FUNDACJA PANOPTYKON

Warszawa, 4 maja 2018 r.

Stanowisko Fundacji Panoptykon[1]

w sprawie projektu ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[2]

Projekt ustawy stanowi próbę implementacji do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady 2016/680 z 27 kwietnia 2016 r.[3] (**dalej: dyrektywa, dyrektywa policyjna**).

Jak zwrócił uwagę unijny prawodawca, szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych – technologia pozwala na przetwarzanie danych na niespotykaną dotąd skalę w celu prowadzenia takich czynności, jak zapobieganie przestępczości. „Aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić prawa osób, których dane dotyczą oraz obowiązki podmiotów, które przetwarzają dane osobowe, jak i odpowiadające im uprawnienia w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych w państwach członkowskich" (por. motyw 7 dyrektywy).

Dotychczasowy sposób i tempo prac nad wdrożeniem dyrektywy do polskiego porządku prawnego, a także jakość przedłożonego do konsultacji projektu wskazują, że realna i skuteczna ochrona danych osobowych przetwarzanych w sektorze bezpieczeństwa nie jest traktowana przez projektodawcę priorytetowo. Wyrażamy ubolewanie, że projekt został opublikowany niemal po dwóch latach od przyjęcia dyrektywy i jednocześnie niecałe trzy tygodnie przed upływem czasu wyznaczonego na jej implementację. Aktualny stan prac przesądza o **naruszeniu przez Polskę artykułu 63 dyrektywy nakładającego na państwa członkowskie obowiązek transpozycji przepisów do 6 maja 2018 r.**

Jednocześnie analizując zasady ochrony danych osobowych w obszarze bezpieczeństwa należy przypomnieć o regulacjach wyższego rzędu, które stanowią wskazówkę, w jaki sposób uregulować ten obszar. I tak Konstytucja Rzeczypospolitej w art. 51 zapewnia każdemu obywatelowi prawo do zachowania autonomii informacyjnej. Zgodnie z ust. 3 tego artykułu, każdemu przysługuje prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Z kolei ustęp 4 przyznaje każdemu obywatelowi prawo do żądania sprostowania lub usunięcia informacji nieprawdziwych, niepełnych czy zebranych w sposób sprzeczny z prawem. Uprawnienia te nie mają oczywiście charakteru absolutnego, niemniej ich ograniczenia

[1] Stanowisko przygotowane przez Wojciecha Klickiego.
[2] Projekt w wersji z dnia 18 kwietnia 2018 r.
[3] Dyrektywa Parlamentu Europejskiego i Rady 2016/680 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

dopuszczalne są wyłącznie po spełnieniu wymogów konstytucyjnych wynikających z art. 31 ust. 3 Konstytucji. Podobne regulacje zawiera Karta Praw Podstawowych Unii Europejskiej (por. art. 8 Karty). **Ani Konstytucja, ani Karta Praw Podstawowych nie uzależniają samego faktu ochrony prawa do prywatności i ochrony danych osobowych od tego, jaki podmiot i w jakim celu przetwarza dane osobowe.**

W pierwszej części naszego stanowiska przedstawiamy ogólną ocenę projektu. W drugiej części odnosimy się do konkretnych propozycji legislacyjnych. Na tę część składa się omówienie:

a. proponowanych ograniczeń praw jednostki;

b. środków ochrony prawnej i odpowiedzialności prawnej;

c. zakresu ustawy, definicji i pozostałych propozycji.

1. Ogólna ocena projektu

Porównanie rozwiązań wynikających z dyrektywy oraz projektu wskazuje, że projekt w ogromnym stopniu ogranicza prawa podmiotu danych, m.in. uzależniając możliwość ich realizacji od wykazania interesu przez podmiot danych, a także wprowadzając nieznane dyrektywie przesłanki umożliwiające odmowę udostępnienia informacji, m.in. ze względu na ochronę informacji niejawnych. Wykorzystanie tej podstawy do ograniczenia praw jednostki nie będzie podlegać kontroli Prezesa Urzędu Ochrony Danych Osobowych.

Uprawnienia Prezesa Urzędu, w szczególności związane z podejmowaną na wniosek podmiotu danych kontrolą zgodności działań właściwych organów z prawem, są niejasne i niespójne.

Zakres projektu wyłącza spod jej stosowania wszystkie służby specjalne, mimo że ma to uzasadnienie wyłącznie w przypadku działań związanych z bezpieczeństwem narodowym. Tymczasem trudno przyjąć, że np. działania CBA związane z korupcją w sporcie dotyczą bezpieczeństwa narodowego.

Podsumowując, szczegółowa analiza projektu prowadzi do wniosku, że intencją projektodawców było jedynie fasadowe wdrożenie przepisów dyrektywy. Dowodzi tego liczba zaproponowanych rozwiązań, które w jednoznaczny sposób wykraczają poza rozwiązania przyjęte w dyrektywie.

2. Uwagi szczegółowe

a. ograniczenia praw osoby, której dane dotyczą

- **Art. 24 ust. 1 – „z zastrzeżeniem przepisów ustawy o ochronie informacji niejawnych"**

Zgodnie z projektem, osobie, której dane dotyczą przysługuje prawo do uzyskania od administratora różnych informacji, **z zastrzeżeniem przepisów ustawy o ochronie informacji niejawnych.** Jednocześnie w art. 24 ust. 3 projektodawca wprowadza katalog sytuacji, w których administrator nie przekazuje informacji osobie, której dane dotyczą.

Wprowadzone sformułowanie „z zastrzeżeniem przepisów ustawy o ochronie informacji niejawnych" jest zatem dodatkową (względem katalogu wymienionego w ust. 3) przesłanką umożliwiającą nierealizowanie uprawnienia jednostki i nieprzekazanie informacji o przetwarzanych danych. Ograniczenie to ma tym większe znaczenie, że zgodnie z art. 28 ust. 1 projektu, osoba, której dane dotyczą może m.in. zwrócić się do Prezesa Urzędu o weryfikację zasadności zastosowania przez administratora przesłanek, o których mowa w art. 24 ust. 3[4]. Innymi słowy, jeśli administrator nie przekaże podmiotowi danych informacji, o których mowa w art. 24 ust. 1 **powołując się na przewidziane w tej jednostce redakcyjnej zastrzeżenie dotyczące ustawy o ochronie informacji niejawnych**, działanie to pozostanie poza kontrolą Prezesa Urzędu Ochrony Danych Osobowych.

W naszej ocenie omawiany przepis wprowadza daleko idące, nieuzasadnione (uzasadnienie do projektu nie porusza tej kwestii) i niezgodne z dyrektywą ograniczenie praw jednostki.

- **Art. 24 ust. 3 – podstawy ograniczenia prawa do informacji oraz prawa do uzupełnienia/sprostowania/usunięcia danych**

Zgodnie z projektem, administrator nie przekazuje osobie, której dane dotyczą, informacji, o których mowa w art. 24 ust. 1 oraz 25 ust. 1 (w związku z art. 25 ust. 2), a także nie dokonuje uzupełnienia, aktualizacji, sprostowania albo usunięcia danych osobowych (w związku z art. 26 ust. 3). Artykuł 24 ust. 3 ma więc fundamentalne znaczenie jako podstawa do ograniczania praw osób, której dane dotyczą.

Przesłanki umożliwiające ograniczenie praw informacyjnych jednostki wymienia art. 13 ust. 3 dyrektywy. **Naszym zdaniem projektodawca wykroczył poza przesłanki wskazane w dyrektywie**.

- **Brak przesłanki niezbędności i proporcjonalności ograniczenia**

Przede wszystkim, dyrektywa umożliwia ograniczenie prawa do informacji wyłącznie w sytuacji, w której jest to konieczne i proporcjonalne w społeczeństwie demokratycznym. Projektodawca nie wprowadził analogicznego rozwiązania.

- **Czynności operacyjno-rozpoznawcze**

Przewidziane w dyrektywie dopuszczalne ograniczenia praw jednostki wiążą się z zagrożeniami, które może wywołać ujawnienie informacji (np. związanymi z bezpieczeństwem publicznym czy narodowym) lub ze sprawnym przeprowadzeniem czynności urzędowych i zapobieganiem przestępczości. Tymczasem zgodnie z projektem (art. 24 ust. 3 pkt 1) nie mogą być ujawniane informacje uzyskane w wyniku czynności operacyjno-rozpoznawczych. Oznacza to, że projektodawca przyjął **źródło informacji**, jako kryterium umożliwiające odmowę realizacji prawa jednostki. Jednak pozyskanie informacji w ramach czynności operacyjno-rozpoznawczych nie zawsze będzie wiązać się z jedną z przesłanek przewidzianych w dyrektywie, zwłaszcza w obliczu upływu czasu od przeprowadzenia czynności operacyjno-rozpoznawczych.

[4] W art. 28 ust. 1 pkt 2 mowa jest o możliwości weryfikacji przez Prezesa zasadności zastosowania przez administratora przesłanek, o których mowa w **art. 24 ust. 2**, art. 25 ust. 2 oraz art. 26 ust. 3, jednak z kontekstu propozycji należy wnioskować, że projektodawca miał na myśli art. 24 ust. **3**.

- **Art. 24 ust. 4 (uzależnienie prawa do informacji od ochrony żywotnych interesów osoby, której dane dotyczą) [w związku z art. 25 ust. 3, art. 26 ust. 4]**

Zgodnie z projektem, administrator może przekazać osobie, której dane dotyczą, informacje (…), w przypadku, gdy **ich ujawnienie byłoby niezbędne do ochrony jej żywotnych interesów lub innej osoby**. Analogiczne przepisy dotyczą uprawnienia jednostki do uzupełnienia, aktualizacji, sprostowania albo usunięcia danych osobowych.

Dyrektywa nie przewiduje takiej podstawy ograniczenia praw jednostki. Zarówno dyrektywa, jak i Konstytucja nie uzależnia możliwości realizacji prawa informacyjnego od istnienia interesu osoby zainteresowanej. Ograniczenie to podważa istotę całej grupy przepisów normujących prawa osoby, której dane dotyczą.

- **Art. 25 ust. 1 – zakres informacji, jakie uzyskać może osoba, której dane dotyczą (odbiorcy danych oraz wskazanie, jakie dane są przetwarzane oraz wszelkich dostępnych informacji o ich pochodzeniu)**

Zgodnie z projektem, osoba, której dane dotyczą, może wystąpić do administratora z wnioskiem o uzyskanie wskazanych w art. 25 ust. 1 informacji.

Zwracamy uwagę, że:

- zgodnie z dyrektywą (art. 14 lit. c) prawo do informacji obejmuje informacje o **odbiorcach lub kategoriach odbiorców**, którym dane osobowe zostały ujawnione. Tymczasem projekt bezpodstawnie ogranicza zakres tych informacji jedynie do kategorii odbiorców. Innymi słowy, projektodawcy w sposób nieuzasadniony ograniczyli prawo dostępu do informacji o konkretnych odbiorcach danych;
- zgodnie z dyrektywą (art. 14 lit. g) podmiotowi danych przysługuje prawo do wskazania, jakie dane osobowe są przetwarzane oraz wszelkich dostępnych informacji o ich pochodzeniu. **To uprawnienie zostało w całości pominięte przez projektodawców.**

- **Art. 26 ust. 1 pkt 2 – prawo do żądania usunięcia danych**

Zgodnie z art. 26 ust. 1 pkt 2 projektu, osobie, której dane dotyczą przysługuje możliwość wystąpienia z wnioskiem do administratora o niezwłoczne usunięcie danych osobowych w przypadku, gdy dane – **znajdujące się w jawnych zbiorach danych osobowych** – zostały zebrane z naruszeniem przepisów. Niezrozumiałe i wykraczające poza regulacje przewidziane w dyrektywie jest ograniczenie tego uprawnienia jedynie do danych znajdujących się w jawnych zbiorach danych.

b. środki ochrony prawnej i odpowiedzialność prawna

Dyrektywa w art. 52 przyznaje każdej osobie, której dane dotyczą, prawo wniesienia skargi do organu nadzorczego. To fundamentalne dla całego systemu ochrony danych przewidzianego

w dyrektywie prawo jednostki do poddania kontroli zgodności z prawem przetwarzania jej danych osobowych.

Tymczasem w artykule 50 projektu przewidziana została możliwość złożenia zażalenia do Prezesa Urzędu, natomiast w art. 26 ust. 7 – prawo zwrócenia się do Prezesa z wnioskiem „o nakazanie dopełnienia obowiązku" (informacyjnego), art. 28 ust. 1 pkt 2 przewiduje możliwość wystąpienia do Prezesa z wnioskiem o „weryfikację zasadności zastosowania przez administratora przesłanek (…)". Jednocześnie zgodnie z art. 13 projektu postępowanie w sprawach uregulowanych w ustawie prowadzi się na podstawie Kodeksu postępowania administracyjnego.

Zaproponowane przepisy dotyczące weryfikacji rozmaitych działań właściwych organów (np. ograniczenia prawa do informacji) są niejasne i niespójne. Dla przykładu, artykuł 51 przyznaje jednostce uprawnienie do zwrócenia się do Prezesa z wnioskiem o ponowne rozpatrzenie sprawy. Prezes Urzędu rozpatruje wniosek o ponowne rozpatrzenie sprawy i informuje osobę, która wystąpiła z wnioskiem o ponowne rozpatrzenie sprawy, o sposobie jej rozstrzygnięcia (ust. 3). Projekt nie przewiduje jednakże, w jaki sposób rozstrzygany jest taki wniosek.

- **Art. 54 – prawo do skutecznego środka prawnego przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu dane**

Autorzy projektu nie wdrożyli art. 54 dyrektywy, który zobowiązuje Państwa członkowskie do przyznania jednostkom prawa do skutecznego środka prawnego przed sądem przeciwko administratorowi lub podmiotowi przetwarzającemu. To jedno z podstawowych uprawnień jednostki umożliwiające jej nie tylko dochodzenia realizacji takich praw, jak prawo do informacji, ale także ubieganie się o odszkodowanie za naruszenie ochrony danych.

Na marginesie zwracamy uwagę, że analogiczny przepis zawarty jest w przyjętym przez Radę Ministrów projekcie ustawy o ochronie danych osobowych.

c. Zakres ustawy, definicje i pozostałe uwagi

- **art. 1 – zakres ustawy**

Zgodnie z projektem przepisów ustawy nie stosuje się m.in. do ochrony danych osobowych przetwarzanych „w związku z zapewnieniem bezpieczeństwa narodowego, w tym w ramach realizacji zadań ustawowych ABW, AW, SKW, SWW oraz CBA".

Zgodnie z dyrektywą, jej przepisy nie znajdują zastosowania do przetwarzania danych osobowych w zakresie bezpieczeństwa narodowego. Pojęcie to nie jest jednak zdefiniowane. Jego wykładni należy zatem poszukiwać na gruncie art. 73 Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którym państwa członkowskie mogą organizować współpracę między służbami odpowiedzialnymi właśnie za zapewnienie bezpieczeństwa narodowego. Jak zwracają uwagę autorzy komentarza[5] do tego przepisu *„Bezpieczeństwo narodowe* (ang. *national security*) najczęściej rozumiane jest jako jedna z podstawowych funkcji każdego państwa, która obejmuje

[5] Miąsik Dawid (red.), Półtorak Nina (red.), Wróbel Andrzej (red.), Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom I (art. 1-89)

problematykę przeciwstawienia się wszelkim zagrożeniom zewnętrznym oraz wewnętrznym dla istnienia oraz rozwoju narodu i państwa".

Nie sposób zgodzić z zaproponowanym przez projektodawcę podejściem, że wszystkie działania podejmowane przez służby specjalne (ABW, AW, SKW, SWW i CBA) mieszczą się w zakresie tego pojęcia. Szczególnie jest to widoczne w kontekście zadań ustawowych Centralnego Biura Antykorupcyjnego, wśród których wymienić można rozpoznawanie, zapobieganie i wykrywanie przestępstw przeciwko zasadom rywalizacji sportowej.

Należy przy tym zwrócić uwagę, że bez względu na zakres dyrektywy policyjnej, konieczność ochrony danych osobowych w służbach specjalnych wynika także z omawianych na wstępie zasad konstytucyjnych. Tymczasem w obecnym brzmieniu projektu nie sposób dopatrzeć się zasad, na jakich przetwarzane i chronione będą dane osobowe np. w ABW.

- **art. 3 – definicja danych osobowych (w związku z art. 18 dotyczącym zasad postępowania ze zbędnymi danymi osobowymi)**

Projekt narusza zawartą w dyrektywie definicję danych osobowych (art. 3 pkt 1 dyrektywy). Po pierwsze, wiąże uznanie informacji na temat konkretnej osoby za dane osobowe z celem, w jakim te informacje są przetwarzane (ust. 1). Po drugie, projekt wprowadza nieznane dyrektywie, a także RODO, ograniczenie, zgodnie z którym „informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań" (ust. 3).

Takie rozwiązanie, wbrew informacji zawartej w uzasadnieniu, jest niezgodne z dyrektywą oraz RODO. Zaproponowana definicja, zaczerpnięta z obowiązującej ustawy o ochronie danych osobowych z 1997 r., ma istotne znaczenie także w kontekście art. 18 projektu, zgodnie z którym dane uznane za zbędne można przekształcić w taki sposób, że przyporządkowanie informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej wymagałoby nadmiernych kosztów, czasu lub działań. Oznacza to, że takie przyporządkowanie **będzie możliwe**, a więc zbędne dane nie będą usuwane ani anonimizowane w skuteczny sposób.

- **art. 4 pkt 11 – definicja organu właściwego**

Zgodnie z dyrektywą „właściwym organem" może być nie tylko organ publiczny, ale także inny organ lub podmiot, któremu prawo państwa członkowskiego powierza sprawowanie władzy publicznej i wykonywanie uprawnień publicznych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom (por. art. 3 pkt 7 lit. b dyrektywy).

Z kolei w art. 4 pkt 11 projektu organ właściwy zdefiniowany jest jako **organ** uprawniony na podstawie odrębnych przepisów do przetwarzania danych osobowych w celach określonych w art. 1 ust. 1 pkt 1 projektu. Użycie przez projektodawcę słowa **organ** nasuwa wątpliwość, czy projektodawca nie ograniczył tej definicji jedynie do instytucji publicznych.

W polskim systemie prawnym istnieją rozwiązania upoważniające instytucje prywatne do przetwarzania danych osobowych w celu przeciwdziałania przestępczości. Zgodnie z art. 38 ustawy z 20 marca 2009 r. o bezpieczeństwie imprez masowych, organizatorzy takich imprez

uprawnieni są do przetwarzania w niektórych sytuacjach danych osobowych w celu zapobiegania przestępstwom i wykroczeniom związanym z imprezami masowymi (por. art. 35 ustawy o bezpieczeństwie imprez masowych). Jednocześnie zgodnie z art. 2 ust. 2 lit. d RODO, ogólne rozporządzenie o ochronie danych osobowych nie ma zastosowania do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości.

Ze względu na uprawnienia osób, których dane są przetwarzane, a także w celu uniknięcia niejasnej sytuacji prawnej, w naszej ocenie ustawodawca powinien jednoznacznie rozstrzygnąć, że definicja „właściwych organów", o których mowa w projekcie, obejmuje także podmioty prywatne, którym przepisy powierzają wykonywanie określonych zadań w związku z przeciwdziałaniem przestępczości.

- **art. 9 ust. 3 – dane zebrane z naruszeniem prawa**

Prezes Urzędu Ochrony Danych Osobowych w przypadku naruszenia przepisów o ochronie danych osobowych upoważniony będzie do nakazania administratorowi m.in. usunięcia danych osobowych. Jednak zgodnie z art. 9 ust. 3 projektu decyzja ta nie będzie mogła dotyczyć danych zebranych w toku czynności operacyjno-rozpoznawczych. W takiej sytuacji administrator jest zobowiązany jedynie do niezwłocznego przywrócenia zgodnego z prawem sposobu przetwarzania danych.

Po pierwsze zwracamy uwagę, że możliwość żądania usunięcia danych zebranych sprzecznie z prawem jest wartością konstytucyjną wynikającą z art. 51 ust. 4 Konstytucji.

Po drugie, możliwa jest sytuacja, w której nie będzie możliwości przywrócenia zgodnego z prawem sposobu przetwarzania danych w sposób inny, niż poprzez ich usunięcie. Przykładem takiej sytuacji jest pozyskanie przez właściwy organ danych osobowych objętych tajemnicą obrończą lub pobieranie przez Policję danych telekomunikacyjnych w sprawach dotyczących wykroczeń.

Po trzecie, Prezes Urzędu może stwierdzić naruszenie art. 14 projektu, zgodnie z którym właściwe organy przetwarzają dane osobowe wyłącznie w zakresie **niezbędnym** do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. W takiej sytuacji również nie ma możliwości przywrócenia stanu zgodnego z prawem w inny sposób, niż poprzez usunięcie danych.

Proponowany przepis prowadzi więc do wniosku, że mimo stwierdzenia przez Prezesa Urzędu, że właściwy organ przetwarza dane osobowe z naruszeniem prawa, dane te będą wciąż przetwarzane.

- **Art. 17 i art. 18 – retencja danych**

Zgodnie z art. 17 projektu, administrator dokonuje weryfikacji danych osobowych w terminach określonych przez przepisy szczególne, a jeśli nie określają one terminu – nie rzadziej niż co 10 lat. Weryfikacja dokonywana jest w celu ustalenia, czy istnieją dane, których dalsze przechowywanie jest zbędne. Zbędne dane są usuwane lub – na podstawie art. 18 – anonimizowane lub pseudonimizowane (por. uwagi do art. 3 projektu).

Cykliczna weryfikacja zasadności przechowywania danych osobowych nie jest nowym rozwiązaniem w polskim porządku prawnym (por. np. art. 20 ust. 17 ustawy o Policji). Jednak to

rozwiązanie jest niezgodne z przyjętą przez unijnego prawodawcę zasadą domyślnej ochrony danych (por. motyw 53 dyrektywy). W wypadku komentowanego przepisu wymaga ona odwrócenia zasady cyklicznej weryfikacji dalszej przydatności przechowywania danych w taki sposób, by zasadą było niszczenie danych, a po upływie wskazanego okresu przechowywanie jedynie tych danych, które wciąż są niezbędne.

- **Art. 20 i art. 21 – rozróżnienie danych**

W pierwszej kolejności zwracamy uwagę na sformułowanie zawarte w art. 20, zgodnie z którym administrator zapewnia podział na dane osobowe, **„o ile rozróżnienie to jest niemożliwe lub dalece utrudnione”**. Zakładamy, że brzmienie projektu nie jest tożsame z intencją projektodawców.

Zakładając, że projektodawca zamierzał wprowadzić rozróżnienie danych w zależności od kategorii osób, które one dotyczą, a także w zależności od tego, czy dane mają swe źródło w faktach czy w indywidualnych ocenach, zwracamy uwagę, że dyrektywa wymaga nie tylko wprowadzenia tego typu kategoryzacji, ale przede wszystkim – wyciągnięcia z tych podziałów konsekwencji, np. w zakresie długości przechowywania danych – zgodnie z zasadą uwzględniania ochrony danych w fazie projektowania oraz domyślną ochroną danych.