URZĄD OCHRONY DANYCH OSOBOWYCH

Urząd Zamówień Publicznych

OD „CALL HOME” DO END-OF-SUPPORT: JAK OGRANICZAĆ UKRYTE PRZEPŁYWY DANYCH I RYZYKO NABYWANIA PODATNYCH TECHNOLOGII

Dr Adam Behan

Katedra Prawa Karnego UJ

Wydział Informatyki, Elektroniki i Telekomunikacji AGH

Urząd Ochrony Danych Osobowych
ul. Stanisława Moniuszki 1A, 00-014 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

POJĘCIA BAZOWE

Call home - automatyczna łączność z producentem (mechanizm komunikacyjny)

Telemetria - dane o stanie i użyciu

Zdalne zarządzanie - zdalna konfiguracja i serwis

Connected experiences - funkcje chmurowe produktu

End of support - koniec wsparcia bezpieczeństwa

Ochrona danych w urzędzie nie kończy się na polityce prywatności na stronie www. Ona zaczyna się w szafie rackowej. Jeśli nie kontrolujemy telemetrii, nie kontrolujemy danych. Państwa rolą jako IOD-ów jest wymuszenie na działach IT i zamówień publicznych, by przestali kupować „wygodę", a zaczęli kupować „bezpieczeństwo przez izolację".

ALE CZY TO SĄ DANE OSOBOWE?

- **Metadane jako dane osobowe:** W plikach konfiguracyjnych znajdują się opisy interfejsów.
- Pełna konfiguracja zawiera listy kontroli dostępu (ACL), definicje VLAN-ów i mapę routingu. Te informacje pozwalają na stworzenie precyzyjnego profilu podatności urzędu.
- Kupujemy router, system EDR, drukarkę lub urządzenie MFP. Po instalacji pojawia się stały ruch do domen producenta. Czy to jest jeszcze wsparcie serwisowe, czy już transfer danych i źródło ryzyka?
- **Iluzja maskowania (Data Scrubbing):** Producenci deklarują, że hasła są usuwane przed wysyłką. Jednak historia luki **CVE-2024-20440** pokazała, że błędy w oprogramowaniu telemetrycznym (tzw. „excessive verbosity”) mogą doprowadzić do wycieku logów zawierających poświadczenia do API w formie jawnej.

Czy w Państwa urzędzie istnieje **umowa powierzenia przetwarzania danych (DPA)** z producentem sprzętu, która obejmuje te „niezamierzone” dane osobowe?

Producent staje się podmiotem przetwarzającym (art. 28 RODO). Czy w Państwa urzędach istnieją umowy powierzenia z Cisco czy Fortinetem obejmujące telemetrię?

NIE TYLKO SPRZĘT. ZAKUP OPROGRAMOWANIA = ZAKUP MODELU PRZEPŁYWU DANYCH

Postępowanie EDPS przeciwko Komisji Europejskiej dotyczące używania Microsoft 365 i tego, czy warunki umowne, techniczne i organizacyjne nie prowadziły do niekontrolowanego przekazywania danych osobowych do Microsoftu oraz jego ekosystemu usługowego.

- EDPS stwierdził naruszenia dotyczące **ograniczenia celu, transferów międzynarodowych i nieuprawnionych ujawnień** w związku z użyciem Microsoft 365 przez Komisję Europejską.
- Istota problemu nie sprowadzała się do „chmury” jako takiej, lecz do tego, że administrator **nie potrafił precyzyjnie wskazać: jakie dane, do kogo, do jakich państw i po co są przesyłane**.
- To precedens dla zamówień publicznych: **wadliwie skonstruowana SWZ lub umowa na oprogramowanie może otworzyć kanał telemetryczny do producenta i jego podmiotów**, jeśli nie reguluje celów, odbiorców, transferów, connected experiences, audytu i centralnego wyłączania określonych funkcji.
- Postępowanie miało realny skutek: EDPS nakazał od 9 grudnia 2024 r. zawiesić przepływy do państw trzecich bez decyzji adekwatności, a w lipcu 2025 r. uznał, że po wdrożeniu dodatkowych środków umownych, technicznych i organizacyjnych Komisja usunęła naruszenia wskazane w decyzji z 8 marca 2024 r.

EDPS VS KOMISJA EUROPEJSKA

- Najważniejsze ustalenie EDPS było paradoksalne: **pełny katalog danych nie był prawidłowo określony**, a *diagnostic data* i *service generated data* mogły obejmować zasadniczo dowolne dane osobowe poza *operational personal data*; nawet kategorie szczególne nie były wyłączone.
- Zidentyfikowano co najmniej takie kategorie danych: **IP address, creation time, site URL, user email address**, a także **organisational identifiers, subscriptions, technical settings, resource names, configuration and device information, timestamps, URLs**.
- W przepływach telemetrycznych, licencyjnych i katalogowych pojawiały się również **user ID / ObjectID, device ID, Entra/Azure AD data (w tym username i email address)** oraz pseudonimizowane **IP/MAC addresses**.
- EDPS wskazał też na **directly identifying personal data** w *required service data* z OneDrive, np. **readable username, file path, email address**; w analizach przywołanych przez EDPS pojawiały się ponadto **titles/pathnames/subjects** plików lub e-maili, adresaci **to/cc/bcc**, informacje o załącznikach i dokładne znaczniki czasu.
- Dane te mogły przepływać nie tylko „dla działania usługi”, ale również w ramach **telemetrii, connected experiences, licencjonowania i aktywacji, synchronizacji atrybutów katalogowych, wsparcia technicznego, zdalnego dostępu personelu Microsoft oraz analityki bezpieczeństwa**.

DATA FLOW MAP

1. Data flow map

co, dokąd, po co, kiedy
porty, protokoły, odbiorcy, dane

2. Jak odbierać

default deny + allow-lista
logowanie każdej próby

3. Test A1

72 h - 7 dni
restart, aktualizacja, błąd

Kryterium niezgodności

każdy nowy endpoint albo nowy typ danych bez uprzedniej dokumentacji i akceptacji

MAPOWANIE PRZEPŁYWÓW DANYCH

- Call home ≠ zło. Call home bez kontroli = ryzyko
- Mapa przepływów danych jako załącznik do umowy: *Field → Destination → Purpose → Role → Retention*.

(1) deklaracja wykonawcy/producenta (data flow map) + (2) weryfikacja techniczna + (3) kontrola ciągła po wdrożeniu.

- W sieci odbiorowej ustawmy **default-deny** (na firewall/proxy) i dopuszczanie tylko tego co jest w data flow map (allow-lista). Wtedy **nawet jeśli ruch jest raz w tygodniu**, to i tak wykryjemy próbę połączenia - bo zostanie zablokowana i zalogowana. (**Defense in Depth**)
- Testy odbiorowe w oknie czasowym, **minimum 72 godziny**, a przy urządzeniach IoT / sieciowych często **7 dni** obserwacji (w tym restart, aktualizacja, błąd, symulacja awarii DNS, symulacja braku internetu).

„Jakakolwiek nieudokumentowana komunikacja wychodząca = niezgodność z umową” (chyba że Zamawiający zaakceptuje zmianę data flow map w trybie aneksu/zmiany zakresu).

CRA I ŁAŃCUCH DOSTAW: CZEGO MOŻNA WYMAGAĆ JUŻ DZIŚ

1
obowiązek aktualizacji bezpieczeństwa przez cały okres wsparcia

2
terminy zgłoszenia podatności, incydentu i zmiany modelu komunikacji

3
prawo audytu ruchu, logów oraz zmiany endpointów

4
zakaz nowych połączeń wychodzących bez zgody zamawiającego

5
exit / replace, gdy kończy się wsparcie lub zmieniają się transfery danych

CRA I RYZYKO DOSTAWCY: JAK WYKORZYSTAĆ NOWE UNIJNE REGUŁY JUŻ W 2026 R.

- support period ma co do zasady wynosić co najmniej 5 lat; wyjątek dotyczy produktów, których przewidywany czas używania jest krótszy
- data końca wsparcia ma być jasno wskazana już przy zakupie, co najmniej miesiąc i rok
- każda aktualizacja bezpieczeństwa udostępniona w okresie wsparcia ma pozostać dostępna co najmniej 10 lat albo do końca support period (zależnie od tego, co jest dłuższe)
- Producenci, importerzy i dystrybutorzy mają własne obowiązki zgodności oraz dokumentacyjne.

Nowy unijny ICT Supply Chain Security Toolbox (2026) rekomenduje ocenę krytycznych dostawców, strategie multi-vendor i ograniczanie zależności od podmiotów wysokiego ryzyka. To wzmacnia argument za ostrzejszymi wymaganiami dla urządzeń monitoringu, sieci, kontroli dostępu i innych systemów z ciągłą łącznością.

END-OF-SUPPORT = REALNE RYZYKO NARUSZENIA RODO

- Brak aktualizacji = brak adekwatnych środków bezpieczeństwa
- Naruszenie zasady „odpowiednich środków technicznych”
- Odpowiedzialność administratora (nie producenta)
- Ryzyko incydentu = ryzyko naruszenia danych

JAK SIĘ ZABEZPIECZYĆ?

„Zamawiający wymaga, aby oferowane urządzenia posiadały pełną funkcjonalność (w tym wydajność i parametry bezpieczeństwa) w trybie całkowitej izolacji od sieci zewnętrznych. Jakiekolwiek funkcje wymagające stałego połączenia z infrastrukturą producenta (np. chmurowa weryfikacja licencji) muszą być domyślnie wyłączone”.

„Warunkiem podpisania protokołu odbioru końcowego jest przeprowadzenie testów szczelności (egress testing). Wykrycie jakiejkolwiek nieudokumentowanej w dokumentacji technicznej komunikacji urządzenia z adresami zewnętrznymi będzie traktowane jako wada istotna przedmiotu zamówienia”.

„Wykonawca zobowiązany jest dostarczyć pełną listę komend i parametrów konfiguracyjnych, które podlegają automatycznemu maskowaniu przed wysyłką danych diagnostycznych, wraz z gwarancją ich aktualizacji w całym cyklu życia produktu”.

LISTA KONTROLNA

- **Mapowanie przepływów danych (Data Flow Map)**
Wymagaj kompletnej mapy przepływów (adresy IP, kierunki transmisji, cele przetwarzania, okresy retencji, role podmiotów) jako obligatoryjnego załącznika do oferty, z możliwością objęcia jej tajemnicą przedsiębiorstwa (art. 18 PZP).

- **Weryfikacja techniczna przy odbiorze (Test A1)**
Nie opieraj się na deklaracjach zgodności. Wymagaj przeprowadzenia testów w środowisku z domyślną blokadą ruchu wychodzącego (default-deny) oraz identyfikacji rzeczywistych połączeń inicjowanych przez urządzenie.

- **Kontrola transmisji danych**
Dopuszczaj wyłącznie komunikację jednoznacznie udokumentowaną i uzasadnioną funkcjonalnie; każda dodatkowa transmisja powinna podlegać zatwierdzeniu lub stanowić podstawę do odmowy odbioru.

- **Minimalizacja danych i telemetria**
Ogranicz przetwarzanie do danych niezbędnych do działania usługi („required service data”). Wymagaj trwałej możliwości wyłączenia telemetrii oraz funkcji przesyłających dane o charakterze diagnostycznym lub analitycznym.

LISTA KONTROLNA

- **Niezależność operacyjna od producenta**
  Wymagaj, aby podstawowe funkcje urządzenia działały bez stałego połączenia z infrastrukturą producenta (tryb offline / on-premise / proxy kontrolowane przez zamawiającego).

- **Zarządzanie aktualizacjami i wsparciem (EoS)**
  Wymagaj wskazania konkretnej daty zakończenia wsparcia (End-of-Support) już na etapie zakupu oraz zapewnienia minimalnego okresu aktualizacji bezpieczeństwa (co najmniej 5 lat, zgodnie z kierunkiem CRA).

- **Aktualizacje bezpieczeństwa pod kontrolą zamawiającego**
  Zapewnij możliwość instalowania aktualizacji bez bezpośredniej komunikacji urządzenia z serwerami producenta (repozytorium lokalne / kontrolowany kanał dystrybucji).

- **Audytowalność i kontrola infrastrukturalna**
  Zastrzeż prawo do monitorowania i analizy ruchu sieciowego oraz weryfikacji zachowania urządzeń w trakcie eksploatacji.

DZIĘKUJĘ ZA UWAGĘ!

Adam Behan

Dr nauk prawnych | Katedra Prawa Karnego UJ

Wydział Informatyki, Elektroniki i Telekomunikacji AGH

Urząd Ochrony Danych Osobowych

ul. Stanisława Moniuszki 1A, 00-014 Warszawa

www.uodo.gov.pl

kancelaria@uodo.gov.pl