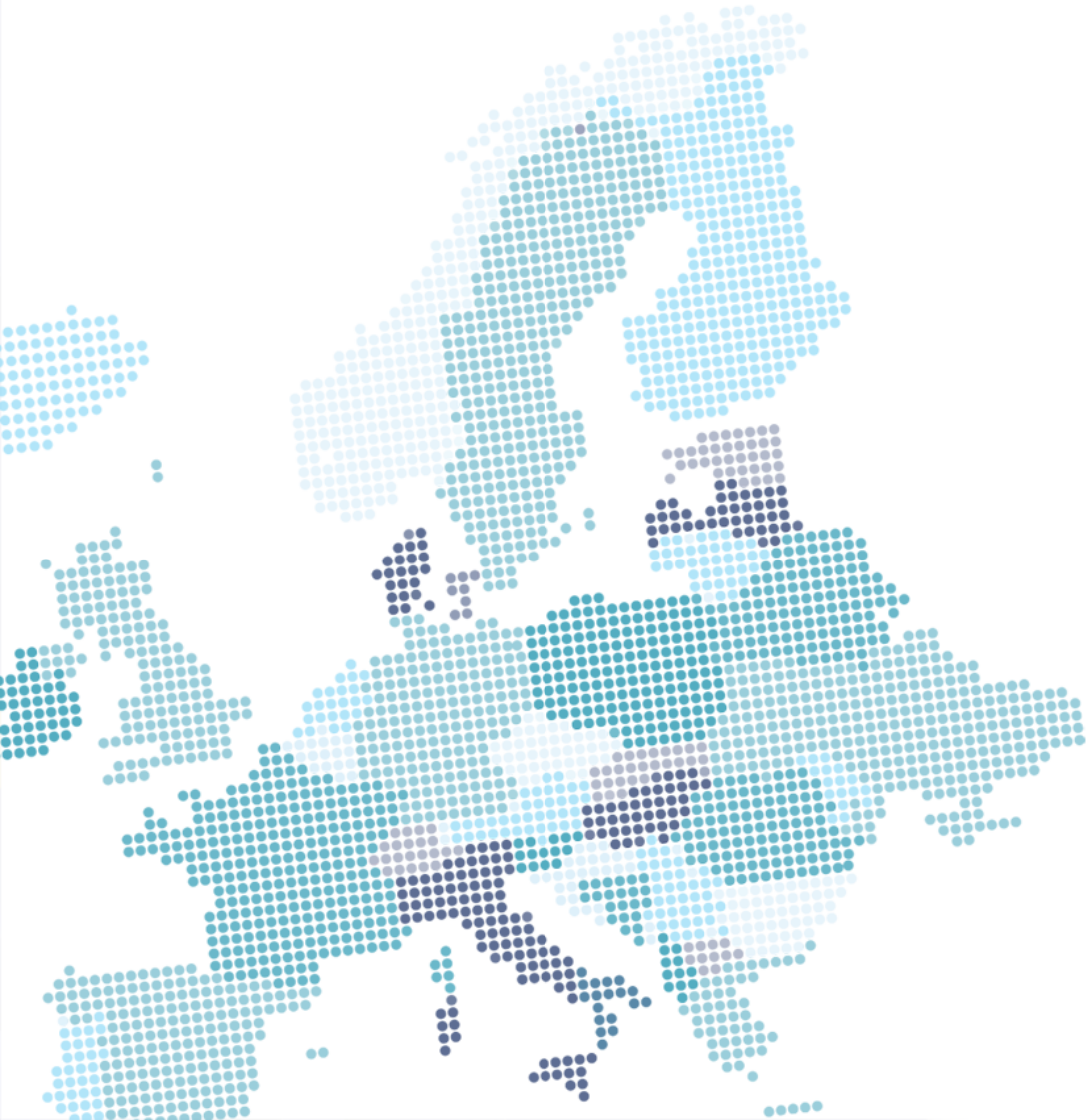
RODO
A SYSTEMY CRM

evolpe

Co to jest RODO?

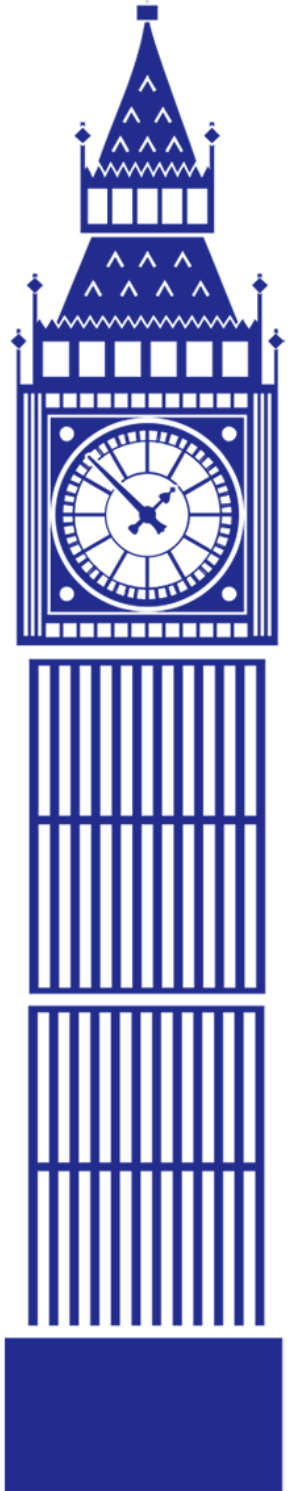
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.



Rozporządzenie o Ochronie Danych Osobowych (RODO) to akt prawny przyjęty jednogłośnie 27 kwietnia 2016 przez Parlament Europejski oraz Radę (UE) w celu ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych oraz swobodnego przepływu informacji personalnych. Przepisy wchodzą w życie **25 maja 2018 roku**. Dotyczą każdej jednostki, firmy, organizacji lub organu publicznego **posiadających siedzibę w Unii Europejskiej** i przetwarzających dane osobowe oraz każdej jednostki, firmy, organizacji lub **organu publicznego spoza Unii Europejskiej, jeżeli ich działania ukierunkowane są na osoby zamieszkałe w UE**.

Warto wiedzieć...

Rozporządzenie to, w ramach Unii Europejskiej, akt prawny o najszerszym zasięgu, który po wprowadzeniu w życie staje się obowiązujący dla wszystkich państw członkowskich równocześnie. W odróżnieniu od dyrektywy **rozporządzenie nie wymaga uchwalenia dodatkowych przepisów krajowych, jest wiążące i ma zastosowanie w sposób bezpośredni.**



Słownik RODO

Administrator danych osobowych oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który **samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych**. Jeśli osoba lub organizacja zainicjowała proces gromadzenia danych osobowych (bezpośrednio lub pośrednio), jest ich administratorem. Przykładem działalności administratora może być: prowadzenie strony internetowej, gromadzenie danych klientów do celów marketingowych, interakcja z klientami w sposób uporządkowany, czy dostarczanie plików do pobrania w zamian za rejestrację.

Dane osobowe oznaczają informacje o zidentyfikowanej osobie fizycznej lub osobie możliwej do zidentyfikowania.

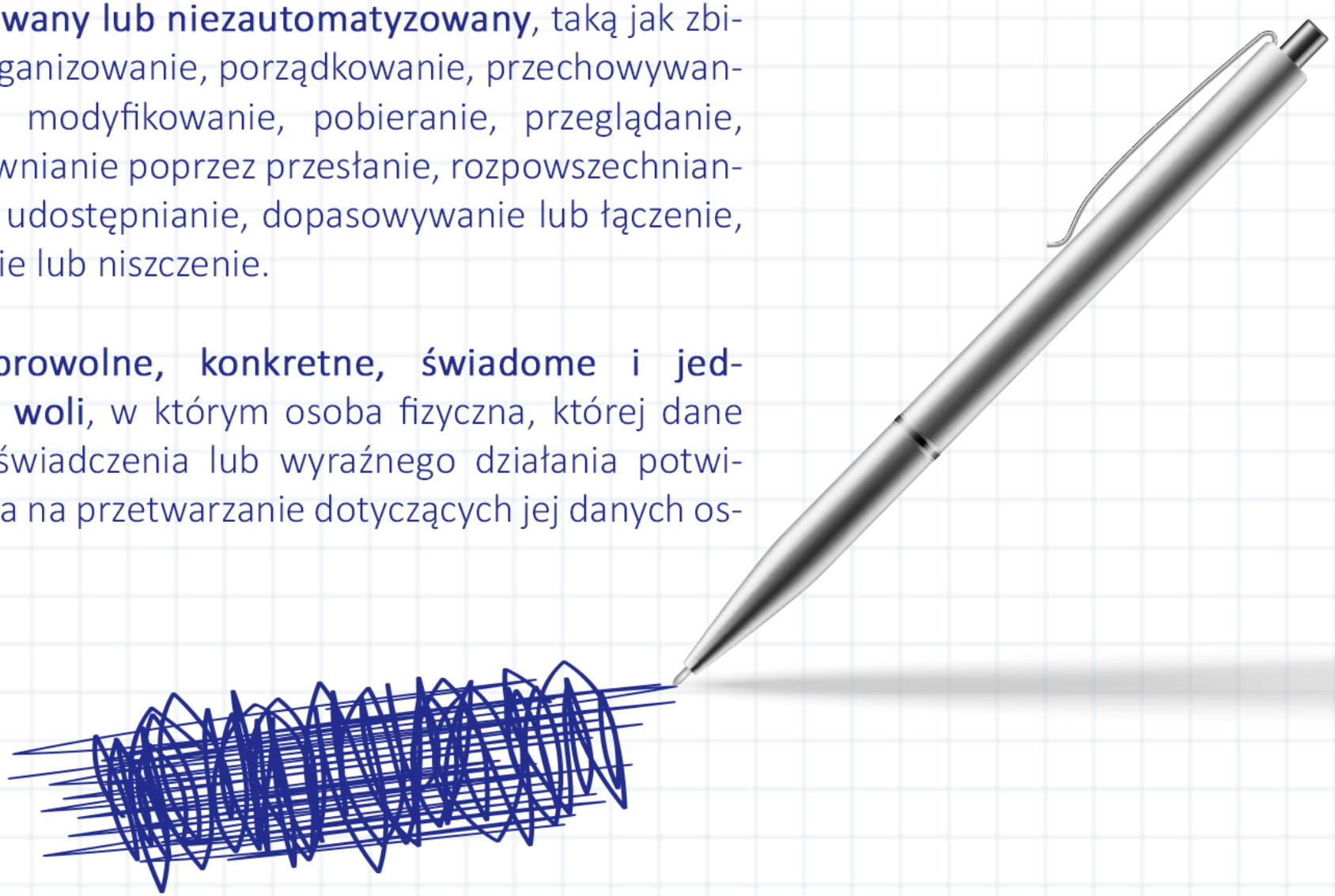
Podmiot przetwarzający dane oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe. Przykładem podmiotu przetwarzającego są: agencja badania rynku, agencja marketingowa, czy zewnętrzna firma obsługująca klienta w imieniu zleceniodawcy.

Profilowanie oznacza **dowolną formę zautomatyzowanego przetwarzania danych osobowych**, które **polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej**, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Słownik RODO

Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych, lub zestawach danych osobowych **w sposób zautomatyzowany lub niezautomatyzowany**, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Zgoda oznacza **dobrowolne, konkretne, świadome i jednoznaczne okazanie woli**, w którym osoba fizyczna, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.



Obowiązki
podmiotu przetwarzającego dane

Artykuł 6: Zgodność przetwarzania z prawem

- **jawność zbierania zgody** na przetwarzanie danych zgodnie z warunkami zdefiniowanymi w Artykule 7 rozporządzenia;
- przechowywanie informacji o zgodnym z prawem przetwarzaniu danych **ze względu na prawne lub kontraktowe zobowiązanie, lub uzasadnienie**. Na przykład w sytuacji, w której przetwarzanie jest niezbędne do wykonania umowy, której dana osoba jest stroną lub do wypełnienia obowiązku prawnego ciążącego na administratorze.

Artykuł 9: Przetwarzanie szczególnych kategorii danych

- oznaczanie danych osobowych specjalnej kategorii oraz zapewnienie restrykcyjnego do nich dostępu, a także ograniczonego ich wykorzystania.

Obowiązki
podmiotu przetwarzającego dane

Artykuł 12: Informowanie i przejrzysta komunikacja

- **zrozumiały format przedstawienia informacji** w przypadku konieczności ich udostępnienia na wniosek, osoby, której dane dotyczą.
- zbieranie informacji o tego typu wnioskach; zarówno o tym, że takowe zostały złożone, jak i o tym, czy i w jaki sposób je zrealizowano.

Artykuł 16: Prawo do sprostowania danych

- **obowiązek poprawy zawartości bazy zgodnie z wnioskiem o sprostowanie** złożonym przez osobę, której dane dotyczą oraz udostępnienia dowodu przeprowadzenia takiej czynności.
- informowanie osoby, której dane dotyczą o poprawieniu wiedzy zawartej w bazie na jej wniosek.

Obowiązki
podmiotu przetwarzającego dane

Artykuł 17: „prawo do bycia zapomnianym"

- **przypadek uzasadniony:** skasowanie wskazanych obszarów bazy danych oraz wygenerowanie powiadomienia o przeprowadzeniu tejże czynności;
- **przypadek nieuzasadniony:** wysłanie powiadomienia wraz z załączeniem listy obszarów, w których administrator nie dysponował wiedzą na temat wnioskującego.

Artykuł 18: Prawo do ograniczenia przetwarzania

- **umożliwienie czasowego usunięcia lub zablokowania wskazanego zakresu danych** na bezpośredni wniosek osoby, której dane dotyczą.

Artykuł 19: Obowiązek powiadomienia o usunięciu danych

- **informowanie o fakcie sprostowania lub usunięcia danych** każdego odbiorcy, któremu zostały one wcześniej udostępnione.
- informowanie osoby, której dane dotyczą (na wniosek) o istnieniu takich odbiorców.

Obowiązki
podmiotu przetwarzającego dane

Artykuł 20: Prawo do przenoszenia danych

- **udostępnianie danych w ustrukturyzowanym, powszechnie używanym formacie** nadającym się do odczytu maszynowego i przekazania innemu podmiotowi, na wniosek osoby, której dane dotyczą.

Artykuł 21: Prawo do sprzeciwu wobec profilowania

- **umożliwienie wyłączenia automatyzacji profilowania danych** (np. następny najlepszy produkt, następna najlepsza oferta, ocena ryzyka, potencjalny zakup itp.), w sytuacji gdy osoba, której dane dotyczą, nie wyraża zgody na profilowanie.

Obowiązki
podmiotu przetwarzającego dane

Artykuł 25: Domyślna ochrona danych

- **identyfikacja i oznaczanie**, jakie dane są przechowywane;
- **ustalenie warunków dostępu do informacji** przez konkretne grupy lub poszczególnych pracowników, a także kryteriów przesyłu wiedzy do innych baz;
- **reguła ujawniania minimalnej ilości danych personalnych koniecznych do wykonania określonego zadania**.

Artykuł 34: Zawiadamianie o naruszeniu ochrony danych

- w przypadku wycieku informacji, gdy ryzyko naruszenia praw i wolności osoby, której dane dotyczą, jest wysokie, bezzwłoczne przekazanie informacji o tym zdarzeniu.

Kary za nieprzestrzeganie RODO

Kary za nieprzestrzeganie RODO to jeden z najchętniej komentowanych aspektów nowej rzeczywistości prawnej w UE. Liczne publikacje, które zalały rynek po uchwaleniu rozporządzenia, dotyczą przede wszystkim horrendalnych sankcji finansowych w wysokości **4% rocznego światowego obrotu firmy lub 20 milionów EUR**. Jest to faktycznie najwyższy wymiar administracyjnej kary pieniężnej, który przewidziano w rozporządzeniu. Czytając dokument, znajdujemy jednak długą listę okoliczności łagodzących, jakie należy uwzględnić, nim jakakolwiek kara zostanie wymierzona (por. Artykuł 83 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016).

Jeżeli nałożenie kary administracyjnej okaże się zasadne, **jej wysokość ustalana jest adekwatnie do argumentów obciążających podmiot przetwarzający dane**. Dobra informacja jest taka, że pod uwagę brane są również wszelkie zaistniałe czynniki łagodzące. **Sankcja jest zasadna jeżeli przepisy łamane są długotrwale, bezsprzecznie, a podmiot przetwarzający dane działa z premedytacją i na szkodę osoby, której dane dotyczą.** Przewidziane przez RODO kary muszą być bez wyjątku proporcjonalne, skuteczne i odstraszające, nigdy zaś wymierzone bezpośrednio, bez wcześniejszej analizy konkretnego przypadku.

Artykuł 83

1. Każdy organ nadzorczy zapewnia, by (...) administracyjne kary pieniężne (...) były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające.

2. Administracyjne kary pieniężne nakłada się zależnie od okoliczności każdego indywidualnego przypadku (...). Decydując, czy nałożyć administracyjną karę pieniężną,

oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:

a) charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób,

których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;

b) umyślny lub nieumyślny charakter naruszenia;

c) działania podjęte (...) w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;

d) stopień odpowiedzialności (...) z uwzględnieniem środków technicznych i organizacyjnych;

e) wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;

f) stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;

g) kategorie danych osobowych, których dotyczyło naruszenie;

h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;

i) jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane

w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków;

j) stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42; oraz

k) wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio

lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

(...)

RODO - rewolucja w UE?

W wielu miejscach, zwłaszcza w Internecie można przeczytać, że RODO wprowadza prawdziwą rewolucję w ochronie danych osobowych i, że przedsiębiorcy powinni zapomnieć o wszystkim, co do tej pory obowiązywało w tym zakresie. Rozporządzenie istotnie nakłada obowiązki na administratorów danych oraz zwiększa ich odpowiedzialność za ochronę informacji. **Zmiany dotyczą jednak przede wszystkim dokumentacji, wewnętrznych procedur, sposobu zabezpieczenia danych (adekwatnie do ryzyka) oraz zakresu odpowiedzialności administratora i podmiotu przetwarzającego.** Ogólne zasady przetwarzania danych osobowych, takie jak zgodność z prawem, adekwatność, integralność, poufność, czy ograniczenie zakresu zbieranych danych celem przetwarzania, były znane i wykorzystywane dużo wcześniej.

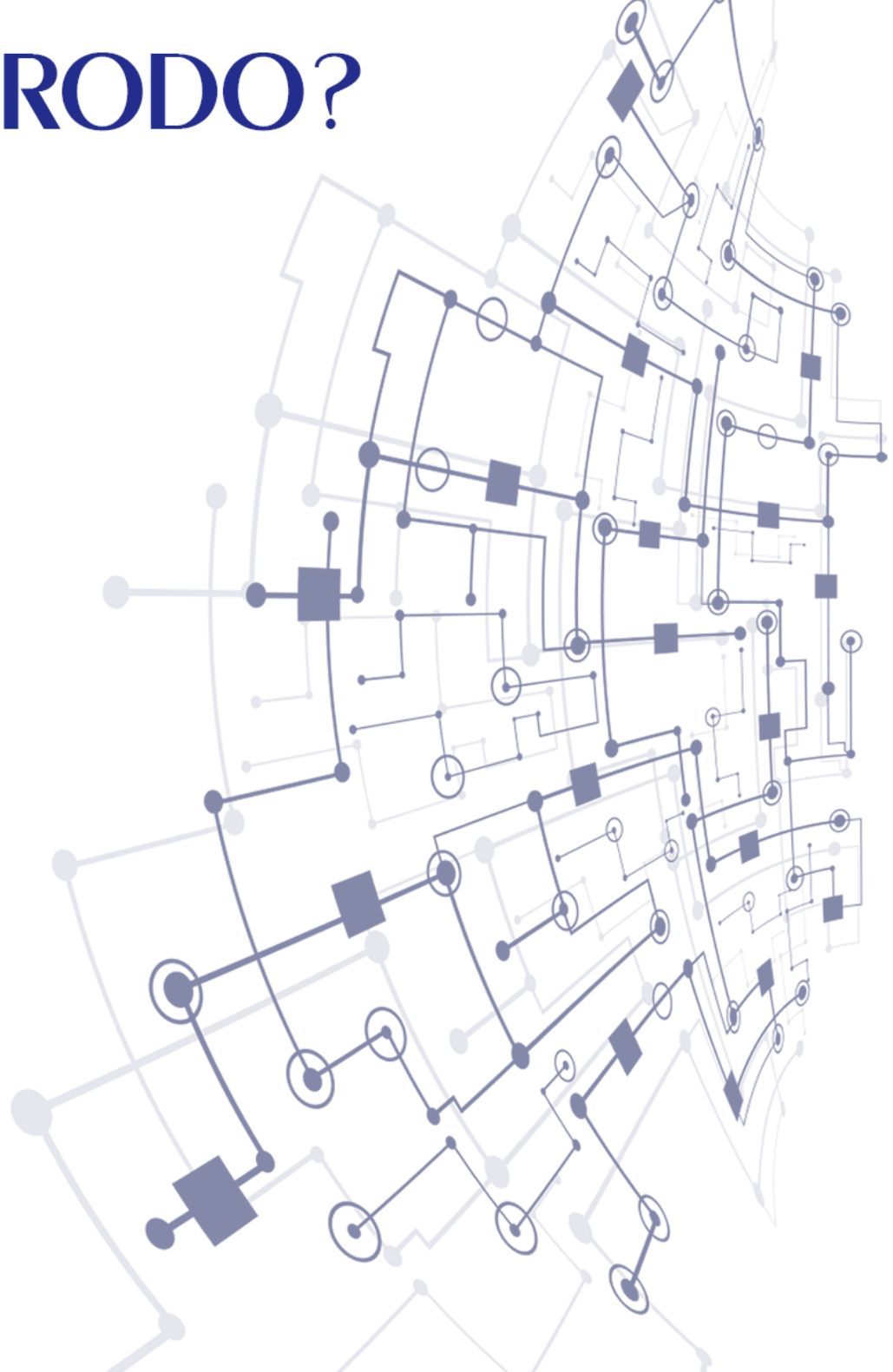
Decydenci UE uchwalając przepisy RODO jednogłośnie, dali wyraz idei rozszerzenia praw obywatelskich w wirtualnym świecie. Punktem wyjścia w pracach nad rozporządzeniem był przy tym inny unijny akt prawny – **Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995** w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Zadbano zatem o ciągłość ustawodawczą i płynne wprowadzenie udoskonalonych zapisów. Z tego względu była to raczej ewolucja niż rewolucja.

> **rewolucja** «proces gwałtownych zmian w jakiejś dziedzinie»
>
> **ewolucja** «proces przeobrażeń, przechodzenia do stanów bardziej złożonych»

System IT zgodny z RODO?

Zgodnie z treścią RODO, producent, dostawca oprogramowania, czy sam system, jakkolwiek rozbudowany by nie był, nie ponoszą odpowiedzialności za dopełnienie norm określonych w rozporządzeniu. Te kwestie pozostają w gestii administratora oraz podmiotu przetwarzającego dane osobowe, tj. organizacji, która się nimi posługuje. **System IT może być narzędziem do osiągnięcia zgodności z RODO, ale sam w sobie nie jest jej definicją.**

> *Wdrożenie RODO w rozumieniu pozyskania nowego oprogramowania mija się z celem i jest niewystarczające.*



W kontekście nowych przepisów należy postępować dwutorowo, tzn. zapewnić synergię podejścia prawnego oraz koncepcji organizacyjnej (w tym systemu IT, ale nie tylko). Konieczne są: analiza wewnętrznych procedur, dostosowanie obowiązujących procesów do nowych przepisów (oba etapy najlepiej we współpracy z kancelarią prawną), a dopiero na końcu – przełożenie otrzymanych wniosków na system informatyczny.

Oprogramowanie IT dla uzyskania zgodności procesu biznesowego z RODO

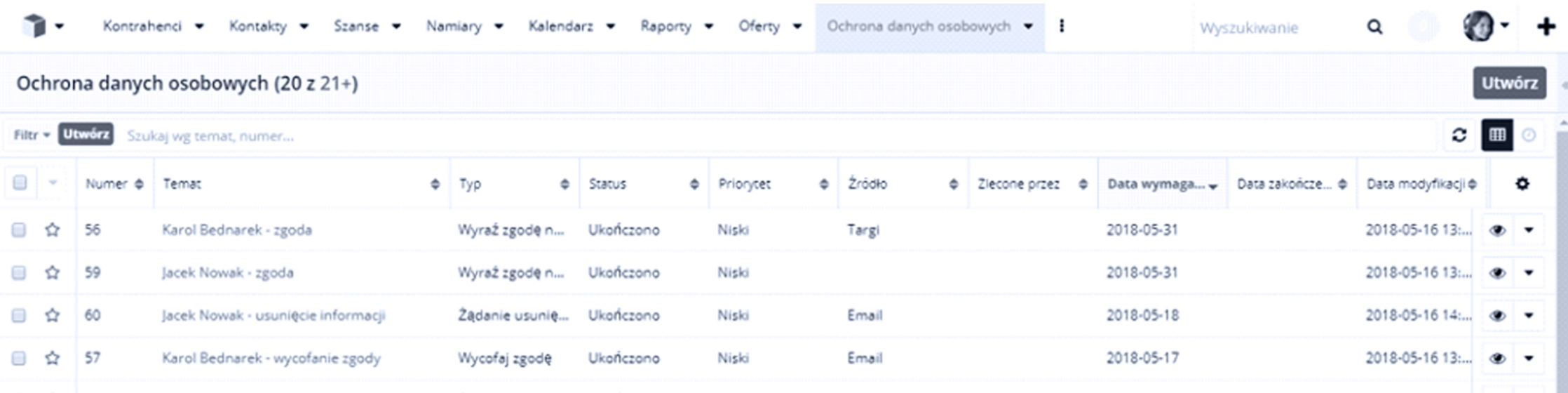
Z RODO zgodny musi być każdy proces biznesowy, w którym przetwarzane są dane osobowe. Nie istnieje system IT w swej naturze zgodny z RODO. Można go natomiast przystosować, by służył firmie jako narzędzie do osiągania tego nadrzędnego celu.

Na tym polega przewaga oprogramowania Open Source, gdyż takowe można dowolnie kastomizować.

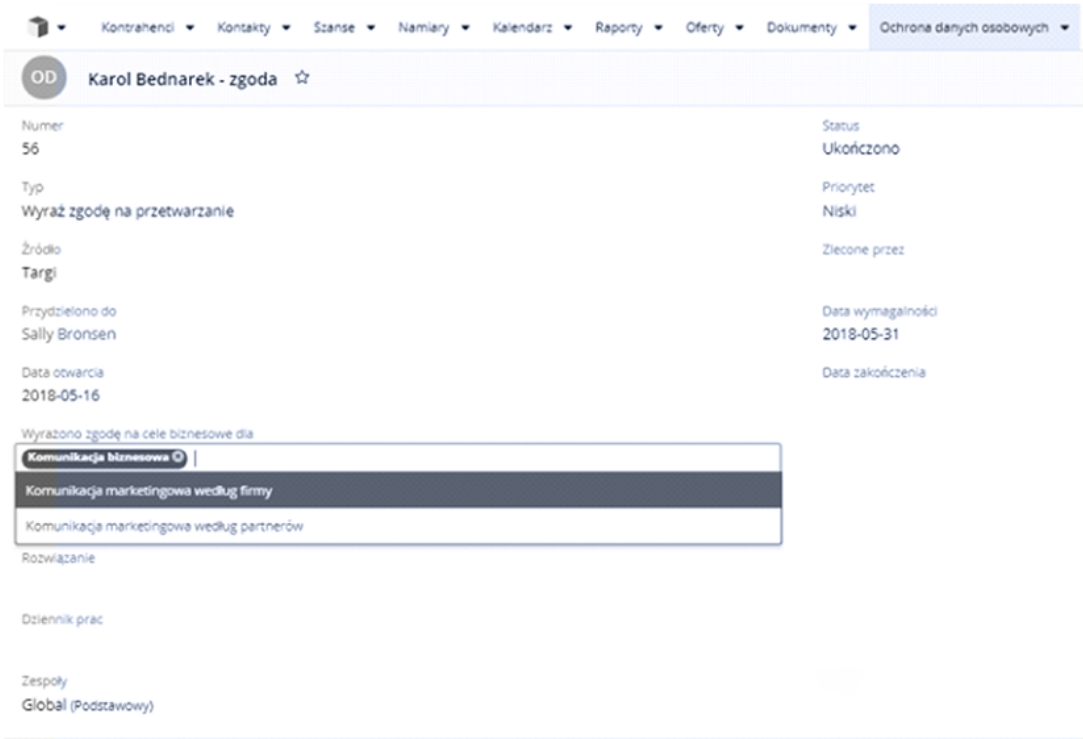
Klientom eVolpe proponujemy dwie alternatywy. Rozwiązanie komercyjne – **Sugar** oraz pozbawione opłat licencyjnych – **SuiteCRM**. Aplikacja firmy SugarCRM nadaje się raczej dla dużych korporacji o bardzo rozbudowanych wymaganiach. Sugar to jeden z liderów na rynku, stawiany w tym samym szeregu co Salesforce i Microsoft Dynamics CRM. SuiteCRM oferujemy natomiast tym firmom, które na rzecz oszczędności na licencjach są w stanie poświęcić pewne udogodnienia z zakresu User

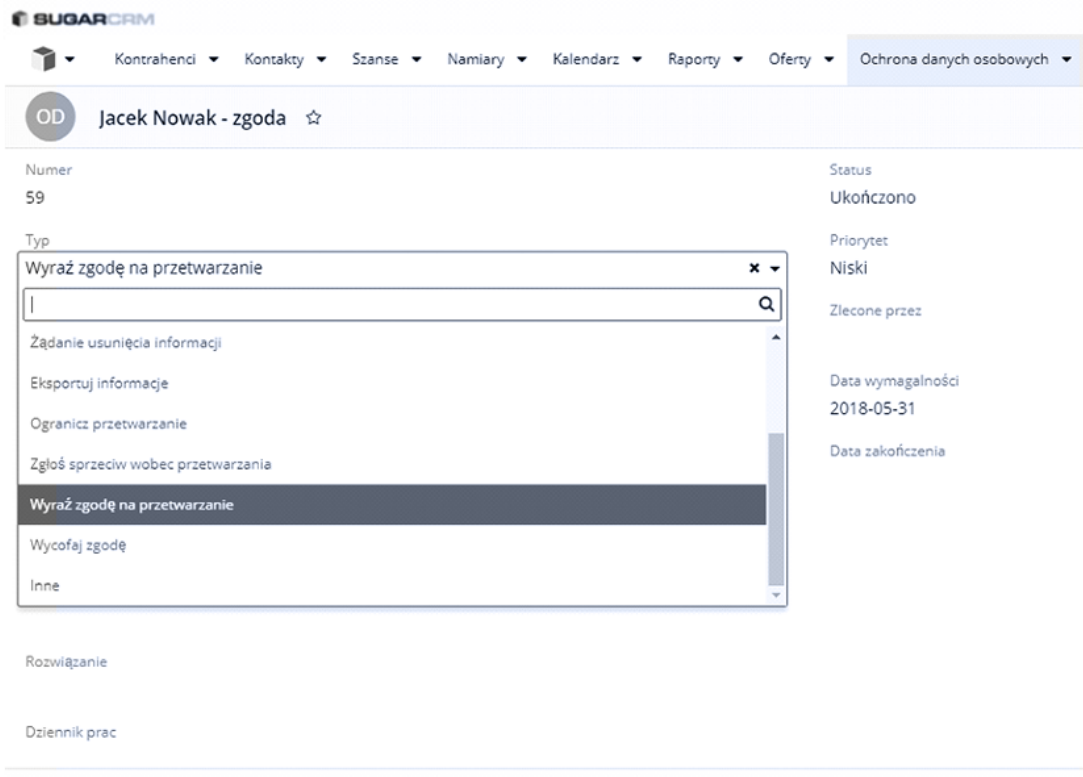
Sugar 8.0 a RODO

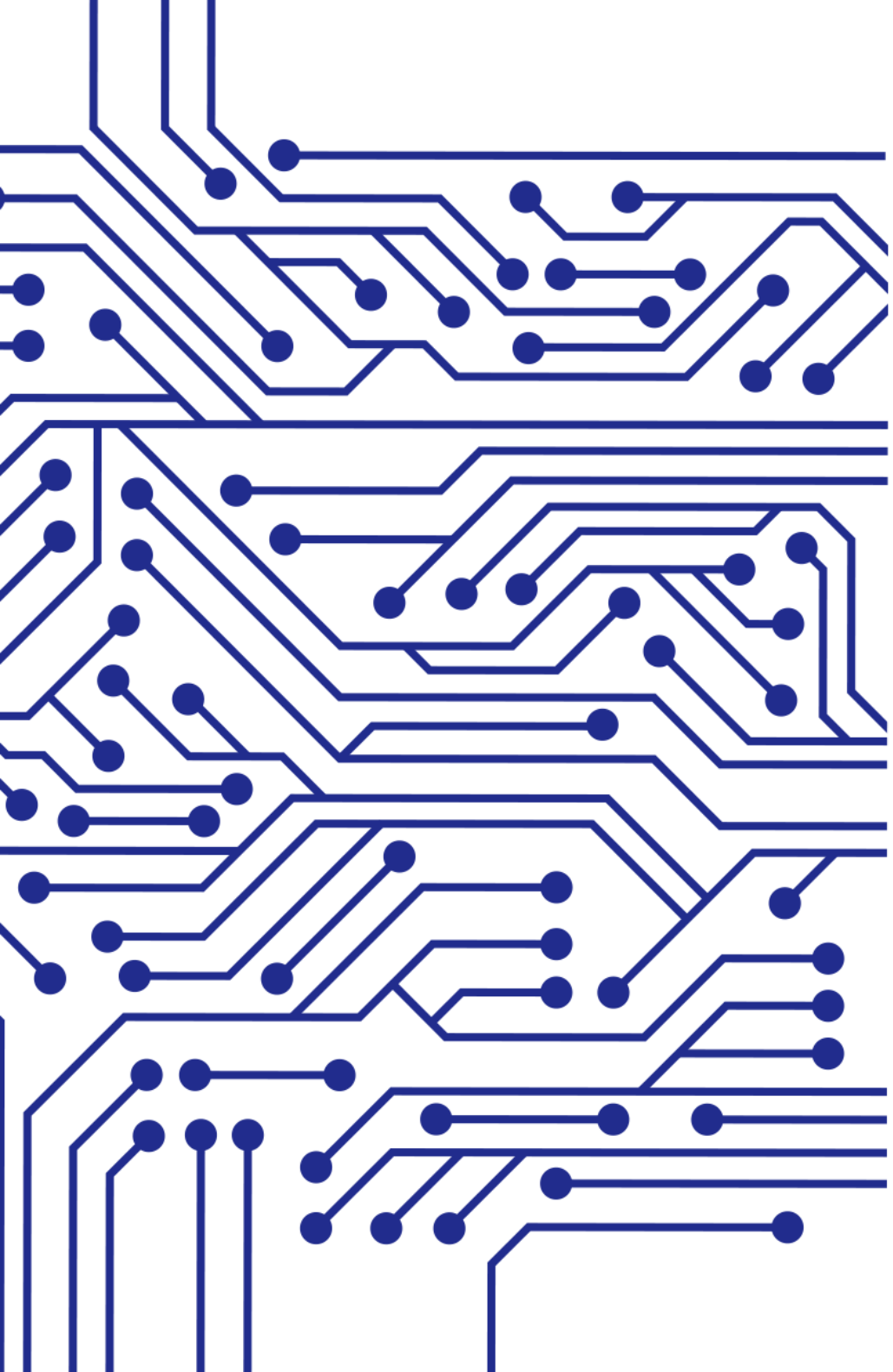
SugarCRM wydał właśnie najnowszą edycję swojego produktu: Sugar 8.0 (on-premise) tudzież Sugar Spring'18 (chmura producenta). Oba warianty są komplementarne i oferują użytkownikom ten sam pakiet funkcjonalności. Z pewnością najbardziej zauważalnym usprawnieniem jest całkowicie odświeżony interfejs systemu. Nie na tym jednak chcemy się teraz skupić. SugarCRM rozbudował bowiem architekturę swojego produktu o **dodatkowy moduł o nazwie Ochrona danych osobowych!** Jest to zdecydowanie największa zmiana w systemie w kontekście przepisów RODO.



Od 25 maja 2018 każdy z podmiotów przetwarzających i/lub administrujących danymi osobowymi na dużą skalę, zobowiązany jest wyznaczyć inspektora danych osobowych. Wspomniany obszar systemu Sugar ma za zadanie usprawniać pracę takiej osoby. Z założenia widoczny jest tylko dla osób, którym przypisano rolę **Manager Danych Osobowych**. Użytkownicy o uprawnieniach z zakresu administrowania danymi osobowymi, posiadają szeroki dostęp do rekordów tworzących moduł. Sam **obszar skonstruowano w formie powiązanej relacją z Odbiorcami, Namiarami, Kontaktami i Kontrahentami listy**. Dzięki oprogramowaniu Sugar 8.0 możliwe jest zatem uporządkowanie procesu przechowywania informacji o zgodach, ograniczeniach, sprzeciwach, sprostowaniach i innych procesach związanych z obsługą wiedzy na temat Twoich klientów, partnerów i pracowników.







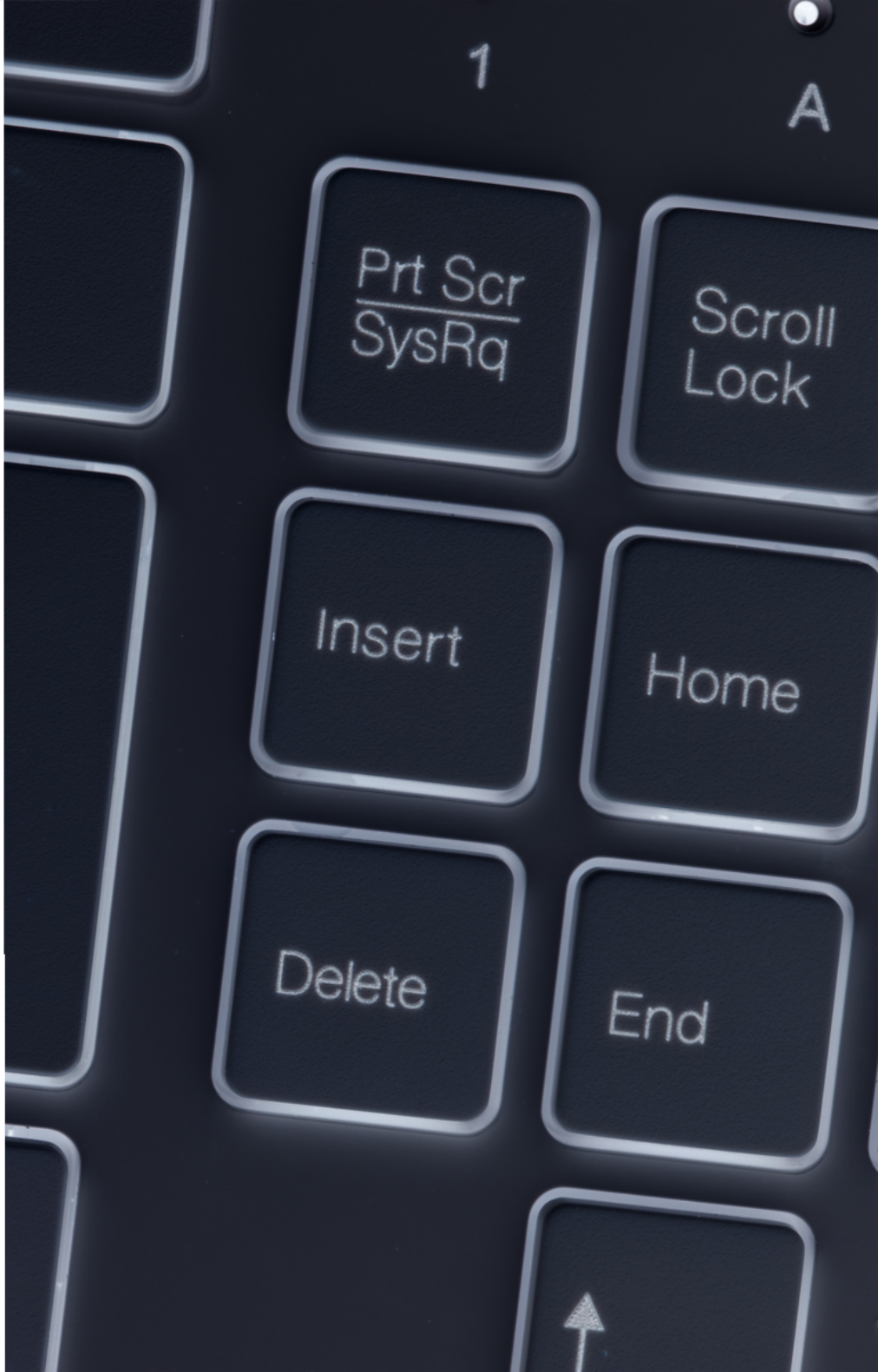
Każda z poszczególnych pozycji w module Ochrona Danych Osobowych jest klikalna i zawiera szeroki kontekst przetwarzanych przez firmę danych osobowych. Z poziomu tego widoku można administrować informacjami takimi jak: **status, typ, priorytet, źródło, przeznaczenie, czy data wyrażenia i data wygaśnięcia zgody**.

W dalszej części uwidocznione są pozostałe obszary systemu pozostające w relacji z rekordem w ramach modułu **Ochrona Danych Osobowych**. W ten sposób wyróżnione są wszystkie przechowywane, powiązane z konkretną osobą informacje. Usprawnia to miedzy innymi procedurę reagowania na wniosek o udostępnienie wiedzy na temat przetwarzanych przez firmę danych.

Użytkownik posiadający właściwe uprawnienia w systemie Sugar, może również usuwać informacje na wniosek osoby, której one dotyczą. Po wybraniu opcji „**Zaznacz do usunięcia**” pojawia się lista przechowywanych danych osobowych.

Zaledwie kilka klików wystarczy, aby na trwałe usunąć odpowiednie dane. Po wykonaniu tej czynności w miejscu, w którym wcześniej znajdowała się niepożądana informacja, system wyświetla baner „**Wartość usunięta**”.

Dzięki opisanej funkcji w prosty sposób wywiążesz się ze zobowiązania nałożonego przez RODO, tj. usunięcia danych na wniosek osoby, której one dotyczą. Jednocześnie zachowasz ślad po tym, że do pewnego czasu Twoja firma była w posiadaniu rzeczonej informacji.



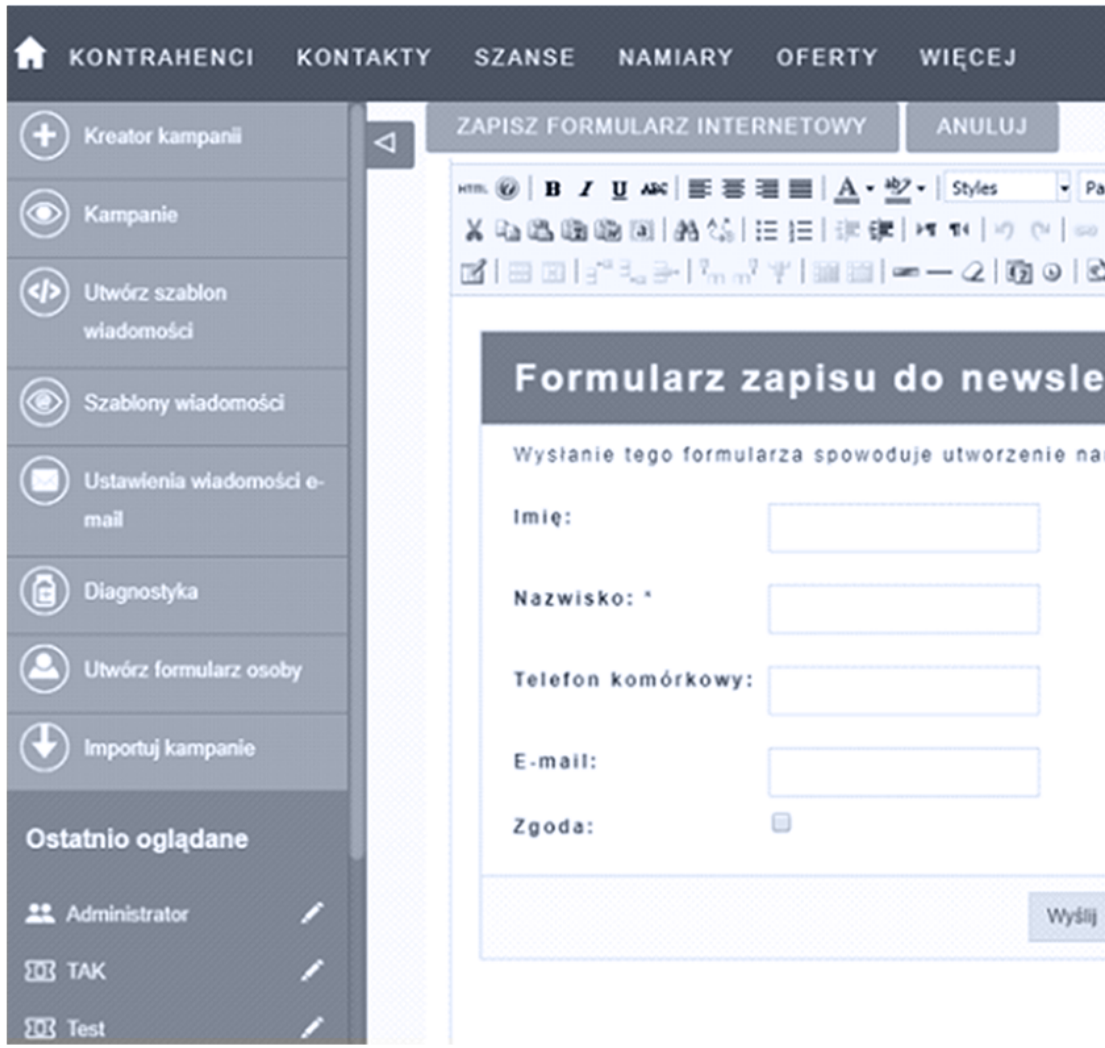
Kampanie E-mail w Sugar 8 a RODO

Ważny element systemu, w kontekście zapewnienia zgodności procesów biznesowych z przepisami RODO, stanowi **mechanizm opt-in oraz opt-out** dla kampanii marketingowych. Korzystając z oprogramowania Sugar 8 istnieje możliwość takiego przygotowania formularzy web-to-lead, aby zapewnić zgodną z RODO procedurę zapisu do i wypisu z newslettera. W praktyce polega to na dołączeniu do pola „adres e-mail" odpowiedniego check-boxu.

W ten sposób w dość wygodny sposób odróżnisz adresy E-mail, na które możesz kierować przekaz reklamowy od tych, które powinny być wykorzystywane wyłącznie w celach komunikacji biznesowej, zgodnie z podstawową treścią zgody na przetwarzanie danych osobowych.

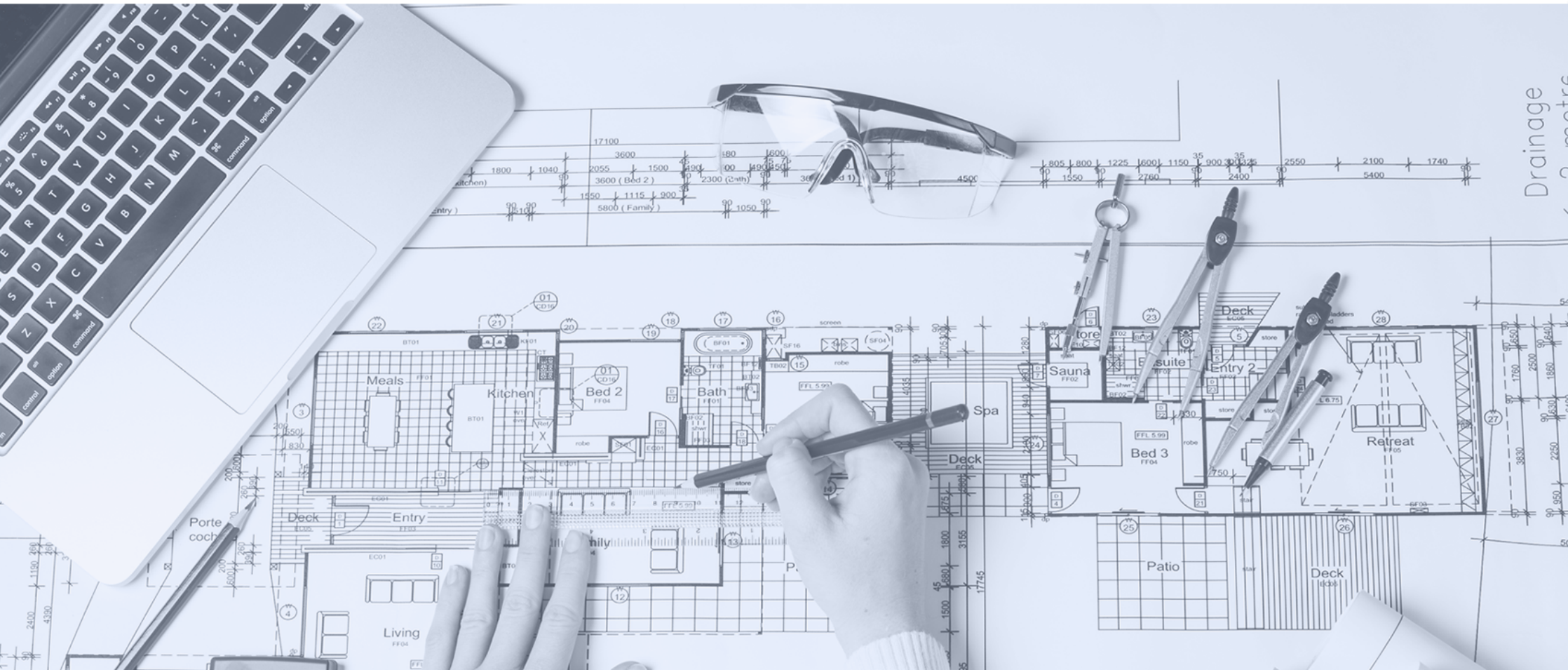
SuiteCRM a RODO

Producent SuiteCRM w dostosowaniu systemu do przepisów RODO skupił się przede wszystkim na elemencie kampanii mailingowych. Podobnie jak w przypadku Sugar 8.0, do aktualnej wersji oprogramowania SuiteCRM, dodano mechanizm **potwierdzonego opt-in (double opt-in)**. Po wypełnieniu formularza web-to-lead (przygotowanego w SuiteCRM), na wskazany adres E-mail trafia automatycznie generowana wiadomość z linkiem do potwierdzenia intencji zapisu. Jeżeli osoba, która wypełniła formularz, nie potwierdzi w ten sposób zgody na wykorzystanie maila, żadne treści nie będą mogły być na niego kierowane. Jest to zabezpieczenie, które blokuje możliwość podania cudzego maila do komunikacji marketingowej. Tylko osoba, która ma dostęp do skrzynki pocztowej może zwrotnie potwierdzić wyrażenie zgody.



Uwaga! na Open Source!

Ponieważ Sugar i SuiteCRM pozostają systemami o otwartym kodzie, we współpracy eVolpe dokonasz w nich dowolnych przeobrażeń. Zaproponowany przez SugarCRM Inc. moduł Ochrona Danych Osobowych, możemy opatrzyć dodatkowymi automatyzacjami (przy pomocy narzędzia Process Author lub dzięki pracom deweloperskim). Podobnie funkcjonalnośc SuiteCRM skrywa spory potencjał. Nie zwlekaj! Skontaktuj się z nami już TERAZ!




Zapytać eVolpe o system CRM,
który pomoże osiągnąć
zgodność procesów
biznesowych z RODO!
Kupić mleko.

eVolpe Consulting Group
Winogrady Business Center
Aleje Solidarności 46
61-696 Poznań
Tel.: +48 518 105 108

www.evolpe.pl
biuro@evolpe.pl