veracomp
inspirujemy IT

Budowa systemu bezpieczeństwa danych osobowych. Przegląd technologii w aspekcie RODO.

Piotr Borkowski
Veracomp SA

veracomp
inspirujemy IT

Wstęp

- GDPR/RODO jest bardzo dobre
- Szczególnie prywatnie dla nas jako osób fizycznych
- Cytat:

„Przetwarzanie danych osobowych należy zorganizować w taki sposób, aby **służyło ludzkości**.”

veracomp
inspirujemy IT

Przegląd zapisów dotykających kwestii technicznych

veracomp
inspirujemy IT

Aspekty techniczne RODO

- **„(…)ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik(…)”**

veracomp
inspirujemy IT

Aspekty techniczne RODO

- „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 (…)**”

veracomp
inspirujemy IT

Aspekty techniczne RODO

- **„(…) Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.”**

veracomp
inspirujemy IT

Aspekty techniczne RODO

- „Administrator powinien skorzystać z **wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych (…)**”

veracomp
inspirujemy IT

Aspekty techniczne RODO

- Należy nałożyć na administratora obowiązki i ustanowić odpowiedzialność prawną administratora za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. W szczególności **administrator* powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z niniejszym rozporządzeniem oraz, że są skuteczne.** Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.

*administrator danych osobowych a nie administrator IT

veracomp
inspirujemy IT

Aspekty techniczne RODO

- „Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych **osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów** niniejszego rozporządzenia. Aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i **wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych.** Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, **jak najszybszej pseudonimizacji danych osobowych**, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, **monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń.**”

veracomp
inspirujemy IT

Aspekty techniczne RODO

- „W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający **powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie.** Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – **takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych** (...)”

veracomp
inspirujemy IT

Aspekty techniczne RODO

- „**Należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych** i szybko poinformować organ nadzorczy i osobę, której dane dotyczą. To, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w **szczególności charakteru i wagi naruszenia ochrony danych osobowych**, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą.”

veracomp
inspirujemy IT

Podsumowanie wymagań technicznych

veracomp
inspirujemy IT

Podsumowanie

- Dane osobowe: każda informacja, która może zostać użyta do bezpośredniej identyfikacji osoby fizycznej (podmiotu danych), imię, zdjęcie, e-mail, dane bankowe, posty na stronie sieci społecznościowej, dane medyczne, czy adres IP komputera (i wiele więcej)
- Administrator: podmiot, który określa cele, warunki i środki służące przetwarzaniu
- Procesor: podmiot przetwarzający dane osobowe w imieniu i na rzecz administratora danych

veracomp
inspirujemy IT

Podsumowanie

- Kary: nierejestrowanie przetwarzania, niezgłoszenie naruszenia ochrony, niedokonanie oceny skutków przetwarzania
- Ochrona: utrzymywana na najwyższym, możliwym poziomie, cyklicznie audytowana i dopasowująca się do zmieniających się zagrożeń
- Rozwiązania: **powszechnie dostępne, stabilne i dojrzałe technologicznie, uznane za skuteczne**
- **Neutralność technologiczna** zaaprobowana przez lobby biznesowe

veracomp
inspirujemy IT

Technologie bezpieczeństwa przydatne w kontekście RODO

veracomp
inspirujemy IT

Wstęp

- Wdrożenie wszystkich technologii bezpieczeństwa w pełnym zakresie nie jest możliwe w każdym przypadku
- Zwykle nie zaczynamy od zera
- Budowa systemu bezpieczeństwa to proces, który wymaga wsparcia od producentów, dystrybutorów i partnerów
- Pamiętajmy, że chodzi o bezpieczeństwo, a nie tylko RODO

veracomp
inspirujemy IT

Najważniejsze obszary bezpieczeństwa

- Bezpieczeństwo sieci, serwerów, stacji i zdalnego dostępu
- Bezpieczeństwo baz danych oraz aplikacji webowych
- Silna autentykacja i kontrola dostępu
- Monitorowanie przepływu danych i przeciwdziałanie ich utracie (Data Loss Prevention)
- Szyfrowanie, pseudonimizacja
- Analiza i korelacja zdarzeń pochodzących z systemów przetwarzających dane (SOC)
- Backup/archiwizacja

veracomp
inspirujemy IT

GDPR Obszary – UTM/NGFW/Web Proxy/Sandbox/APT

- Podstawa bezpieczeństwa sieciowego w obszarach przetwarzających dane.
- Zaawansowane metody zapobiegania i wykrywania włamań.
- Wykrywanie i zapobieganie skutkom incydentów bezpieczeństwa.

veracomp
inspirujemy IT

GDPR Obszary – Deszyfracja SSL

- Szyfrowanie ruchu zapewnia prywatność i integralność przesyłanych danych, ale równocześnie pozostawia ogromną furtkę w systemach bezpieczeństwa, bardzo chętnie wykorzystywaną przez hakerów oraz zaawansowany malware.
- Z punktu widzenia GDPR/RODO jakikolwiek audyt i wykrywanie wycieków danych musi się wiązać z wglądem w całą komunikację.

veracomp
inspirujemy IT

GDPR Obszary – Uwierzytelnianie, Kontrola Dostępu

- Zarządzanie prawami dostępu i tożsamością.
- Multi-factor authentication.
- Analiza/wymuszanie haseł.
- Audyt i kontrola dostępów uprzywilejowanych

veracomp
inspirujemy IT

GDPR Obszary – Network Access Control

- Kontrola dostępu do sieci od poziomu fizycznego (Ethernet, WiFi itp.)
- Zapewnienie dostępu tylko do wybranych obszarów sieci zgodnie z uprawnieniami.

veracomp
inspirujemy IT

GDPR Obszary – Ochrona Stacji Końcowych

- Podstawa bezpieczeństwa dla stacji z dostępem do danych wrażliwych.
- Zaawansowane metody zapobiegania włamaniom.
- Wykrywanie i zapobieganie skutkom incydentów bezpieczeństwa.
- Audyt, DLP.
- Ochrona urządzeń mobilnych (Android, IOS).

veracomp
inspirujemy IT

GDPR Obszary – Izolacja sieci Web

- Absolutna izolacja od zagrożeń związanych z siecią Web.
- Bezpiecznie otwieranie załączników i linków w wiadomościach.
- Wizualny strumień dostarczany użytkownikowi niezależnie od przeglądarki czy systemu operacyjnego.
- Praca bez instalacji agentów.

veracomp
inspirujemy IT

GDPR Obszary – Szyfrowanie Stacji Roboczych/Nośników

- Komponenty szyfrujące dyski twarde i nośniki pamięci.
- Ochrona w przypadku kradzieży lub zagubienia, nieuprawnionego dostępu fizycznego.
- Zabezpieczenie przed wyciekiem danych z uszkodzonych, wymienionych czy wyrzuconych komponentów.

veracomp
inspirujemy IT

GDPR Obszary – Szyfrowanie Poczty Elektronicznej

- Zabezpieczenie przed wyciekiem danych z użyciem poczty email.

veracomp
inspirujemy IT

GDPR Obszary – Data Loss Prevention

- Klasyfikowanie tworzonych treści.
- Kontrola przepływu informacji.
- Zabezpieczenia klasy DLP instalowane na stacjach roboczych, dla usług (np. mail) i na poziomie sieci.

veracomp
inspirujemy IT

GDPR Obszary – Web Application Firewall

- Ochrona aplikacji webowych – najpopularniejszy interfejs dla użytkowników, najbardziej narażony na skuteczne ataki związane z wyciekiem danych.

veracomp
inspirujemy IT

GDPR Obszary – Anonimizacja Danych, Antifraud

- Pseudonimizacja na najwcześniejszym poziomie już u użytkownika.
- Szyfrowanie danych wprowadzanych przez użytkownika, zapobieganie wyciekom po stronie użytkownika.
- Szyfracja na poziomie danych w sieci.
- Zabezpieczenie przed włamaniami, które mogą prowadzić do wycieków.

veracomp
inspirujemy IT

GDPR Obszary – Audyt, Zgodność z Regulacjami (Compliance)

- Audyt zasobów sieciowych.
- Analiza stacji roboczych i serwerów.
- Analiza aplikacji webowych.
- Analiza kodu aplikacji.
- Analiza polityk systemów zabezpieczeń.

veracomp
inspirujemy IT

GDPR Obszary – Audyt Ruchu do Chmury

- Kontrola aplikacji chmurowych, bardziej zaawansowana niż na poziomie URL, uwzględniająca wiele atrybutów, np. zgodność z regulacjami.
- Kontrola i tokenizacja danych w aplikacjach chmurowych.

veracomp
inspirujemy IT

GDPR Obszary – Zbieranie Ruchu do Analizy/Deszyfracji

- Network TAP, Network Packet Brocker (NPB) – niezbędny w wykrywaniu incydentów i wycieków na poziomie analizy ruchu wchodzącego lub wychodzącego z różnych segmentów sieci.
- Nagrywanie całego ruchu wchodzącego i wychodzącego.

veracomp
inspirujemy IT

GDPR Obszary – Korelacja Zdarzeń, Przechowywanie Logów, Raportowanie

- Systemy SIEM zbierające i korelujące logi.
- Systemy analityczne.
- Budowa SOC (Security Operation Center) dla organizacji.

veracomp
inspirujemy IT

GDPR Obszary - Backup i archiwizacja Danych

- Lokalizacja danych strukturalnych (np. bazy danych) i niestrukturalnych (pliki biurowe, tekstowe, graficzne), przeszukiwanie i monitorowanie wykorzystania.
- Ochrona przed utratą, uszkodzeniem i naruszeniem.
- Minimalizacja przechowywanych danych, retencja i skuteczne usuwanie.

veracomp
inspirujemy IT

Jak znaleźć się w świecie z RODO

- Okazja do:
- Uzupełnienia systemu bezpieczeństwa.
- Ochrony w nowych obszarach.
- Modernizacji urządzeń do nowych polityk (wydajność, deszyfracja, większy zakres).
- Analizy stanu posiadania/ryzyka.
- Wdrożenia lepszego monitorowania.

veracomp
inspirujemy IT

Jak znaleźć się w świecie z RODO

- W ofercie Veracomp mamy rozwiązania w dowolnej skali.
  - np. DLP w UTM/NGFW FortiGate i DLP Symantec
  - w zależności od oceny ryzyka można skupić się tylko na określonych kanałach komunikacji np. http czy poczta

- W ofercie Veracomp mamy rozwiązania praktycznie we wszystkich obszarach które są pomocne w związku z RODO/GDPR.
  - zachęcamy do kontaktu z nami, jeśli pojawią się jakiekolwiek potrzeby
  - chętnie pomożemy również w kwestiach projektowych i strategicznych

- Jak zawsze zalecamy zdrowy rozsądek :)

- Mogą się Państwo skontaktować z nami przez stronę: **Veracomp.pl/rodo**

veracomp

inspirujemy IT

Dziękuję!

Piotr Borkowski