LOGmanager a przestrzeganie RODO

Dokument ten przedstawia, w jaki sposób wdrożenie LOGmanagera pomaga zapewnić zgodność z wymaganiami ROZPORZĄDZENIA (EU) 2016/679 PARLAMENTU EUROPEJSKIEGO I RADY (GDPR/RODO).

RODO ustanawia obowiązujące przepisy dotyczące ochrony danych osobowych obywateli państw członkowskich podczas ich pozyskiwania, przetwarzania i przechowywania.

W 2012 roku Komisja Europejska zaproponowała dogłębny przegląd dyrektywy 95/46/WE (Rozporządzenie o Ochronie Danych Osobowych). Stało się to podstawą nowego rozporządzenia ogólnie znanego jako Rozporządzenie o Ochronie Danych Osobowych (zwane dalej "RODO"), zatwierdzonego w kwietniu 2016 r. Rozporządzenie zostało opracowane w celu zharmonizowania dotychczasowych przepisów dotyczących ochrony i przetwarzania danych osobowych we wszystkich państwach członkowskich UE. Weszło ono w życie w dniu 25 maja 2018 i jest stosowane we wszystkich organizacjach przetwarzających dane osobowe obywateli UE, zarówno w Unii Europejskiej, jak i poza nią. Kluczowe wymagania dotyczące RODO obejmują w szczególności:

- Podniesienie poziomu bezpieczeństwa obywateli EU w zakresie przetwarzania ich danych osobowych.
- Uwzględnienie wymagań dotyczących bezpieczeństwa danych i własnych systemów w procesie opracowywania i wdrażania oprogramowania służącego do przetwarzania danych osobowych (uwzględnienie ochrony prywatności już w fazie projektowania i domyślna ochrona prywatności).
- Ochrona danych osobowych w największym możliwym stopniu poprzez zastosowanie anonimizacji, pseudonimizacji oraz szyfrowania.
- Ochrona danych osobowych, zapewnienie ich dostępności, poufności i właściwego przetwarzania.
- Tworzenie nowych ról i procesów biznesowych w celu wzmocnienia nadzoru nad bezpieczeństwem danych osobowych.
- Regularne sprawdzanie, badanie i ocenianie skuteczności środków technicznych i organizacyjnych w celu zwiększenia bezpieczeństwa przetwarzania danych.
- Obowiązkowe powiadomienia odpowiednich organów nadzoru nie później niż 72 godziny od momentu otrzymania informacji o naruszeniu zasad RODO lub wycieku danych osobowych.

Aby zapewnić skuteczną egzekucję stosowania się przez organizacje do wymogów dyrektywy, RODO obejmuje również przepisy dotyczące kar za nieprzestrzeganie, a przewidziane grzywny są bardzo dotkliwe. Dodatkowo rozporządzenie (UE) 2016/679 Parlamentu Europejskiego oraz Rady stanowi, iż te sankcje muszą być stosowane w największym stopniu, z możliwością zastosowania alternatywnych środków tylko w przypadku osób fizycznych.
Ze względu na to, że rozporządzenie nie wskazuje konkretnych rozwiązań, wiele organizacji zastanawia się, jakie środki zgodne z wymogami RODO i w jakich obszarach powinny być zastosowane.
Niniejszy dokument wskazuje w jaki sposób, dzięki zastosowaniu platformy LOGmanager, służącej do zcentralizowanego przechowywania i zarządzania informacjami o naruszeniach bezpieczeństwa danych, organizacja może osiągnąć zgodność z najważniejszymi wymaganiami RODO.

Streszczenie dla CISOs/CIOs:
RODO i LOGmanager

LOGmanager i jego związek z RODO: LOGmanager umożliwia organizacjom wykonywanie bieżących, jak i jednorazowych audytów, oraz przejrzyste dokumentowanie wszystkich zidentyfikowanych naruszeń dotyczących danych osobowych tj. **kto, kiedy i w jaki sposób uzyskał dostęp do danych podlegających RODO**.

LOGmanager to platforma, która otrzymała certyfikat do zarządzania zapisami audytów zgodny z ISO/27001:2013. W zaszyfrowanym* repozytorium system przechowuje długoterminowo dzienniki zdarzeń w zarządzanej, scentralizowanej, indeksowanej i skompresowanej bazie danych. W celu umożliwienia wygodnego i wydajnego korzystania, dzienniki zdarzeń są konwertowane do znormalizowanego formatu, ale niezależnie są też przechowywane w oryginalnej formie. Wszystkie rekordy posiadają unikalny identyfikator oraz są chronione zaufanym znacznikiem czasu. Stosowane przez LOGmanagera mechanizmy weryfikacji i autoryzacji, a także wbudowane mechanizmy kontrolne zapewniają, że dostęp do przechowywanych danych mogą uzyskać tylko osoby z odpowiednimi uprawnieniami, nie mając jednocześnie żadnych możliwości modyfikacji ani usuwania danych.

** Szyfrowanie jest dostępne tylko dla LOGmanagera działającego na serwerach HPE z wykorzystaniem szyfrowania HPE Secure Encryption.*

Wdrożenie narzędzi wspierających audyt jest ważną częścią całego łańcucha działań, ale jest to tylko jeden z wielu ważnych elementów. Z drugiej strony, wdrożenie wszystkich środków technicznych i organizacyjnych określonych w rozporządzeniu nie zwalnia przedsiębiorstwa z odpowiedzialności za nieprzestrzeganie celów rozporządzenia. (Tak, regulacje te mogą mieć istotne konsekwencje. Nie ma potrzeby przewidywać czy sugerować żadnych czarnych scenariuszy. Przyszłość pokaże, jak przepisy są egzekwowane w praktyce i jak będą wyglądać orzeczenia sądowe dotyczące przypadków naruszenia RODO).

LOGmanager

Szczegółowe informacje dla specjalistów ds. Bezpieczeństwa IT w organizacjach.

W których dokładnie obszarach związanych z RODO może nam się przydać LOGmanager.
Artykuł 32 - Bezpieczeństwo przetwarzania danych.
Artykuł 33 - Powiadomienie organu nadzorczego o naruszeniu danych osobowych.
Artykuł 34 - Przekazywanie danych osobowych podmiotowi, którego dane dotyczą.
Artykuł 58 – Uprawnienia.

Monitorowanie bezpieczeństwa przetwarzania danych oraz dostępu do prywatnych danych:
LOGmanager został zaprojektowany jako scentralizowany system zarządzania dostarczanymi dziennikami zdarzeń, zapewniający prosty wgląd do wszystkich danych w organizacji, które zostały wygenerowane komputerowo. LOGmanager gromadzi, ujednolica i zapewnia długoterminowe przechowywanie dzienników i zdarzeń uzyskanych z aktywnych elementów sieci, systemów bezpieczeństwa, systemów operacyjnych oraz aplikacji. Logmanager w czasie zbliżonym do rzeczywistego zapisuje zgromadzone dane w wysokowydajnej bazie danych, do której wyłączny dostęp mają specjaliści od bezpieczeństwa IT, za pośrednictwem zestawu predefiniowanych pulpitów lub zapytań strukturalnych oraz pełnotekstowych. Otrzymane wyniki analizy i zapytań są prezentowane w formie graficznej.

Doskonale dopracowana możliwość śledzenia logów, zdarzeń i innych danych maszyny - to wszystko pozwala bezstresowo wdrożyć środki wymagane przez RODO. Ponadto, LOGmanager oferuje API umożliwiające integrację z innymi używanymi przez organizację narzędziami, zarówno do celów monitorowania, jak i bezpieczeństwa.

Aby zachować zgodność z wyżej opisanymi wymaganiami, LOGmanager dostarcza mechanizmy zarządzania dziennikami i gwarantuje możliwość śledzenia zdarzeń systemowych oraz zdarzeń generowanych przez użytkowników, w tym możliwości przeprowadzania bieżących lub jednorazowych audytów. Jest to niezwykle ważne by zapobiegać, wykrywać lub minimalizować skutki narażania danych lub systemów podlegających RODO. LOGmanager oferuje widok wszystkich danych komputerowych w jednym oknie, dzięki czemu można szczegółowo śledzić, powiadamiać i analizować dane w przypadku wykrycia naruszenia bezpieczeństwa. Krótko mówiąc, jest to kompleksowy system do gromadzenia, przechowywania i analizowania logów, który umożliwia zoptymalizowaną kosztowo automatyzację i proaktywną ochronę systemów oraz sieci IT.

LOGmanager to narzędzie, które umożliwia spełnienie wielu zaleceń RODO. Oprócz tego jest narzędziem przydatnym do ochrony przed atakami cybernetycznymi i incydentami. Dla specjalistów ds. bezpieczeństwa IT jest narzędziem kontroli i audytu. W jednoznaczny i bezdyskusyjny sposób rejestruje działanie systemów umożliwiając wykrywanie, gromadzenie i ocenę zdarzeń bezpieczeństwa.

Obowiązek zgłaszania incydentów i współpracy z organem nadzorczym:
LOGmanager pozwala na tworzenie dokumentów w odpowiednich formatach, niezbędnych do zgłaszania incydentów bezpieczeństwa oraz umożliwia organizacjom dokumentowanie bezpieczeństwa ich systemów podlegających pod RODO. Dzięki wystarczającej retencji przechowywanych danych komputerowych pozwala tworzyć dowody audytowe i przygotować dokumenty, które są wymagane do raportowania i późniejszej analizy kryminalistycznej wykrytych zdarzeń bezpieczeństwa, nawet jeśli czas wystąpienia incydentu bezpieczeństwa, jak i czas jego wykrycia znacznie różnią się*.

** Możliwość przechowywania danych zależy od wersji LOGmanagera oraz od wielkości i typu zebranych danych. Wersja XL LOGmanager wykorzystuje bazę danych o pojemności 100 TB i gromadzi 3500 zdarzeń na sekundę, osiąga średnią retencję danych wynoszącą 450 dni. Zgodnie z zaleceniami National Center for Cyber Security, wszystkie wersje LOGmanagera spełniają odpowiednie wymagania dotyczące: przechowywania i integralności danych, ich szyfrowania, a także zapewnienia szyfrowanej komunikacji pomiędzy monitorowanymi systemami a LOGmanagerem.*

LOGmanager pozwala generować tabele zawierające dane dotyczące kondycji środowiska IT oraz informacje wymagane do zapewnienia zgodności z wymaganiami.

LOGmanager oraz gromadzenie i przetwarzanie danych osobowych - FAQ:

Czy konieczna jest zgoda osób podczas przetwarzania ich danych osobowych w LOGmanagerze?

Nie jest wymagana żadna dodatkowa zgoda. Jeśli dana osoba wyraziła zgodę na przetwarzanie swoich danych przez Twoją organizację, to jest wysoce prawdopodobne, że niektóre jej dane osobowe pojawią się w zapisach przechowywanych w systemie. Wśród danych osobowych, które mogą pojawić się w LOGmanagerze, najczęściej występują: nazwa, nazwa użytkownika, adres IP oraz adres e-mail.

LOGmanager przetwarza logi, zdarzenia, dane dotyczące systemów wyłącznie w celu zapewnienia bezpieczeństwa, audytu i analizy dochodzeniowej. Już same względy bezpieczeństwa i audytu są uzasadnionym interesem. Niemniej jednak, zdecydowanie zalecamy, aby specjalista ds. ochrony informacji w firmie opracował dokumentację dotyczącą stosowania LOGmanagera:

a) **Zdefiniuj cel zbierania danych** - w tym przypadku jest to platforma bezpieczeństwa, audytu i analizy śledczej do badania incydentów bezpieczeństwa i zapobiegania utracie lub naruszeniu integralności danych osobowych.
b) **Udokumentuj środki używane do przetwarzania** – LOGmanager jest kolektorem i systemem centralnym do przechowywania logów, które mogą również zawierać dane osobowe pochodzące z narzędzi audytu, systemów przetwarzających dane osobowe oraz innych źródeł, które udostępniają zdarzenia, dzienniki i dane komputerowe.

c) **Opisz zastosowane środki ograniczenia dostępu i środki bezpieczeństwa zastosowane w celu ochrony potencjalnych danych osobowych przechowywanych w LOGmanager** - opisz, w jaki sposób skonfigurowane są uprawnienia dostępu do LOGmanagera, kto jest członkiem zespołu, który ma dostęp do LOGmanagera i jakie uprawnienia do bazy danych osobowych posiada.

d) **Sporządź dokumentację, opisująca w jaki sposób dane historyczne są z LOGmanagera usuwane** – wspomnij o tym, że dane w LOGmanagerze nie mogą być w żaden sposób modyfikowane. Gdy przestrzeń bazy danych zapełni się, dane historyczne są automatycznie usuwane zgodnie ze skonfigurowaną polityką retencji. Jeśli tworzysz kopie zapasowe danych w systemach zewnętrznych, musisz także wskazać, w jaki sposób są one przechowywane i chronione przed nieautoryzowanym dostępem. Ponadto należy wskazać, w jaki sposób kopie zapasowe, które nie są już potrzebne są usuwane.

e) **Zdefiniuj i udokumentuj wszystkie zabezpieczenia związane z LOGmanager**.

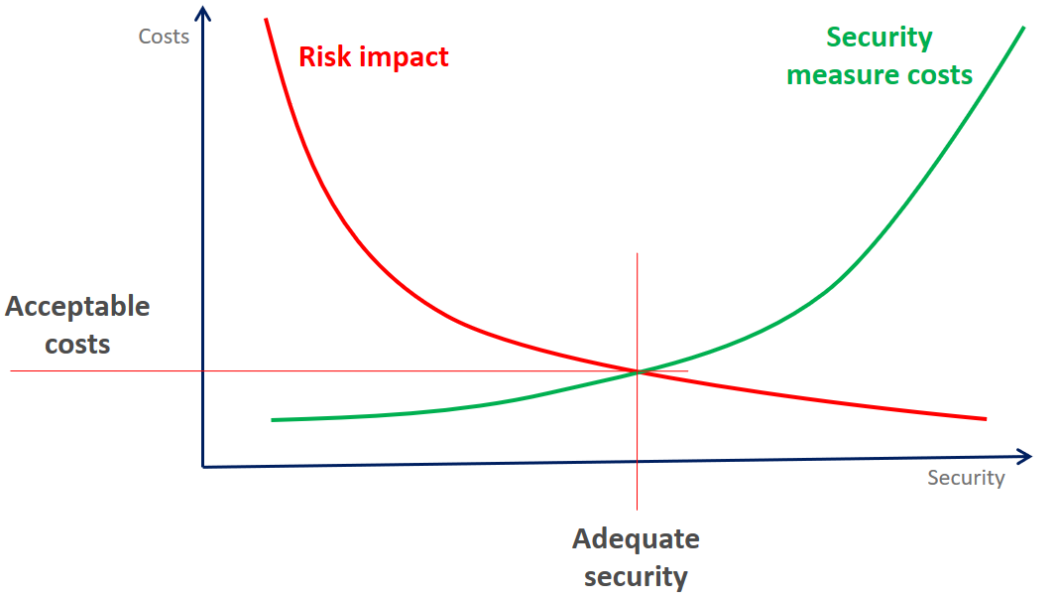
Jeśli osoba nie wyraża zgody, to czy konieczne jest również usunięcie jego danych osobowych z LOGmanagera?

Nie ma takiej konieczności. Przetwarzanie dzienników zdarzeń w LOGmanager jest uzasadnionym interesem podmiotu przetwarzającego dane osobowe. Nawet po wycofaniu zgody przez podmiot konieczne jest przechowywanie wygenerowanych wcześniej danych. Dokumentowanie poprzednich operacji przetwarzania i możliwych dowodów usunięcia z systemów produkcyjnych jest głównym powodem, dla którego nie należy usuwać danych.

Obraz - LOGmanager-L może gromadzić ponad 1 i pół miliarda danych maszynowych tygodniowo w systemach organizacyjnych

LOGmanager – właściwy wybór do zapewnienia zgodności z RODO

Przed wdrożeniem zabezpieczeń zgodnych z wymogami regulacyjnymi, konieczne jest przeprowadzenie analizy ryzyka i ocena całkowitych kosztów poszczególnych zabezpieczeń przy jednoczesnym zapewnieniu maksymalnej zgodności z przepisami. Wszystko to bez pominięcia ogólnej efektywności danego środka dla organizacji.



LOGmanager oferuje następujące najważniejsze korzyści dla organizacji poszukujących optymalnej równowagi między poziomem bezpieczeństwa a rozsądnymi kosztami:

- Szybki proces wdrożenia. Wdrożenie zapewniające zgodność z przepisami to kwestia kilku dni.
- Łatwe szkolenie personelu, pozwalające posiąść wszystkie wymagane umiejętności już po 2 dniach przeszkolenia.
- Przyjazny i intuicyjny interfejs użytkownika.
- Szczegółowa dokumentacja w języku angielskim oraz instrukcje, jak prawidłowo skonfigurować źródła zdarzeń.
- Forum użytkowników LOGmanager z dodatkowymi poradami technicznymi i podpowiedziami.
- Niskie, a przede wszystkim dobrze określone koszty operacyjne. Sprzęt, oprogramowanie i usługi są wliczone w cenę.
- Brak ukrytych kosztów przy zakupie licencji. LOGmanager nie ma żadnych ograniczeń licencyjnych.
- Pełna zgodność z normą ISO/IEC 27001:2013, zgodność z wymogami regulacyjnymi obowiązującymi w poszczególnych krajach UE.