Fakty:

Mało czasu na zmiany. Nowe przepisy nie wymagają wdrożenia.

4 maja 2016 r. ogłoszono tekst Rozporządzenia 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 95/45/WE („GDPR").

GDPR weszło już w życie, jednakże zgodnie z przepisem przejściowym będzie mieć zastosowanie dopiero od 25 maja 2018 r.

Zasada przejrzystości - jasne i zrozumiałe informacje.

Jednym z filarów GDPR, jest zasada przejrzystości w stosunku do osób fizycznych, których dane osobowe są przetwarzane. Przejrzystość przejawiać się będzie w wielu obowiązkach związanych z przetwarzaniem danych osobowych (przede wszystkie w zakresie obowiązków informacyjnych).

Prawo do bycia zapomnianym (usunięcie danych)

GDPR gwarantuje każdej osobie fizycznej prawo do „bycia zapomnianym", czyli do tego, by dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli nie są one już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane, a osoba, której dane dotyczą, cofnęła zgodę lub wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących lub też przetwarzanie jej danych osobowych nie jest z innego powodu zgodne z GDPR. Rozporządzenie wprowadza jednak pewne wyjątki od tej zasady.

W odniesieniu do bycia zapomnianym w sieci, GDPR formułuje szczególne obowiązki dla administratorów.

Zasada ochrony prywatności by design

Zgodnie z zasadą ochrony prywatności *by design* (tzw. zasada prywatności „w fazie projektowania") administrator już na etapie projektowania danego rozwiązania związanego z przetwarzaniem danych osobowych ma uwzględnić stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele

ul. Bagno 2 lok. 5 | 00-112 Warszawa | biuro@appeal.pl | www.appeal.pl

przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, a następnie przy określaniu sposobów przetwarzania ma wdrożyć odpowiednie środki techniczne i organizacyjne.

Zasada ochrony prywatności by default

Zasada ochrony prywatności *by default* obliguje z kolei administratora, aby w/w środki zapewniały, iż domyślnie przetwarzane będą tylko te dane osobowe, które są niezbędnie dla osiągnięcia konkretnego celu przetwarzania, odnosząc to także do ilości zbieranych danych, zakresu ich przetwarzania, okresu i ich przechowywania, jak i dostępności.

Privacy impact assesment

GDPR nakłada na administratorów obowiązek samooceny pod kątem oceny skutków i zagrożeń (ryzyka) wynikających z przetwarzania dla ochrony danych osobowych. Administrator ma oceniać jakie dane przetwarza i jakie zagrożenie może mieć miejsce przy przetwarzaniu danych. Ma to także prowadzić do oceny, jakie środki należy podjąć w celu ochrony danych w ramach ich przetwarzania.

Zupełną nowością jest obowiązek zgłaszania organowi nadzoru zaistnienia zdarzenia skutkującego naruszeniem ochrony danych osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Obowiązek ten ma dotyczyć zarówno administratorów (ci informują w Polsce GIODO), ale i przetwarzających (ci informują administratora). Co najważniejsze, o niektórych naruszeniach (z wysokim ryzykiem) należy także zawiadomić podmiot, którego dane zostały zagrożone czy naruszone.

Obowiązek wyznaczenia inspektora ochrony danych (obecnego ABI-Administrator Bezpieczeństwa Informacji)

Zgodnie z art. 37 zarówno administrator jak i podmiot przetwarzający, będą mieć obowiązek wyznaczenia inspektora ochrony danych we wskazanych przypadkach (np. gdy przetwarzanie wiąże się z regularnym i systematycznym monitorowaniem osób, których dane dotyczą, na dużą skalę). Obowiązek wyznaczenia inspektora, może nałożyć także prawo krajowe.

Odszkodowanie i wysokie kary

GDPR przewiduje surowe kary administracyjne za jego naruszenie – za jedną grupę naruszeń do 10.000.000 EUR, a w przypadku przedsiębiorców do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, bądź w ramach drugiej grupy naruszeń do 20.000.000 EUR, a w przypadku przedsiębiorców w ramach grup naruszeń do 4 % całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym w obu przypadkach zastosowanie ma kwota wyższa).

Poza tym GDPR reguluje prawo do dochodzenia odszkodowania od administratora lub podmiotu przetwarzającego za szkodę majątkową lub niemajątkową w wyniku naruszenia GDPR.

ul. Bagno 2 lok. 5 | 00-112 Warszawa | biuro@appeal.pl | www.appeal.pl | NIP 525-265-03-55| KRS 0000605648

Wyzwania technologiczne

Bez udziału rozwiązań technologicznych jedynie tworząc procedury niemożliwe jest spełnienie wymogów stawianych przez ustawę. Od strony technologicznej największymi wyzwaniami są pytania:

Jak zastąpić Audyt natywny?

Jak w skuteczny sposób audytować zmiany zachodzące w środowisku?

W jaki sposób pozyskać wiedzę, gdzie znajdują się dane osobowe i inne dane wrażliwe?

Jak zarządzać ryzykiem związanym z danymi? W jaki sposób je zdefiniować?

Na serwerze plików Windows i niektórych urządzeniach NAS, audyt zdarzeń najczęściej nie jest włączony ze względu bardzo poważne obciążenie środowiska IT. Dzienniki rejestrujące zdarzenia są przechowywane przez krótki okres czasu lub zostają nadpisane.

Bez efektywnego i niezawodnego mechanizmu monitorowania aktywności na serwerze plików, organizacje są całkowicie bezradne. Nie wiedzą kto uzyskuje dostęp do danych, kiedy, skąd i jakie rodzaje aktywności są podejmowane. W odniesieniu do GDPR, brak świadomości jakie przekazujemy dane i jak je likwidujemy może skutkować karami. Poleganie na natywnych logach praktycznie nie pozwala stworzyć strategii monitorowania aktywności.

W jaki sposób otrzymywać właściwe dane do analizy?

Jak stworzyć wydają, elastyczną i łatwą w zarządzaniu architekturę zabezpieczająca dane osobowe i inne dane wrażliwe?

Jak zbudować system alarmów i powiadomień?

Jak integrować nowe rozwiązanie w ramach istniejącej architektury?

Z powodu tego, że dane są przechowywane w różnych środowiskach, z których różnej jakości informacje możliwe są do wyciągnięcia z audytów natywnych, ciężko jest korelować zdarzenia security bez ich wcześniejszej wstępnej analizy.

Brak scentralizowanych kontroli sprawia, że wyciągnięcie informacji możliwej do zinterpretowania jest w najlepszym razie niezwykle trudne, czy wręcz niemożliwe bez użycia zaawansowanych reguł w systemie SIEM.

Uzyskanie zgodność z UE GDPR opiera się na gruntownym zrozumieniu dostępu i zarządzania danymi osobowymi. Nie każdy system lub technologia dostarcza informacji potrzebnych do tego rodzaju wszechstronnego podejścia, wymaganego dla nowych standardów.

Kto powinien odpowiadać za przestrzeganie zasad bezpieczeństwa?

Jak przekonać użytkownika biznesowego do ochrony danych osobowych i informacji wrażliwej?

Zwiększenie świadomości użytkownika biznesowego i dostarczenie mu narzędzi do ochrony informacji wrażliwej jest jednym z najważniejszych wyzwań projektu. Zapewnienie ochrony danych poprzez klasyfikowanie ich już podczas tworzenia, oraz zasilenie systemów bezpieczeństwa informacją o tym, gdzie znajdują się dane osobowe stanowi kluczowy element uzyskania zgodność z UE GDPR.

ul. Bagno 2 lok. 5 | 00-112 Warszawa | biuro@appeal.pl | www.appeal.pl | NIP 525-265-03-55| KRS 0000605648

Podejście Appeal

Nasze podejście zakłada iteracje, których celem jest zbudowanie kompleksowego rozwiązania chroniącego dane w Organizacji. Szczególną uwagę zwracamy na integrację rozwiązania z istniejącymi w organizacji systemami. Każde działanie jest prowadzone z zapewnieniem najwyższej jakość i bezpieczeństwa środowisk oraz przy użyciu najlepszych dostępnych na rynku narzędzi.

Poprzez spełnienie dwóch założeń:

- przeniesienie na użytkownika biznesowego dbałości o ochronę informacji
- kompleksową architekturę rozwiązania

uzyskujemy zapewnienie zgodności z wymogami GDPR-a w tym, w szczególności zapewniamy ”default-ową” ochronę prywatności jednocześnie tak porządkujemy obszar danych, że wymuszamy ochronę również w fazie projektowania (by design).

Przykładowe iteracje:

1. Analiza projektu uzyskania zgodności

Wstępna analiza wymagań klienta z definiowaniem obszarów istotnych dla uzyskania zgodności z zapisami ustawy

2. Inwentaryzacja infrastruktury informatycznej i danych pod kątem analizy ryzyka, w tym:

- Wykrywanie użytkowników uprzywilejowanych
- Wykrywanie obiektów w sieci i ich konfiguracji
- Wyszukiwanie informacji wrażliwych w danych pod kątem wymagań bezpieczeństwa
- Wyszukiwanie danych osobowych pod kątem wymagań Europejskiej Ustawy o Ochronie Danych Osobowych
- Data Governance
- Wykrywanie zagrożeń w sieci bazując na unikalnym mechanizmie samodzielnego uczenia się zachowania ludzi maszyn i sieci (bez sygnatur i reguł)
- Wizualizacja sieci w trybie rzeczywistym i w 3D
- Odtwarzanie historii incydentu
- Wykrywanie zagrożeń w sieci niezauważalnych przez tradycyjne rozwiązania do Security

3. Audyt środowiska Microsoft/Linux/Baz danych/Sieci, w tym:

- Optymalizacja uprawnień
- Optymalizacja audytu zdarzeń (autorski audyt)
- Optymalizacja zbędnych obiektów/danych
- Wykrywanie potencjalnych naruszeń w bezpieczeństwie wśród aplikacji

ul. Bagno 2 lok. 5 | 00-112 Warszawa | biuro@appeal.pl | www.appeal.pl | NIP 525-265-03-55| KRS 0000605648

- Analiza ról i właścicieli obiektów w środowisku Microsoft
- Automatyzacja i zarządzanie danymi
- Analiza wektorów ataku, dróg przejścia i prawidłowej konfiguracji urządzeń sieciowych

4. Monitorowanie infrastruktury Microsoft i blokowanie dostępów, w tym:

- Monitorowanie i wymuszanie polityki bezpieczeństwa
- Filtrowanie dużej ilości niepotrzebnych informacji
- Firewall do bezpieczeństwa środowiska Microsoft
- Integracja z SIEM
- Zabezpieczanie krytycznych obiektów infrastruktury (obiekty, skrzynki pocztowe, pliki/foldery)
- Zarządzanie zmianą w infrastrukturze- audyt zmiany
- Automatyzacja polityk bezpieczeństwa

5. Monitorowanie i zarządzanie kontami uprzywilejowanymi, w tym:

- Nagrywanie i dokumentowanie pracy konsultantów zewnętrznych
- Zarządzanie hasłami dla kont uprzywilejowanych
- Pojedynczy punkt styku środowiska kont uprzywilejowanych/administratorów i użytkowników

6. Zarządzanie i ochrona informacji (oraz własnością intelektualna) w przedsiębiorstwie

- Automatyczna klasyfikacja informacji zgodna z polityką bezpieczeństwa
- Przeniesienie odpowiedzialności za ochronę danych na twórców dokumentów
- Monitorowanie aktywności na dokumentach (pliki) i wiadomościach e-mail w przedsiębiorstwie i poza
- Zabezpieczanie dokumentów (pliki) oraz wiadomości e-mail przed niepowołanym dostępem
- Przeciwdziałanie przed wyciekiem informacji
- Śledzenie aktywności użytkowników na plikach i e-mail'ach
- Znakowanie, opisywanie dokumentów i e-mail'i zgodnie z polityką bezpieczeństwa w firmie
- Szyfrowanie kluczowych informacji

7. Zapewnienie zgodności (ang. Compliance) z wymaganiami w kontekście dokumentów,

- Rekomendacja „D” Komisji Nadzoru Finansowego dla instytucji finansowych,
- Rozporządzenie Prezesa Rady Ministrów w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności.
- Spełnienie wymogów Europejskiej Ustawy o Ochronie Danych Osobowych

ul. Bagno 2 lok. 5 | 00-112 Warszawa | biuro@appeal.pl | www.appeal.pl | NIP 525-265-03-55| KRS 0000605648

Tabela technologiczna

Kluczowe elementy	Podejście Appeal
Sensitive Data Discovery- wykrywanie danych wrażliwych (SSD)	Jednym z elementów projektu jest wykrywanie danych wrażliwych. Inwentaryzujemy środowisko IT, sprawdzamy w których miejscach znajdują się dane, a poprzez korelacje z uprawnieniami możemy określić i przypisać ryzyka do informacji przechowywanej w środowisku.
Audyt infrastruktury	Poprzez zdefiniowanie środowiska IT poznanie struktury uprawnień i powiązanie jej z danymi wrażliwymi uzyskujemy unikalną wiedzę o danych.
SIEM	Z naszych systemów przesyłamy do SIEM-a już zinterpretowane informacje dotyczące aktywności na danych. Informujemy system SIEM o realnych zagrożeniach albo o poziomie poufności informacji która jest objęta aktywnością użytkownika. Dzięki temu w realny sposób jesteśmy wstanie zinterpretować zagrożenia.
Klasyfikacja	Klasyfikowanie informacji nie jest rozumiane przez nas tylko jako dostarczanie dodatkowych metadanych do plików, ale podchodzimy do niego jako do kluczowego rozwiązania zapewniającego DLP.
Data Governance- Zarządzanie danymi	Dzięki unikalnej architekturze i monitorowaniu zmian na środowisku nie tylko jesteśmy w stanie sprawdzić jak wygląda aktywność użytkowników na danych, ale również zarządzać strukturą danych pozostałych w spoczynku. Oznacza to, że możemy proaktywnie ją nadzorować w powiązaniu z uprawnieniami w organizacji oraz oddelegować kontrolę nad nią na właścicieli biznesowych.
Zabezpieczenie baz danych	Analizujemy aktywność na bazach danych, chronimy dostęp poprzez firewall'e bazodanowe zapobiegające wyciekowi danych.
Zabezpieczenie środowiska Microsoft	Analizujemy logowania użytkowników i zmiany w środowisku Microsoft, zabezpieczamy wrażliwe obiekty infrastruktury, oraz niechciane logowania kont na zasadzie dodatkowej warstwy ochronnej.
Uporządkowanie środowiska IT	Nie można mówić o bezpieczeństwie danych bez uporządkowanego środowiska. Narzędzia dostarczane przez Appeal w ramach projektów pozwalają na zarządzanie środowiskiem w bezpośredni, bezpieczny i efektywny sposób.
Konta uprzywilejowane	Zarządzanie kontami z rozbudowanymi uprawnieniami jest ważnym elementem bezpieczeństwa każdej nowoczesnej organizacji, w naszym projekcie jesteśmy w stanie zautomatyzować te dostępy, monitorować je również przez polityki i zintegrowane narzędzia.
Zarządzanie tożsamością -IDM	W naszym podejściu nie tylko przygotowujemy środowisko do projektów IDM'owych, ale na wielu poziomach potrafimy monitorować tożsamość rozumianą jako uprawnienia do systemów.
Zarządzanie zmianą	Istotną częścią projektu jest monitorowanie i zdefiniowanie Kto? Co? Gdzie? Skąd? Jak? Kiedy? Dlaczego? wykonał zmiany w środowisku.

ul. Bagno 2 lok. 5 | 00-112 Warszawa | biuro@appeal.pl | www.appeal.pl | NIP 525-265-03-55| KRS 0000605648