NR 6 - PAŹDZIERNIK/LISTOPAD 2021

NEWSLETTER
RODO

W numerze:

Traple
Konarski
Podrecki
& Wspólnicy

TKP

Zapraszamy na szkolenie

25.11.2021
SZKOLENIE ONLINE

Podsumowanie 2021 roku w ochronie danych osobowych

Centrum Promocji Informatyki z Kancelarią Traple Konarski Podrecki i Wspólnicy zapraszają na warsztaty, podczas których zostaną podsumowane aktualne i istotne problemy dot. przepisów o ochronie danych osobowych i ich stosowania, jakie zaistniały w tym roku.

Odpowiemy m.in. na następujące pytania:

- Co wydarzyło się po wyroku TSUE ws. Schrems II i jakie znaczenia ma data 27.09.2021 r.? Jakie kroki należy podjąć, aby prawidłowo przekazywać dane osobowe do państw trzecich?
- Jak prawidłowo powierzać przetwarzanie danych stosując standardowe klauzule umowne KE? Czy standardowe klauzule umowne KE rzeczywiście ułatwiają powierzenie przetwarzania? W jaki sposób uniknąć błędów przy powierzaniu przetwarzania przy pomocy klauzul umownych?
- Co jest głównym powodem naruszeń ochrony danych ochrony wg Prezesa UODO? Jak zarządzać naruszeniami ochrony danych osobowych?
- Co zrobić w przypadku otrzymania od NOYB żądań dot. cookie banera? Jaki wpływ mają ostatnie działania organów nadzorczych na realizację obowiązków w zakresie stosowania plików cookies?
- Co nas czeka w ochronie danych osobowych w 2022 r.?

Rejestacja

Warsztaty poprowadzą specjaliści z zespołu ochrony danych osobowych kancelarii Traple Konarski Podrecki i Wspólnicy:

- adw. prof. INP PAN dr hab. Grzegorz Sibiga
- dr inż. Andrzej Kaczmarek
- r.pr. Dominika Nowak
- adw. Katarzyna Syska
- Mateusz Kupiec

Organizatorzy:

cpi centrum promocji informatyki

TKP Traple Konarski Podrecki & Wspólnicy

Projekt wytycznych CNIL dotyczących rekrutacji

Katarzyna Syska

Francuski organ nadzorczy (CNIL) opublikował projekt wytycznych dotyczących przetwarzania danych osobowych w ramach procesów rekrutacji. Wytyczne zostały przygotowane w formie odpowiedzi na pytania w sprawie przetwarzania danych kandydatów do pracy. Pytania te odnoszą się do 19 zakresów tematycznych, m.in. statusu administratora danych przetwarzanych w toku rekrutacji, podstawy prawnej przetwarzania danych kandydatów, obowiązku informacyjnego wobec kandydatów do pracy, okresu przechowywania danych, używania narzędzi służących do oceny osobowości kandydata, zbierania danych o kandydacie, które są publicznie dostępne w Internecie, używania narzędzi do zautomatyzowanej oceny lub selekcji kandydatów.

Aktualnie prowadzone są konsultacje publiczne dotyczące projektu wytycznych – potrwają one do połowy listopada 2021 r. Spodziewanym terminem publikacji ostatecznej wersji wytycznych jest luty 2022 r.

Poniżej przedstawiamy zawarte w wytycznych stanowiska CNIL co do kilku wybranych zagadnień.

Administratorzy i podmioty przetwarzające w procesie rekrutacyjnym

CNIL zwraca uwagę, że w procesie rekrutacji mogą brać udział bezpośrednio lub pośrednio różne podmioty, w tym pracodawcy, agencje rekrutacyjne, platformy internetowe, agencje pracy tymczasowej, usługodawcy outsourcingowi procesu rekrutacji.

Organ szczegółowo tłumaczy w wytycznych, na podstawie jakich kryteriów należy przypisać poszczególnym podmiotom rolę administratora, współadministratora lub podmiotu przetwarzającego.

CNIL podaje następujące przykłady podmiotów będących administratorami danych kandydatów do pracy:

- pracodawca;
- agencja rekrutacyjna zbierająca dane w celu utworzenia bazy danych kandydatów, z której korzysta w ramach klasycznej działalności pośrednictwa pracy (tzw. headhuntera).

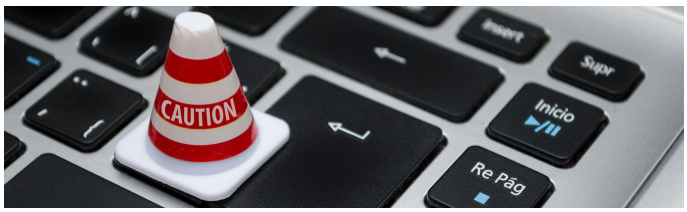
Przykładami podmiotów przetwarzających dane w ramach rekrutacji są:

- usługodawca świadczący całość lub część procesu rekrutacji w imieniu klienta (pracodawcy), który zleca całość lub część tego procesu;
- zewnętrzny usługodawca, któremu administrator powierza zaprojektowanie i hosting swojej strony internetowej i który na zlecenie administratora danych tworzy na stronie funkcjonalność związaną z rekrutacją pracowników (np. pozwalającą na wysyłanie CV);
- podmiot specjalizujący się w organizowaniu testów, o ile rodzaj i zasady przeprowadzania testu są ustalone przez pracodawcę, a uzyskane wyniki są przekazywane pracodawcy.

Przeprowadzanie DPIA

Francuski regulator przedstawił kilka przykładów sytuacji, w których ze względu na wysokie ryzyko naruszenia praw lub wolności osób fizycznych konieczne jest przeprowadzenie oceny skutków dla ochrony danych:

- przetwarzanie danych z sieci społecznościowych i publicznie dostępnych baz danych w celu wyszukania potencjalnych kandydatów na stanowiska kierownicze i skontaktowania się z najlepszymi kandydatami;
- wykorzystanie algorytmu predykcyjnego umożliwiającego znalezienie w bazie ofert pracy propozycji, które są odpowiednie dla umiejętności wskazanych w CV kandydata;
- testowanie kandydatów do pracy za pomocą gier – np. gier logicznych, odgrywania ról (*smart/serious/business games*) – w celu określenia osobowości kandydata lub pomiaru jego umiejętności zawodowych.



Dokonywanie oceny osobowości kandydata do pracy

CNIL zwrócił uwagę, że rekrutujący korzystają z różnego rodzaju narzędzi oceny osobowości kandydata, np. zaklasyfikowania kandydatów do konkretnego „typu osobowości" czy też pomiaru ich wybranych umiejętności, takich jak odporność na stres, kreatywność, praca w zespole itp. W metodach tych chodzi o określenie zachowania kandydata (umiejętności interpersonalnych), a niekoniecznie tego, co wie lub co potrafi zrobić.

Zdaniem francuskiego organu stosowanie tego typu narzędzi – a w konsekwencji zbieranie danych dotyczących osobowości czy szczególnych umiejętności kandydata – może być w pewnych sytuacjach uzasadnione.

Jeśli chodzi o podstawę prawną takiego przetwarzania danych, zdaniem CNIL zgoda ani niezbędność danych do zawarcia umowy nie byłyby właściwymi przesłankami w tym przypadku. Odpowiednią podstawą prawną może być prawnie uzasadniony interes administratora, oczywiście pod warunkiem że jest on nadrzędny wobec praw, wolności i interesów kandydata do pracy.

W związku z tym bardzo ważne jest wykazanie, że dane uzyskane lub wygenerowane za pomocą zastosowanych metod oceny osobowości są rzeczywiście niezbędne i istotne w procesie rekrutacji. Innymi słowy, zastosowanie takich narzędzi jest konieczne do tego, aby ocenić umiejętności zawodowe kandydata i jego zdolność do wykonywania pracy na konkretnym stanowisku.

Ponadto CNIL rekomenduje przeprowadzenie DPIA, aby zidentyfikować i zminimalizować ryzyko naruszenia praw i interesów kandydatów do pracy. Konieczne jest także przejrzyste informowanie kandydatów do pracy o stosowanych metodach oceny osobowości.

Zbieranie danych publicznie dostępnych w Internecie

CNIL podkreślił, że zbieranie danych osobowych kandydatów, które są publicznie dostępne w Internecie, stanowi „przetwarzanie danych", a zatem konieczne jest spełnienie wszystkich wymogów prawnych z tym związanych. Rekrutujący musi m.in. określić cel przetwarzania danych, zapewnić adekwatność i minimalizację gromadzonych danych, ustalić podstawę prawną przetwarzania, a także spełnić obowiązek informacyjny wobec kandydatów do pracy.

CNIL wskazał, że dane osobowe zbierane z publicznie dostępnych źródeł – podobnie jak inne dane kandydata do pracy – mogą być wykorzystywane przez rekrutujących wyłącznie do oceny umiejętności zawodowych kandydata oraz jego zdolności (predyspozycji) do wykonywania pracy na konkretnym stanowisku (wynika to z francuskiego kodeksu pracy).

Francuski organ podał też przykłady sytuacji, w których zbieranie publicznie dostępnych online danych o kandydatach jest dopuszczalne:

- Gdy zbieranie danych z publicznie dostępnych źródeł online następuje z inicjatywy rekrutującego i ma na celu uzupełnienie lub ocenę spójności informacji dostarczonych przez kandydata, np. rekrutujący zbiera informacje ogólnie dostępne o kilku kandydatach, których wybrał do ostatniego etapu rekrutacji. Z uwagi na dużą ilość danych dostępnych w Internecie rekrutujący musi uważnie wybierać dane, które przegląda, i brać pod uwagę tylko te, które są adekwatne oraz ściśle związane z działalnością zawodową kandydatów, jak np. ich profile w serwisie społecznościowym dla profesjonalistów.

- Gdy kandydat z własnej inicjatywy zwrócił uwagę rekrutującego na określone treści online w celu uzupełnienia lub zilustrowania pewnych umiejętności lub informacji przekazanych rekrutującemu, np. kandydat na stanowisko grafika przekazuje w ramach podania link do bloga, na którym publikuje swoje obrazy/grafiki. Tego rodzaju treści mogą być uznane za wyraźnie związane z działalnością zawodową kandydata i konieczne do oceny jego umiejętności.

Datatilsynet publikuje wytyczne dotyczące wykorzystania danych osobowych do testowania systemów informatycznych

Mateusz Kupiec

Testowanie systemów informatycznych ma dostarczać informacji zwrotnej, czy tworzony system spełnia wszystkie wymagania i założenia jego twórców. W zależności od przeznaczenia i specyfiki konkretnego projektu na potrzeby testowania systemu informatycznego mogą być wykorzystywane dane osobowe osób fizycznych. Duński organ nadzorczy z zakresu ochrony danych osobowych (Datatilsynet) opublikował wytyczne, które mogą pomóc administratorom przeprowadzającym walidację i weryfikację działania systemów informatycznych na podstawie informacji pozwalających na bezpośrednią lub pośrednią identyfikację osób fizycznych. Datatilsynet w szczególności wskazuje na następujące kwestie:

- Na potrzeby opracowywania i eksploatacji systemu informatycznego co do zasady wykorzystywane są fikcyjne dane testowe oraz dane produkcyjne, które są zazwyczaj danymi pochodzącymi z już działającego systemu (np. informacje o klientach znajdujące się w systemie obsługi klienta). Niekiedy jednak wykorzystuje się w tym celu dane produkcyjne, które stają się w takim przypadku danymi testowymi. Organ przypomina, że prawo nie przewiduje niższego poziomu ochrony dla danych osobowych, które są wykorzystywane do celów testowych, tylko dlatego, że nadano im charakter danych testowych.

- Nie należy używać danych osobowych do przeprowadzania testów systemów informatycznych, jeśli można to zrobić bez użycia danych osobowych.

- Wykorzystywanie danych osobowych do testowania systemów informatycznych może być czasem konieczne, w szczególności w związku z końcowymi testami integracji konkretnego systemu z innymi zewnętrznymi systemami informatycznymi, w przypadku gdy trudno jest stworzyć dokładne, zanonimizowane dane testowe dostatecznie odzwierciedlające wszystkie błędy i nieprawidłowości, które mogą wystąpić w środowisku produkcyjnym. Konieczność przeprowadzenia testu systemu informatycznego przy użyciu danych osobowych może wzrastać w końcowych fazach projektu.

- W sytuacji gdy środowisko testowe ma być później wykorzystywane jako środowisko produkcyjne, administrator powinien zadbać o uprzednie usunięcie wszystkich danych osobowych, które były używane wyłącznie do celów testowych.

- Przetwarzanie danych osobowych do celów testowych wymaga od administratora dokonania prawidłowej oceny ryzyka dla osób, których dane dotyczą, oraz wdrożenia odpowiednich środków bezpieczeństwa zgodnie z oceną ryzyka. Zdaniem Datatilsynet za punkt wyjścia w tym zakresie należy uznać przyjęcie w środowisku testowym takich samych środków bezpieczeństwa, jakie zostały uznane za odpowiednie w środowisku produkcyjnym.

- Jeżeli testowanie i rozwój systemów informatycznych nie są konieczne, aby przetwarzanie danych osobowych w pierwotnym celu mogło mieć miejsce, przetwarzanie danych w celu testowania systemu informatycznego będzie najczęściej niezgodne z pierwotnym celem. Oznacza to, że w takich przypadkach nie można wykorzystać zebranych danych osobowych do testowania systemów informatycznych.

Z całością wytycznych Datatilsynet w języku duńskim można zapoznać się tutaj: https://www.datatilsynet.dk/presse-og-nyheder/nyhedsarkiv/2021/okt/brug-af-personoplysninger-i-testoejemed.

Przekazywanie danych osobowych za pomocą faksu niezgodne z RODO

Mateusz Kupiec

Zgodnie z definicją słownikową „faks" to „urządzenie służące do odbioru i przesyłania na odległość nieruchomych obrazów i tekstów za pomocą sieci telefonicznej"[1]. Chociaż okres największej popularności faksu jako środka komunikacji przypadł na lata 80. i 90. ubiegłego wieku[2], to jest on nadal chętnie używany przez wiele podmiotów[3]. Heski organ nadzorczy z zakresu ochrony danych osobowych (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit, dalej: „HBfDI" lub „organ") uznał, że przekazywanie danych osobowych za pomocą faksu może naruszać zasadę integralności i poufności przetwarzania z art. 5 ust. 1 lit. f RODO[4].

W opublikowanym komunikacie HBfDI wskazuje na następujące kwestie:

- Przesyłanie danych osobowych za pomocą faksu stwarza zagrożenia dla praw i wolności osób fizycznych porównywalne z tymi, które występują, gdy dane osobowe są przekazywane w niezaszyfrowanej wiadomości e-mail. W przypadku powszechnie stosowanej obecnie praktyki przesyłania i otrzymywania faksów poprzez sieć FoIP (Fax over IP) lub przy wykorzystaniu usług, które automatycznie zamieniają faksy na pocztę elektroniczną, dane nie są z reguły szyfrowane, a tym samym są przekazywane bez ochrony.
- Dane osobowe przesyłane faksem mogą zostać udostępnione nieuprawnionym osobom trzecim z powodu błędnego wprowadzenia numeru faksu docelowego. Ponadto nadawca faksu często nie wie, gdzie znajduje się urządzenie odbiorcze ani kto może mieć do niego dostęp.
- Szczególne kategorie danych, o których mowa w art. 9 ust. 1 RODO, nie powinny być co do zasady przesyłane faksem, jeżeli nadawca i odbiorca nie wprowadzili dodatkowych środków ochronnych. Organ przypomina, że im bardziej wrażliwe są dane osobowe, tym większa jest potrzeba ich ochrony, którą administrator powinien przyjąć za podstawę przy wyborze środków, jakie należy zastosować.
- Dane osobowe należące do szczególnych kategorii danych mogą być przekazywane faksem w wyjątkowych sytuacjach, gdy jest to konieczne ze względu na bardzo pilny charakter sprawy, a nadawca nie dysponuje alternatywnym, bezpieczniejszym kanałem komunikacji. Niemniej administrator powinien zapewnić, aby przekazane dane dotarły wyłącznie do właściwego odbiorcy (np. dzięki korzystaniu z zapisanych numerów docelowych).
- Organy publiczne powinny jedynie tymczasowo korzystać z faksu i rozpocząć proces przejścia na inne rozwiązania cyfrowe w celu zapewnienia obywatelom szybkiej i zgodnej z ochroną danych komunikacji.

Wobec powyższego w ocenie heskiego organu nadzorczego administratorzy powinni sprawdzić, z jakich alternatywnych, bezpiecznych środków komunikacji mogą korzystać zamiast faksu. W szczególności mogą rozważyć np. korzystanie z komunikacji elektronicznej zwyczajowo używanej w danym sektorze, wysyłanie wiadomości e-mail z szyfrowaniem treści (PGP lub S/MIME).

Źródło: https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/zur-%C3%BCbermittlung-personenbezogener-daten-per-fax.

[1] Zob. https://sjp.pwn.pl/slowniki/faks.html (dostęp: 28.10.2021).
[2] B. Rhodes, *When Fax was the Future: A Brief History of the Fax Machine*, 1.08.2020, [online] https://medium.com/tech-is-a-tool/when-fax-was-the-future-a-brief-history-of-the-fax-machine-696a88a833ce (28.10.2021).
[3] J. Coopersmith, *Why do people still use fax machines?,* 6.02.2019, [online] https://theconversation.com/why-do-people-still-use-fax-machines-109064 (dostęp: 28.10.2021).
[4] Rozporządzenie 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 95/46/WE (ogólne rozporządzenie o ochronie danych).

Ustawa o ochronie danych osobowych Chińskiej Republiki Ludowej

Mateusz Kupiec

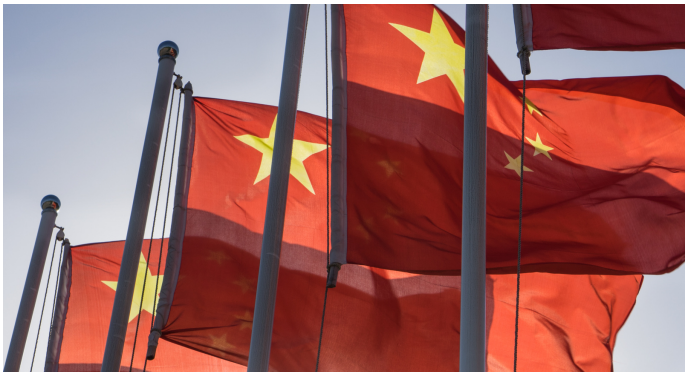
Według standardów europejskich ochrona danych osobowych przez długi czas odgrywała raczej podrzędną rolę w Chińskiej Republice Ludowej. Chiny nie posiadały bowiem kompleksowego systemu ochrony danych osobowych – rozproszone gwarancje dla autonomii informacyjnej jednostki znajdowały się w przepisach wielu ustaw z różnych gałęzi prawa[1]. Badacze przyczynę takiego fragmentarycznego stanu prawnego upatrywali między innymi w:

- nieuwzględnieniu w konstytucji ChRL[2] przepisu, który wprost i jednoznacznie odnosiłby się do ochrony prywatności;
- nieutworzeniu centralnego wiodącego organu nadzorczego z zakresu ochrony danych osobowych;
- zbytnim skupieniu rządu ChRL na kwestiach związanych z bezpieczeństwem narodowym[3].

Niemniej jednak w ciągu kilku ostatnich lat, chiński rząd wykazał jednak rosnące zainteresowanie budową silniejszego systemu ochrony danych osobowych i podjął szereg działań w celu zagwarantowania pewnego minimum efektywności systemu ochrony danych osobowych[4]. Starania te przyniosły efekty - 20 sierpnia 2021 r. Ogólnochińskie Zgromadzenie Przedstawicieli Ludowych przyjęło Ustawę o ochronie danych osobowych Chińskiej Republiki Ludowej (Personal Information Protection Law of the People's Republic of China, dalej też: „**PIPL**") która weszła w życie 1 listopada 2021 r. Celem nowego prawa jest poprawa ochrony danych osobowych i podjęcie bardziej zdecydowanych działań przeciwko nadużyciom w zakresie danych.

Podstawowe informacje o PIPL

PIPL składa się z ośmiu rozdziałów i 74 artykułów, na które składają się: przepisy ogólne, zasady przetwarzania danych osobowych, zasady transgranicznego udostępniania danych osobowych, prawa osób fizycznych, przepisy określające obowiązki podmiotów przetwarzających dane osobowe, przepisy dotyczące odpowiedzialności organów za egzekwowanie przepisów ustawy, przepisy określające zasady odpowiedzialności oraz przepisy uzupełniające. Na razie władze chińskie nie opublikowały oficjalnego tłumaczenia PIPL na j.angielski, co powoduje że analizując przepisy tej ustawy trzeba odnosić się do dostępnych nieoficjalnych tłumaczeń przygotowanych przez niezależnych badaczy[5].



- Podobnie jak RODO, PIPL stosuje się eksterytorialnie. Przepisy ustawy mają zastosowanie do przetwarzania danych osobowych przez podmioty spoza ChRL, gdy:

  a) celem przetwarzania jest oferowanie towarów lub usług osobom przebywającym w ChRL;
  b) celem przetwarzania jest monitorowanie i ocena zachowania osób przebywających w ChRL;
  c) mają miejsce inne okoliczności przewidziane w prawie krajowym;

[1] Zob. P. De Hert, E.Papakonstantinou, The data protection regime in China, s.14, https://cris.vub.be/ws/files/17639565/pdh15_vpThe_data_protection_regime_in_ChinaIPOL_IDA_2015_536472_EN.pdf,(dostęp: 1.11.2021 r.). 021.
[2] Konstytucja Chińskiej Republiki Ludowej z dnia 4 grudnia 1982 r. http://www.npc.gov.cn/englishnpc/constitution2019/201911/1f65146fb6104dd3a2793875d19b5b29.shtml, (dostęp: 1.11.2021 r.).
[3] Szerz. A. Geller, How Comprehensive Is Chinese Data Protection Law? A Systematisation of Chinese Data Protection Law from a European Perspective, GRUR International, Volume 69, Issue 12, December 2020, s. 1202, https://doi.org/10.1093/grurint/ikaa136., (dostęp: 1.11.2021 r.).
[4] Szerz. A. Geller, How Comprehensive Is Chinese Data Protection Law..., s. 1191.
[5] Anglojęzyczne tłumaczenie ustawy: https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, (dostęp: 1.11.2021 r.).

- PIPL określa, że chińskie organy państwowe mogą przetwarzać dane osobowe jedynie w celu wypełnienia swoich prawnych obowiązków ustawowych, t.j. nie mogą przetwarzać danych w sposób wykraczający poza zakres niezbędny do wypełnienia tych obowiązków. Ponadto, organy publiczne muszą przechowywać dane osobowe wyłącznie na terenie Chin;

- PIPL przewiduje kilka podstaw przetwarzania, t.j. zgodę, niezbędność przetwarzania do zawarcia lub wykonania umowy (w tym umowy o pracę), niezbędność przetwarzania do wykonania obowiązków prawnych. Odmiennie niż RODO, PIPL nie uznaje jednak "prawnie uzasadnionego interesu administratora jako podstawy prawnej przetwarzania danych osobowych. Niemniej jednak rozszerzenie katalogu podstaw przetwarzania stanowi ważną „nowość" dla chińskiego systemu ochrony danych osobowych, ponieważ do tej pory główną podstawą przetwarzania przewidzianą w obowiązujących w ChRL ustawach (np. w chińskim kodeks cywilny) była zgoda podmiotu danych.

- w PIPL wprost zakazano podmiotom biorącym udział w obrocie danymi osobowymi traktować osoby fizyczne w obrocie handlowym w nieuzasadniony zróżnicowany sposób. Chiński prawodawca w szczególności zabronił praktyk dyskryminacji cenowej, poprzez stosowanie przez administratorów zautomatyzowanego podejmowania decyzji wobec osób, których dane dotyczą. W tym miejscu wskazać należy, że w rozumieniu przepisów PIPL "zautomatyzowane podejmowanie decyzji" to "działalność polegającą na wykorzystaniu programów komputerowych do automatycznej analizy lub oceny osobistych zachowań, nawyków, zainteresowań lub hobby, lub statusu finansowego, zdrowotnego, kredytowego lub innego, oraz podejmowania decyzji na ich podstawie".

- Podmioty przekazujące dane osobowe poza terytorium ChRL muszą pozyskać na takie działania zgodę osoby, której dane dotyczą oraz przekazać jej m.in. następujące informacje: tożsamość odbiorcy danych spoza ChRL oraz jego dane kontaktowe; cel i sposoby przetwarzania, kategorie danych osobowych, a także sposoby lub wykonywania jej praw.

- PIPL przewiduje liczne sankcje dla podmiotów, które nie wypełniają swoich obowiązków w zakresie ochrony danych osobowych wynikających z ustawy. Organizacje naruszające przepisy PIPL w sposób rażący mogą zostać ukarane m.in. administracyjną karą pieniężną w wysokości do 50 milionów juanów lub w wysokości do 4 % jego całkowitego rocznego światowego obrotu.
- Za egzekwowanie przestrzegania przepisów PIPL i opracowywanie strategii w zakresie ochrony danych osobowych nie jest odpowiedzialny jeden organ, lecz zadania te są rozdzielone pomiędzy kilka podmiotów z sektora publicznego znajdujących się na różnych szczeblach administracji publicznej.

Komentarz

Niniejsza notatka nie ma charakteru wyczerpującego i w żadnym wypadku nie jest kompleksowym przewodnikiem po chińskim systemie ochrony danych osobowych. Jej celem jest przekazanie polskojęzycznemu odbiorcy podstawowych informacji o PIPL, aby zwrócić jego uwagę na dopsniosłe zmiany w zakresie ochrony prywatności w ChRL.

Nowe przepisy na pewno przyczynią się do zwiększenia świadomości obywateli ChRL na temat przetwarzania ich danych osobowych. Europejskie przedsiębiorstwa współpracujące z chińskimi podmiotami gospodarczymi powinny mieć zatem na uwadze przepisy PIPL w szczególności z racji eksterytorialnego zakresu stosowania ustawy. Przepisy „chińskiego RODO" mają bowiem nie tylko znaczenie lokalne, lecz aktywnie przyczyniają się do tworzenia zasad dotyczących międzynarodowego transferu danych[6]. Wielu komentujących podkreśla podobieństwa PIPL i RODO podkreślając inspirację chińskiego ustawodawcy unijnym systemem ochrony danych osobowych. Niemniej jednak administratorzy przekazujący dane osobowe do ChRL nadal powinni kierować się szczególną ostrożnością i odpowiednio zabezpieczyć transfer danych.

Jest jeszcze zbyt wcześnie na jakąkolwiek ocenę PIPL. W Chinach nadal brakuje niestety (faktycznie) niezależnego, centralnego organu nadzorczego z zakresu danych osobowych, który mógłby skutecznie egzekwować przepisy PIPL i ustanowić jednolite standardy w zakresie ochrony prywatności. Tym samym istnieje ryzyko, że przepisy PIPL będą w praktyce egzekwowane instrumentalnie przez chińskie władze i staną się kolejnym (odstraszającym) narzędziem kontroli społeczeństwa, przedsiębiorców.

[6] Podobnie S. Tang, Extraterritorial Application of Chinese Personal Information Protection Law: A Comparative Study with GDPR, https://conflictoflaws.net/2021/extraterritorial-application-of-chinese-personal-information-protection-law-a-comparative-study-with-gdpr/, (dostęp: 1.11.2021 r.).

Obsługa zgłoszeń sygnalistów a pełnienie funkcji IOD w organizacji

Grzegorz Sibiga, Mateusz Kupiec

Państwa członkowskie UE mają dokonać transpozycji Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii (dalej: „dyrektywa 2019/1937" do dnia 17 grudnia 2021 r. W Polsce wykonywać dyrektywę ma ustawa o ochronie osób zgłaszających naruszenia prawa, której projekt został opublikowany 18 października 2021 r. Nowe przepisy dotyczące gwarancji dla sygnalistów oraz postępowania z ich zgłoszeniami będą miały znaczenie dla kilku gałęzi prawa (prawo pracy, administracyjne i karne), w tym będą także określać zasady ochrony danych osobowych sygnalistów. Ponadto nowe przepisy wpłyną na różne aspekty stosowania przepisów o ochronie danych osobowych, w tym wykonywania swoich zadań przez inspektora ochrony danych.

Prezes UODO zajmuje stanowisko ws. dopuszczalności łączenia wykonywania funkcji IOD z realizacją obowiązków w zakresie obsługi zgłoszeń sygnalistów

Jedną z instytucji przepisów o ochronie danych osobowych jest inspektor ochrony danych, który wykonuje w sferze wewnętrznej administratorów i podmiotów przetwarzających określone w RODO zadania związane z zapewnieniem przestrzegania przepisów prawa i polityk ochrony danych. W związku z przepisami dyrektywy 2019/1937 dotyczącymi obowiązków w zakresie rozpatrywania zgłoszeń sygnalistów zasadne staje się pytanie, czy IOD może przyjmować ewentualne zawiadomienia takich osób o występowaniu nieprawidłowości w organizacji oraz prowadzić postępowania wyjaśniające dotyczące zgłaszanych przez nich naruszeń.

3 listopada 2021 r. na stronie internetowej Urzędu Ochrony Danych Osobowych opublikowano komunikat pt. „Czy można łączyć funkcję IOD z zadaniami związanymi z obsługą wniosków od sygnalistów?". W stanowisku UODO odnosząc się do motywów preambuły do dyrektywy 2019/1937 wskazał wymagania, które muszą spełniać członkowie personelu pracodawcy odpowiedzialni za obsługę zgłoszeń sygnalistów (m.in. obowiązek odbycia specjalnego przeszkolenia). W komunikacie zwrócono natomiast uwagę, że „przepisy dyrektywy [2019/1937] nie regulują [...] kwestii łączenia zadań osób zajmujących się obsługą zgłoszeń z innymi zadaniami". **Wydaje się, że organ co do zasady nie wyklucza możliwości realizowania przez IOD zadań dotyczących ochrony sygnalistów pod warunkiem, że administrator przed powierzeniem IOD takich obowiązków**:

- podejmie działania w celu zapewnienia IOD właściwych warunków dla zachowania jego niezależności i prawidłowego wykonywania zadań;
- dokona indywidualnej oceny, czy przyjmowanie i rozpatrywanie zgłoszeń sygnalistów przez IOD w konkretnym stanie faktycznym nie prowadzi do powstania konfliktu interesów po jego stronie.

W omawianym stanowisku organ przypomniał kolejny raz podstawowe zasady dotyczące powierzania nowych obowiązków IOD oraz kryteria pozwalające ocenić, kiedy IOD nie będzie w stanie wypełniać powierzonych mu zadań w sposób niezależny. Co istotne, zdaniem UODO zakazany dla IOD konflikt interesów może występuje nie tylko ze względów merytorycznych (gdy inne zadanie uniemożliwia inspektorowi niezależne wykonywanie jego zadań), ale także „może być również rezultatem nadmiaru obowiązków przydzielonych do wykonania IOD, jeśli IOD musi wybrać między obowiązkami, jakie będzie realizował, a tymi, którym nie podoła z powodu braku czasu koniecznego na ich wykonanie".

Biorąc pod uwagę nie tylko stanowisko UODO z dnia 3 listopada 2021 r., ale także specyfikę obsługi zgłoszeń, należy jednak niezwykle ostrożnie podchodzić do nakładania na osoby pełniące funkcję IOD dodatkowych obowiązków dotyczących rozpatrywania zgłoszeń sygnalistów. W szczególności, że zgłaszane naruszenia mogą bowiem dotyczyć działań lub zaniechań w organizacji w zakresie ochrony danych osobowych, w tym sytuacji związanych z nieprawidłowym wykonywaniem obowiązków przez IOD. Nie można również zapomnieć, że do zadań IOD należy monitorowanie przestrzegania przepisów o ochronie danych osobowych, co z punktu widzenia unikania konfliktu interesów nie może prowadzić do ew. kontroli przez IOD zgodności własnej działalności związanej z obsługą zgłoszeń sygnalistów z przepisami o ochronie danych.

Z całym komunikatem na stronie UODO można zapoznać się tutaj https://uodo.gov.pl/pl/223/2201?fbclid=IwAR3bnJrtTmT6Zj09Ylgqgz5Eq_mwHaO9MhiGaM_0woyKRgZZy1Rkg4nGoXw

Europejska Rada Ochrony Danych o kryteriach właściwości terytorialnej organów nadzorczych w celu egzekwowania art. 5 ust. 3 dyrektywy 2002/58/WE

Dominika Nowak

Europejska Rada Ochrony Danych przyjęła wewnętrzny dokument nr 4/2021 dotyczący kryteriów właściwości terytorialnej organów nadzorczych w celu egzekwowania art. 5 ust. 3 dyrektywy o e-prywatności[1]. Dokument został udostępniony 27 sierpnia 2021 r. przez OneTrust DataGuidance.

Decyzje przyjęte przez krajowe organy nadzorcze właściwe do egzekwowania art. 5 ust. 3 dyrektywy 2002/58/WE pokazały, że terytorialne zastosowanie tej dyrektywy będzie się różnić w zależności od organu nadzorczego, zwłaszcza jeżeli administrator / dostawca usługi ma siedzibę w kilku państwach członkowskich. Celem dokumentu przyjętego przez EROD jest ustalenie wspólnej wykładni właściwości terytorialnej organu nadzorczego właściwego do egzekwowania art. 5 ust. 3 dyrektywy 2002/58/WE bez względu na dokonane przez państwa członkowskie wybory w ramach implementacji dyrektywy 2002/58/WE do krajowego porządku prawnego. To zagadnienie nie zostało omówione w opinii EROD nr 5/2019 w sprawie wzajemnej zależności między dyrektywą o prywatności i łączności elektronicznej a RODO, przyjętej 12 marca 2019 r., w szczególności w zakresie właściwości, zadań i uprawnień organów ochrony danych.

Zgodnie z art. 17 ust. 1 dyrektywy 2002/58/WE państwa członkowskie zostały zobowiązane do wprowadzenia w życie przepisów niezbędnych do wykonania dyrektywy. Natomiast zgodnie z art. 15 ust. 1 dyrektywy 2002/58/WE: „Państwa członkowskie ustanawiają przepisy dotyczące kar, w tym w stosownych przypadkach sankcji karnych, mających zastosowanie w przypadku naruszeń krajowych przepisów przyjętych zgodnie z niniejszą dyrektywą, i podejmują wszelkie niezbędne środki w celu zapewnienia, aby zasady te zostały wdrożone". Na podstawie tych przepisów każde państwo członkowskie jest zobowiązane do zapewnienia środków niezbędnych do tego, aby cele dyrektywy zostały osiągnięte. W dyrektywie 2002/58/WE nie uregulowano kwestii jej terytorialnego zastosowania.

Jednakże orzecznictwo TSUE dotyczące terytorialnego zastosowania uchylonej dyrektywy 95/46/WE rozstrzyga, w jaki sposób powinno być ono zorganizowane. W wyroku ws. Wirtschaftsakademie Schleswig-Holstein (C-210/16) z dnia 5 czerwca 2018 r. Trybunał wskazał, że organ nadzorczy był uprawniony do wykonywania swoich uprawnień wobec podmiotu z siedzibą na jego terytorium, w ramach którego działalności dokonuje się przetwarzania, nawet jeżeli jednostka odpowiedzialna za zbieranie i przetwarzanie danych osobowych jest usytuowana w innym państwie członkowskim. Jeżeli administrator / dostawca usługi nie ma siedziby w państwie członkowskim, to prawo tego państwa członkowskiego może określać inne kryteria niż siedziba, aby egzekwować prawo krajowe w odniesieniu do administratora / dostawcy usługi. Wynika z tego, że każdy właściwy organ nadzorczy jest uprawniony do egzekwowania prawa krajowego implementującego dyrektywę 2002/58/WE w zakresie, w jakim dotyczy on użytkowników zlokalizowanych w ramach terytorialnej jurysdykcji. Ponadto żadne przepisy implementujące dyrektywę e-Privacy nie mogą uniemożliwiać organowi nadzorczemu innego państwa członkowskiego egzekwowania dyrektywy 2002/58/WE, ponieważ byłoby to niezgodne z jej celem, czyli ochroną podstawowych praw i wolności osób, których dane dotyczą.

[1] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz. U. UE L z 2002 r. Nr 201, z późn. zm., str. 37; dalej „dyrektywa 2002/58/WE" lub „dyrektywa e-Privacy".

Nałożenie kary pieniężnej mogłoby zależeć od prawa krajowego danego państwa członkowskiego. Biorąc pod uwagę, że maksymalne sankcje za naruszenie dyrektywy e-Privacy różnią się w zależności od państwa członkowskiego, sankcje te mogłyby nie być skutecznym środkiem ochrony danych użytkowników ze względu na ryzyko poszukiwania przez administratorów / dostawców usług najkorzystniejszego prawa w danym przypadku (*forum shopping*). Nie należy natomiast wykluczyć inicjowania przez państwa członkowskie dialogu transgranicznego w celu zharmonizowania kwestii przepływu danych zgodnie z art. 15a ust. 4 dyrektywy ePrivacy[2].

Wnioski

EROD zaproponował kryteria określania właściwości krajowych organów nadzorczych. Jeżeli przetwarzanie jest regulo-wane wyłącznie przepisami prawa krajowego implementują-cymi art. 5 ust. 3 dyrektywy 2002/58/WE, to właściwe organy nadzorcze są właściwe do egzekwowania przestrzegania tego przepisu zgodnie z prawem krajowym, gdy:

- administrator/dostawca usługi ma siedzibę w ramach właściwości terytorialnej danego organu nadzorczego;
- przetwarzanie odbywa się w ramach czynności tego podmiotu znajdującego się na terytorium objętym właściwością danego organu nadzorczego, nawet jeżeli wyłączna odpowiedzialność za zbieranie i przetwarzanie na terytorium Unii Europejskiej należy do podmiotu znajdującego się w innym państwie członkowskim.

W przypadku braku administratora / dostawcy usług lub jego siedziby we właściwości terytorialnej organu nadzorczego prawo krajowe powinno przewidywać kolejne kryteria egzekwowania przepisów.

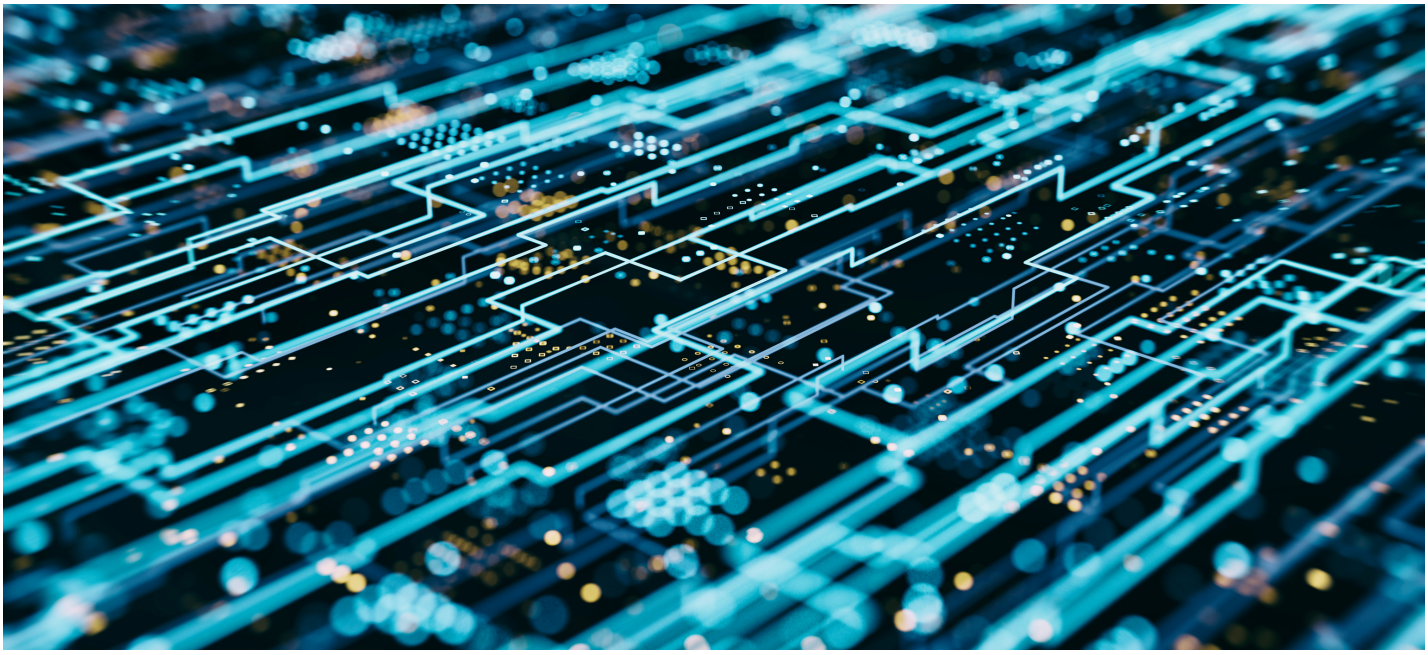
W żadnym wypadku podejmowane środki nie powinny:

- dotyczyć użytkowników znajdujących się we właściwości terytorialnej, dla której dany organ nadzorczy nie jest właściwy;
- uniemożliwiać innym organom nadzorczym egzekwowania dyrektywy 2002/58/WE.

Więcej informacji: https://www.dataguidance.com/news/eu-edpb-provides-interpretation-territorial-application.

Treść dokumentu w języku angielskim: https://www.dataguidance.com/sites/default/files/document_case_2021-21.pdf.

[2] Artykuł 15a ust. 4: „Właściwe krajowe organy regulacyjne mogą przyjmować środki w celu zapewnienia efektywnej współpracy transgranicznej w zakresie egzekwowania przepisów krajowych przyjętych zgodnie z niniejszą dyrektywą oraz tworzenia zharmonizowanych warunków świadczenia usług obejmujących transgraniczny przepływ danych".



Aktualny stan normalizacji sztucznej inteligencji w świetle projektu rozporządzenia UE dotyczącego SI i dalsze potrzeby w tym zakresie

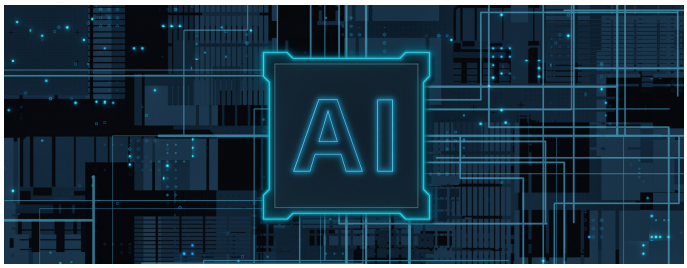
Andrzej Kaczmarek

21 kwietnia 2021 r. Komisja Europejska opublikowała projekt unijnego rozporządzenia w sprawie sztucznej inteligencji (Artificial Intelligence Act, dalej: „AIA")[1], o którym wspomniano w czerwcowym wydaniu newslettera. Głównym celem rozporządzenia jest ustanowienie przepisów, które spowodują, że wprowadzane w UE systemy sztucznej inteligencji będą bezpieczne, przejrzyste, etyczne, bezstronne i w całym cyklu ich tworzenia i stosowania kontrolowane przez człowieka. W związku z tym w przeglądzie skoordynowanego planu w zakresie SI z 2021 r.[2] postanowiono, że Komisja i państwa członkowskie będą kontynuować współpracę z europejskimi organizacjami normalizacyjnymi (ESO), międzynarodowymi organizacjami rozwoju norm (SDO) i wszystkimi zainteresowanymi stronami, aby zapewnić terminowe przyjęcie norm zharmonizowanych, niezbędnych do operacjonalizacji wymogów i obowiązków przewidzianych w ramach prawnych dotyczących w szczególności systemów SI z grupy wysokiego ryzyka dla bezpieczeństwa ludzi lub ich praw podstawowych. Tematem niniejszego artykułu jest prezentacja norm europejskich i międzynarodowych w kontekście ich wykorzystania do oceny wymagań nałożonych przez projekt rozporządzenia AIA dla systemów sztucznej inteligencji z grupy wysokiego ryzyka, przedstawiona w raporcie Wspólnego Centrum Badawczego (JRC)[3] Komisji Europejskiej z 14 lipca 2021 r. zatytułowanym „Krajobraz normalizacji systemów SI. Stan obecny i powiązanie z propozycją KE dotyczącą ram regulacyjnych SI"[4]. W raporcie tym dokonano przeglądu działalności normalizacyjnej w zakresie systemów SI prowadzonej przez europejskie organizacje normalizacyjne (ESO) i międzynarodowe organizacje rozwoju norm (SDO) w celu identyfikacji możliwych luk i niedostatecznie rozwiniętych obszarów, a tym samym wniesienia wkładu do europejskiej mapy drogowej normalizacji w celu wdrożenia przedstawionego projektu rozporządzenia AIA.

1. Rola i rodzaje norm

Według Komisji Europejskiej norma jest definiowana jako „specyfikacja techniczna zatwierdzona przez uznaną instytucję normalizacyjną do wielokrotnego lub ciągłego stosowania, z którą zgodność nie jest obowiązkowa i która jest jedną z poniższych" (Komisja Europejska, 1998):

- norma międzynarodowa: norma przyjęta przez międzynarodową organizację normalizacyjną i udostępniona publicznie;
- norma europejska: norma przyjęta przez europejską organizację normalizacyjną i dostępna publicznie;
- norma krajowa: norma przyjęta przez krajowy organ normalizacyjny i dostępna publicznie.



Zgodnie z rozporządzeniem nr 1025/2012 w sprawie normalizacji podstawowym celem norm jest określenie dobrowolnych specyfikacji technicznych lub jakościowych, z którymi mogą być zgodne obecne lub przyszłe produkty, procesy produkcyjne lub usługi. Normalizacja może obejmować różne kwestie, takie jak normalizacja różnych gatunków lub rozmiarów danego produktu czy specyfikacje techniczne na rynkach produktów lub usług, na których kompatybilność i interoperacyjność z innymi produk-tami lub systemami ma zasadnicze znaczenie. Normy dotyczące zrównoważonego rozwoju i bezpieczeństwa pomagają chronić ludzi i środowisko. W Europie normy pełnią szczególną funkcję: pomagają urzeczywistnić jednolity rynek,

[1] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts; https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 (dostęp: 26.10.2021).
[2] Coordinated Plan on Artificial Intelligence 2021 Review; https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review (dostęp: 26.10.2021).
[3] JRC (Joint Research Centre) – jedna z Dyrekcji Generalnych Komisji Europejskiej, której celem jest zapewnienie, zgodnie z potrzebami klientów, wsparcia naukowego i technicznego dla koncepcji, rozwoju, wdrażania i monitorowania polityki Unii Europejskiej.
[4] S. Nativi, S. De Nigris, AI Watch, *AI standardisation landscape state of play and link to the EC proposal for an AI regulatory framework*, JRC Ispra, Italy 2021.

umożliwiają transformację cyfrową, zwiększają międzynarodową konkurencyjność i wspierają regulacje. W Unii Europejskiej tylko normy opracowane przez CEN, CENELEC i ETSI są uznawane za „normy europejskie" (rozporządzenie nr 1025/2012). Te europejskie organizacje normalizacyjne (ESO) pracują w interesie harmonizacji europejskiej, tworząc zarówno normy wymagane przez rynek, jak i normy zharmonizowane, wspierające prawodawstwo europejskie.

1.1. Normy de facto a normy de iure

Norma *de facto* to norma, która została powszechnie zaakceptowana (np. przez klientów/użytkowników lub przez rynek) i stała się dobrze ocenianą (lub popularną) normą dla swojego celu – nawet jeśli nie ma oficjalnego statusu. Akceptacja jest często oparta na udowodnionej skuteczności i niezawodności. Standardy *de facto*, które są akceptowane przez daną branżę, są również znane jako standardy branżowe lub zawodowe.

Normy *de iure* opisują praktykę, która jest formalnie uznana, niezależnie od tego, czy istnieje ona w rzeczywistości. Dlatego normy *de iure* (lub normy zgodne z prawem) to te, które zostały zatwierdzone przez oficjalne organizacje, takie jak ISO i IEEE. Normy te są krytycznie oceniane przed ich zatwierdzeniem. Przykładami norm sprzętowych *de iure* są USB, FireWire i HDMI.

Normy *de facto* mogą z czasem stać się normami *de iure* (tj. poprzez otrzymanie oficjalnego statusu od międzynarodowych organizacji rozwoju norm) – np. formaty HTML i PDF. HTML po raz pierwszy stał się normą *de iure* w 1995 r. dzięki wysiłkom normalizacyjnym prowadzonym przez Internet Engineering Task Force (IETF), a PDF stał się w 2008 r. normą ISO (ISO 32000-1).

1.2. Normy założycielskie a normy wdrożeniowe

Normy założycielskie lub podstawowe są zwykle bazą serii specyfikacji standardowych zdefiniowanych przez SDO. Prace te koncentrują się na tych aspektach, które wymagają wspólnego słownictwa, jak również uzgodnionych taksonomii i definicji. Ostatecznie normy te będą oznaczać, że praktyk może mówić tym samym językiem co regulator, a obaj mogą mówić tym samym językiem co ekspert techniczny. Na przykład prace ISO/IEC nad systemami SI obejmują szereg kluczowych obszarów obejmujących kwestie technologiczne, społeczne i etyczne. Ponieważ dotyczy to wielu różnych interesariuszy, istnieje potrzeba określenia punktu wyjścia poprzez wprowadzenie zestawu podstawowych norm.

Przykład: ISO/IEC DIS 22989 – Information technology – Artificial intelligence – Artificial intelligence concepts and terminology.

Dokument ustanawia terminologię dla sztucznej inteligencji (SI) i opisuje koncepcje w dziedzinie SI. Dokument może być wykorzystywany przy opracowywaniu innych norm oraz do wspierania komunikacji pomiędzy różnymi zainteresowanymi stronami/interesariuszami.

Normy wdrożeniowe różnią się od abstrakcyjnej specyfikacji norm założycielskich, ponieważ są one napisane dla bardziej technicznych odbiorców i szczegółowo opisują aspekty techniczne, takie jak struktura interfejsu pomiędzy komponentami oprogramowania.

Przykład: IEEE 802.3-2018 – IEEE Standard for Ethernet – Ethernet local area network operation is specified for selected speeds of operation from 1 Mb/s to 400 Gb/s using a common media access control (MAC) specification and management information base (MIB).

1.3. Specyfikacje horyzontalne i wertykalne

Podobnie jak w wielu innych dziedzinach normalizacji, mogą istnieć dwa poziomy działań normalizacyjnych: jeden zajmujący się ogólnymi kwestiami, które mają zastosowanie w sposób przekrojowy do kilku obszarów (poziomy), i drugi zajmujący się bardziej szczegółowymi kwestiami, istotnymi dla danego sektora działalności lub obszaru zastosowania (pionowy).

Specyfikacja horyzontalna zawiera podstawowe zasady, pojęcia, definicje i podobne informacje ogólne, które mają zastosowanie w wielu dziedzinach tematycznych.

Przykład: ISO/IEC AWI TR 24372 – Information technology – Artificial intelligence (AI) – Overview of computational approaches for AI systems.

Specyfikacja ma na celu przedstawienie przeglądu stanu wiedzy na temat podejść obliczeniowych dla systemów AI poprzez opisanie: a) głównych cech obliczeniowych systemów AI, b) głównych algorytmów i podejść stosowanych w systemach AI w odniesieniu do przypadków użycia zawartych w ISO/IEC TR 24030.

Specyfikacje pionowe natomiast mają na celu uwzględnienie obszarów specyficznych dla danego zastosowania lub sektora, a zatem koncentrują się jedynie na niezbędnych informacjach specyficznych dla danego zastosowania lub sektora. Specyfikacje takie mogą być jednak ponownie wykorzystane w innych sektorach, z ewentualną potrzebą adaptacji.

Przykład: ETSI DES/eHEALTH-008 – eHEALTH – Wymagania dotyczące rejestracji danych dla e-Zdrowia.

Celem pracy jest identyfikacja wymagań dotyczących rejestracji zdarzeń e-Zdrowia, tj. pochodzących z urządzeń e-Zdrowia opartych na ICT oraz od praktyków zdrowia. Przy założeniu, jak pokazano w dokumencie dotyczącym przypadków użycia i białej księdze, że dokumentacja zdrowotna podlega ograniczeniom w zakresie bezpieczeństwa i prywatności, ale jednocześnie musi być dostępna dla wielu różnych zainteresowanych stron w czasie i przestrzeni bez wcześniejszego rozpoznania, kim są te zainteresowane strony.

1.4. Zależności od norm

Specyfikacje norm zazwyczaj opierają się na innych już istniejących normach, aby zachować spójność, uniknąć konfliktów i powielania pracy. Implementacja standardu zwykle wymaga więc implementacji innych, bazowych standardów; te ostatnie, zwane standardami drugiego poziomu, mogą być z kolei powiązane z innymi, bazowymi itd. W związku z tym wyróżnia się:

- normy pierwszego poziomu: normy, o których wdrożenie organizacja jest proszona i które powszechnie opierają się na innych istniejących (drugiego poziomu) normach (specyfikacjach);
- normy drugiego poziomu: normy, o których wdrożenie organizacja może być poproszona, ponieważ są one podstawą do wdrożenia innej normy – np. normy pierwszego poziomu.

2. Metodologia badań przyjęta przez autorów raportu

Mając na uwadze, że dziedzina technologii informacyjnych (ICT) i zarządzania jakością związana z procesami sztucznej inteligencji jest dość rozległa, a tym samym dziedzina normalizacji systemów SI jest obszerna, autorzy badania przyjęli następującą metodologię:

Krok 1. Gromadzenie norm dotyczących systemów SI. Zebranie istniejących badań ankietowych związanych z normalizacją SI poprzez bezpośredni dostęp do portali i dokumentów ESO i międzynarodowych SDO oraz zebranie informacji od ekspertów ds. normalizacji.

Krok 2. Analiza wysokiego poziomu i mapowanie do wymagań AIA (dopracowanie populacji norm). Analiza zebranego zbioru norm dotyczących SI i kategoryzacja różnych typów norm na de iure i de facto, fundamentalne i wdrożeniowe oraz specyfikacje horyzontalne i wertykalne.

Dalsze dopracowanie listy zebranych norm według trzech kryteriów:

- uwzględnienie norm dotyczących zagrożeń związanych ze sztuczną inteligencją;
- uprzywilejowanie horyzontalnych norm wdrożeniowych pochodzących od międzynarodowych SDO w stosunku do norm założycielskich i wertykalnych;
- uwzględnienie norm pierwszego poziomu.

Krok 3. Dogłębna analiza i mapowanie do wymagań AIA (oszacowanie wskaźników operacjonalizacji i przydatności mniejszej grupy norm). Systematyczna analiza pełnego tekstu mniejszej grupy odpowiednich norm (tj. tych, które zostały rozpoznane w wyniku wysokopoziomowego mapowania) i oszacowanie, na ile są one odpowiednie (obecnie) do operacjonalizacji celów technologicznych leżących u podstaw wymagań zawartych w AIA.

Krok 4. Analiza wyników przydatności i operacjonalizacji (rozpoznanie luk). Na podstawie poziomu operacyjności i przydatności oszacowanego wcześniej dla każdej dogłębnie przeanalizowanej normy rozpoznaje się ewentualne luki (i niedostatecznie reprezentowane wymagania AIA). W ten sposób sformułowane zostaną wstępne zalecenia.

Schematycznie zastosowana metodologia przedstawiona została na rys. 1.

Rys. 1. Ogólna metodologia przyjęta w celu zidentyfikowania najistotniejszych norm, rozpoznania luk i przedstawienia zaleceń.

3. Wymagania rozporządzenia AIA i obowiązujące normy

Zebrane w pierwszym kroku badań normy dotyczące systemów SI zostały poddane analizie i zmapowane do wymagań systemów SI wysokiego ryzyka określonych w rozporządzeniu AIA. Główne wymagania, według których dokonano mapowania zebranego zestawu norm, znajdują się poniżej w tabeli 1.

Temat wymagania	Opis wykonawczy
Dane i zarządzanie danymi	Systemy SI wysokiego ryzyka, które wykorzystują techniki obejmujące szkolenie modeli przy użyciu danych, są opracowywane na podstawie zbiorów danych szkoleniowych, walidacji i testowania zbiorów danych, które spełniają wymagany zestaw kryteriów jakości.
Dokumentacja techniczna	Dokumentacja techniczna systemu SI jest sporządzana przed wprowadzeniem tego systemu na rynek lub do użytku i jest aktualizowana. Dokumentację techniczną sporządza się w taki sposób, aby wykazać, że system SI wysokiego ryzyka jest zgodny z wymaganiami AIA.
Prowadzenie rejestru zdarzeń	Systemy SI wysokiego ryzyka projektuje się i opracowuje w taki sposób, aby zawierały funkcję umożliwiającą automatyczne rejestrowanie zdarzeń („rejestry zdarzeń") podczas działania tych systemów. Funkcja rejestracji zdarzeń musi być zgodna z uznanymi normami lub wspólnymi specyfikacjami.
Przejrzystość i udostępnianie informacji użytkownikom	Systemy SI wysokiego ryzyka projektuje się i opracowuje w sposób zapewniający wystarczającą przejrzystość ich działania, umożliwiającą użytkownikom interpretację wyników działania systemu i ich właściwe wykorzystanie. Zapewnia się odpowiedni rodzaj i stopień przejrzystości w celu osiągnięcia zgodności z odpowiednimi obowiązkami użytkownika i dostawcy określonymi w rozdziale 3 AIA.
Nadzór ze strony człowieka	Systemy SI wysokiego ryzyka projektuje się i opracowuje w sposób zapewniający odpowiedni interfejs człowiek–maszyna, aby w okresie jego wykorzystywania mógł on być skutecznie nadzorowany przez człowieka.
Dokładność, solidność i cyberbezpieczeństwo	Systemy SI wysokiego ryzyka projektuje się i opracowuje w taki sposób, aby osiągały, z uwagi na ich przeznaczenie, odpowiedni poziom dokładności, solidności i cyberbezpieczeństwa oraz działały konsekwentnie pod tymi względami w całym cyklu życia.
Zarządzanie ryzykiem	System SI wysokiego ryzyka w ramach kontroli wewnętrznej wymaga pełnej, skutecznej i odpowiednio udokumentowanej ex ante oceny zgodności z wszystkimi wymogami rozporządzenia AIA oraz z solidnymi systemami zarządzania jakością i ryzykiem, a także monitorowania po wprowadzeniu do obrotu. System zarządzania ryzykiem dla tych systemów powinien być ustanowiony, wdrożony, udokumentowany i utrzymywany w całym cyklu użytkowania.
Zarządzanie ryzykiem	Dostawcy systemów SI wysokiego ryzyka wprowadzają system zarządzania jakością, który zapewnia zgodność z AIA. Dostawca powinien ustanowić skuteczny system zarządzania jakością, zapewnić przeprowadzenie wymaganej procedury oceny zgodności, sporządzić odpowiednią dokumentację i ustanowić solidny system monitorowania po wprowadzeniu do obrotu.

Tabela 1. Główne wymagania dla systemów SI wysokiego ryzyka określone w projekcie rozporządzenia AIA. Źródło: S. Nativi, S. De Nigris S., *AI standardisation landscape state of play and link to the EC proposal for an AI regulatory framework*, JRC Ispra, Italy 2021.

Wymaganie AIA	ISO oraz ISO/IEC JTC 1	IEEE	ETSI	ITU-T
Dane i zarządzanie danymi	ISO/IEC 25024; ISO/IEC 5259; ISO/IEC 24668	ECPAIS Bias; IEEE P7002; IEEE P7003; IEEE P7004; IEEE P7005; IEEE P7006; IEEE P7009; IEEE P2801; IEEE P2807; IEEE P2863	DES/eHEALTH-008; GR CIM 007; GS CIM 009; ENI GS 001; GR NFV-IFA 041; DGR SAI 002; TR 103 674; TR 103 675; TS 103 327; TS 103 194; TS 103 195.2; SAREF Ontologies	ITU-T Y.3170; ITU-T Y.MecTA-ML; ITU-T Y.3531; ITU-T Y.3172; ITU-T H.CUAV-AIF; ITU-T F.VS-AIMC; ITU-T Y.4470; Y.Supp.63 to ITU-T Y.4000 series
Dane techniczne i rejestr zadań	ISO/IEC 5338; ISO/IEC 5469; ISO/IEC 24368; ISO/IEC 24372; ISO/IEC 24668	ECPAIS Transparency; IEEE P7000; IEEE P7001; IEEE P7006; IEEE P2801; IEEE P2802; IEEE P2807; IEEE P2863; IEEE P3333.1.3	DES/eHEALTH-008; ENI GS 005; DGR SAI 002, SAREF Ontologies; GR CIM 007; GS CIM 009	
Przejrzystość i udostępnianie informacji użytkownikom	ISO/IEC 24027; ISO/IEC 24028; ISO/IEC 5338; ISO/IEC 24368; ISO/IEC 24372; ISO/IEC 24668; ISO/IEC 4213	ECPAIS Bias; ECPAIS Transparency; ECPAIS Accountability; IEEE P7000; IEEE P7001; IEEE P7003; IEEE P7004; IEEE P7005; IEEE P7007; IEEE P7008; IEEE P7009; IEEE P7011; IEEE P7012; IEEE P7014; IEEE P2863; IEEE P3652.1	DES/eHEALTH-008; GS CIM 009; DGR SAI 002; SAREF Ontologies	ITU-T Y.4470
Nadzór ze strony człowieka		ECPAIS Accountability; ECPAIS Transparency; IEEE P7000; IEEE P7006; IEEE 7010; IEEE P7014; IEEE P2863	DES/eHEALTH-008; DGR SAI 005	
Dokładność, solidność i cyberbezpie-czeństwo	ISO/IEC 24027; ISO/IEC 24028; ISO/IEC 24029; ISO/IEC 5469	ECPAIS Transparency; IEEE P7007; IEEE P7009; IEEE P7011; IEEE P7012; IEEE P2802; IEEE P2807; IEEE P2846; IEEE P2863; IEEE P3333.1.3	GS ARF 003; GR CIM 007; ENI GS 001; ENI GR 007; DGR SAI 001; DGR SAI 002; DGS SAI 003; GR SAI 004; GS ZSM 002; TR 103 674; TR 103 675; TS 103 327; GS 102 181; GS 102 182	ITU-T Y.3170; ITU-T Y.qos-ml-arc; ITU-T Y.MecTA-ML; ITU-T Y.3531; ITU-T Y.3172; ITU-T H.CUAV-AIF; ITU-T F.VS-AIMC; ITU-T Y.4470
Zarządzanie ryzykiem	ISO/IEC 4213; ISO/IEC 25059; ISO/IEC 24029 -2	IEEE P7009; IEEE P2807; IEEE P2846	GS ARF 003; GR CIM 007; ENI GS 005; GR NFV-IFA 041; DGS SAI 003; EG 203 341; TS 103 194; TS 103 195.2; TR 103 821	ITU-T Y.qos-ml-arc; ITU-T Y.3172; ITU-T H.CUAV-AIF; ITU-T F.VS-AIMC; ITU-T Y.4470
Zarządzanie ryzykiem	ISO/IEC 23894; ISO/IEC 38507; ISO/IEC 42001; ISO/IEC 25059	IEEE 2801; IEEE P2863; IEEE P7000		

Tabela 2. Wykaz norm dotyczących wymagań określonych w AIA dla systemów SI wysokiego ryzyka (normy już opublikowane są pogrubione). Źródło: S. Nativi, S. De Nigris S., AI standardisation landscape state of play and link to the EC proposal for an AI regulatory framework, JRC Ispra, Italy 2021.

Jak wynika z przedstawionego wyżej wykazu, większość powołanych norm jest w trakcie opracowywania – zakończenie prac przewiduje się na lata 2021–2023. Przyporządkowanie poszczególnych norm do wymagań określonych w AIA, przedstawione w tabeli 2, dokonane zostało na podstawie streszczeń tych norm i ogólnego opisu wymagań. Jest to zatem odwzorowanie bardzo uogólnione, które nie uwzględnia pewnych szczegółów, w tym struktury i opisu prawnego poszczególnych wymogów AIA.

4. Dogłębna analiza norm i ocena ich przydatności

W kolejnej części raportu autorzy przedstawili wyniki systematycznej analizy poszczególnych norm w celu oszacowania, na ile są one odpowiednie i przydatne do określenia stopnia spełnienia wymagań AIA. To odwzorowanie, nazywane operacjonalizacją, polegało na przyporządkowaniu pewnych wskaźników dopasowania określonych norm do oceny zgodności systemu SI z wymaganiami AIA według schematu przedstawionego na rys. 2.

Rys. 2. Działania związane z szacowaniem operacjonalizacji, norm w zakresie ich przydatności do oceny zgodności systemów SI z wymaganiami AIA. Źródło: S. Nativi, S. De Nigris, AI standardisation landscape state of play and link to the EC proposal for an AI regulatory framework, JRC Ispra, Italy 2021.

Badania przeprowadzono, przekształciwszy zbiór wymagań określonych w projekcie rozporządzenia AIA w formie nieustrukturyzowanego tekstu do postaci wykonawczej składającej się z zestawu hierarchicznie uporządkowanych wymagań cząstkowych (ang. *subrequirements*) oznaczonych skrótami SR.#.# (np. SR.1 lub SR.1.1). Ostatecznie wyróżniono 24 takie podwymagania, do których wygenerowano reprezentatywne słowa kluczowe służące do eksploracji danych i wydobycia istotnych treści z analizowanych norm. Dogłębna analiza skoncentrowana została głównie na normach ISO/IEC zarządzanych przez JRC1/SC42 (sztuczna inteligencja). Podkomitet ten opracował specjalną normę (w fazie zapytania) dotyczącą „Koncepcji i terminologii sztucznej inteligencji" (tj. ISO/IEC DIS 22989). Norma ta definiuje SI zarówno z inżynierskiego, jak i dziedzinowego (tematycznego) punktu widzenia. Jest to norma fundamentalna, do której odnoszą się inne normy ISO dotyczące SI. Zgodnie z obecnym projektem ISO/IEC DIS 22989 SI to „zestaw metod lub zautomatyzowanych jednostek, które wspólnie budują, optymalizują i stosują model tak, aby system mógł, dla danego zestawu predefiniowanych zadań, obliczyć przewidywania, zalecenia lub decyzje. Systemy SI są zaprojektowane do działania z różnymi poziomami automatyzacji".

W wyniku przeprowadzonych badań dla każdej analizowanej normy wygenerowano kartę przedstawiającą odpowiednie wartości operacjonalizacji i przydatności do oceny zgodności systemu SI z wymaganiami określonymi w AIA. W dalszej części dla każdego z tych wymagań przedstawiono graficznie na wykresach radarowych cztery grupy norm charakteryzujących się zakresami odległości od celu, jakimi są te wymagania. Dla poszczególnych grup przyjęto następujące zakresy poziomu operacjonalizacji (p.o.):

- G1– bardzo wysoki poziom operacjonalizacji danego wymagania (p.o. ≥ 0,7);
- G2 – wysoki poziom operacjonalizacji danego wymagania (0,5 ≤ p.o. < 0,7);
- G3 – średni poziom operacjonalizacji danego wymagania (0,25 ≤ p.o. < 0,5);
- G4 – niski poziom operacjonalizacji danego wymagania (0,125 ≤ p.o. < 0,25).

Czytaj więcej

PUBLIKACJE

„Przebyliśmy długą drogę” – debata o dostępie do informacji publicznej opublikowana w „Dzienniku Gazecie Prawnej” z okazji 20-lecia uchwalenia ustawy o dostępie do informacji publicznej. W debacie wziął udział adw. dr hab. Grzegorz Sibiga, prof. INP PAN.

Publikacja debaty jest dostępna w ramach płatnego dostępu.

Czytaj więcej

Wywiad z adw. dr hab. Grzegorzem Sibiga, prof. INP PAN pt. **„Aktualne wyzwania w pracy Inspektorów ochrony danych”** opublikowany na łamach nr 9/2021 Newslettera Urzędu Ochrony Danych Osobowych dla Inspektorów Ochrony Danych Osobowych.

Czytaj więcej

„Przetwarzanie danych w systemach AI” - artykuł autorstwa adw. Katarzyny Syski, który ukazał się w kwartalniku ABI Expert (nr 3/2021)

Czytaj więcej

„Stan dziurawy informacyjnie” – artykuł autorstwa adw. dr hab. Grzegorza Sibiga, prof. INP PAN, który ukazał się na łamach Rzeczpospolitej

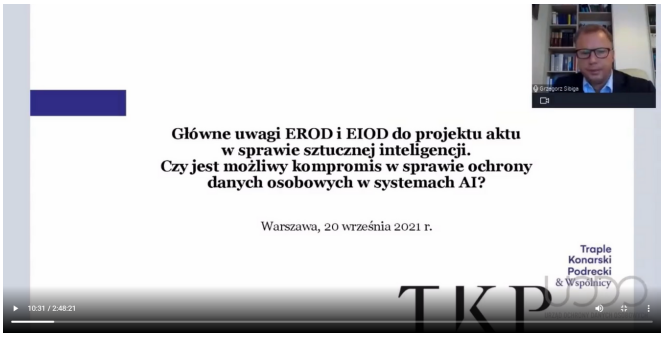
Czytaj więcej

„Wykorzystywanie danych biometrycznych uczniów tylko za dobrowolną zgodą” - analiza autorstwa Mateusza Kupca, która ukazała się na łamach portalu prawo.pl

Czytaj więcej

„Przetwarzanie danych osobowych przez pracodawców” – artykuł Mateusza Kupca, który ukazał się w kwartalniku ABI Expert (nr 3/2021)

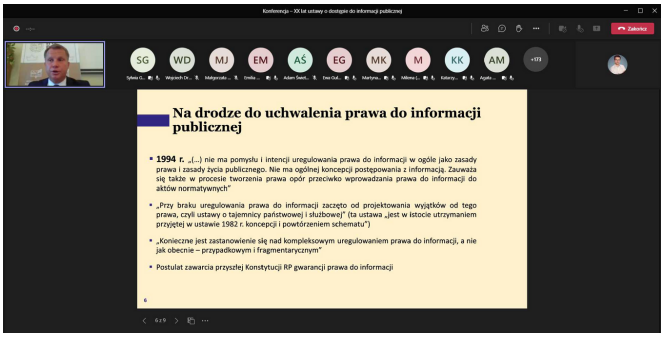
Czytaj więcej



Seminarium naukowe - 20 września 2021

Prelekcja adw. dr hab. Grzegorza Sibiga, prof. INP PAN pt. „Główne uwagi EROD i EIOD do projektu aktu w sprawie sztucznej inteligencji. Czy jest możliwy kompromis w sprawie ochrony danych osobowych w systemach Al?" wygłoszona podczas seminarium naukowego „Sztuczna Inteligencja a prawa podstawowe" organizowanego przez Urząd Ochrony Danych Osobowych.

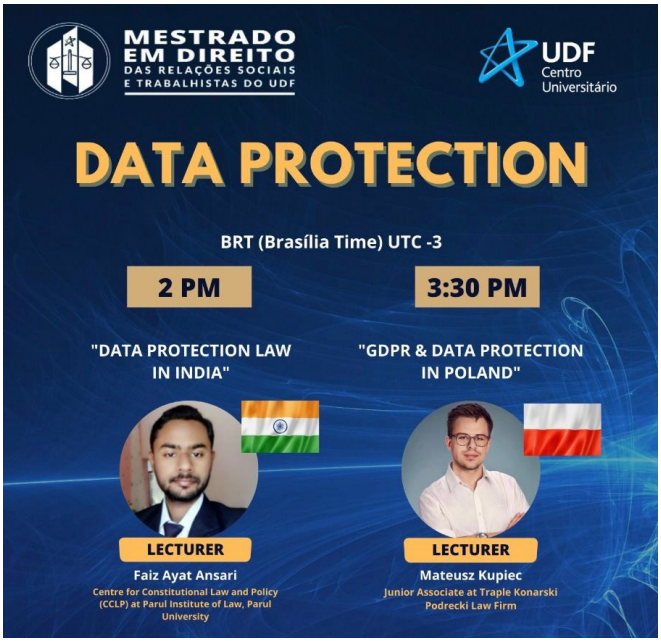
Więcej informacji



Konferencja naukowa - 28 października 2021

Wykład wprowadzający i udział w panelu dyskusyjnym adw. dr hab. Grzegorza Sibiga, prof. INP PAN podczas konferencji naukowej „XX lat ustawy o dostępie do informacji publicznej – podsumowanie i perspektywy ustawowej regulacji prawa do informacji publicznej" organizowanej przez Zakład Prawa Administracyjnego INP PAN.

Więcej informacji



Wykład online - 22 października 2021

Gościnny wykład online Mateusza Kupca dla słuchaczy programu Master of Laws na brazylijskim uniwersytecie UDF Centro Universitário dotyczący stosowania RODO w Polsce.

ZESPÓŁ RODO

Xawery Konarski
Adwokat, Senior Partner
xawery.konarski@traple.pl

Prof. INP PAN dr hab. Grzegorz Sibiga
Adwokat, Partner
grzegorz.sibiga@traple.pl

dr inż. Andrzej Kaczmarek
Of counsel
andrzej.kaczmarek@traple.pl

Katarzyna Syska
Adwokatka, Senior Associate
katarzyna.syska@traple.pl

Dominika Nowak
Radczyni prawna, Senior Associate
dominika.nowak@traple.pl

Mateusz Kupiec
Junior Associate
mateusz.kupiec@traple.pl

Redaktor newslettera:
Mateusz Kupiec

Pytania prosimy kierować na adres:
rodo@traple.pl