technologicznych i organizacyjnych w celu zapewnienia i potwierdzenia, iż dane są przetwarzane zgodnie z regulatorem (np. pseudonimizacja, szyfrowanie, maskowanie)
- Przetwarzania danych zgodnie z celem ich zbierania
- Przechowywania danych wyłącznie przez określony czas, który jest niezbędny do określonego celu
- Zgłoszenia wycieku danych oraz powiadamiania o naruszeniu w ciągu 72h od chwili jego wykrycia przez administratora danych
- Posiadania śladu związanego z naruszeniem

Za brak dostosowania się do nowego prawa przedsiębiorstwo może zapłacić grzywnę w kwocie do 10 mln EUR, albo 2% całkowitego światowego obrotu podmiotu. Ale to nie wszystko.

Jeżeli administrator danych naruszy przepisy dotyczące praw obywatelskich (np. udostępni informacje na temat wyznania lub poglądów politycznych) będzie to równoznaczne z karą w kwocie do 20 mln EUR, albo 4% całkowitego światowego obrotu, przy czym bierze się pod uwagę tę kwotę, która jest wyższa w przypadku danego podmiotu.

Krok po kroku w stronę GDPR

Przed samym rozpoczęciem wdrażania wymogów GDPR warto zastanowić się, jakie narzędzia ułatwią to zadanie. Poniżej prezentujemy cztery instrumenty, które pomogą szybko i sprawnie dostosować organizację do nowego stanu prawnego.

KROK 1 // Kierownik projektu

Pierwszym z instrumentów, o którym należy pomyśleć przy wdrażaniu GDPR, jest przygotowanie odpowiednich zasobów ludzkich do przeprowadzenia tego projektu. Na czele każdego projektu powinien stać jego kierownik lub manager. W tej roli najlepiej sprawdzi się "ABI". Innym rozwiązaniem jest skorzystanie z pomocy firm zewnętrznych. Wówczas na czele projektu stanie niezależna osoba zawodowo zajmująca się ochroną danych osobowych. Doradcy zewnętrzni posiadają praktykę w zarządzaniu projektami oraz doświadczenie we wdrażaniu zaleceń.

KROK 2 // Zespół wdrożeniowy

Wdrożenie GDPR nie jest zadaniem dla jednej osoby. Nad dostosowaniem przedsiębiorstwa do wymogów GDPR powinien pracować cały zespół osób reprezentujących różne działy w organizacji (np. sprzedaż, marketing, dział informatyczny i prawny).

KROK 3 // Mapy procesów

Kolejnym ważnym instrumentem jest znajomość procesów funkcjonujących w organizacji. Dużo łatwiej, w tym wypadku, jest organizacjom, które posiadają „zmapowane" oraz „poukładane" procesy.

KROK 4 // Technologia

Ostatnim środkiem, który ułatwi wdrażanie GDPR jest wsparcie technologiczne. Zespół wdrożeniowy powinien być wspierany narzędziami informatycznymi. Powinny one umożliwiać zarządzanie wdrożeniem, a w szczególności mierzenie stopnia realizacji wdrożenia.

K3 system it solutions

Partner
Godny Zaufania

Nasi partnerzy

IBM Gold Business Partner

Silver Partner

veeam GOLD pro partner

vmware PARTNER ENTERPRISE SOLUTION PROVIDER

Business Partner Premium Gold Lenovo

Masz pytanie?

Napisz lub zadzwoń

04-767 Warszawa
ul. Patriotów 303

tel. +48 22 610 55 02 (03 / 21 / 26)
fax +48 22 610 55 04

office@k3system.com.pl
www.k3system.com.pl
www.k3cloud.pl

Microsoft Partner
Silver Volume Licensing

Extreme networks

NetApp
Gold Partner