PRZYGOTUJ FIRMĘ NA RODO

Rozporządzenie Ogólne o Ochronie Danych Osobowych

SPIS TREŚCI

RODO
– PODSTAWOWE INFORMACJE

Definicja

RODO", zwane także „GDPR" lub „Ogólnym Rozporządzeniem o Ochronie Danych", to 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 zacznie obowiązywać bezpośrednio w krajowych porządkach prawnych od 25 maja 2018 r. Niniejsze Rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą przebywających w Unii przez Administratora lub podmiot przetwarzający , jeżeli czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom, których dane dotyczą lub monitorowaniem ich zachowań.

RODO wprowadza zmiany w zakresie ochrony danych osobowych, ale nie określa ścisłych reguł jakie mają zostać spełnione w konkretnej firmie.

To od każdej firmy, specyfiki jej działania oraz organizacji pracy, zakresu i specyfiki przetwarzanych danych osobowych zależeć będą wdrożone mechanizmy, procedury, wymagane dokumenty itp. mające na celu zapewnienie właściwej ochrony danych osobowych.

W przepisach **RODO** sformułowanych zostało **siedem zasad przetwarzania danych** osobowych.

Są nimi:

1. **ZASADA ZGODNOŚCI Z PRAWEM, RZETELNOŚCI I PRZEJRZYSTOŚCI** – ART.5 UST.1

   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość")

2. **ZASADA OGRANICZENIA CELU PRZETWARZANIA DANYCH,** – ART.5 UST.1

   b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; („ograniczenie celu")

3. **ZASADA MINIMALIZACJI DANYCH** ART.5 UST.1

   c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych")

4. **ZASADA PRAWIDŁOWOŚCI DANYCH** ART.5 UST.1

   d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość")

5. **ZASADA OGRANICZENIA PRZECHOWANIA DANYCH** ART.5 UST.

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania")

6. **ZASADA INTEGRALNOŚCI I POUFNOŚCI DANYCH** ART. 5 UST.1

f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność")

7. **ZASADA ROZLICZALNOŚCI** oznacza, że administrator musi być w stanie wykazać, że podejmowane przez niego działania są zgodne z w/w zasadami

WAŻNE POJĘCIA

Dane osobowe

- wg art. 4 ust. 1 RODO – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej
- wg art. 4 ust. 1 – możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak:
  - imię i nazwisko
  - numer identyfikacyjny
  - dane o lokalizacji
  - identyfikator internetowy
  - jeden bądź kilka szczególnych czynników określających: fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej
  - dane osobowe dzielą się na zwykłe oraz „zaliczające się do szczególnej kategorii danych" (dawniej nazywało się je „danymi wrażliwymi"), czyli np. te dotyczące pochodzenia, religii, światopoglądu, zdrowia, seksualności itp.

DLA LEPSZEGO ZROZUMIENIA DEFINICJI DANYCH OSOBOWYCH, ZERKNIJMY DO DOKUMENTU ŹRÓDŁOWEGO I ZACYTUJMY TREŚĆ RODO:

- **motyw 26 preambuły** – „Aby stwierdzić, czy dana osoba jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób identyfikacji może być z uzasadnionym prawdopodobieństwem wykorzystany do identyfikacji danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebny do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny"
- **motyw 30 preambuły** – „osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawieniem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i identyfikowania tych osób"

- Zbiór danych (art. 4 pkt. 6) oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie

- Przetwarzanie (art. 4 pkt. 2) – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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

- Administrator (art.4 pkt.7) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania

- Podmiot przetwarzający (art.4 pkt.8) – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora

- Zgoda osoby, której dane dotyczą (art.4 pkt.11) – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych

- Naruszenie ochrony danych osobowych (art.4 pkt.12) – oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

AUDYT RODO

Do wejścia w życie rozporządzenia zostało jeszcze nieco czasu – wykorzystaj go, by sprawdzić, czy środki bezpieczeństwa i procedury dotyczące ochrony danych osobowych stosowane w Twojej firmie nie narażą Cię na przykre konsekwencje. Najlepiej będzie, jeśli **krok po kroku** przeanalizujesz, jak dotychczas wyglądały przetwarzanie i ochrona danych osobowych w Twojej organizacji – spróbuj to zrobić wg następującego porządku:

Zbadaj jakie dane osobowe są przetwarzane w firmie – i czy robisz to legalnie. Upewnij się, że masz zgodę na przetwarzanie danych od osób, których te dane dotyczą – i że przetwarzanie jest niezbędne, np. do wykonania umowy czy wypełnienia obowiązków prawnych.

Zweryfikuj zakres i cel przetwarzania danych, a także ich merytoryczną poprawność. Sprawdź, czy pasują do celu, w jakim je przetwarzasz – np. czy nie przetwarzasz danych takich jak adres zamieszkania w sytuacji, gdy do realizacji celu potrzebny jest Ci tylko adres e-mail.

Zweryfikuj system techniczno-organizacyjny ochrony danych osobowych. Przeanalizuj fizyczne i logiczne zabezpieczenia infrastruktury informatycznej.

Sprawdź czy Twoja dokumentacja ochrony danych osobowych jest aktualna i zgodna z RODO.

Przeanalizuj polityki bezpieczeństwa, backupu i zarządzania uprawnieniami oraz określ ich wpływ na poziom zabezpieczenia zbiorów danych przetwarzanych w formie elektronicznej.

Zweryfikuj funkcjonalności aplikacji i poziom ich zabezpieczeń, a w przypadku wykrycia nieprawidłowości – zaproponuj optymalne rozwiązania.

Sprawdź poziom zabezpieczeń dla zbiorów danych przetwarzanych w formie papierowej.

Zweryfikuj poziom wiedzy i świadomości pracowników w zakresie ochrony danych osobowych.

Zweryfikuj zawarte umowy pod kątem ewentualnej konieczności uzupełnienia ich umowami powierzenia przetwarzania danych osobowych.

Ważne!
Sprawdź dokładnie wszystkie miejsca, gdzie przechowywane są dane osobowe – mogą to być nie tylko komputerowe repozytoria, serwery, arkusze Excel, systemy CRM itp., ale także... Twoje biurko, gdzie trzymasz wizytówki obecnych lub potencjalnych klientów. Dokładnie przeanalizuj, którzy pracownicy maja dostęp do danych osobowych i czy na pewno jest to uzasadnione. Zwróć uwagę także na to, czy firmom, z którymi współpracujesz, także przekazujesz dane – a jeśli tak, to czy masz z nimi zawarte umowy o ich powierzeniu.

Po przeprowadzonym audycie – w zależności od jego wyników – wprowadź w życie konieczne zmiany.

W SZCZEGÓLNOŚCI POWINIENEŚ POMYŚLEĆ O:

- działaniach w zakresie legalności przetwarzania danych osobowych
- działaniach w zakresie wymaganej dokumentacji
- analizie ryzyka
- powołaniu Inspektora Ochrony Danych Osobowych czy Administratora Bezpieczeństwa Informacji
- poinformowaniu i przeszkoleniu pracowników w zakresie bezpieczeństwa i zasad przetwarzania danych oraz obowiązku zgłoszenia naruszeń ochrony danych w ciągu 72 godzin

WDROŻENIE RODO W TWOJEJ FIRMIE

Legalność przetwarzania danych

ABY MÓC POWIEDZIEĆ, ŻE DANE OSOBOWE SĄ W TWOJEJ FIRMIE PRZETWARZANE LEGALNIE, MUSISZ:

- posiadać właściwe zgody na przetwarzanie danych osobowych, dostosowane do wymogów rozporządzenia oraz specyfiki Twojej firmy – sprawdź art. 6, 12, 13 RODO
- ustalić i wprowadzić zgodną z nowym rozporządzeniem klauzulę informacyjną, podawaną każdorazowo, kiedy pozyskujesz nowe dane osobowe – sprawdź art. 13 RODO
- ustalić, czy posiadasz obowiązujące umowy powierzenia przetwarzania danych oraz zawrzeć takowe w przypadkach obowiązkowego ich posiadania
- przygotować upoważnienia do przetwarzania danych dla pracowników czy współpracowników, którzy mają z nimi styczność

Zwłaszcza jeżeli dysponujesz pokaźną bazą danych osobowych – np. chociażby listą e-mailingową czy spisem kontrahentów – odnalezienie wymaganych zgód na przetwarzanie może być kłopotliwe. Dlatego dobrze jest nie polegać tylko na ulotnej pamięci lub niezabezpieczonych nośnikach, ale zaufać systemowi IT: Comarch wyposaży wszystkie swoje systemy klasy ERP w specjalną funkcjonalność prowadzenia rejestru zgód na przetwarzanie danych, zgód na przesyłanie informacji handlowych, zgód na profilowanie z datą udzielenia zgody, z IP oraz archiwizacją treści zgody. Dostępna będzie także funkcja umożliwiająca złożenie oświadczenia o cofnięciu zgody na przetwarzanie danych w takiej samej formie jak złożenie zgody.

COMARCH ERP

Rejestr czynności przetwarzania

Art. 30 rozporządzenia RODO wprowadza obowiązek prowadzenia przez administratora danych „rejestru czynności przetwarzania".

OBOWIĄZEK PROWADZENIA REJESTRU CZYNNOŚCI PRZETWARZANIA MAJĄ:

- przedsiębiorcy lub podmioty zatrudniające powyżej 250 osób;
- przedsiębiorcy lub podmioty zatrudniające mniej niż 250 osób, jeżeli:
  - przetwarzanie, którego dokonują, mogą powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą
  - przetwarzanie nie ma charakteru sporadycznego
  - obejmują szczególną kategorie danych osobowych, o których mowa w art. 9 ust 1 rozporządzenia RODO

Zaleca się jednak prowadzenie rejestru czynności przetwarzania nawet, jeśli według oceny Administratora jego prowadzenie nie jest obligatoryjne. Należy zaznaczyć, iż za nieprowadzenie rejestru będzie groziła kara pieniężna w wysokości do 10.000.000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Rejestr czynności przetwarzania musi być prowadzony w czytelny, przejrzysty i zarazem kompleksowy sposób. Comarch zadbał, aby wszystkie systemy ERP posiadały funkcjonalność umożliwiącą prowadzenie Rejestru przetwarzania ze wskazaniem jego obowiązkowych elementów wskazanych w art.30 ust.1 tj.

- imię nazwisko lub nazwę oraz dane kontaktowe administratora
- cele przetwarzania
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione
- informacja o przekazaniu danych do państwa trzeciego
- planowane terminy usunięcia poszczególnych kategorii danych
- opis technicznych i organizacyjnych środków bezpieczeństwa

COMARCH ERP

Analiza ryzyka

Zgodnie z przewidzianym w RODO podejściem opartym na analizie ryzyka, przeprowadzenie oceny skutków dla ochrony danych jest procesem budowania i wskazywania zgodności z RODO. Analiza ryzyka i zagrożeń to dokument będący wynikiem procesu szacowania ryzyka związanego z bezpieczeństwem przetwarzania danych. Oznacza to, że powinna być ona tworzona indywidualnie dla każdego podmiotu. Szacowanie ryzyka to proces, który wymaga:

- ustalenia zasobów, które mają być chronione (obszary przetwarzania danych, sprzęt komputerowy, bazy danych)
- ustalenia rodzajów i poziomów zagrożeń (zagrożenia ze strony działań ludzi, zagrożenia losowe, zagrożenia teleinformatyczne itd.)
- ustalenia zasad postępowania z ryzykiem, tzn. działań, które mają je zmniejszyć (np. wprowadzenie procedur niszczenia dokumentów)
- ustalenia zasad monitorowania ryzyka (kiedy powinna być prowadzona kolejna analiza)

Przeprowadzenie tego procesu stanowi wstęp do opracowania dokumentacji bezpieczeństwa i ochrony danych osobowych.

Dokumentacja ochrony danych

Przedsiębiorcy zobowiązani byli prowadzić dokumentację ochrony danych osobowych również dotychczas, RODO wprowadza jednak istotne zmiany w jej kształcie. Według zaleceń rozporządzenia dokumentacja ochrony danych powinna składać się z:

- **Strategii bezpieczeństwa**
- **Polityki bezpieczeństwa** dostosowanej do specyfiki danej firmy
- **Rejestru operacji** przetwarzania danych osobowych
- **Polityki monitorowania i reagowania** na naruszenia ochrony danych osobowych
- **Rejestru incydentów**
- **Rejestru upoważnień**
- **Polityki zarządzania ryzykiem** utraty prywatności (Privacy Impact Assessment)
- **Raportu z analizy ryzyka** (Privacy Impact Assessment)
- **Procedury zarządzania zmianą** / zarządzania projektami (Privacy by Design)
- **Planu awaryjnego** / polityki zarządzania kopiami zapasowymi
- **Procedury zarządzania użytkownikami** i dostępem
- **Standardy zabezpieczeń**

Wszystkie systemy Comarch ERP zostaną wyposażone w funkcjonalność umożliwiającą prowadzenie rejestru nadanych przez administratora upoważnień do przetwarzania danych – wraz z ich treścią i datą udzielenia.

COMARCH ERP

Powołanie Inspektora Ochrony Danych Osobowych

Powołanie IOD jest obligatoryjne we wskazanych w RODO przypadkach, podczas gdy powołanie ABI (administratora bezpieczeństwa informacji) ma zawsze charakter fakultatywny. Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych, a Administrator musi dbać o zachowanie jego niezależności.

OBOWIĄZEK NOMINOWANIA IOD POWSTANIE, GDY:

- przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości, przy czym Grupa Robocza Artykułu 29 ds. Ochrony Danych („Grupa art. 29") wskazuje, że dobrą praktyką byłoby powoływanie inspektora także przez podmioty prywatne, które prowadzą działalność z zakresu zadań publicznych tj. transport publiczny, dostawa wody, energii, czy infrastruktura drogowa

- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę

- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, czyli danych wrażliwych oraz danych dotyczących wyroków skazujących i naruszeń prawa

Ważne!
Jeśli podmiot uznaje, że nie ma obowiązku powołania inspektora, Grupa art. 29 zaleca sporządzenie dokumentacji, która wskazuje na brak takiego obowiązku. Dzięki temu, w razie wątpliwości, możliwe będzie zweryfikowanie, czy Administrator lub podmiot przetwarzający dane uwzględnił istotne czynniki podczas oceny. Zachęca się administratorów do powołania inspektora także wtedy, gdy nie jest to obligatoryjne.

ZADANIA INSPEKTORA OCHRONY DANYCH WSKAZUJE ART.39 RODO:

- informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie

- monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty

- udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35

- współpraca z organem nadzorczym

- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach

RODO W PRAKTYCE
– WYBRANE ZAGADNIENIA

Obowiązek zgłaszania naruszeń

W przypadku naruszenia ochrony danych osobowych w swoim przedsiębiorstwie, administrator danych bez zbędnej zwłoki, w terminie 72 godzin po stwierdzeniu naruszenia, będzie zobowiązany zgłosić takie naruszenie organowi nadzorczemu, tj. GIODO, chyba że jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Naruszeniem praw lub wolności osób fizycznych zgodnie z RODO będzie m.in. powstanie uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych – takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

Ważne!
To administrator będzie musiał ocenić (na nim będzie spoczywał ciężar dowodu), czy jest mało prawdopodobne, że dane naruszenie będzie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Wszystkie programy z rodziny Comarch ERP będą miały wbudowaną funkcję prowadzenia rejestru naruszeń przetwarzania danych osobowych w formie elektronicznej.

COMARCH ERP

Prawo do bycia zapomnianym

Zgodnie z art. 17 RODO, każda osoba fizyczna może żądać „bycia zapomnianym", jeżeli zatrzymywanie jej danych naruszałoby rozporządzenie, prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator.

Osoba, której dane dotyczą, ma prawo żądać od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane
- osoba, której dane dotyczą, cofnęła zgodę, na której opierało się przetwarzanie i nie ma innej podstawy prawnej przetwarzania
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania dotyczących jej danych osobowych
- dane osobowe były przetwarzane niezgodnie z prawem
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator
- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 GDPR

Prawo do bycia zapomnianym z łatwością wyegzekwujesz dzięki specjalnej funkcji, która będzie dołączona do systemów Comarch ERP – zaoferuje ona możliwość usunięcia czy pseudonimizacji danych osoby, która wystąpi z wnioskiem prawa do zapomnienia. Ponadto pojawi się funkcja umożliwiająca wgląd do danych dla osoby, której dane dotyczą, wprowadzenia w nich zmiany, wydania kopii (w taki sposób, aby dane uwidocznione dla wnioskującej osoby dotyczyły wyłącznie jej, bez możliwości widoczności danych innych osób).

COMARCH ERP

Wyłączenia prawa do bycia zapomnianym

Prawo do bycia zapomnianym nie ma zastosowania w zakresie, w jakim przetwarzanie jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi
- z uwagi na:
  - cele zdrowotne
  - interes publiczny w dziedzinie zdrowia publicznego
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania lub
- do ustalenia, dochodzenia lub obrony roszczeń

Możliwość profilowania zgodnie z RODO

RODO wprowadza definicję legalną profilowania, zgodnie z którą oznacza ono „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".

Możesz przeprowadzić audyt procesów przetwarzania danych osobowych w Twojej firmie, aby określić, czy te procesy stanowią profilowanie w rozumieniu definicji zawartej w RODO i dalej: ustalić cele i kryteria profilowania, wprowadzić mechanizmy wyrażania zgody na profilowanie przez konsumentów oraz dostosować ewentualne procesy decyzyjne oparte na zautomatyzowanym przetwarzaniu danych osobowych do nowych przepisów.

Naruszenia, za które zgodnie z RODO możesz dostać karę

BRAK UWZGLĘDNIENIA OCHRONY DANYCH w fazie projektowania

BRAK UMOWY powierzenia przetwarzania danych osobowych

BRAK REJESTRU czynności przetwarzania danych osobowych

NIEZGŁOSZENIE INCYDENTU godzącego w bezpieczeństwo przetwarzania danych osobowych

NARUSZENIE ZASADY bezpieczeństwa

NARUSZENIE STATUSU inspektora ochrony danych osobowych

NARUSZENIE ZASADY CELOWOŚCI

ŁĄCZENIE ZGÓD na przetwarzanie danych osobowych

BRAK PODSTAWY prawnej do przetwarzania danych

Zasady ustalania wysokości kar

Zastosowane administracyjne kary pieniężne muszą być w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające. Organ nadzorczy, decydując, czy nałożyć administracyjną karę pieniężną oraz ustalając jej wysokość, powinien zwracać w każdym indywidualnym przypadku uwagę na:

- charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania
- liczbę poszkodowanych osób, których dane dotyczą
- rozmiar poniesionej przez nie szkody
- umyślny lub nieumyślny charakter naruszenia

Pod uwagę brane powinny być także wszelkie wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego oraz kategorie danych osobowych, których dotyczyło naruszenie. Warto zauważyć, że w przypadku ewentualnej kontroli inspektorzy będą mieli prawo do nałożenia kilku kar pieniężnych za każde z wykrytych uchybień.

Ważne!
Podejmij przygotowania do stosowania RODO już dziś. Wykorzystaj czas, który pozostał do momentu wejścia rozporządzenia w życie na rzetelny przegląd wszystkich prowadzonych czynności przetwarzania danych – tak, by 25 maja 2018 r. móc już wykazać zgodność procedur w Twojej firmie z nowymi przepisami:

- **przygotuj** odpowiednią dokumentację
- **zawrzyj** z odpowiednimi podmiotami umowy powierzenia przetwarzania danych
- **przeprowadź** analizę ryzyka
- **wprowadź** odpowiednie środki techniczne i organizacyjne mające na celu ochronę danych osobowych
- **powołaj** Inspektora Ochrony Danych lub wskaż osobę odpowiedzialną za ochronę danych osobowych w Twojej firmie.

SYSTEMY COMARCH ERP GOTOWE NA RODO

W systemach Comarch ERP XT, Comarch ERP Optima, Comarch ERP Altum i Comarch ERP XL znajdziesz funkcjonalności, które pomogą uporać się z RODO.

REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

umożliwi prowadzenie i aktualizację rejestru przetwarzania danych osobowych w systemie

REJESTR ZGÓD NA PRZETWARZANIE DANYCH OSOBOWYCH

będzie zawierał informacje o udzieleniu lub cofnięciu zgód na przetwarzanie danych, jak również zgód na przesyłanie informacji handlowych wraz z historią ich udzielenia tzn. treścią udzielonego oświadczenia, datą oraz źródłem pozyskania takiej zgody

REJESTR UPOWAŻNIEŃ PRZETWARZANIA DANYCH OSOBOWYCH

czyli zbiór informacji o tym, kto wewnątrz oraz spoza danej firmy otrzymał prawo do wglądu w dane osobowe, w jakim zakresie i na jaki okres

WGLĄD DO DANYCH OSOBOWYCH

czyli czytelny wydruk danych dla osoby fizycznej oraz eksport tych danych w postaci XML, konieczne do udostępnienia osobie na jej wyraźną prośbę

REJESTR NARUSZEŃ PRZETWARZANIA DANYCH OSOBOWYCH

umożliwi zapisanie incydentów, gdyby dane nie były przetwarzane zgodnie z prawem

ANONIMIZACJA DANYCH

czyli trwałe usuniecie danych osobowych na żądanie osoby uprawnionej, pod warunkiem, że w systemie nie istnieją dokumenty, których przechowywanie jest wymagane prawnie

LOGOWANIE DZIAŁAŃ OPERATORÓW

zapisywanie informacji o tym, jakie czynności wykonywał operator, np. jakich zmian w danych osobowych czy jakich wydruków dokonywał

Jeśli chcesz dowiedzieć się więcej o RODO i dostosowaniu firmy do jego wymogów **– skontaktuj się z nami!**

Telefon: 12 681 43 00 wew. 1 lub 12 684 90 01 wew. 1

e-mail: info.erp@comarch.pl

COMARCH ERP

COMARCH