FUNDACJA PANOPTYKON

Warszawa, 28 lutego 2020 r.

Uwagi Fundacji Panoptykon[1] do projektu Kodeksu postępowania w zakresie przetwarzania danych osobowych w organizacji społecznych[2]

1. Uwagi ogólne: deklarowany cel projektu a jego realny kształt

Zgodnie z deklaracjami autorów projektu, celem Kodeksu postępowania w zakresie przetwarzania danych osobowych w organizacjach społecznych (dalej: projekt) jest m.in. „ułatwienie skutecznego stosowania RODO" oraz „budowa dobrego wizerunku organizacji pozarządowych oraz zaufania pomiędzy organizacjami pozarządowymi a ich beneficjantami, kontrahentami, darczyńcami a także innymi interesariuszami organizacji pozarządowych".

Doceniamy, że autorzy projektu – na poziomie deklaracji – dostrzegli, że przestrzeganie RODO może stanowić podstawę do budowy zaufania pomiędzy organizacjami społecznymi a odbiorcami ich działań.

Niestety, w naszej ocenie projekt kodeksu nie realizuje założonych celów, lecz wręcz przeciwnie: poprzez niejasność konstrukcyjną, pominięcia ważnych dla organizacji obszarów oraz skupienie się na rzekomych wymogach formalnych zamiast podejściu opartym na analizie ryzyka zaciemnia obraz utrudniając organizacjom stosowanie RODO zgodnie z duchem tych przepisów, a w konsekwencji – utrudnia budowę zaufania społecznego do organizacji.

Nieprzydatność kodeksu wynika między innymi z:

a) niemal całkowitego pominięcia obszaru danych wrażliwych

Autorzy projektu nie wzięli pod uwagę różnorodności specyfiki organizacji pozarządowych i nie poświęcili wystarczającej uwagi (przy jednoczesnym podaniu błędnych informacji, o czym będzie mowa poniżej) przetwarzaniu tzw. danych wrażliwych. Tymczasem pośród organizacji pozarządowych aż 7% zajmuje się ochroną zdrowia[3], co z ogromnym prawdopodobieństwem wiąże się z przetwarzaniem przez nie danych o stanie zdrowia odbiorców ich działań.

b) pominięcia niektórych podstaw prawnych przetwarzania danych

Autorzy słusznie zwracają uwagę, że organizacje powinny opierać przetwarzanie danych na zgodzie dopiero wtedy, gdy nie znajdą innych przesłanek legalizujących przetwarzanie danych. Jednocześnie autorzy tylko wspomnieli podstawę prawną wskazaną w art. 6 ust. 1 lit. b, mimo że ma ona fundamentalne znaczenie w działalności organizacji, bo – wbrew twierdzeniom autorów

1 Uwagi przygotowane przez Wojciecha Klickiego.
2 Projekt w wersji z dnia 13 stycznia 2020.
3 Dane za rok 2015, na podstawie: https://publicystyka.ngo.pl/podstawowe-informacje-o-organizacjach-pozarzadowych

projektu[4] jest m.in. główną podstawą prawną przetwarzania danych kontrahentów organizacji. Co więcej, autorzy projektu nie omawiają podstaw prawnych przetwarzania danych wskazanych w art. 6 ust. 1 lit. c-e, jedynie w kilku procesach przetwarzania powołując się na art. 6 ust. 1 lit. c – bez wskazania podstawowych informacji na temat tej podstawy prawnej. Tymczasem np. dla organizacji prowadzących taką działalność jak zapewnienie oświaty, opieki zdrowotnej i pomocy społecznej, kluczową podstawą przetwarzania danych będzie art. 6 ust. 1 lit. e.

Zwracamy przy tym uwagę, że jedynie przy omawianiu zgody jako podstawy prawnej przetwarzania danych, poruszono temat **praw osób, których dane dotyczą i które wyraziły zgodę na ich przetwarzanie**. Poruszenie tego wątku wyłącznie w ramach omawiania zgody rodzi błędne wrażenie, że np. prawo do sprostowania danych czy dostępu do nich nie obejmuje przetwarzania danych z wykorzystaniem innych podstaw prawnych niż zgoda

Podobne uwagi należy sformułować w kontekście przetwarzania danych wrażliwych. Zgodnie z informacjami zawartymi na stronie 4 projektu, organizacja może przetwarzać dane, o których mowa w art. 9 RODO na podstawie wskazanej w art. 9 ust. 2 lit. d lub na podstawie zgody. Tymczasem istnieją inne podstawy przetwarzania tzw. danych wrażliwych, jak np. wskazana w art. 9 ust. 2 lit. c niezbędność do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej, a osoba, której dane dotyczą jest fizycznie lub prawnie niezdolna do wyrażenia zgody. Taka podstawa prawna może być istotna w związku z prowadzeniem, pominiętej przez autorów, działalności w obszarze ochrony zdrowia.

c) forma projektu

Zgodnie z wytycznymi 1/2019 Europejskiej Rady Ochrony Danych z dnia 4 czerwca 2019 r. w sprawie kodeksów postępowania[5], dwa z kryteriów zatwierdzenia kodeksu to ułatwienie skutecznego zastosowanie RODO w konkretnym sektorze oraz uszczegółowienie przepisów. EROD kładzie szczególny nacisk na takie przedstawienie zawartości kodeksu, które jest zrozumiałe, zwłaszcza dla osób, które nie zajmują się zawodowo prawem, oraz realnie ułatwia stosowanie RODO w konkretnym sektorze. EROD podkreśla także, że kodeks nie powinien powtarzać treści przepisów rozporządzenia, tylko podawać jasne i precyzyjne zasady uszczegóławiające przepisy RODO. Naszym zdaniem projekt kodeksu w obecnym kształcie nie spełnia tych kryteriów ze względu na swój stopień skomplikowania oraz długość. Uważamy, że nie służy to ułatwieniu interpretacji RODO, ale wręcz ją komplikuje, zwłaszcza z perspektywy małych organizacji pozarządowych. Wskazane byłoby np. zastosowanie wykresów czy tabelek, które porównywałyby np. właściwe podstawy prawne w różnych sytuacjach i konsekwencje przyjęcia takiej a nie innej podstawy.

Uderzająca jest też niespójność kodeksu – o ile niektóre części kodeksu są przejrzyste i zrozumiałe, o tyle inne (np. poświęcone innym niż wycofanie zgody uprawnieniom podmiotów danych) ograniczają się do hasłowych wzmianek, bez wyjaśnienia praktycznych wątpliwości związanych z tymi przepisami. W konsekwencji projekt nie będzie pomocny w działaniu organizacji.

---

[4] Na stronie 63 projektu autorzy wskazują, że podstawą prawną przetwarzania danych w celu kontaktu z kontrahentami jest art. 6 ust. 1 lit. f. Jednak w typowej sytuacji kontakt z kontrahentami odbywa się w celu realizacji umowy, a więc ich dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit b RODO.

5 Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, Version 2.0, dostępne pod adresem:
https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf.

2. Uwagi szczegółowe

Projekt zawiera szereg daleko kontrowersyjnych tez, dlatego ograniczymy się do wskazania wyłącznie kilku z nich.

a) „papierologia" zamiast podejścia opartego na analizie ryzyka (środki bezpieczeństwa)

Zgodnie z art. 32 RODO, administrator powinien zastosować różne środki techniczne uwzględniając **ryzyko naruszenia praw lub wolności osób fizycznych.** Wdrażane zabezpieczenia powinny bowiem odpowiadać wynikom przeprowadzonej w organizacji oceny ryzyka.

Tymczasem zgodnie z projektem organizacja „ustala możliwe do zastosowania środki bezpieczeństwa i ocenia koszt ich wdrożenia". Wobec braku jednoznacznej informacji, że kryterium decydującym o zastosowaniu różnych środków ochrony jest ocena ryzyka, kodeks wprowadza mylne wrażenie, że liczne wymienione w nim środki bezpieczeństwa **są obowiązkowe** (ewentualnie, że kryterium decydującym są koszty wdrożenia danych). Szczególnie rażące jest to w kontekście zabezpieczeń organizacyjnych i prawnych, bowiem:

- wbrew projektowi powołanie Inspektora Ochrony Danych Osobowych (IOD) nie jest obowiązkowe (por. art. 37 RODO);
- wbrew projektowi[6] przyjęcie polityki ochrony danych osobowych nie jest obowiązkowe.

Z rozdziału tego wynika zatem, że organizacje – zamiast stosować środki bezpieczeństwa adekwatne do ryzyk – powinny skupić się na papierologii i „szafach zgodnych z RODO" (projekt przewiduje konieczność przechowywania akt w zamykanych na klucz szafach). Zastosowanie środków zabezpieczenia danych jest istotne z punktu widzenia zasady integralności danych, a prowadzenie dokumentacji może sprzyjać realizacji zasady rozliczalności, ale przedstawienie tych zagadnień jako obowiązkowych, a nie uzależnionych od oceny ryzyka, wprowadza odbiorców kodeksu w błąd.

b) Wymuszanie zmiany haseł

Zgodnie z załączonym wzorem Instrukcji zarządzania systemami informatycznymi hasła dostępu do serwera, sieci czy programów wykorzystywanych przez organizacje muszą być zmieniane nie rzadziej niż raz na 60 dni, a zmiana ta jest wymuszana przez system.

W naszej ocenie takie podejście stoi w sprzeczności z aktualną wiedzą na temat tego problemu, a jednocześnie pomija skutecznie metody zapewnienia integralności danych. Zgodnie z informacjami wskazanymi na portalu UODO[7] „wymóg częstych zmian powoduje, że użytkownicy tworzą słabe hasła lub po prostu nieznacznie modyfikują swoje obecne. Istnieje wiele dowodów sugerujących, że użytkownicy, którzy są zobowiązani do zmiany swoich haseł, często wybierają słabsze hasła, a następnie zmieniają je w przewidywalny sposób np. poprzez zwiększanie liczby, zmiany litery na podobnie wyglądający symbol … usuwanie znaku specjalnego … albo przełączanie kolejności cyfr lub znaków specjalnych".

6 Por. Punkt I – Podstawa prawna Polityki ochrony danych osobowych stanowiącej załącznik nr 3 do projektu.

7 https://techinfo.uodo.gov.pl/hasla-praktyczne-wskazowki-czy-naprawde-trzeba-zmienic-haslo-co-30-dni/

Jednocześnie Instrukcja zarządzania systemami informatycznymi pomija uznawanie aktualnie za najbardziej skuteczne metody zapewnienia integralności danych, a mianowicie wykorzystywanie menadżerów haseł oraz uwierzytelniania dwuetapowego.

3. Forma przeprowadzania konsultacji – formularz uwag

Na marginesie zwracamy uwagę, że konsultacje projektu kodeksu prowadzone są przy wykorzystaniu „formularza konsultacji Kodeksu postępowania w zakresie przetwarzania danych osobowych w organizacjach społecznych". Zgodnie z klauzulą informacyjną udostępnioną na jego końcu, dane osobowe uczestnika konsultacji przetwarzane są na podstawie art. 6 ust. 1 lit. f RODO (uzasadniony interes) i będą przechowywane **bezterminowo**. „W każdej chwili przysługuje Panu/Pani prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych. W takim przypadku dane podane przez Pana/Panią w niniejszym formularzu zostaną usunięte niezwłocznie po upływie przewidzianego w przepisach prawa okresu przedawnienia ewentualnych roszczeń".

W naszej ocenie nie ma najmniejszych podstaw dla bezterminowego przechowywania danych użytkowników konsultacji, zwłaszcza że organizatorzy (niejako przy okazji) wskazują, kiedy bez wątpienia ich uzasadniony interes przestanie obowiązywać, a mianowicie po upływie przewidzianego w przepisach prawa okresu przedawnienia ewentualnych roszczeń.

4. Podsumowanie: zły pomysł

Kodeksy postępowania są niezwykle potrzebnym instrumentem, który może pomóc w praktycznym zastosowaniu RODO i może realnie ułatwić pracę podmiotom go stosującym, zwłaszcza małym organizacjom społecznym. Dlatego popieramy wszelkie inicjatywy zmierzające do wsparcia organizacji w realizacji RODO. Uznajemy bowiem, że ochrona danych osobowych jest nie tylko obowiązkiem prawnym organizacji, ale także elementem ich odpowiedzialności społecznej, a właściwa realizacja przepisów rozporządzenia może wzmocnić zaufanie do organizacji.

Niemniej naszym zdaniem projekt kodeksu **nie realizuje** zakładanych celów. Po pierwsze, projekt zawiera daleko kontrowersyjne tezy, które – naszym zdaniem – stoją w sprzeczności z rozporządzeniem. Po drugie, kodeks jest nieczytelny i nieprzejrzysty (w szczególności dla osób nie zajmujących się zawodowo ochroną danych osobowych), po trzecie – jego twórcom przyświecało błędne założenie, a mianowicie uznanie, że organizacje społeczne są spójnym, jednolitym środowiskiem, które mierzy się z podobnymi problemami w zakresie przetwarzania danych osobowych. Tymczasem naszym zdaniem organizacje społeczne są zbyt zróżnicowane, by istniała możliwość stworzenia jednego, przydatnego dla wszystkich kodeksu.