



SYSTEM INFORMATYCZNY

AlfaERP

Ostatnia aktualizacja: 11.05.2018 11:32

Część : **RODO**

Spis treści

Opis	2
Dane wrażliwe	2
A) Zabezpieczenie serwerów	3
B) Zabezpieczenie eksportu danych wrażliwych z systemu ALFAERP	3
C) Zabezpieczenie widoczności w modułach danych wrażliwych z systemu ALFAERP	3
D) Dostosowanie i kasowanie danych wrażliwych na żądanie (anonimizacja danych).	3
E) Wgląd do danych osobowych	4
F) Rejestr upoważnień przetwarzania danych osobowych	4

Opis

Nowe przepisy dotyczące RODO narzucają wiele obowiązków na firmy gromadzące i przetwarzające dane osób prywatnych. Dotyczy to danych wrażliwych podmiotów niebędących firmami. Przepisy RODO dotyczą wielu aspektów. Zaczynając od komputerów, ich przechowywania, dostępu fizycznych do nich, okablowania sieciowego, zabezpieczeń antywłamaniowych, kontroli dostępu tylko uprawnionych osób.

Pierwszą częścią jest opracowanie zabezpieczeń fizycznych komputerów czy innych nośników i nadanie uprawnień dostępu tylko dla określonych osób. Tą częścią nie zajmuje się firma ALFA STUDIO.

Druga część to zabezpieczenie danych gromadzonych w komputerze i kontrola dostępu. W tej części firma ALFA STUDIO zajmuje się tylko zabezpieczeniem oprogramowanie, którego jest producentem.

Kara za nieprzestrzeganie RODO i brak zabezpieczeń wynosi ustawowo do 4% obrotu firmy.

Zabezpieczenia przygotowane w systemie AlfaERP składają się z kilku etapów i jest realizowane indywidualnie, ponieważ każda fabryka ma inne zbiory danych, które ustawowo podlegają pod politykę RODO. Wdrożenie jest realizowane jest z roboczogodzin określonych przed pracą po wyborze, które punkty mamy realizować. W zależności od wybranych opcji i złożoności programu w danej firmie zostanie przedstawiona oferta na zabezpieczenia RODO dla konkretnej wersji systemu AlfaERP.

Dane wrażliwe

W celu ochrony prywatności przepisy RODO chronią informacje o osobach prywatnych. Dane wrażliwe to informacje o osobie fizycznej jednoznacznie pozwalające na jej identyfikację. Samo imię i nazwisko nie są danymi wrażliwymi, bo może w Polsce być dwudziestu Janów Kowalski. Natomiast dane te w połączeniu z innymi danymi – tworzą w efekcie dane wrażliwe np. z adresem korespondencyjnym lub adresem email. Wszystkie dane, które jednoznacznie określają osobę typu: **telefon, email, adres** są danymi wrażliwymi i musimy ich strzec, aby nie dostały się w niepowołane ręce.

Należy pamiętać o tym, że o ile firma może nie współpracować z osobami prywatnymi biznesowo i teoretycznie nie gromadzić danych wrażliwych o tyle systemy finansowo księgowo a zwłaszcza kadrowe gromadzą dane o pracownikach, które już są danymi wrażliwymi.

A) Zabezpieczenie serwerów

Zabezpieczenie serwerów dotyczy części IT/SOFTWARE, czyli oprogramowania wgranego do serwera. Pojawiają się tu ogromne problemy z uprawnieniami, ponieważ bardzo często do tego samego serwera wgrane jest oprogramowanie innych firm, którym zarządza informatyk wewnętrzny firmy.

W takich przypadkach dostarczamy dokumentację, na jakich portach i jakie oprogramowanie jest wgrane z firmy ALFA ERP. Określamy gdzie przechowuje dane wrażliwe program, i które zbiory należy zabezpieczyć na dysku. W jaki sposób funkcjonują bazy danych gdzie są ich kopie bezpieczeństwa.

W dokumentacji pojawiają się również opis systemu narzędzi do analizy danych (używanych przez serwis AlfaERP) instalowanych na serwerze oraz zabezpieczenie dostępu do nich. Narzędzia te w prosty sposób mogą eksportować dane całej firmy i muszą być zabezpieczone.

Informacje te pozwalają wewnętrznemu informatykowi zbudować zabezpieczenie danych i kontrolować dostęp do nich w ramach infrastruktury komputerowej firmy.

B) Zabezpieczenie eksportu danych wrażliwych z systemu ALFAERP

Podstawowym podatnością na wyciek danych w programie AlfaERP, która przed RODO była bardzo przydatną opcją jest eksportowanie danych do innych programów np. excel. W myśl nowych przepisów jest to praktycznie niedozwolona operacja pozwalająca wyeksportować z komputera użytkownikowi całe zbiory danych wrażliwych.

Podstawowym zabezpieczeniem, jaka podlega analizie jest określenie w firmie gdzie w bazie danych, w jakich polach są gromadzone dane wrażliwe. Po tej analizie zostanie zbudowane zabezpieczenie i program nie będzie pozwalał na eksportowanie tych danych do innych programów klawiszem F5. Zabezpieczenie będzie globalne, czyli nikt z użytkowników niezależnie od uprawnień nie będzie mógł eksportować na zewnątrz programu danych określonych, jako wrażliwe. Dotyczy to również wydruków z klawisza F8.

C) Zabezpieczenie widoczności w modułach danych wrażliwych z systemu ALFAERP

W niektórych firmach może być potrzeba analiza widoczności danych wrażliwych w poszczególnych modułach (zakresach uprawnień dla użytkowników) programu. Dane teleadresowe klienta powinny być niewidoczne w module produkcyjnym, aby osoby nieuprawnione nie mogły ich podejrzeć.

D) Dostosowanie i kasowanie danych wrażliwych na żądanie (anonimizacja danych).

Największym problemem, jaki narzucają przepisy RODO jest przygotowanie oprogramowania do usuwania danych z bazy danych, jeśli osoba sobie tego zażyczyła. Jest to tzw. Prawo do bycia zapomnianym

Problem jest o tyle złożony, że często była to wystawiona faktura a do niej udzielona gwarancja. Dotyczy to też innych dokumentów, których przechowywanie jest wymagane ustawowo.

Skasowanie takich informacji niszczy raporty i analizy ze sprzedaży czy produkcji.

ALFA STUDIO opracowało rozwiązanie aby dane nie były usuwane fizycznie i nie zmieniały stanu raportów czy analiz, a jedynie dany kontrahent w tych dokumentach i bazie danych będzie miał „wymazane” dane wrażliwe na żądanie.

Oprogramowanie jest o tyle skomplikowane, że w przypadku awarii serwera bazy danych i odzyskania ich z kopii będzie trzeba jeszcze raz wszystkich „wyczyszczonych” wcześniej z danych automatycznie jeszcze raz „wyczyścić z danych wrażliwych”. W systemie ALFAERP musi powstać wykaz kontrahentów usuniętych z danych wrażliwych wraz z informacją kiedy doszło do zanonimizowania danych w systemie.

E) Wgląd do danych osobowych

Kolejną funkcją w systemie AlfaERP będzie obsługa przypadku gdzie klient ma mieć możliwość wglądu w swoje dane osobowe. Zgodnie z przepisami RODO każdy klient może poprosić o wgląd do danych osobowych zapisanych w bazie danych systemu informatycznego. Realizowane to jest poprzez czytelny wydruk danych osobowych oraz eksport do formatu XML danych osobowych. Tak przygotowany zestaw danych można będzie wysłać osobie żądającej wglądu w dane.

F) Rejestr upoważnień przetwarzania danych osobowych

Aby ułatwić zarządzanie dostępami i uprawnieniami do danych osobowych – będzie możliwe prowadzenie rejestru upoważnień do przetwarzania danych osobowych. Będzie to przydatne w przypadku udzielania uprawnień do wglądu wewnątrz w firmie (pracownikom firmy), ale również podmiotom zewnętrznym. Chociażby firmom, które ze względu na jakieś prace utrzymaniowe – będą się łączyć z bazą danych. Rejestr będzie zawierał listę upoważnień wraz z informacjami - kto dostał upoważnienie, w jakim zakresie oraz zakres czasowy, w jakim ono obowiązuje. Każde takie upoważnienie będzie można wydrukować w formie papierowej a podpisane przez odpowiednie osoby – załączyć w formie skanu do rejestru.