

Ujednolicone zarządzanie punktami końcowymi (unified endpoint management – UEM) jako podstawa zapewnienia zgodności z przepisami RODO

Od maja 2018 r. przedsiębiorstwa zobowiązane są stosować się do wymogów w zakresie ochrony danych osobowych określonych w nowym rozporządzeniu unijnym – RODO (ogólne rozporządzenie o ochronie danych). Gromadzenie, przekazywanie i przechowywanie danych osobowych w sposób zgodny z przepisami o ich ochronie stanowi dla przedsiębiorstw nie lada wyzwanie. Aby zapewnić zgodność z obowiązującymi przepisami należy ustanowić wewnętrzne procedury (np. wykazy procedur), dokonać ich oceny (np. analiza ryzyka), prowadzić odpowiednią dokumentację oraz przeprowadzać regularne aktualizacje. Konieczne jest opracowanie środków technicznych i organizacyjnych (TOM) oraz wdrożenie zasady RODO w infrastrukturę informatyczną przedsiębiorstw. W każdym przedsiębiorstwie kompleksowy system UEM stanowi istotny element zapewnienia zgodności z przepisami RODO. Jest to jednak bardzo złożony proces, wymagający uwzględnienia różnych czynników, takich jak technologie, polityka firmy oraz kwestie organizacyjne. Oprogramowanie baramundi Management Suite (bMS) to system UEM, który obejmuje wiele przypadków użycia związanych z zapewnianiem zgodności z RODO. Poniżej przedstawiono rozwiązania dla stacjonarnej i mobilnej infrastruktury przedsiębiorstwa oferowane przez bMS.

	Przepisy RODO	Przypadek użycia w przedsiębiorstwie	Rozwiązania oferowane przez bMS
Zgodność z RODO	Zgodność systemów operacyjnych	Komputery pracowników przedsiębiorstwa muszą być wyposażone w system Windows 10 . Przed aktualizacją osoby odpowiedzialne za obszar IT powinny jednak zdefiniować ustawienia, które spełniałyby wymogi dot. prywatności .	baramundi OS Install umożliwia instalację i konfigurację systemu Windows 10 . System może zostać skonfigurowany zgodnie z wymogami dotyczącymi prywatności właściwymi dla danego przedsiębiorstwa (np. z wyłączeniem Cortany, z pominięciem wysyłania statystyk dotyczących użytkownika) – pod warunkiem, że odpowiednie wersje systemu Windows takie rozwiązania oferują.
	Zgodność aplikacji mobilnych.	W przedsiębiorstwie obowiązuje surowa polityka prywatności, w związku z czym wszyscy pracownicy na swoich urządzeniach mobilnych mogą korzystać jedynie z aplikacji, które spełniają wymogi RODO .	Dzięki mobilnemu zarządzaniu aplikacjami, administratorzy ustalają, z jakich aplikacji mogą korzystać pracownicy przedsiębiorstwa. Jest to możliwe dzięki stworzeniu białej i czarnej listy aplikacji w systemie baramundi . Dzięki utworzeniu czarnej i białej listy aplikacji możliwa jest ochrona urządzenia przez potencjalnie niebezpiecznymi lub niepożądanymi aplikacjami, które np. wymagają zbyt szerokiego dostępu do danych.
	Zgodność ustawień właściwych dla poszczególnych aplikacji	Niektóre z aplikacji zainstalowanych na smartfonach pracowników wykorzystują ogromne ilości danych; powód ich gromadzenia bywa dyskusyjny. Jednak ze względu na wydane zgody lub przydatność danych osobowych przedsiębiorstwo nie może całkowicie zakazać ich użytkowania. W związku z powyższym, administrator zobowiązany jest skonfigurować takie aplikacje, aby były odpowiednio zabezpieczone i działały zgodnie z przepisami dotyczącymi ochrony danych osobowych.	Dzięki wcześniejszemu skonfigurowaniu aplikacji przedsiębiorstwo jest w stanie zapewnić, iż dane będą wykorzystywane zgodnie z przeznaczeniem. baramundi Mobile Devices umożliwia dystrybucję i konfigurację aplikacji (np. drogą szyfrowanej komunikacji HTTPS) poprzez wykorzystanie programów wbudowanych dostarczonych przez dostawców systemów operacyjnych ze standardowym mechanizmem AppConfig .
	Ochrona danych osobowych na urządzeniach mobilnych	Pracownicy wprowadzają dane osobowe również w swoich urządzeniach mobilnych (np. kontakty, dane dot. umówionych spotkań, prywatne notatki i e-maile). Takie dane muszą zostać oddzielone od innych danych przedsiębiorstwa.	Jedną z dostępnych opcji jest rozwiązanie kontenerowe . Dzięki baramundi Mobile Devices skonfigurowanie rozwiązania kontenerowego jest proste i intuicyjne. Kolejnym rozwiązaniem jest wykorzystanie wbudowanych opcji systemu Android i iOS w celu rozdzielania przechowywanych danych. Konfiguracja tych opcji możliwa jest poprzez bMS wersja 2019 R2.
Wymagania	Art. 32 paragraf 1a RODO: Szyfrowanie danych osobowych	Nieumyślne ujawnienie wrażliwych danych biznesowych, utrata lub kradzież urządzeń mobilnych takich jak laptopy, tablety i smartfony może skutkować milionowymi stratami dla przedsiębiorstwa. Osoby odpowiedzialne za obszar IT chcą zminimalizować takie ryzyko.	Dzięki ochronie plików i dysków od baramundi zasilanej DriveLock możliwe jest szyfrowanie dysków twardych, urządzeń mobilnych (np. kart pamięci), a nawet określonych plików zgodnie z certyfikowanymi procedurami. W rezultacie, wrażliwe informacje są odpowiednio chronione przed dostępem nieupoważnionych stron trzecich. BitLocker , czyli rozwiązanie ofertowane przez system operacyjny Windows umożliwiające szyfrowanie dysków jest również obsługiwane przez bMS.
	Art. 32, paragraf 1d RODO: Regularne testowanie skuteczności środków mających zapewnić bezpieczeństwo przetwarzania	Osoby odpowiedzialne za obszar IT w przedsiębiorstwie dążą do zabezpieczenia swojej własnej infrastruktury IT zgodnie z wymogami RODO, znalezienia luk w zabezpieczeniach, zminimalizowania ryzyka i ustalenia kolejności wdrażania środków mających zapewnić bezpieczeństwo przetwarzania.	baramundi Vulnerability Scanner umożliwia regularne testowanie skuteczności środków mających zapewnić bezpieczeństwo przetwarzania. Program regularnie skanuje infrastrukturę IT w celu wyszukiwania luk, uruchamia procesy mające na celu ich usunięcie (np. instalacja łatek lub aktualizacja oprogramowania przy pomocy baramundi Patch Management) i informuje, czy działania zostały przeprowadzone pomyślnie.

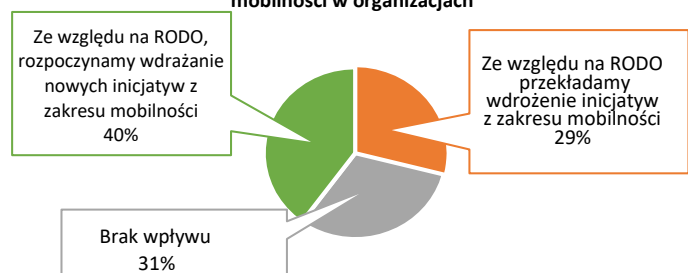
	Przepisy RODO	Wykorzystanie w przedsiębiorstwie	Rozwiązania oferowane przez bMS
Wymagania	Art. 15 RODO: Prawo dostępu przysługujące osobie, której dane dotyczą	Pracownik przedsiębiorstwa zwraca się do administratora z pytaniem, jakiego rodzaju dane osobowe, które go dotyczą, są przechowywane.	Administrator może przejrzeć i wyeksportować dane osobowe wykorzystywane przez bMS (np. Adres IP), jeżeli zachodzi taka potrzeba.
	Art. 25 RODO: Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych	Pracownik nie życzy sobie, aby dane dotyczące zużycia energii lub korzystania z aplikacji na jego komputerze były gromadzone.	Zbieranie danych dotyczących zużycia energii (baramundi Energy Management) lub korzystania z aplikacji (baramundi AUT) jest domyślnie wyłączone dla każdego klienta w bMS i może zostać włączone ręcznie, jeżeli zachodzi taka potrzeba.
	Art. 17 RODO: Prawo do usunięcia danych („prawo do bycia zapomnianym”)	Pracownik odchodzi z przedsiębiorstwa i życzy sobie, aby jego dane osobowe zostały usunięte .	W bMS, administrator ma możliwość wyświetlenia przechowywanych danych osobowych i usunięcia ich.
Ogólne	Art. 5 RODO: Prawidłowość	Wszelkie dane dotyczące infrastruktury muszą być aktualne , dzięki czemu administrator IT może podjąć właściwe kroki w celu zarządzania infrastrukturą.	Dzięki baramundi Inventory i baramundi Network Devices , możliwe jest przeprowadzenie inwentaryzacji całej infrastruktury i przedstawienie aktualnego stanu oprogramowania i sprzętu.
	Art. 5 RODO: Poufność i integralność	Aby usunąć błąd, konieczne może być anonimowe przesłanie baz danych klienta lub ich części do baramundi.	baramundi może przeprowadzić analizę błędów wykorzystując anonimowe dane. Za pomocą baramundi DBAnonymizer możliwe jest anonimizowanie baz danych klienta i wykorzystanie ich w celu przeprowadzenia analizy.
	Art. 5 RODO: Ograniczenia dla określonych celów	Osoby odpowiedzialne za obszar IT przedsiębiorstwa muszą zostać poinformowane, jakie dane osobowe przetwarza wykorzystywane przez nich oprogramowanie.	Ograniczenie celu wykorzystania gromadzonych danych jest na ogół określone w dokumentacji dołączonej do oprogramowania. Informacje na temat rodzaju danych osobowych przetwarzanych przez bMS oraz celu ich przetwarzania dostępne są w instrukcji obsługi dla każdego modułu.

Więcej informacji znaleźć można pod adresem: baramundi.com/RODO

RODO jako szansa

Wykorzystanie technologii mobilnych w przedsiębiorstwach jest nieuniknione. W wyniku wdrożenia RODO, większość przedsiębiorstw uważa za konieczne zastosowanie nowych rozwiązań z zakresu mobilności w celu zwiększenia bezpieczeństwa danych przedsiębiorstwa przechowywanych na urządzeniach mobilnych i zapewnienia zgodności z rozporządzeniem. Dodatkowo, RODO stanowi obowiązującą strukturę zabezpieczeń oraz gwarancję opartego na przepisach prawa systemu zapewniania bezpieczeństwa danych osobowych. Dla przedsiębiorców ustawa stanowi również motywację do inwestowania w zabezpieczenia.

Konsekwencje wdrożenia RODO dotyczące inicjatyw mobilności w organizacjach



zgodność z polityką prywatności bMS

„Od lat bMS działa zgodnie z wytycznymi niemieckiej ustawy o ochronie danych osobowych, tym samym przyczyniając się do zapewnienia ochrony danych osobowych naszych klientów
Wersja 2018 R1 bMS spełnia również wymogi RODO.”

Dr. Lars Lippert, Dyrektor Generalny baramundi software

Bez skutecznego rozwiązania UEM, przedsiębiorstwom trudno będzie zastosować się do wymogów dotyczących ochrony danych osobowych w zakresie technologii informatycznych stawianych przez RODO w odniesieniu do struktury IT firmy.