RAPORT MAGAZYNU MENEDŻERÓW I INFORMATYKÓW

WWW.COMPUTERWORLD.PL

COMPUTERWORLD
FROM IDG

SIERPIEŃ 2017

# PRZYGOTOWANIA DO RODO W POLSKICH ORGANIZACJACH

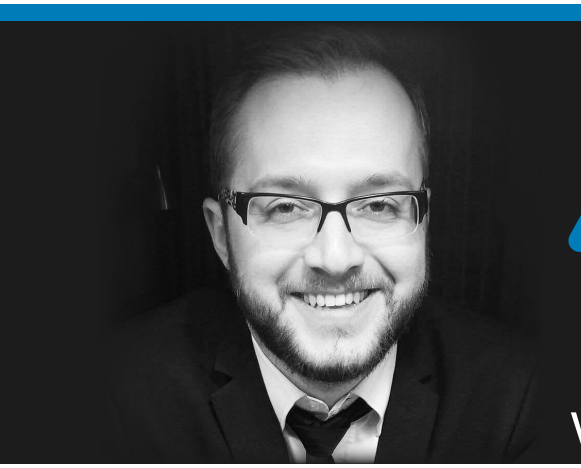
## ŚWIADOMOŚĆ WYZWANIA, KORZYŚCI I ZAGROŻENIA, ZAAWANSOWANIE PRAC WDROŻENIOWYCH, OCZEKIWANIA

Rozporządzenie ogólne o ochronie danych osobowych będzie miało krytyczne znaczenie dla organizacji przetwarzających dane. Dowiedz się, jak przebiegają przygotowania w polskich przedsiębiorstwach oraz jak na tym tle prezentuje się Twoja firma.

PARTNERZY BADANIA

sas

Sygnity
Business-Innovation-Now



# wstępniak

Szanowni Państwo!

25 maja 2018 roku wejdzie w życie Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), szerzej znane jako Rozporządzenie ogólne o ochronie danych osobowych (RODO, opisywane także pod angielskim akronimem GDPR).

Mając na uwadze związane z nowymi przepisami doniosłe konsekwencje dla przedsiębiorstw i organizacji przetwarzających dane osobowe, w lipcu bieżącego roku redakcja „Computerworld" we współpracy z SAS Institute oraz Sygnity przeprowadziła badanie dotyczące stopnia gotowości polskich organizacji na wejście w życie RODO. Analizowaliśmy m.in., co nowego z punktu widzenia biznesu wnoszą przepisy Rozporządzenia do porządku prawnego, jaka jest świadomość wyzwania wśród polskich firm, co oznaczać mają zasady adekwatności, Privacy by Design czy Privacy by Deafault oraz jak przełożą się na funkcjonowanie przedsiębiorstw, jak przebiegają prace przygotowawcze w polskich organizacjach, a także jak oceniane jest samo RODO.

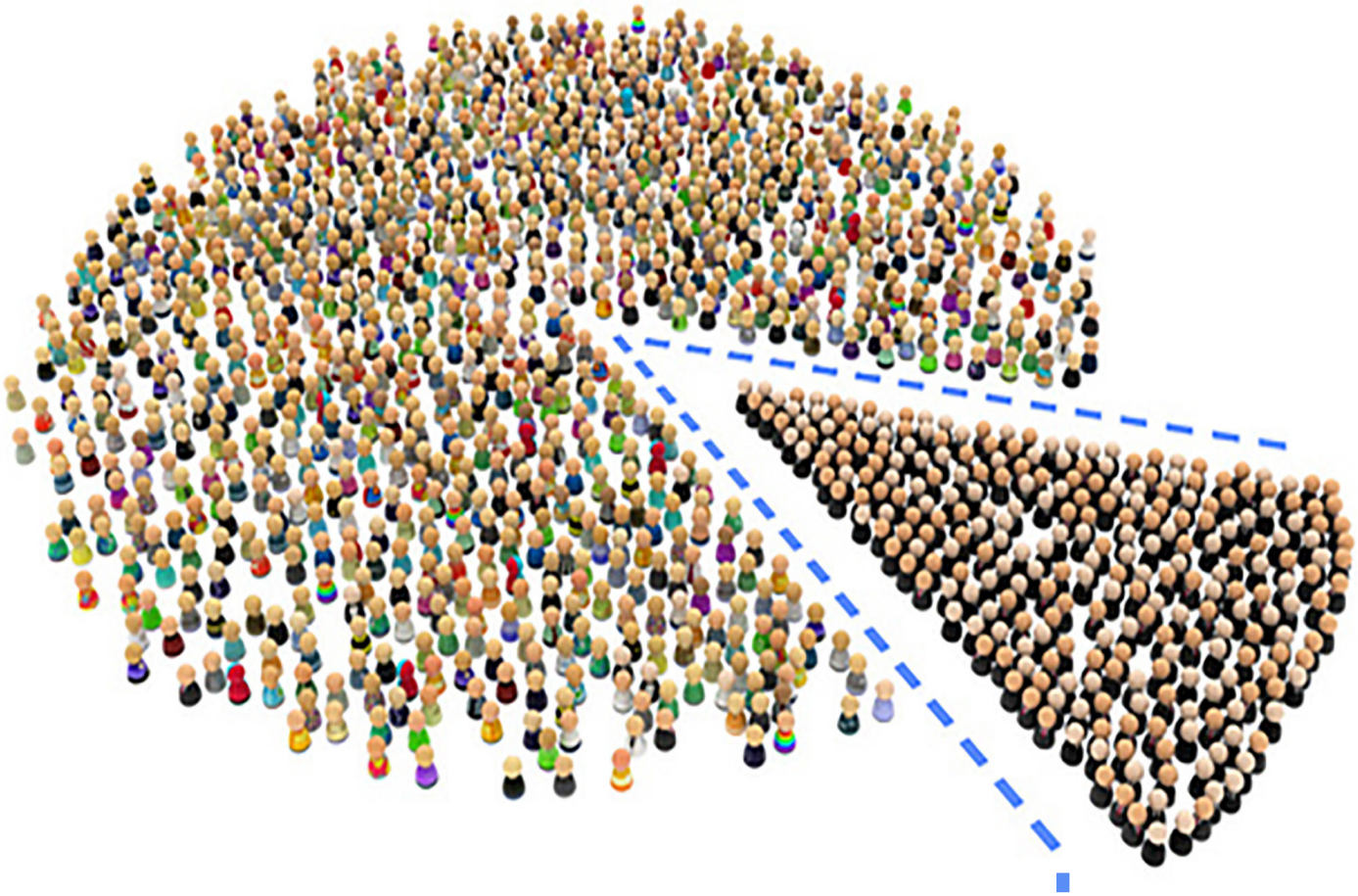
Raport z badania został podzielony na kilka części dotyczących najważniejszych aspektów przetwarzania danych osobowych, których funkcjonowanie będzie musiało zostać dostosowane do RODO: właściwej identyfikacji i lokalizacji posiadanych danych, kontroli i zarządzania nimi, oceny stopnia gotowości na wejście w życie Rozporządzenia, a także oczekiwanego wpływu RODO na procesy biznesowe przedsiębiorstw.

Czasu na przygotowanie się do RODO pozostało już niewiele. Czytając i analizując materiały zawarte w opracowaniu, będą mieli Państwo okazję sprawdzić, jak prezentuje się stopień gotowości polskich firm na wejście w życie RODO oraz jak na tym tle wypada Państwa organizacja.

Zapraszam do lektury!

Piotr Pietruszyński
redaktor prowadzący

# spis treści



ARTUR PĘCZAK

# RODO: oddajmy głos dyrektorom IT

**W zrealizowanym przez „Computerworld" we współpracy z Sygnity i SAS Institute badaniu udział wzięło 114 dyrektorów IT (CIO) reprezentujących średnie i duże przedsiębiorstwa zatrudniające co najmniej 80 pracowników.**

25 maja 2018 roku wchodzi w życie Ogólne Rozporządzenie o Ochronie Danych Osobowych (RODO), znane też pod akronimem GDPR (General Data Protection Regulation), które wprowadza szereg zmian w przepisach oraz istotnie rozszerza odpowiedzialność administratorów danych i podmiotów przetwarzających dane osobowe.
Na przygotowania zostało raptem kilka miesięcy. To doskonały moment, aby sprawdzić i podsumować, jaki jest stopień gotowości polskich organizacji na wejście w życie RODO, jak przebiegają prace wdrożeniowe w różnych branżach, czy też które wynikające z Rozporządzenia przepisy sprawiają firmom najwięcej trudności. W ankiecie nie omieszkaliśmy również zapytać, jakie pozytywne efekty można osiągnąć w związku z adaptacją procesów i zaplecza technologicznego firmy do nowych przepisów.

## Respondentów portret własny

Na pytania dotyczące stanu implementacji wytycznych RODO w polskich organizacjach odpowiadało 114 respondentów – dyrektorów i menedżerów IT (CIO) wywodzących się ze średnich firm oraz dużych przedsiębiorstw i korporacji, w których kompetencjach znajdują się kwestie związane z ochroną danych oraz administrowaniem bezpieczeństwem informacji. Taki dobór próby miał na celu poznanie stanowiska osób decyzyjnych, bezpośrednio odpowiedzialnych za funkcjonowanie IT w reprezentowanych przez siebie firmach oraz mających istotny wpływ na rozwój obszarów związanych z zarządzaniem informacją i ochroną danych osobowych.
Badanie zostało przeprowadzone w modelu CATI (Computer-Assisted Telephone Interview) oraz poprzez pojedynczy mailing CAWI (Computer-Assisted Web Interview); dane gromadzone były na początku lipca 2017 roku.

## Stan zatrudnienia

Badani reprezentują szeroki przekrój średnich i dużych przedsiębiorstw działających w Polsce. 69 respondentów (61%) reprezentuje duże firmy i korporacje zatrudniające powyżej 250 pracowników, podczas gdy pozostałe 45 ankietowanych (39%) odpowiada za obszar IT i zarządzania informacją w średniej wielkości organizacjach sklasyfikowanych przez nas według stanu zatrudnienia na poziomie 81–250 pracowników.
Wśród organizacji średniej wielkości łatwo zauważyć zbliżoną liczbę firm, które wzięły udział w badaniu. Podmiotów w przedziałach: 81–150 oraz 151–250 zatrudnionych zanotowaliśmy odpowiednio 22% i 18%. W odniesieniu do największych przedsiębiorstw widać wyraźną dominację firm, które dopiero aspirują do tego grona, a więc zatrudniają między 251 a 500 pracowników (27%) oraz największych przedsiębiorstw i korporacji, dających pracę dla ponad 2000 osób (18%). Spośród firm, których stan zatrudnienia wynosi 501–1000 oraz 1001–2000 pracowników, do wzięcia udziału w badaniu udało nam się przekonać odpowiednio 12 oraz 6 podmiotów, co łącznie daje 16% ankietowanych.

## Charakterystyka branżowa respondentów

Wśród biorących udział w badaniu 114 organizacji najliczniej reprezentowane były przedsiębiorstwa działające w sektorze przemysłu, produkcji i wydobycia (25%), firmy informatyczne (13%) oraz przedsiębiorstwa FMCG, handlowe i dystrybucyjne (11%). Dostateczna liczba reprezentantów tych branż pozwoliła nam ocenić gotowość firm z perspektywy sektora gospodarki, w którym działają, oraz wpływu regulacji RODO na konkretne branże.
Liczebność firm z konkretnych branż wykazuje korelacje z ich znaczeniem na gospodarczej mapie Polski. W rezultacie każdy głos uznaliśmy za ważny i w niniejszym badaniu poddaliśmy szczegółowej analizie. W gronie ankietowanych licznie reprezentowany był również sektor naukowy, edukacyjny i szkoleniowy (9%). Po kilka ankiet udało nam się ponadto zebrać od respondentów zatrudnionych w sektorze finansowym, administracji publicznej oraz przedsiębiorstwach użyteczności publicznej (utilities), w energetycznych. Dane te wnoszą pewien ogólny ogląd w aktualny stan adaptacji nadchodzących zmian prawa w tak wrażliwych na kwestie ochrony danych osobowych instytucjach.

**114**

dyrektorów IT (CIO) odpowiadało na pytania dotyczące gotowości przedsiębiorstw na wytyczne RODO.

PIOTR PIETRUSZYŃSKI

# Uporządkowane procesy identyfikacji danych

**Uczestnicy przeprowadzonego przez „Computerworld" we współpracy z Sygnity i SAS Institute badania poświęconego gotowości polskich firm na wejście w życie RODO deklarują, że ich firmy i instytucje prawidłowo identyfikują oraz lokalizują posiadane przez siebie dane osobowe. To istotne, ponieważ skuteczne zapewnienie zgodności z nowymi przepisami wymaga najpierw ustalenia, których danych w organizacji dotyczą nowe przepisy.**

Przepisy Ogólnego rozporządzenia o ochronie danych osobowych (RODO) stanowią, że danymi osobowymi są informacje dotyczące zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych. Choć pojęcie „osoby zidentyfikowanej" nie jest jednoznacznie zdefiniowane, przyjmuje się, że jest to osoba, której identyfikować nie trzeba, ponieważ jej tożsamość jest znana. „Osoba możliwa do zidentyfikowania" to z kolei według art. 4 ust. 1 RODO osoba, „którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak: imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej". Podobnie jak w świetle obowiązujących obecnie przepisów ustalenie, czy dana osoba jest „możliwa do zidentyfikowania", wymaga wzięcia pod uwagę nie tylko fizycznej możliwości zrealizowania tej czynności, ale i „uzasadnionego prawdopodobieństwa" podjęcia próby identyfikacji przez administratora danych oraz uwzględnienia niezbędnych do tego zasobów, np. czasu czy pieniędzy.

O ile zatem zasadnicza koncepcja definiowania danych osobowych w RODO nie zmieniła się w stosunku do obowiązującej jeszcze Ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (UODO), o tyle RODO wprowadza m.in. nowe kategorie danych osobowych, jak choćby wskazane „identyfikatory internetowe" – numery IP czy pliki cookie – oraz tzw. szczególne kategorie danych, które nie pokrywają się ze stosowaną obecnie w Polsce koncepcją danych wrażliwych. Rzetelne przygotowanie do wejścia w życie RODO będzie zatem wymagało weryfikacji posiadanych zbiorów danych pod kątem ich dopasowania do wprowadzonych zmian.

## Skuteczna identyfikacja danych...

Zważywszy, że polska Ustawa o ochronie danych osobowych funkcjonuje już 20 lat, a koncepcja jej definiowania w ramach RODO istotnie się nie zmieniła, można było spodziewać się, że polskie organizacje będą w stanie prawidłowo identyfikować posiadane dane także po wejściu w życie nowego prawa.

Uczestnicy badania zostali zapytani, czy ich organizacje potrafią określić, które spośród posiadanych przez nie danych wyczerpują definicję danych osobowych według RODO. 70% respondentów zadeklarowało, że ich organizacje potrafią wskazać wszystkie posiadane dane osobowe. Kolejne 18% badanych potrafi ustalić dane osobowe pod warunkiem, że są to dane o charakterze ustrukturyzowanym. Jedynie 12% organizacji nie potrafi zidentyfikować swoich danych, nie analizowało ich pod tym kątem, bądź nie umiało odpowiedzieć jednoznacznie ustosunkować się do tej kwestii.

Wskazane wyżej proporcje są bardzo zbliżone zarówno w dużych organizacjach (251 i więcej pracowników), jak i średniej wielkości przedsiębiorstwach (81–250 pracowników), z jednym zastrzeżeniem: 7% respondentów z tej pierwszej grupy zadeklarowało, że nie analizowałootąd danych pod kątem zgodności z RODO. W przypadku średniej wielkości organizacji takie wskazania w ogóle nie zostały udzielone, a 7% respondentów nie potrafiło określić, czy ich

**Mariusz Olszewski,**
**Data Management Solution Manager**

Wyniki ankiety, pokazujące jakoby większość organizacji potrafiła bez problemu zidentyfikować wszystkie miejsca przetwarzania i przechowywania danych osobowych, są dla mnie zaskakujące. Może to jednak wynikać ze zbytniego uproszczenia rzeczywistości. W dużych organizacjach trudno jest bowiem szybko i jednoznacznie wskazać wszystkie miejsca przechowywania i przetwarzania danych osobowych w systemach produkcyjnych. Pamiętajmy, że istnieją jeszcze środowiska testowe, deweloperskie i szkoleniowe, w których także mogą znajdować się dane osobowe. Może zatem kluczowy jest tu czas potrzebny do ustalenia i zidentyfikowania tychże danych? Ta sama grupa rozmówców jednoznacznie stwierdza, że nie posiada wiedzy i narzędzi wspomagających inwentaryzację danych osobowych w źródłach nieustrukturyzowanych. Nic dziwnego – takie narzędzia pojawiły się stosunkowo niedawno.

**Czy Twoja organizacja potrafi określić, które spośród posiadanych przez nią danych wyczerpują definicję danych osobowych według RODO?**

| | |
|---|---|
| Tak, potrafimy wskazać wszystkie posiadane dane osobowe. | 70% |
| Tak, potrafimy wskazać dane osobowe, ale dotyczy to jedynie danych ustrukturyzowanych. | 18% |
| Nie potrafimy jednoznacznie ocenić, które spośród danych w organizacji są danymi osobowymi według przepisów RODO. | 4% |
| Nie analizowaliśmy dotąd danych pod kątem odpowiedzi na to pytanie. | 4% |
| Trudno powiedzieć. | 4% |

**Czy Twoja organizacja potrafi identyfikować i lokalizować wszystkie miejsca przetwarzania i przechowywania posiadanych danych osobowych?**

| | |
|---|---|
| Tak, potrafimy ustalić i zidentyfikować wszystkie miejsca przetwarzania i przechowywania danych osobowych. | 78% |
| Tak, potrafimy ustalić i zidentyfikować miejsca przetwarzania i przechowywania danych osobowych, ale tylko ustrukturyzowanych. | 14% |
| Potrafimy ustalić i zidentyfikować miejsca przetwarzania i przechowywania części danych ustrukturyzowanych. | 4% |
| Nie potrafimy jednoznacznie ustalić i zidentyfikować miejsc przetwarzania i przechowywania posiadanych danych osobowych. | 4% |

**Identyfikacja i lokalizacja danych osobowych – najważniejsze różnice między RODO a UODO**

- Uznanie identyfikatorów internetowych za dane osobowe.
- Zastąpienie kategorii danych wrażliwych koncepcją „danych szczególnych". Co istotne, nie wszystkie dane uznawane dotąd za wrażliwe w świetle przepisów RODO będą danymi szczególnymi.
- Wprowadzenie i zdefiniowanie pojęć danych genetycznych oraz biometrycznych.

firmy potrafią identyfikować wszystkie posiadane dane osobowe.

## ...oraz miejsc ich przetwarzania

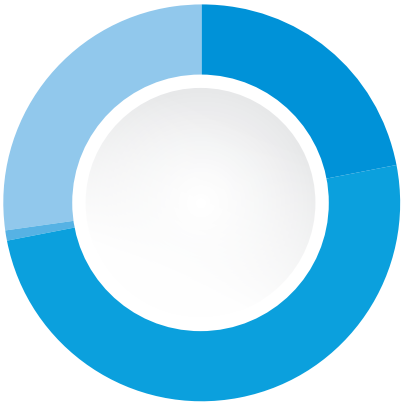
Określenie, które spośród posiadanych przez organizację danych wyczerpują definicję danych osobowych, to jedno. Drugą kluczową sprawą jest ustalenie, gdzie wszystkie dane są przetwarzane i przechowywane. Okazało się, że i w tym przypadku polskie organizacje radzą sobie dobrze; blisko czterech na pięciu uczestników badania (78%) stwierdziło, że ich organizacje potrafią ustalić wszystkie miejsca przetwarzania i przechowywania posiadanych danych osobowych. Kolejne 14% respondentów zadeklarowało, że potrafi zlokalizować takie dane, zastrzegając jednak, że mają na myśli tylko dane ustrukturyzowane. Po 4% badanych wskazało, że jest w stanie zidentyfikować tylko część danych ustrukturyzowanych lub w ogóle nie potrafi jednoznacznie określić miejsc przetwarzania i przechowywania swoich danych osobowych.

Warto zaznaczyć, że wielkość badanych organizacji miała wpływ na zdolność lokalizowania posiadanych danych. O ile aż 87% organizacji średniej wielkości potrafi zidentyfikować miejsca przetwarzania i składowania wszystkich swoich danych, o tyle w przypadku przedsiębiorstw zatrudniających więcej niż 250 pracowników liczba analogicznych deklaracji była już o 15 pkt proc. mniejsza. Duże organizacje blisko dwa razy częściej niż średnie (17% w stosunku do 9%) są w stanie zlokalizować jedynie dane o charakterze ustrukturyzowanym. Co istotne, brak możliwości jednoznacznego ustalenia lokalizacji posiadanych danych występuje tylko wśród dużych przedsiębiorstw. Deklaracje te nie są zaskakujące – duże firmy i przedsiębiorstwa dysponują z zasady wieloma źródłami danych czy miejsc ich przetwarzania, a posiadana przez nie infrastruktura często zawiera wiele elementów dziedzicznych (tzw. legacy). Średnie (i mniejsze organizacje) nie ma tego problemu, co umożliwia im łatwiejsze zapanowanie nad posiadanymi zasobami.

## Ocena jakości danych osobowych

Uczestnicy badania „RODO w polskich organizacjach" zostali poproszeni również o ocenę jakości posiadanych danych osobowych. Połowa z nich (50%) dobrze

### Jak oceniasz jakość danych osobowych posiadanych przez Twoją organizację?



| | |
|---|---|
| 22% | Bardzo dobrze. |
| 50% | Dobrze. |
| 1% | Słabo. |
| 27% | Trudno powiedzieć - jakość poszczególnych zbiorów/baz danych istotnie różni się od siebie. |

oceniła jakość posiadanych danych. Jako bardzo dobre określiło je kolejne 22% respondentów. 27% z nich stwierdziło natomiast, że nie umie jednoznacznie ocenić jakości danych, ponieważ poszczególne ich zbiory różnią się od siebie w istotny sposób. Oczywiście, ostatnia odpowiedź była szczególnie często formułowana przez przedstawicieli dużych organizacji – niemożność jednoznacznej oceny jakości danych zadeklarowała ⅓ z nich (w porównaniu do 18% jednostek średniej wielkości). Respondenci wywodzący się z dużych organizacji zauważalnie rzadziej także niż ci ze średnich oceniali jakość swoich danych jako dobrą lub bardzo dobrą – odpowiednio 65% w porównaniu do 82%.

Ocena jakości posiadanych danych siłą rzeczy wiąże się z możliwością ich zdefiniowania – udział ocen dobrych i bardzo dobrych w pytaniu dotyczącym jakości posiadanych danych osobowych wykazał korelację z możliwością ich identyfikacji oraz lokalizacji. Dobrą lub bardzo dobrą ocenę jakości danych przedstawiło 83% uczestników badania, którzy zadeklarowali, że potrafią zidentyfikować wszystkie posiadane dane, oraz 76% tych, którzy potrafią ustalić miejsca ich przetwarzania (w porównaniu do 72% analogicznych odpowiedzi ogólnej puli respondentów).

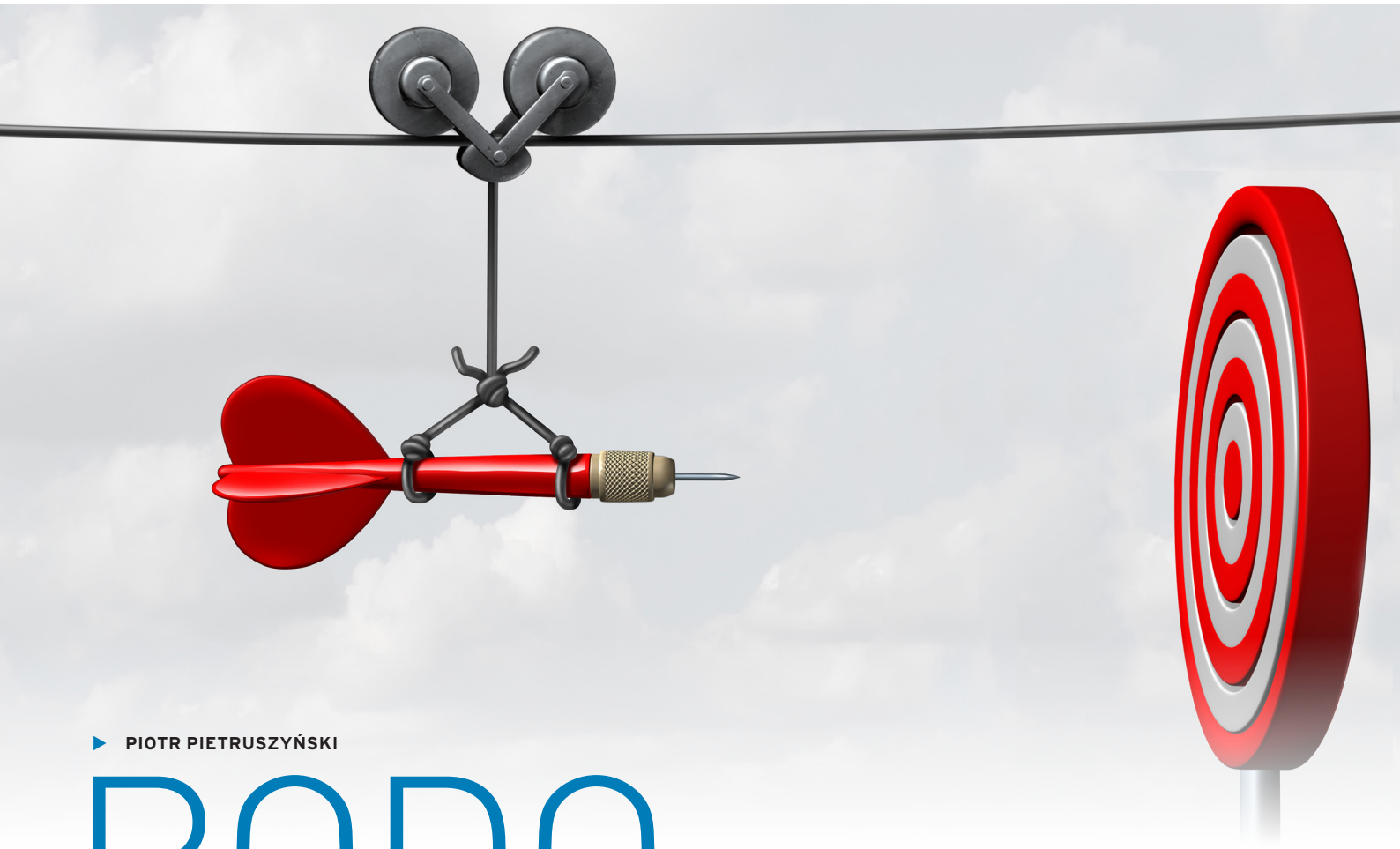
**Mariusz Olszewski,**
**Data Management Solution Manager**

Jakość danych osobowych to temat dość drażliwy i organizacje w większości przypadków niechętnie mówią o problemach jakości danych znajdujących się w ich systemach. Często także mogą sobie nie zdawać z tego sprawy. Problem jakości w danych istnieje, a należy pamiętać, że wpływa on bezpośrednio na wymagania RODO – choćby na słynne już prawo klienta do bycia zapomnianym. Jak bowiem zidentyfikować klienta, jeśli często nawet w jednym systemie jest zapisany na kilka sposobów, i to w dodatku z błędami?

Im większa organizacja, tym więcej błędów w danych. Wynika to zazwyczaj z kilku czynników:

1) Duże organizacje przeszły swego czasu transformację systemów transakcyjnych ze zdecentralizowanych do scentralizowanych – migracje danych często bez odpowiedniego procesu czyszczenia i walidacji spowodowały zwiększenie ilości błędnych danych.
2) Źle zaprojektowane interfejsy do wprowadzania danych i braki walidacji spowodowały generowanie błędów przez osoby wprowadzające dane.
3) Brak odpowiednich procedur i kultury organizacyjnej motywującej do prawidłowego wprowadzania danych w organizacji to jeden z poważniejszych czynników wpływających na pojawianie się błędnych danych.

Aby rozmawiać szczerze o jakości danych w organizacji, niezbędne jest zdobycie zaufania jej przedstawicieli, np. poprzez pokazanie know-how i narzędzi mogących pomóc w rozwiązaniu problemu.



PIOTR PIETRUSZYŃSKI

# RODO uporządkuje procesy zarządzania danymi i kontroli nad nimi

**Polskie organizacje dobrze identyfikują i lokalizują posiadane dane, jednak wychodząca naprzeciw zapisom RODO kontrola nad tymi danymi oraz ich przetwarzaniem będzie wymagała od przedsiębiorców przepracowania polityk zarządzania ryzykiem oraz dostosowania środowisk IT.**

Właściwa identyfikacja danych oraz kontrola nad miejscami ich przetwarzania to za mało, by mówić o gotowości na RODO. Według wyników badania przeprowadzonego przez „Computerworld" we współpracy z Sygnity i SAS Institute, jedynie niecała połowa polskich organizacji w pełnym zakresie analizuje ryzyka związane z przetwarzaniem danych osobowych, a niewiele więcej niż co dziesiąta posiada rozwiązanie do zarządzania i dokumentowania całościowego przepływu informacji.

## Kontrola nad przetwarzaniem i składowaniem danych

Uporządkowane podejście do zapewnienia zgodności z RODO wymaga – po uprzedniej identyfikacji posiadanych danych osobowych – analizy stopnia kontroli nad źródłami przetwarzanych danych. W tym zakresie polskie przedsiębiorstwa radzą sobie nieźle; 63% uczestników badania zadeklarowało pełną kontrolę nad miejscami przetwarzania wszystkich posiadanych danych osobowych, wraz z monitoringiem ich wykorzystania, raportowaniem oraz możliwością ustalenia lokalizacji. Kolejne 18% respondentów udzieliło podobnej odpowiedzi, jednak z zastrzeżeniem, że pełna kontrola dotyczy w ich przypadku tylko danych ustrukturyzowanych. Na różnego rodzaju trudności i braki ograniczające możliwość kontroli i zarządzania danymi wskazało 19% badanych.

Interesujące obserwacje niesie rozdzielenie opisanych wyżej wyników na odpowiedzi udzielone przez przedstawicieli dużych i średnich organizacji; o ile pełną kontrolę nad danymi sprawuje 69% firm średniej wielkości, o tyle w przypadku największych przedsiębiorstw i instytucji podobnej deklaracji udzieliło 59% respondentów. Grupa ta częściej z kolei wskazuje różne ograniczenia co do możliwości i zakresu kontroli posiadanych danych osobowych (razem 16%) bądź zupełny brak takiej możliwości (3%) niż w przypadku organizacji o mniejszej skali (odpowiednio 13% i brak wskazań). Duże przedsiębiorstwa mają zwykle najwięcej źródeł danych oraz dziedzicznych, silosowych systemów IT, co w niektórych przypadkach skutecznie uniemożliwia określenie, gdzie i w jaki sposób przetwarzane i składowane są informacje spełniające definicję danych osobowych.

## Zarządzanie ryzykiem i stopniem zabezpieczenia danych

Zarządzanie ryzykiem jest jednym z fundamentalnych wymagań RODO. Przepisy rozporządzenia wymagają, by podmioty przetwarzające dane osobowe analizowały poziom ryzyka naruszenia tych danych w odniesieniu do konkretnego kontekstu danej firmy, a także oceniały skutki planowanych działań w zakresie przetwarzania danych (zasada „Privacy by Design"). Na podstawie takiej analizy organizacja będzie musiała wdrożyć adekwatne środki zapobiegawcze – zarówno organizacyjne, jak i technologiczne. Co więcej, przed-

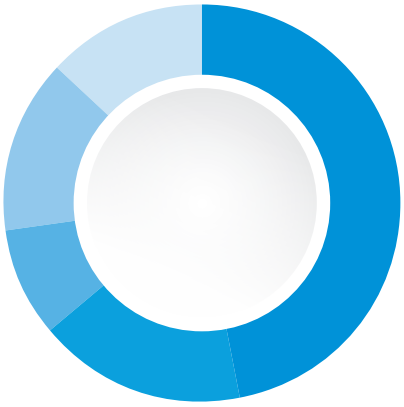
**Mariusz Olszewski,**
**Data Management Solution Manager**

63% to dość dobry wynik. Sytuacja byłaby rewelacyjna, gdyby te 63% ankietowanych firm wdrożyła rozwiązania typu Data Governance i Identity Governance lub była w trakcie ich wdrożenia, bo nie da się kontrolować wszystkiego bez tego rodzaju narzędzi. Niestety, tylko 11% respondentów zadeklarowało posiadanie rozwiązań wspierających aspekt Data Governance. Być może po raz kolejny jest to efekt zbyt optymistycznego postrzegania rzeczywistości wynikający z braku wiedzy co do istnienia obszarów pozostających poza kontrolą. Warto jednak zaznaczyć, że sytuację nieco poprawia deklaracja 32% respondentów o toczących się pracach związanych z katalogowaniem całościowego przepływu informacji w organizacji w kontekście danych osobowych.

**Czy Twoja organizacja kontroluje wszystkie miejsca przetwarzania i przechowywania posiadanych danych osobowych oraz dostęp do nich?**

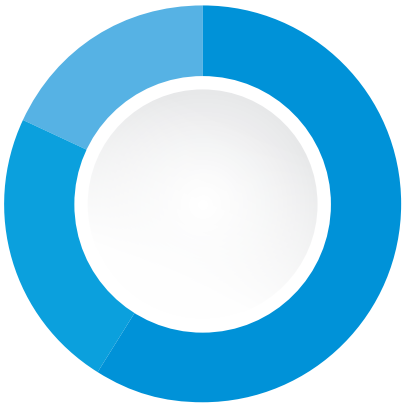
| | |
|---|---|
| Kontrolujemy wszystkie miejsca przetwarzania danych osobowych, wraz z dostępem, monitoringiem aktywności, raportowaniem oraz możliwością ustalenia ich lokalizacji. | 63% |
| Kontrolujemy tylko miejsca przetwarzania ustrukturyzowanych danych osobowych, wraz z dostępem, monitoringiem aktywności, raportowaniem oraz możliwością ustalenia ich lokalizacji.w | 18% |
| Kontrolujemy tylko miejsca przetwarzania ustrukturyzowanych danych osobowych, wraz z dostępem, monitoringiem aktywności i raportowaniem, ale bez możliwości ustalenia ich lokalizacji. | 2% |
| Kontrolujemy tylko ustrukturyzowane miejsca przetwarzania danych, wraz z zarządzaniem dostępem, ale bez monitoringu aktywności, raportowania czy możliwości ustalenia ich lokalizacji. | 5% |
| Kontrolujemy tylko część ustrukturyzowanych miejsc przetwarzania danych osobowych. | 8% |
| Nie kontrolujemy miejsc przetwarzania danych osobowych w organizacji. | 2% |
| Trudno powiedzieć. | 2% |

### Czy Twoja organizacja potrafi określić poziom ryzyka dla poszczególnych miejsc przetwarzania i przechowywania danych osobowych?



| | |
|---|---|
| 47% | Tak, włącznie z oceną konsekwencji wystąpienia naruszenia danych. |
| 17% | Tak, ale z wyłączeniem oceny konsekwencji wystąpienia naruszenia danych. |
| 9% | Organizacja nie rozróżnia poziomów ryzyka dla poszczególnych miejsc przetwarzania i przechowywania danych. |
| 14% | Organizacja nie analizuje ryzyka wystąpienia naruszeń danych. |
| 13% | Trudno powiedzieć. |

### Czy Twoja organizacja wykorzystuje mechanizmy anonimizacji, pseudonimizacji oraz szyfrowanie danych?



| | |
|---|---|
| 59% | Tak |
| 23% | Nie |
| 18% | Trudno powiedzieć |

siębiorca będzie zobligowany do zapewnienia tzw. rozliczalności, tj. możliwości wykazania i udokumentowania zgodności stosowanych rozwiązań z prawem.Wbrew pozorom może to okazać się bardzo trudne, ponieważ wymaga od firmy zaangażowania w opracownie własnej metodyki zarządzania danymi, a nie odtwórczego wdrożenia odgórnie narzuconego pakietu rozwiązań. Związana z tym odpowiedzialność oraz ryzyko spoczywać będą na administratorach danych.

Zdolność do pełnozakresowego szacowania ryzyka związanego z przetwarzaniem danych osobowych zadeklarował mniej niż co drugi (47%) uczestnik badania. Kolejne 17% respondentów szacuje ryzyka, nie podejmując jednak analiz dotyczących potencjalnych konsekwencji naruszenia danych w którymś z miejsc ich przetwarzania bądź składowania. Więcej niż co trzeci (36%) ankietowany powiedział, że jego organizacja nie różnicuje poziomu ryzyka, w ogóle (!) nie analizuje możliwości wystąpienia naruszeń w obszarze danych osobowych, lub nie potrafił udzielić jednoznacznej odpowiedzi.

Co ciekawe, o ile duże organizacje mają więcej problemów z kontrolą nad miejscami, w których przetwarzane sąich dane, o tyle znacznie lepiej wypadają w odniesieniu do kwestii związanych z szacowaniem ryzyka, z jakim wiąże się praca na danych osobowych. 54% respondentów wywodzących się z organizacji zatrudniających więcej niż 250 pracowników zadeklarowało pełną zdolność do analizy potencjalnych zagrożeń wraz z ich możliwymi konsekwencjami – to o 16 pkt proc. więcej niż w przypadku średnich organizacji. Te ostatnie ponadto dwa razy częściej niż duże (20% w porównaniu do 10%) wskazywały, że nie prowadzą żadnych analiz dotyczących ryzyka wystąpienia naruszeń danych. 22% uczestników badania reprezentujących średniej wielkości firmy i instytucje nie umiało ustosunkować się do pytania o zakres takich analiz. Podobnych deklaracji w grupie ankietowanych z dużych organizacji było o 15 pkt proc. mniej.

Nierozerwalnie związana z analizą ryzyka wystąpienia naruszeń w obszarze bezpieczeństwa danych osobowych jest możliwość ich szyfrowania (np. na poziomie baz danych czy pamięci masowych), a także anonimizacji (trwałe uniemożliwienie identyfikacji tożsamości) lub pseudonimizacji (według art. 4 ust. 5 RODO oznaczającej „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”).

59% organizacji, których przedstawiciele wzięli udział w badaniu, szyfruje posiadane dane oraz stosuje różnego rodzaju mechanizmy ich anonimizacji i pseudonimizacji. Z takich rozwiązań nie korzysta 23% przedsiębiorstw, w szczególności średniej wielkości (27%, tj. o 7 pkt proc. więcej niż w przypadku dużych organizacji).

Szyfrowanie danych jest jednym z czynników skutecznej kontroli oraz zarządzania danymi pod kątem zapewniania zgodności z RODO rozumianej jako adresowanie właściwego stopnia zabezpieczeń w zależności od skali, na jaką przedsiębiorstwo przetwarza dane, a także kontekstu, w którym działa. Nie dziwi więc fakt, że w grupie organizacji, które pełnozakresowo podchodzą do problemu oceny ryzyka wystąpienia zagrożenia danych, wykorzystanie wymienionych wyżej mechanizmów jest zauważalnie częste niż w ogóle próby (72%). A contrario, w firmach, które w ogóle nie analizują ryzyka związanego z przetwarzaniem danych osobowych, szyfrowanie danych, pseudonimizację czy anonimizację wykorzystuje raptem 31% respondentów, zaś dokładnie połowa z nich w ogóle nie stosuje takich rozwiązań.

Podobna korelacja zachodzi w przypadku kontroli nad miejscami przetwarzania danych. Wśród firm, które kontrolują jedynie część swoich danych, nie kontrolują ich wcale bądź nie potrafią określić stopnia kontroli, wykorzystanie mechanizmów

anonimizacji, pseudonimizacji oraz szyfrowania danych było 30 pkt proc. niższe niż w przypadku ogólnej puli respondentów.

## IT z myślą o RODO

Istotna będzie rola właściwego zaplecza technologicznego w zagwarantowaniu zgodności z RODO. Konieczna będzie pełnozakresowa kontrola nad miejscami przetwarzania danych, dostarczenie mechanizmów umożliwiających ich monitoring, usuwanie na życzenie – w tym z kopii bezpieczeństwa czy zarchiwizowanych zbiorów danych, czy też stworzenie notyfikacji dotyczących naruszeń danych.

Wśród uczestników badania jedynie niewielka część posiada przygotowane do wejścia w życie RODO zaplecze IT (11%). Znaczna część respondentów zadeklarowała jednak, że w ich firmach i jednostkach rozpoczęto już prace mające na celu skatalogowanie całościowego przepływu informacji w organizacji w kontekście danych osobowych (32%).Warto zaznaczyć, że wskazań tych udzieliło blisko dwa razy więcej przedstawicieli dużych organizacji niż średniej wielkości przedsiębiorstw (39% do 22%).

Kolejne 28% ankietowanych stwierdziło, że w ich firmach wykorzystuje się różnego rodzaju silosowe systemy do zarządzania danymi, zaś 11% nie potrafiło wskazać jednoznacznej odpowiedzi.

Blisko co piąta (18%) organizacja nie ma rozwiązań do zarządzania danymi. W grupie tej wyraźnie dominują respondenci z firm o mniejszym zatrudnieniu (27% wskazań w porównaniu do 13% wśród dużych przedsiębiorstw).

Jak w tym kontekście wyglądają plany inwestycyjne i rozwojowe polskich organizacji? Blisko co trzecia (32%) firma jest w trakcie adaptacji lub wdrażania systemu do zarządzania danymi, bądź też planuje podjąć taki wysiłek w ciągu najbliższych miesięcy, poprzedzających wejście w życie RODO, tj. 25 maja 2018 roku. Plany inwestycyjne wykraczające poza tę datę ma 7% przedsiębiorstw. Ankietowani często deklarowali brak planów dotyczących wdrażania bądź wymiany rozwiązania do zarządzania danymi (36%), a co czwarty respondent nie potrafił odpowiedzieć na pytanie dotyczące zakupów w tym obszarze.

Udział organizacji realizujących wdrożenia rozwiązań klasy Data Governance bądź planujących wdrożenie w ciągu najbliższego roku jest zauważalnie wyższy wśród tych, które deklarowały trwający proces katalogowania całościowego przepływu informacji w kontekście danych osobowych (o 14 pkt proc. niż w ogólnej puli badanych), oraz – w mniejszym stopniu – w grupie przedsiębiorstw mających dane zarządzane silosowo (o 6 pkt proc. więcej niż w przypadku ogółu respondentów). Obserwacja ta wskazuje, że efektami wejścia w życie RODO będzie m.in. integrowanie i porządkowanie zbiorów danych oraz ujednolicenie sposobów zarządzania nimi.

Co ciekawe, w grupie firm, które nie mają rozwiązań do zarządzania danymi, aż 43% respondentów nie potrafiło jednoznacznie odpowiedzieć na pytanie dotyczące planów ich wdrażania. Wiele organizacji analizuje prawdopodobnie, czy zapewnienie zgodności z RODO będzie wymagało zastosowania narzędzi IT. Liczne wskazania od-

**Mariusz Olszewski,**
**Data Management Solution Manager**

Z tygodnia na tydzień rośnie liczba organizacji rozpoczynających działania przygotowawcze do RODO. Niemniej 25% organizacji jeszcze nie rozpoczęło przygotowań i tym firmom doradzałbym pośpiech. Przygotowanie do RODO nie jest projektem łatwym ani tym bardziej krótkotrwałym. Wymaga zarówno inwestycji w sferze infrastruktury IT jak i – ze względu na przekrojowy charakter wdrożenia – współpracy większości działów w organizacji oraz zaangażowania jej kierownictwa.

**Czy Twoja firma posiada rozwiązanie do zarządzania i dokumentowania całościowego przepływu informacji w organizacji?**

| | |
|---|---|
| Posiadamy dostosowane do RODO rozwiązanie wspierające ten aspekt Data Governance (ład danych). | 11% |
| Jesteśmy w trakcie katalogowania całościowego przepływu informacji w organizacji w kontekście danych osobowych. | 32% |
| Posiadamy różne silosowe rozwiązania do zarządzania danymi. | 28% |
| Nie posiadamy tego typu rozwiązania. | 18% |
| Trudno powiedzieć. | 11% |

**Czy Twoja organizacja ma w planach wdrożenie lub wymianę systemu do zarządzania danymi?**

| | |
|---|---|
| Organizacja jest już w trakcie wdrożenia bądź adaptacji systemu do zarządzania danymi. | 12% |
| Tak, w ciągu najbliższych 6 miesięcy. | 4% |
| Tak, w ciągu najbliższych 12 miesięcy. | 16% |
| Tak, ale później niż w ciągu roku. | 7% |
| Nie zamierzamy wdrażać lub wymieniać systemu do zarządzania danymi w dającym się przewidzieć okresie. | 36% |
| Trudno powiedzieć. | 25% |

powiedzi „trudno powiedzieć” sugerują, że znaczna część polskich firm wciąż nie wie, w jaki sposób ma antycypować przepisy wynikające z RODO.

## Kontrola nad danymi i co dalej?

Ani poprawne identyfikowanie i lokalizowanie źródeł danych osobowych w organizacji, ani szacowanie ryzyka czy kontrola nad miejscami przetwarzania danych nie oznaczają, że dane przedsiębiorstwo jest przygotowane na RODO. Nawet jeżeli firma wie, gdzie i kto przetwarza dane w jej imieniu, oraz potrafi ocenić potencjalne konsekwencje naruszeń, wciąż musi dostosować swoje zaplecze technologiczne do takich wymogów, jak prawo do bycia zapomnianym i przenoszenia danych czy też rozróżnienia zgód na poszczególne rodzaje usług.

### Zarządzanie danymi – najważniejsze założenia RODO

- Konieczność wprowadzenia proaktywnych, adekwatnych działań w zakresie oceny skutków planowanych działań w odniesieniu do danych osobowych oraz zarządzania ryzykiem w tym obszarze (zasada „Privacy by Design”).
- Zasada „Privacy by Default”, zgodnie z którą przetwarzane ma być jedynie minimum danych, niezbędnych do realizacji danej usługi (celu przetwarzania).
- Wprowadzenie obowiązku powołania inspektora ochrony danych w przypadku przetwarzania danych osobowych na dużą skalę.
- Wprowadzenie obowiązku notyfikowania naruszeń bezpieczeństwa do organu ochrony danych osobowych.
- Zniesienie wymogu uzyskania zgody na piśmie w odniesieniu do danych szczególnych...
- ... oraz wprowadzenie obowiązku uzyskania zgody na profilowanie przed rozpoczęciem procesu gromadzenia danych.
- Zapewnienie prawa do bycia zapomnianym, prawa do przeniesienia danych oraz wglądu do nich.
- Zasada rozliczalności – przedsiębiorca musi mieć możliwość udokumentowania zgodności stosowanych rozwiązań z przepisami RODO.

### Na jakim etapie przygotowań do wejścia w życie RODO jest Twoja organizacja?

| | |
|---|---|
| Moja organizacja jest już gotowa na wejście w życie nowych przepisów. | 4% |
| Jesteśmy w trakcie koniecznej adaptacji procesów oraz infrastruktury IT. | 41% |
| Przygotowujemy koncepcję koniecznej adaptacji procesów oraz infrastruktury IT. | 30% |
| Poszukujemy partnerów i rozwiązań mających wesprzeć organizację w adaptacji procesów oraz infrastruktury IT na rzecz RODO. | 6% |
| Nie rozpoczęliśmy jeszcze żadnych przygotowań z myślą o wejście w życie RODO. | 10% |
| Słyszałem o RODO, ale nie znam szczegółów dotyczących przygotowań do jego wejścia w życie. | 9% |

| Na jakim etapie przygotowań do wejścia w życie RODO jest Twoja organizacja? | Duże firmy i korporacje | Organizacje średniej wielkości |
|---|---|---|
| Moja organizacja jest już gotowa na wejście w życie nowych przepisów. | 4% | 4% |
| Jesteśmy w trakcie koniecznej adaptacji procesów oraz infrastruktury IT. | 48% | 31% |
| Przygotowujemy koncepcję koniecznej adaptacji procesów oraz infrastruktury IT. | 26% | 36% |
| Poszukujemy partnerów i rozwiązań mających wesprzeć organizację w adaptacji procesów oraz infrastruktury IT na rzecz RODO.w | 3% | 11% |
| Nie rozpoczęliśmy jeszcze żadnych przygotowań z myślą o wejście w życie RODO. | 9% | 11% |
| Słyszałem o RODO ale nie znam szczegółów dotyczących przygotowań do jego wejścia w życie. | 10% | 7% |

ARTUR PĘCZAK

# Gotowość na RODO pod znakiem zapytania

**Nowe regulacje dotyczące ochrony danych osobowych wchodzą w życie z dniem 25 maja 2018 roku. To oznacza, że na przygotowanie się do nowych przepisów prawa pod względem organizacyjnym, proceduralnym i technicznym firmom pozostało raptem kilka miesięcy. Jak stan gotowości na wejście w życie RODO ocenili ankietowani dyrektorzy IT w zarządzanych przez siebie przedsiębiorstwach?**

RODO stanowi kolejny krok w kierunku zapewnienia obywatelom Unii Europejskiej wymaganego poziomu ochrony danych osobowych poprzez wprowadzenie unormowań prawnych dostosowanych do aktualnych zagrożeń i zmieniającego się otoczenia technologicznego. Z wprowadzeniem RODO Unia Europejska wraz z krajami członkowskimi kontynuuje działania na rzecz ochrony danych osobowych, opierające się dotychczas na Dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z 1995 roku oraz Ustawie o ochronie danych osobowych z 1997 roku. Czas na zmiany!

## Przygotowania do RODO

Jak wygląda stopień adaptacji do wytycznych RODO w polskich przedsiębiorstwach? Jedynie 4% firm deklaruje, że już jest gotowa na wejście w życie nowych przepisów; kolejne 41% pracuje nad dostosowaniem swoich procesów i infrastruktury IT do zapisów RODO. Adaptacja ta przebiega wyraźnie szybciej w dużych firmach, gdzie gotowość lub pracę nad zmianą systemów deklaruje nieco ponad połowa (52%) respondentów, podczas gdy w grupie organizacji średniej wielkości podobne przekonanie wyraził już niewiele więcej niż co trzeci (35%) ankietowany. Inna sprawa, że brak ostatecznych unormowań prawnych w dziedzinie ustawodawstwa krajowego, czy też jasnych wytycznych branżowych i kodeksów dobrych praktyk każe zastanowić się, na ile ktokolwiek (regulator rynku, dostawcy systemów IT, instytucje publiczne i przedsiębiorcy) jest „w pełni gotowy na RODO".

Podsumujmy zatem to, co wiemy. Prawie połowa przedsiębiorstw jest już w trakcie prac adaptacyjnych, tak aby gotowość na wejście w życie RODO została osiągnięta przed 25 maja 2018 roku. Co z drugą połową firm? 30% ankietowanych odpowiedziało, że jest w trakcie przygotowywania koniecznej adaptacji procesów oraz infrastruktury IT na rzecz RODO; kolejne 6% poszukuje partnerów i rozwiązań mających wesprzeć organizację w tych działaniach. Odpowiedzi te wskazują, że bardzo wiele firm jest dopiero na początku długiej drogi w kierunku zapewnienia zgodności z GIODO. „Mamy świadomość konieczności przeprowadzenia zmian, ale dopiero rozmawiamy o tym, jak wprowadzić je życie" – tak mogłaby brzmieć bardziej precyzyjna odpowiedź niektórych ankietowanych na pytanie o poziom przygotowań do RODO. To o tyle niepokojące, że Rozporządzenie zostało opublikowane już 24 maja 2016 roku; uwzględnia więc dwuletni okres dostosowawczy, z którego szereg przedsiębiorców w zasadzie nie skorzystało.

## Duzi są krok do przodu

Porównanie stopnia przygotowań organizacji średniej wielkości oraz dużych przedsiębiorstw wskazuje, że te pierwsze znacznie częściej deklarują, że są dopiero na etapie przygotowywania koncepcji niezbędnych adaptacji (36%) lub też poszukują wsparcia partnerów i odpowiednich rozwiązań IT (11%). W przypadku firm zatrudniających powyżej 250 osób odsetek ten wynosi odpowiednio 26% oraz 3%. Przytoczone dane potwierdzają, że duże przedsiębiorstwa i korporacje są dzisiaj lepiej przygotowane do wejścia w życie RODO niż mniejsze podmioty.

Dla niemal co piątej badanej firmy RODO pozostaje niewiadomą, a temat ochrony danych jest przez nie mniej lub bardziej ignorowany: 9% respondentów słyszało co prawda o RODO, ale nie zna szczegółów dotyczących przygotowań do jego wejścia w życie (przypomnijmy wyraźnie, że mówimy tu o dyrektorach IT), zaś kolejne 10% ankietowanych wie o nowych obowiązkach, ale nie rozpoczęło jeszcze przygotowań w kierunku ich wypełnienia. Jak widać, o RODO wciąż mówi się za mało, by wiedza o tym, z jak poważnymi zmianami oraz daleko idącymi konsekwencjami będą mieli do czynienia przedsiębiorcy, dotarła do wszystkich. Co istotne, w tym przypadku nie miało znaczenia to, czy ankietowani reprezentują średnie, czy też duże organizacje; w obu przypadkach wyniki kształtowały się podobnie.

W ujęciu sektorowym najlepiej z dostosowaniem się do nowych regulacji radzą sobie firmy informatyczne, które same gromadzą i przetwarzają dane osobowe, ale i dostarczają na rynek rozwiązania do ochrony tych danych. 73% przedstawicieli branży IT deklaruje, że ich firmy są w trakcie prac nad implementacją RODO, a kolejne 20% przygotowuje się do zrobienia tego kroku w najbliższym czasie. Wśród pozostałych podmiotów najbliżej do pełnej adaptacji nowych uwarunkowań prawnych mają firmy z szeroko pojętego sektora FMCG i handlu. 8% z nich jest gotowych na RODO już dzisiaj, zaś kolejne 33% intensywnie pracuje, aby zdążyć przed majem 2018 roku.

Na tym tle blado wypada przemysł i produkcja. Z jednej strony 7% podmiotów tego sektora deklaruje gotowość, z drugiej zaś 40% w ogóle nie rozpoczęło prac nad dostosowaniem procesów i systemów IT do RODO. Wyniki te można interpretować na wiele sposobów – w tej kategorii branżowej mamy dwie różne grupy firm, z jednej strony np. dostawców energii dla sektora B2C posiadających potężne bazy danych osobowych, z drugiej zaś przedsiębiorstwa produkcyjno-przemysłowe, które z uwagi na specyfikę prowadzonego biznesu danych osobowych nie gromadzą, w związku z czym RODO nie dotknie ich w takim stopniu jak pierwszej wymienionej grupy (przypomnijmy zasadę adekwatności).

## Nowe zasady RODO

RODO wprowadza szereg zmian w dotychczasowych zasadach ochrony danych osobowych oraz nakłada wiele nowych obowiązków na podmioty gromadzące i przetwarzające te dane. RODO wiąże się z wyższą odpowiedzialnością podmiotów zbierających dane osobowe, nowymi zasadami uzyskiwania zgód na ich przetwarzanie, profilowanie oraz przekazywanie podmiotom trzecim, obowiązkiem zgłaszania naruszeń do organu nadzorczego, czy w końcu koniecznością powołania (w wybranych podmiotach) inspektora ochronnych danych. W zakresie danych osobowych RODO przyznaje obywatelom nowe prawa, w tym najczęściej komentowane i budzące najwięcej wątpliwości „prawo do bycia zapomnianym" (np. jak realizować to prawo w rozproszonych bazach danych typu Blockchain?). W efekcie RODO stanowi dla przedsiębiorstw i instytucji istotne wyzwanie na płaszczyźnie organizacyjnej i technologicznej, m.in. w zakresie szyfrowania danych czy usuwania wybranych rekordów z kopii zapasowych.

W tym kontekście zapytaliśmy przedstawicieli średnich i dużych przedsiębiorstw o stopień

# Sprawne wdrożenie RODO z platfomą SAS

**Miłosz Trawczyński, Business Consulting Manager, SAS Polska**

Chcąc upewnić się, że polityka firmy jest zgodna z RODO, organizacje muszą w pierwszej kolejności uporządkować informacje którymi dysponują oraz zlokalizować wśród nich dane osobowe. Menedżerowie ankietowanych firm wskazują, że w dużej mierze potrafią zlokalizować dane osobowe (zapewne wg dotychczasowej ich definicji, bazując na zbiorach rejestrowanych w GIODO), jednocześnie wskazując na wyzwania związane z jakością posiadanych danych oraz adekwatnym podejściem do oceny ryzyka. RODO nakłada na firmy nowe obowiązki, związane chociażby z prawem do bycia zapomnianym oraz prawem do uzyskania informacji o posiadanych przez firmę danych klienta i procesach, w jakich są one przetwarzane. Wymagać to będzie od firm sprawności w zintegrowaniu i standaryzacji posiadanych informacji o klientach, dostawcach, pracownikach etc. z rozproszonych systemów, a także skatalogowania posiadanych informacji.

Projekty związane z jakością danych i ich standaryzacją (zwłaszcza danych klienckich) będą nabierały jeszcze większego znaczenia. Istotną rolę w tym procesie odegrają rozwiązania do zarządzania danymi. Dzięki nim przedsiębiorstwa mogą skutecznie analizować przepływ danych osobowych, kontrolować jakość i standardy zapisu, regulować i rejestrować dostęp do informacji, szyfrować treści poufne, a także definiować zasady zarządzania danymi w organizacji. Będzie to niezbędne do skutecznego zarządzania ryzykiem związanym z zarządzaniem danymi osobowymi w organizacji.
SAS dostarcza platformę technologiczną, która umożliwia zaprojektowanie ciągłego, cyklicznego procesu mającego na celu zabezpieczenie i zarządzanie danymi osobowymi oraz zapewnia kontrolę jakości i zintegrowanie posiadanych heterogenicznych danych. Skuteczne wdrożenie rozwiązania SAS Data Governance daje możliwość nawiązania rzeczowego dialogu z regulatorem, dzięki czemu będziemy w stanie odpowiedzieć na najważniejsze pytania: jakie dane osobowe przetwarzamy, w jakich systemach są one przetwarzane, gdzie przechowywane i kto ma do nich dostęp.

przygotowania ich organizacji do realizacji wytycznych RODO w kilku podstawowych obszarach: identyfikacji, sposobu pozyskiwania i zarządzania danymi osobowymi, ich przepływami w organizacji i poza nią oraz mechanizmów zarządzania stwierdzonymi incydentami bezpieczeństwa. Ocena stanu przygotowań do RODO w poszczególnych obszarach ryzyka daje pełniejszy obraz, które wytyczne zostały wypełnione, a które wymagają podjęcia pilnych działań.

## Identyfikacja miejsc przetwarzania danych

Najbardziej zaawansowane prace nad wdrożeniem dyrektyw RODO można dostrzec w obszarze identyfikacji miejsc przechowywania i przetwarzania danych osobowych. 39% ankietowanych już dzisiaj w pełni zaewidencjonowało miejsca składowania i przetwarzania tych danych, zaś kolejne 43% jest na bardzo zaawansowanym etapie tych prac.
Wynik ten nie powinien dziwić, bowiem identyfikacja tych obszarów jest punktem wyjścia w kierunku implementacji RODO w organizacji, zaś sama koncepcja identyfikowania danych w ramach RODO nie zmieniła się istotnie w stosunku do obecnego stanu prawnego. Firmy, które dotychczas poważnie traktowały kwestie ochrony danych osobowych, katalogami źródeł danych powinny dysponować już wcześniej. Dla pozostałych organizacji identyfikacja miejsc przechowywania i przetwarzania ustrukturyzowanych baz danych, plików, archiwów czy kopii zapasowych, zawierających dane osobowe, nie powinna stanowić większego problemu. Co warte odnotowania, pełną gotowość w tym obszarze częściej deklarują średnie firmy (44%) aniżeli ich więksi konkurenci (35%). Blisko co drugi przedstawiciel firm (49%) zatrudniających powyżej 250 pracowników wskazywał jednak, że prace nad identyfikacją tych miejsc są na bardzo zaawansowanym etapie przygotowań. Być może wynika to ze skali i z rozproszenia działalności oraz liczby utrzymywanych baz danych i systemów.

## Zarządzanie danymi osobowymi

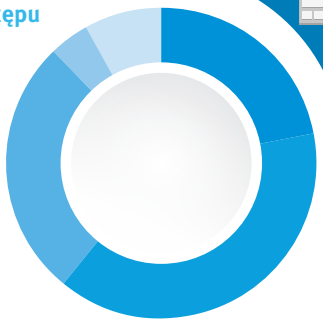
Kolejne trzy miejsca w odniesieniu do podmiotów, które deklarują pełną gotowość lub zaawansowany stan przygotowań, zajęły obszary: zarządzania danymi, ich jakością i dostępnością oraz monitorowaniem dostępu (łącznie 61% wskazań), optymalizacji

# Stopień przygotowania organizacji do wejścia w życie RODO w odniesieniu do wybranych kwestii:

## Wydzielone stanowisko Inspektora ochrony danych osobowych

| | |
|---|---|
| 22% | W pełni przygotowana |
| 30% | Zaawansowany etap przygotowań |
| 23% | Wczesny etap przygotowań |
| 8% | Brak gotowości |
| 18% | Nie dotyczy |

## Zarządzanie danymi, ich jakością i dostępnością, monitorowanie dostępu



| | |
|---|---|
| 22% | W pełni przygotowana |
| 39% | Zaawansowany etap przygotowań |
| 27% | Wczesny etap przygotowań |
| 4% | Brak gotowości |
| 8% | Nie dotyczy |

## Delegowanie przetwarzania do podmiotów trzecich

| | |
|---|---|
| 17% | W pełni przygotowana |
| 22% | Zaawansowany etap przygotowań |
| 15% | Wczesny etap przygotowań |
| 5% | Brak gotowości |
| 41% | Nie dotyczy |

## Identyfikacja miejsc przechowywania i przetwarzania danych osobowych

| | |
|---|---|
| W pełni przygotowana | 39% |
| Zaawansowany etap przygotowań | 43% |
| Wczesny etap przygotowań | 13% |
| Brak gotowości | 2% |
| Nie dotyczy | 4% |

## Procesy związane z przepływem i integracją danych między różnymi aplikacjami i partnerami

| | |
|---|---|
| W pełni przygotowana | 19% |
| Zaawansowany etap przygotowań | 42% |
| Wczesny etap przygotowań | 28% |
| Brak gotowości | 1% |
| Nie dotyczy | 10% |

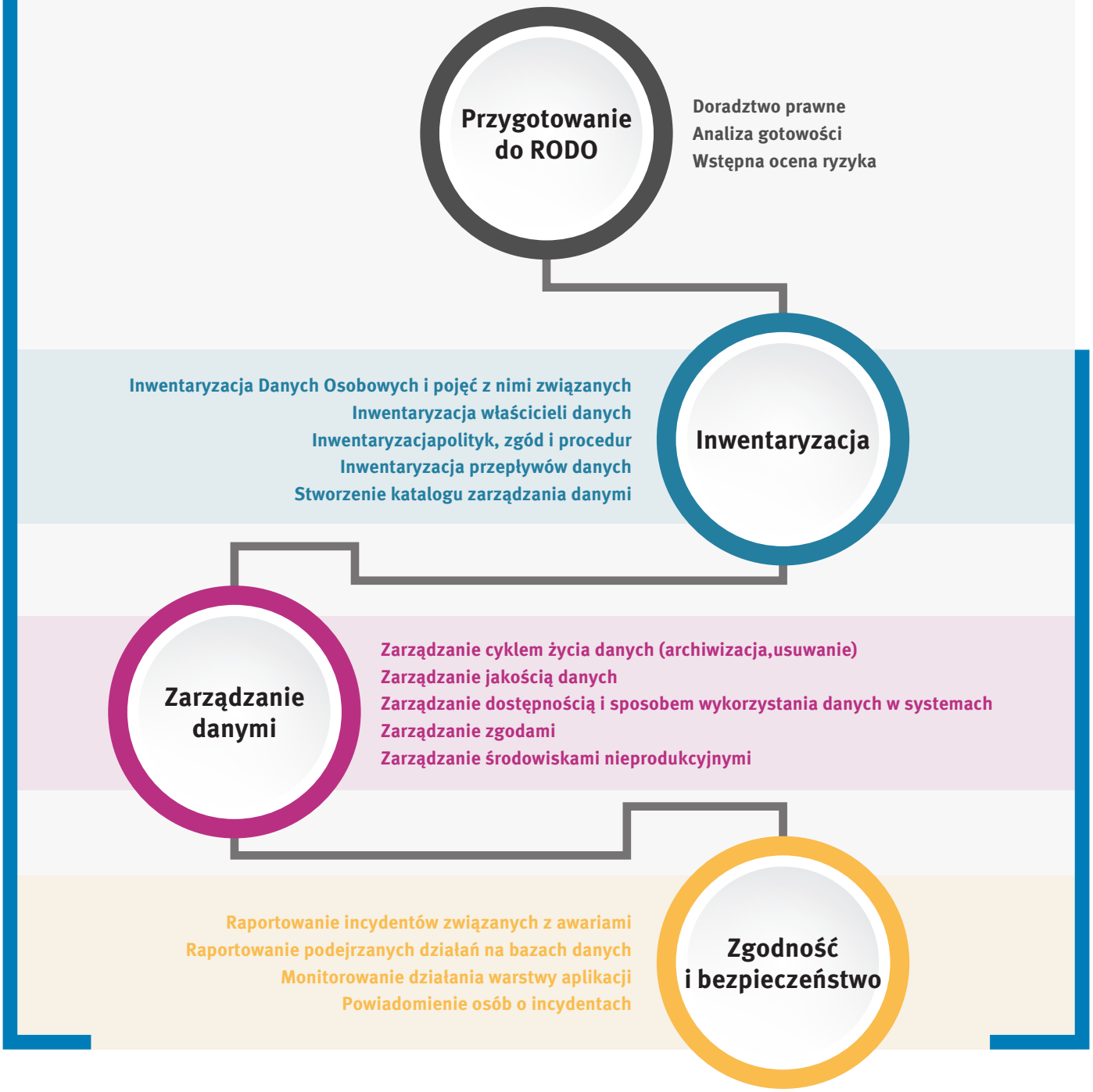
## Procesy pozyskiwania danych i archiwizacji zgód

| | |
|---|---|
| W pełni przygotowana | 24% |
| Zaawansowany etap przygotowań | 39% |
| Wczesny etap przygotowań | 25% |
| Brak gotowości | 4% |
| Nie dotyczy | 9% |

## Identyfikacja wpływu stwierdzonych incydentów bezpieczeństwa

| | |
|---|---|
| W pełni przygotowana | 23% |
| Zaawansowany etap przygotowań | 31% |
| Wczesny etap przygotowań | 38% |
| Brak gotowości | 4% |
| Nie dotyczy | 4% |

Opracowana przez **Sygnity** mapa drogowa dla projektu wdrożenia rozwiązań mających na celu zapewnienie zgodności firm z nowymi wymogami regulacyjnymi RODO oraz specjalnie dobrane wysokiej klasy narzędzia data governance naszych partnerów technologicznych zapewnia sprawną i szybką implementację.



procesów pozyskiwania danych i archiwizacji zgód (63%), a także dostosowania procesów związanych z przepływem i integracją danych między różnymi aplikacjami i partnerami (61%). Jak widać, wskazania te rozłożyły się równomiernie, co prawdopodobnie wynika ze ścisłych powiązań tych obszarów z perspektywy problematyki ochrony danych osobowych. W szczegółach wygląda to tak: mniej więcej co piąta firma uważa się za w pełni przygotowaną, zaś kolejne 39–42% podmiotów deklaruje zaawansowany postęp prac nad adaptacją RODO w omawianym zakresie. Śmiało można wysnuć wniosek, że prace w tych obszarach realizowane są w ramach tych samych zespołów czy grup projektowych, i to na nich skupia się cały ciężar zmian mających na celu dostosowanie organizacyjne i technologiczne przedsiębiorstw do wytycznych RODO. Dotyczy to również zdefiniowania różnego rodzaju procedur związanych z pozyskiwaniem, przechowywaniem, przetwarzaniem i współdzieleniem chronionych prawem danych osobowych wewnątrz organizacji i poza nią. Dodajmy, że co dziesiąty ankietowany uważa, że sprawy te nie dotyczą jego przedsiębiorstwa. Ufamy, że tak rzeczywiście jest.

Więcej różnic dostrzeżemy, gdy na wyniki badania spojrzymy przez pryzmat wielkości firm. Duże przedsiębiorstwa i korporacje wydają się w obszarze zarządzania danymi, ich jakością i dostępnością lepiej przygotowane niż ich konkurencja działająca w mniejszej skali: 23% podmiotów tej grupy deklaruje pełne przygotowanie, podczas gdy w kolejnych 42% prace są na zaawansowanym etapie. Wśród średniej wielkości organizacji analogicznych odpowiedzi udzieliło odpowiednio 20% oraz 36% respondentów. Być może większe podmioty, które już wcześniej implementowały np. rozwiązania do analizy dużych zbiorów danych, są merytorycznie lepiej przygotowane do wdrażania mechanizmów ochrony danych osobowych, jakie w wielu branżach stanowią podstawę prowadzonych analiz biznesowych, kreowania ofert itd. Organizacje średniej wielkości próbują nadrobić braki: co trzecia jest na wczesnym etapie przygotowań do adaptacji procesów zarządzania danymi do wymogów RODO.

W kwestii dostosowania procesów związanych z pozyskiwaniem danych i archiwizacją zgód na przetwarzanie i wykorzystanie danych osobowych 29% respondentów wywodzących się ze średnich organizacji uważa, że zrobili już wszystko, co konieczne. Dla porównania w grupie największych przedsiębiorstw podobne przekonanie wyraża już tylko co piąty ankietowany. Wydaje się, że duże firmy i korporacje intensywnie pracują, aby uporządkować procesy związane pozyskiwaniem danych i archiwizacją zgód – 43% z nich deklaruje, że jest na zaawansowanym etapie prac, podczas gdy w przypadku średnich podmiotów odsetek ten wynosi 12 pkt proc. mniej (31%). Średnie podmioty są dopiero na wczesnym etapie wprowadzania ich w życie – taki pogląd wyraziło kolejne 31% ankietowanych. Wyniki te warto rozpatrywać z dwóch perspektyw. Duże organizacje to duża baza klientów i różnorodność ofert. W rezultacie procesów i baz danych do uporządkowania pozostaje bardzo dużo. Średnie podmioty albo poradziły sobie już z tym procesem, albo dopiero zaczynają to robić.

W obszarze dostosowywania procesów związanych z przepływem i integracją danych między różnymi aplikacjami i partnerami 23% dużych podmiotów wyraża gotowość na RODO, podczas gdy w gronie średnich firm odsetek ten wynosi już tylko 13%. To bardzo obszerna kategoria, obejmująca zarówno kwestie związane z przepływem danych między wewnętrznymi i zewnętrznymi systemami, jak i analityką czy tworzeniem kopii zapasowych. Wobec dwóch ostatnich wymienionych kategorii jest to z pewnością najmocniej osadzony technologicznie obszar spośród wszystkich, o których ocenę poprosiliśmy ankietowanych. Średnie podmioty próbują nadgonić dzielący je dystans – 44% firm z tej grupy deklaruje zaawansowany etap przygotowań w obszarze pozyskiwania danych i archiwizacji zgód, a kolejne 31% właśnie rozpoczyna nad nimi prace. Dla porównania w gronie firm o zatrudnieniu większym niż 250 pracowników odsetek ten wynosi odpowiednio 43% oraz 22%.

## Delegowanie przetwarzania danych

Oddzielną, konieczną do rozważenia kwestią pozostają warunki delegowania przetwarzania danych osobowych do podmiotów trzecich. To bardzo złożony obszar, obejmujący wynoszenie systemów IT, na których przechowywane i przetwarzane są dane osobowe, do dostawców usług hostingowych czy chmurowych, ale także transfer danych osobowych pracowników wybranych przedsiębiorstw do centrum usług wspólnych działających poza granicami kraju.

41% ankietowanych odpowiedziało, że problem ten nie dotyczy ich firm. Co zrozumiałe, odpowiedzi takich więcej padło ze strony przedstawicieli średnich przedsiębiorstw (47%) niż dużych podmiotów i korporacji (38%). Pozostałe firmy mają nad czym pracować, bowiem tylko 17% z nich wprowadziło odpowiednie środki transferu danych osobowych do podmiotów trzecich, zaś kolejne 22% oraz 15% deklaruje, że jest na zaawansowanym lub początkowym etapie przygotowań.

## Inspektor ochrony danych osobowych

Jednym z obowiązków nakładanych przez RODO jest konieczność powołania inspektora ochrony danych osobowych, będącego co do zasady odpowiednikiem dzisiejszego administratora bezpieczeństwa informacji (ABI). Nie wchodząc w szczegóły, obowiązek ten dotyczyć będzie wszystkich instytucji publicznych oraz podmiotów sektora prywatnego, które przetwarzają dane osobowe na dużą skalę. Nic dziwnego, że aż 18% ankietowanych zadeklarowało, że wymóg ten ich nie dotyczy, przy czym odsetek ten jest wyraźnie wyższy wśród średniej wielkości firm (24%) niż u ich dużych konkurentów (13%).

Z drugiej strony 22% wszystkich biorących udział w badaniu organizacji wydzieliło już stanowisko inspektora ds. danych osobowych; nieco rzadziej postąpiono tak w mniejszych firmach (20%) niż wśród tych największych (23%). Przeciętnie 30% ankietowanych deklaruje zaawansowany etap przygotowań w kierunku powołania inspektora danych, natomiast kolejne 23% dopiero zaczyna prace związane z wydzieleniem takiej roli.

## Identyfikacja i zgłaszanie naruszeń

W przypadku naruszeń bezpieczeństwa danych nowe regulacje nakładają obowiązek poinformowania organów ochrony danych osobowych oraz – w pewnych przypadkach – osób, których danych dotyczyło. Na zgłoszenie naruszenia inspektor danych będzie miał 72 godziny od momentu jego stwierdzenia. Zanim się to jednak stanie, przedsiębiorstwa muszą mieć wdrożone mechanizmy pozwalające sprawnie identyfikować naruszenia danych osobowych, ocenić ich wpływ na bezpieczeństwo oraz zagrożenie praw i swobód osób, których dotyczą.

23% ankietowanych podmiotów jest w pełni przygotowanych do przeprowadzenia takich działań, kolejne 31% prowadzi zaawansowane prace nad wdrożeniem organizacyjnych i technologicznych zmian w tym obszarze. Prace te przebiegają szybciej w dużych instytucjach (36%) niż w mniejszych (22%), ale to średnie firmy próbują nadrabiać dystans; 44% przedstawicieli przedsiębiorstw tej wielkości deklaruje podjęcie prac nad wdrożeniem mechanizmów, które pozwolą skutecznie zarządzać incydentami związanymi z naruszeniem danych osobowych.

W wielu przypadkach procesy związane z identyfikacją naruszeń i oceną ich wpływu na bezpieczeństwo danych osobowych będą wspomagane komputerowo, tak aby ułatwić inspektorom danych podjęcie decyzji o konieczności poinformowania organu nadzoru albo uznaniu zarejestrowanego incydentu za nieistotny. W przypadku większych firm automatyzacja tego obszaru prawdopodobnie okaże się niezbędna z uwagi na konieczność analizy dużej liczby potencjalnych incydentów agregowanych z różnych źródeł. Jak widać po wynikach badania, polskie przedsiębiorstwa pracują nad tym i pozostałymi obszarami, aby w maju 2018 roku sprostać wymaganiom RODO.

## Ocena końcowa

Stopień przygotowania badanych organizacji do RODO należy ocenić jako umiarkowany. Na obecnym etapie prac można stwierdzić, że mniej więcej połowa przedsiębiorstw będzie w stanie zapewnić zgodność z wymaganiami RODO w maju 2018 roku, a więc wtedy, kiedy nowe przepisy o ochronie danych osobowych zaczną obowiązywać. Druga połowa firm może mieć wyraźny problem z wypełnieniem obowiązków RODO do tego czasu, bowiem pozostaje albo na wczesnym etapie przygotowań, albo nie wkłada dostatecznych wysiłków w dostosowanie procesów, procedur i narzędzi informatycznych do nowych uwarunkowań prawnych.

Być może problem ten wynika z braku świadomości osób decyzyjnych co do istotności obowiązków nakładanych na nich w ramach RODO oraz związanych z tym konsekwencji. Nowe regulacje ustawiły maksymalny poziom kar na bardzo wysokim poziomie: do 20 mln euro lub 4% całkowitego rocznego, światowego obrotu przedsiębiorcy w przypadku naruszenia przepisów o ochronie danych osobowych.

Z drugiej strony, brak krajowej ustawy o ochronie danych osobowych do Ogólnego rozporządzenia, brak wytycznych branżowych czy systemów certyfikacji sprawiają, że zarówno dostawcy systemów IT, integratory rozwiązań, jak i sami przedsiębiorcy biernie czekają na wykładnię prawa oraz obserwują zachowanie regulatora.

ARTUR PĘCZAK

# RODO zwiększy koszty, ale i zaufanie klientówi

**Według części analityków RODO to ewolucja, a nie rewolucja, z perspektywy przedsiębiorstw wejście w życie przepisów RODO będzie miało istotny wpływ na sposób zarządzania dostępem do danych, zarządzania firmową infrastrukturą IT oraz wykorzystania tych danych w procesach marketingowych i sprzedażowych.**

Nie ulega wątpliwości, że nowe przepisy o ochronie danych osobowych istotnie wpłyną na sferę biznesową, organizacyjną oraz technologiczną przedsiębiorstw działających w Polsce i całej Unii Europejskiej. Firmy mogą podejść do tego zagadnienia dwojako: traktując nowe regulacje jako zło konieczne, jakie prowadzi do zwiększenia kosztów i wydłużenia procesów związanych z zarządzaniem danych, albo jako szansę na zwiększenie zaufania klientów i osób, których dane są przetwarzane. O oczekiwany wpływ RODO na działalność firm oraz bilans zysków i strat, jakie przyniosą nowe regulacje, zapytaliśmy uczestników badania.

## Obszary zmian

Najwięcej – 63% ogółu ankietowanych – uważa, że nowe, wynikające z RODO regulacje będą miały największy wpływ na funkcjonowanie przedsiębiorstw w obszarze zarządzania dostępem do danych. Wynik ten jest niemal identyczny w odniesieniu do średnich organizacji oraz dużych przedsiębiorstw i korporacji. W związku z RODO przedsiębiorstwa staną przed koniecznością przedefiniowania zasad dostępu i przetwarzania danych osobowych.

W wielu przypadkach niezbędne okaże się wdrożenie mechanizmów proceduralnych i informatycznych, które pomogą zidentyfikować chronione prawem dane oraz zabezpieczyć je w sposób wymagany przez RODO. Zmiany dotkną też systemy informatyczne, które trzeba będzie dostosować do nowych wymagań prawnych m.in. w zakresie bezpowrotnego usuwania danych osobowych z baz danych, kopii zapasowych i archiwów. Na konieczność dostosowania systemów IT do nowych przepisów wskazuje niemal co drugi ankietowany (49%). Wejście w życie regulacji RODO będzie prowadziło do zmiany sposobu zarządzania infrastrukturą IT, którą wiele firm będzie musiało uzupełnić (poza wspomnianymi już mechanizmami kasowania danych) m.in. o rozwiązania klasyfikacji treści i obiegu dokumentów czy narzędzia automatyzujące procesy związane z identyfikacją i oceną naruszeń danych osobowych. Na te kwestie częściej zwracali uwagę przedstawiciele dużych przedsiębiorstw (51%) niż średniej wielkości organizacji (47%).

Trzecim najczęściej wskazywanym przez respondentów obszarem, na który RODO będzie miało największy wpływ w ramach ich organizacji, jest obsługa procesów marketingowych i sprzedażowych (38%). Nic dziwnego, bowiem analiza danych, ich profilowanie i przetwarzanie, a w końcu wykorzystywanie w celach dotarcia ze spersonalizowaną ofertą do klientów będą teraz obłożone dodatkowymi obowiązkami.W dalszej kolejności respondenci wskazywali obszary współpracy z partnerami i poddostawcami (31%), informacją zarządczą i zarządzaniem ryzykiem (22%) oraz funkcjonowaniem działów finansów, kontrolingu i HR (22%).

W trakcie analizy danych według rozmiaru przedsiębiorstw zauważyliśmy rzadko spotykaną zgodność między respondentami wywodzącymi się ze średnich i dużych firm; zbliżone wyniki ankiet pozwalają wysnuć wniosek, że dyrektorzy IT postrzegają kwestie wpływu RODO na działalność ich firm podobnie, niezależnie od wielkości organizacji. Jak wspomniano, duże firmy są bardziej skłonne do zmian w posiadanej infrastrukturze IT (51% w porównaniu do 47% wskazań wśród podmiotów średniej wielkości), podczas gdy średnie organizacje zauważalnie więcej uwa-

**Wskaż maksymalnie 3 obszary, na które wejście w życie przepisów RODO będzie miało największy wpływ w ramach Twojej organizacji.**

| Zarządzanie firmową infrastrukturą IT | Zarządzanie dostępem do danych | Marketing i procesy sprzedażowe | Współpraca z partnerami i poddostawcami | Informacja zarządcza i zarządzanie ryzykiem | Finanse, controlling, HR | Inne |
|---|---|---|---|---|---|---|
| 49% | 63% | 38% | 31% | 22% | 22% | 3% |

**Jaki będzie Twoim zdaniem najistotniejszy wpływ RODO na długofalowe funkcjonowanie Twojej organizacji i jej otoczenia biznesowego?**

| To okazja do wdrożenia zwiększenia efektywności zarządzania danymi | RODO ułatwi identyfikację naruszeń i ich źródeł | Wejście w życie RODO zwiększy zaufanie klientów do podmiotów przetwarzających ich dane | RODO zwiększy koszty i wydłuży procesy związane z zarządzaniem danymi | RODO ułatwi funkcjonowanie dużych, międzynarodowych firm kosztem mniejszych, lokalnych organizacji | RODO utrudni wymianę danych między organizacjami, a co za tym idzie - zaburzy związane z tym procesy biznesowe | Nie dostrzegam żadnych szczególnych korzyści ani zagrożeń | Inne |
|---|---|---|---|---|---|---|---|
| 14% | 18% | 21% | 42% | 6% | 13% | 19% | 2% |

gi przywiązują do kwestii zarządzania ryzykiem oraz przetwarzania danych osobowych w działach finansowych i kadrowo-płacowych. W obu tych obszarach liczba wskazań wyniosła 24%, podczas gdy wśród dużych podmiotów odsetek ten był niższy o 4 pkt proc.

## RODO a otoczenie biznesowe

Według 42% ankietowanych RODO zwiększy koszty i wydłuży procesy związane z zarządzaniem danymi; pogląd ten częściej wyrażali przedstawiciele średnich organizacji (47%) niż dużych przedsiębiorstw i korporacji (39%). Dostosowanie przedsiębiorstw do nowych regulacji o ochronie danych osobowych będzie wymagało poniesienia nakładów finansowych – zarówno bezpośrednich, związanych z potrzebą wdrożenia wymaganych rozwiązań IT czy wydzielenia stanowisk pracy, jak i pośrednich, rozłożonych w dłuższej perspektywie czasowej, a związanych z obsługą bardziej złożonych procedur zapewnienia zgodności z RODO.

Zostawmy na boku 19% ankietowanych, którzy z wejściem w życie regulacji RODO nie dostrzegają żadnych szczególnych korzyści ani zagrożeń. Poza kosztami respondenci zdają się bowiem dostrzegać pozytywne efekty proponowanych zmian. Jakie? Według co piątego (21%) wejście w życie RODO zwiększy zaufanie klientów do podmiotów przetwarzających ich dane. Co więcej, RODO ułatwi identyfikację naruszeń i ich źródeł (18% odpowiedzi) oraz pozwoli zwiększyć efektywność zarządzania danymi (13%). Zbliżone wyniki uzyskaliśmy dla firm różnych wielkości, przy czym średnie organizacje częściej zwracały uwagę na możliwość uzyskania dwóch pierwszych korzyści, natomiast duże firmy i korporacje poprzez implementację RODO upatrują szansy w optymalizacji sposobu zarządzania danymi (14%).

**Mariusz Olszewski,**
**Data Management Solution Manager**

42% respondentów uważa, że RODO zwiększy koszty i wydłuży procesy związane z zarządzaniem danymi. Jeśli można tu mówić o pewnej inwestycji w momencie wdrożenia, to myślę, że skatalogowana wiedza na temat danych i uporządkowane zarządzanie danymi w dłuższej perspektywie będą dla każdej organizacji masowo przetwarzającej dane osobowe opłacalne. Tylko Zaledwie 14% upatruje w RODO okazji do wdrożenia i zwiększenia efektywności zarządzania danymi – szkoda, że tylko tyle. Miejmy nadzieję, że po wdrożeniu rozwiązań pod kątem RODO firmy pójdą za ciosem i rozszerzą zarządzanie danymi także poza zakres wynikający z RODO – to przecież w danych są informacje i konkretna wartość, którą można wyłuskać przy pomocy sprawnych analityków. Dajmy im tylko szansę w postaci informacji, gdzie i jakie dane są przetwarzane oraz w jaki sposób uzyskać do nich dostęp.

Mimo że większa część spośród badanych dyrektorów IT potrafi oprócz kosztów dostrzec również korzyści z wdrożenia RODO, to pewna grupa (13%) uważa, że nowe przepisy prawa utrudnią wymianę danych między organizacjami, a co za tym idzie, zaburzą istniejące procesy biznesowe. Co ciekawe, częściej uważają tak przedstawiciele dużych firm (16%) niż średnich organizacji (9%). Niezależnie od nastawienia przedsiębiorcy faktycznie będą musieli zapewnić obywatelom wymagany rozporządzeniem, adekwatny poziom ochrony ich danych osobowych, np. w zakresie przekazywania danych marketingowych między spółkami. Z drugiej strony, RODO może pomóc uporządkować procesy związane z wymianą danych między podmiotami, m.in. w zakresie transferu danych osobowych do zagranicznego centrum usług wspólnych.

Dyrektorzy IT nie przeceniają wpływu RODO na zwiększenie stopnia konkurencji ze strony zagranicznych korporacji. Pogląd, że RODO ułatwi funkcjonowanie dużych, międzynarodowych firm kosztem mniejszych, lokalnych organizacji wyraziło raptem 6% ankietowanych. Być może nie jest to sprawa priorytetowa, ale z uwagi na fakt, że nowe regulacje dotyczyć będą przedsiębiorców działających na terenie Unii Europejskiej (z lokalnymi regulacjami określonymi w legislacji krajowej), śmiało można przyjąć, że wielu z nich odniesie zauważalne korzyści ze stosowania ujednoliconych unormowań prawnych w zakresie ochrony danych osobowych. Jak będzie, przekonamy się już niebawem.

# PRZYGOTOWANIA DO RODO W POLSKICH ORGANIZACJACH

**PARTNERZY BADANIA**



COMPUTERWORLD
FROM IDG