Conseil des barreaux européens

Council of Bars and Law Societies of Europe

Rada Adwokatur i Stowarzyszeń Prawniczych Europy

Association internationale sans but lucratif

Rue Joseph II, 40 /8 – 1000 Bruxelles

T. : +32 (0)2 234 65 10

Email: ccbe@ccbe.eu – www.ccbe.eu

Wytyczne CCBE w sprawie dostosowania prawników do wymogów Rozporządzenia 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 (dalej: „Rozporządzenie").

19/05/2017

W tym dokumencie Rada Adwokatur i Stowarzyszeń Prawniczych Europy (dalej: Rada)[1] dokonuje przeglądu głównych nowych środków dostosowawczych jakie Adwokatury i Stowarzyszenia Prawnicze mogą chcieć zalecić w celu zapewnienia przestrzegania wymogów określonych w Rozporządzeniu.

W kolejnych częściach tego dokumentu zwrócono uwagę na te zagadnienia wskazane w Rozporządzeniu, które skutkują nowymi lub poszerzonymi obowiązkami w zakresie przestrzegania Rozporządzenia dotyczącymi w szczególności prawników i kancelarii prawnych (dalej łącznie zwanych „firmami prawniczymi"). Zagadnienia te zostają ukazane w celu umożliwienia firmom prawniczym zidentyfikowania w prosty sposób tych kwestii problematycznych, które wymagają szczególnej uwagi. Jako że duża większość europejskich firm prawniczych pozostaje poniżej progu 250 pracowników, kwestie omówione poniżej nie odnoszą się zapisów mających zastosowanie wyłącznie do większych kancelarii prawnych (np. wymóg posiadania inspektora ochrony danych). Ponadto, zwraca się uwagę na fakt, że wiele kancelarii prawnych przetwarza dane osobowe, które są zaliczane do „szczególnych kategorii danych osobowych".

[1] Rada reprezentuje ponad milion prawników europejskich poprzez swoich członków – Adwokatury i Stowarzyszenia Prawnicze z 32 państw członkowskich i 13 krajów stowarzyszonych i obserwatorów.

A. Zgłoszenie naruszenia bezpieczeństwa

Zgodnie z zapisem art. 33 Rozporządzenia, firma prawnicza pełniąca rolę administratora zgłasza naruszenie ochrony danych osobowych organowi nadzorczemu bez zbędnej zwłoki, nie później niż w terminie 72 godzin po stwierdzeniu takiego naruszenia. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin należy dołączyć wyjaśnienie przyczyn opóźnienia. Wyjątek stanowi sytuacja gdy jest mało prawdopodobne, by naruszenie ochrony danych skutkowało poniesieniem szkody przez osoby, których dane dotyczą.

Jeżeli firma prawnicza pełni rolę podmiotu przetwarzającego, powiadamia administratora bez zbędnej zwłoki po stwierdzeniu naruszenia ochrony danych osobowych.

Zgłoszenie musi opisywać co najmniej: charakter naruszenia ochrony danych osobowych (wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie); możliwe konsekwencje naruszenia ochrony danych osobowych oraz środki zastosowane lub proponowane w celu zminimalizowania jego ewentualnych negatywnych skutków. Zgłoszenie może być dokonywane na różnych etapach.

Ponadto, administrator dokumentuje wszelkie takie naruszenia w sposób wystarczająco szczegółowy, aby organ nadzorczy był w stanie zweryfikować przestrzeganie zapisów dotyczących zgłaszania naruszenia. Firmy prawnicze muszą także wprowadzić procedury wewnętrzne, które będą stosowane do obsługi przypadków naruszeń danych oraz ustanowić mechanizm przekazywania zgłoszeń do organu nadzorczego.

Niektóre sytuacje wysokiego ryzyka będą wymagały od firmy prawniczej bezpośredniego zawiadomienia jej klientów o wystąpieniu naruszenia (art. 34 Rozporządzenia), choć mają tu zastosowanie szczególne odstępstwa.

Najwyraźniej, rzeczywisty format zgłoszenia, definicja „zbędnej zwłoki”, wymogi dotyczące treści dokumentacji i interpretacji przez organy nadzorcze progów i odstępstw mogą znacznie się różnić w poszczególnych państwach członkowskich.

Toteż firmy prawnicze powinny zostać poinformowane o już istniejących i potencjalnych przyszłych wytycznych w tych obszarach.

Chociaż niektóre państwa członkowskie już wprowadziły do swoich przepisów krajowych wymogi dotyczące zgłaszania naruszeń danych, dyrektywa nr 95/46/WE nie zobowiązywała administratorów do zgłaszania naruszeń danych do organów

nadzorczych. Wymóg taki istnieje jednakże w sektorze telekomunikacyjnym (zob. dyrektywa 2002/58/WE i Rozporządzenie Komisji (UE) 611/2013); obie te regulacje dotyczą dostawców usług łączności elektronicznej). To drugie rozporządzenie wykonawcze zostało określone ponadsektorowo, natomiast niektóre kraje członkowskie mogą posiadać bardziej szczegółowe wytyczne wydane przez organy nadzorcze dla sektora telekomunikacyjnego lub organy ochrony danych. Co ważniejsze, Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych ustanowiona na mocy dyrektywy 95/46/WE (Grupa robocza artykułu 29) wydała także szczegółowe wytyczne dotyczące wdrożenia rozporządzenia z zakresu naruszeń ochrony danych (Opinia 03/2014 (WP 213) w sprawie zgłaszania naruszeń ochrony danych z dnia 25 marca 2014 r. (ang. *WP 213 Opinion 03/2014 on Personal Data Breach Notification, 25 March 2014*)[2]), w którym wskazano wszystkim administratorom najlepsze praktyki w tym obszarze.

Jeżeli chodzi o przyszłe regulacje w tym obszarze, na mocy art. 70 ust. 1 lit. g) i h) Rozporządzenia także Europejska Rada Ochrony Danych będzie prawdopodobnie wydawać wytyczne, zalecenia i najlepsze praktyki z zakresu a) stwierdzania wystąpienia naruszeń, b) definiowania terminu „zbędna zwłoka", c) okoliczności, w których administrator i podmiot przetwarzający dane mają obowiązek zgłosić przypadek naruszenia organowi nadzorczemu lub powiadomić o tym fakcie swoich klientów.

B. Prawo do bycia zapomnianym

Art. 17 Rozporządzenia zawiera prawo do usunięcia danych („prawo do bycia zapomnianym"), które oznacza, że osoby, których dane dotyczą mają prawo żądania od administratora niezwłocznego usunięcia dotyczących ich danych osobowych. Ten sam artykuł nakłada na administratora obowiązek usunięcia danych osobowych bez zbędnej zwłoki gdy zachodzi którakolwiek z okoliczności wskazanych w ust. 1 lit. a) do f). Zapis ma swoje źródło w sprawie **Google Spain SL, Google Inc. przeciw Agencia Española de Protección de Datos, Mario Costeja González[3], w której Sąd stwierdził, że** osoby fizyczne mają prawo (z zastrzeżeniem określonych

[2] Dokument dostępny na stronie: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

[3] http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30d57637cb18820e4ceb913ecf71af33028d.e34KaxiLc3qMb40Rch0SaxuTahn0?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1115616.

wymogów i środków ochrony) żądania od wyszukiwarek usunięcia łączy (linków) zawierających ich dane osobowe. Jednakże ust. 3 lit. e) art. 17 zawiera istotne ograniczenie, na które mogą się powoływać firmy prawnicze w zakresie w jakim przetwarzanie jest niezbędne „do ustalenia, dochodzenia lub obrony roszczeń".

Należy zaznaczyć, że przepis ten nie skutkuje oczywiście unieważnieniem określonych obowiązków lokalnych dotyczących przechowywania danych przez określony okres czasu (np. w celu wywiązania się z obowiązków podatkowych).

C. Inspektor ochrony danych

Obowiązek wyznaczenia inspektora ochrony danych przez kancelarie prawne

Kolejnym nowym elementem jest wymóg wyznaczenia inspektora ochrony danych gdy operacje przetwarzania danych przez organizację wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę lub gdy przetwarzane są na dużą skalę szczególne kategorie danych osobowych (art. 37 Rozporządzenia). Grupa robocza artykułu 29, którą tworzą przedstawiciele organów ochrony danych państw członkowskich UE wydała Wytyczne dotyczące funkcji inspektora ochrony danych (ang. *Guidelines on DPO's*) w celu uściślenia jego roli i zapewnienia zaleceń dotyczących najlepszych praktyk.

W sytuacji wyznaczenia inspektora ochrony danych, organizacja publikuje dane inspektora ochrony danych i przekazuje te informacje właściwemu organowi nadzorczemu.

Art. 9 Rozporządzenia definiuje szczególne kategorie danych osobowych[4], których przetwarzanie jest zabronione, ale podaje też pewne wyjątki: na mocy art. 9 ust. 2 lit. f) zakaz nie ma zastosowania, gdy przetwarzanie danych jest niezbędne do „ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy". Toteż, zapis ten sankcjonuje przetwarzanie szczególnych kategorii danych w kontekście prac wykonywanych przez firmy prawnicze i dotyczących sporów prawnych.

Jednakże art. 37 Rozporządzenia (a także art. 35, zob. poniżej) w dalszym ciągu ma zastosowanie do administratora i podmiotu przetwarzającego szczególne

[4] Tzn. „[...] dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby [...]".

kategorie danych. Zapisy te wymagają *wyznaczenia inspektora ochrony danych* zawsze gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 Rozporządzenia. Zgodnie z Wytycznymi dotyczącymi inspektora ochrony danych, „główna działalność" może być rozumiana jako kluczowa działalność służąca realizacji celów przez administratora lub podmiot przetwarzający dane. Działalność ta obejmuje także wszelką działalność gdzie przetwarzanie danych stanowi nieodłączny element działalności administratora lub podmiotu przetwarzającego dane."

Istotną kwestię stanowi znaczenie terminu „na dużą skalę", ponieważ mniejsza kancelaria prawna może prowadzić sprawy obejmujące duże wolumeny danych. Jednakże, w prosty sposób można argumentować, cytując motyw 91, że wymóg nie będzie miał zastosowania do prawników działających indywidualnie (zob. punkt D poniżej poświęcony ocenom skutków).

Obowiązki i zadania inspektora ochrony danych

Rozporządzenie nakłada na inspektora ochrony danych istotne obowiązki takie jak: wymóg monitorowania przestrzegania Rozporządzenia, innych przepisów unijnych lub przepisów państw członkowskich z zakresu ochrony danych oraz polityk administratora lub podmiotu przetwarzającego, w tym zadania i obowiązki dotyczące budowania świadomości i szkolenia personelu zaangażowanego w przetwarzanie oraz przeprowadzania audytów w tym obszarze. Ponadto inspektor ochrony danych pełni funkcję punktu kontaktowego dla organów ochrony danych.

Niezależnie od tego czy wyznaczony inspektor ochrony danych jest pracownikiem czy też nie firmy prawniczej, osoba taka powinna posiadać wiedzę ekspercką w zakresu przepisów dotyczących ochrony danych i być w stanie w pełni wykonywać zadania określone w art. 39 Rozporządzenia, takie jak przechowywanie dokumentacji wszystkich czynności przetwarzania, monitorowanie ich wykonywania oraz szkolenie pracowników czy przeprowadzanie audytów itd. Stosownie, osoba pełniąca rolę inspektora ochrony danych przyjmuje na siebie dużo ważnych obowiązków.

Prawnicy pełniący rolę inspektora ochrony danych

Można by pomyśleć, że prawnik będzie osobą najbardziej odpowiednią do wyznaczenia na inspektora ochrony danych. Należy jednak mieć na uwadze, że zważywszy na zróżnicowanie obowiązków przewidzianych Rozporządzeniem osoba wyznaczona na inspektora ochrony danych będzie musiała dysponować nie tylko rozległą wiedzą prawniczą.

Asymilacja dwóch funkcji (prawnika/ inspektora ochrony danych) i ryzyko pomylenia tych funkcji stanowią kluczową kwestię dla każdego prawnika, który mógłby zostać wyznaczony na inspektora ochrony danych na prośbę klienta. Prawnik, który zostaje powołany do pełnienia takiej roli, może stwierdzić, że będzie musiał odgrywać naprzemiennie rolę inspektora ochrony danych i rolę prawnika wykonującego zawód regulowany. Prawnik pełniący rolę inspektora ochrony danych będzie musiał zapewnić sobie niezależność i będzie musiał unikać konfliktów interesów, zwłaszcza tych, które mogą wynikać z jednoczesnego pełnienia funkcji punktu kontaktowego dla organu ochrony danych (rola, które obejmuje obowiązki dokonywania zgłoszeń do organów nawet w sytuacji gdy takie zgłoszenie nie jest w interesie administratora lub podmiotu przetwarzającego dane) i wykonywania obowiązku reprezentowania interesów klientów w pełnym zakresie przewidzianym przepisami prawa. Przewidując potencjalny konflikt interesów, Adwokatury i Stowarzyszenia Prawnicze mogą chcieć zalecić prawnikom, aby podejmowali się pełnienia roli inspektora ochrony danych wobec klienta zewnętrznego tylko w sytuacji gdy ani nigdy wcześniej nie działali jako prawnicy w zakresie kwestii objętych zadaniami inspektora ochrony danych ani nie będą przez okres pełnienia roli inspektora ochrony danych działali jako prawnicy w kwestiach, w które byli lub są zaangażowani jako inspektor ochrony danych.

D. Ocena skutków

Zgodnie z art. 35 Rozporządzenia, jeżeli dany rodzaj przetwarzania z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym każde przetwarzanie na dużą skalę szczególnych kategorii danych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania (w szczególności dla przetwarzania z użyciem nowych technologii i mając na uwadze cele przetwarzania itd.).

Należy zaznaczyć, że motyw 91 zawiera wyjaśnienie, że przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych klientów pojedynczego prawnika. Jest to wyjątek, który w jasny sposób ma zastosowanie do prawników działających indywidualnie, jednakże nawet mała firma prawnicza może zostać zobowiązana do okresowego dostarczenia takich ocen skutków.

Kłopot polega na tym, że zgodnie z obecnymi istniejącymi (ponadsektorowymi) standardami w zakresie organizacji oceny skutków dla ochrony danych, taka ocena skutków może okazać się wymogiem zaporowym dla małych firm. Przykładowo, nawet sam wymóg dotyczący administratorów w zakresie identyfikacji oprogramowania i sprzętu komputerowego wykorzystywanych do obsługi danych osobowych może zostać zinterpretowany przez określone organy jako wymóg wdrożenia systemu zarządzania zmianą i konfiguracją. Ogólnie rzecz biorąc, od małych firm prawniczych posiadających kilku pracowników (ale pozostających powyżej progu „pojedynczego prawnika") nie wymaga się z zasady ścisłego przestrzegania tych wymogów w każdym przypadku. System zarządzania zmianą wymagałby kontrolowanego i zaawansowanego korzystania z systemu informatycznego, które to korzystanie nie jest za zwyczaj typowe dla firm tej wielkości (posiadanie ogólnej informacji na temat składowych środowiska informatycznego, którymi dysponuje firma w znaczącym stopniu różni się od posiadania działającego i objętego kontrolą procesu zarządzania zmianą i konfiguracją).

Niestety ani Wytyczne dotyczące funkcji inspektora ochrony danych wydane przez Grupę roboczą artykułu 29 w dniu 13 grudnia 2016 r. ani obecnie dostępny projekt Wytycznych dotyczących oceny skutków dla ochrony danych (ang. *WP29 Guidelines on Data Protection Impact Assessment*) nie zapewniają dalszych wskazówek w tym zakresie. Odnośnie do motywu 91, przypis 14 Wytycznych dotyczących funkcji inspektora ochrony danych wskazuje, że wszystkie kwestie z zakresu pomiędzy przetwarzaniem przez pojedynczego prawnika a przetwarzaniem danych dla całego kraju stanowią obszar niezbadany. Taki brak jasności nieuchronnie będzie skutkował wielością interpretacji.[5]

[5] Jako że w czasie gdy materiał ten był opracowywany Grupa robocza artykułu 29 w dalszym ciągu zbierała uwagi interesariuszy do projektu Wytycznych dotyczących oceny skutków dla ochrony danych, aktualna i ostateczna wersja tego dokumentu może zostać opublikowana w 2017 roku i będzie prawdopodobnie zawierała dalsze wyjaśnienia w zakresie interpretacji terminu „duża skala" w odniesieniu do czynności przetwarzania.

Chociaż skutkuje to nowym obciążeniem dla firm prawniczych, poprzez przeprowadzanie ocen skutków regulacja ma nadzieję umożliwić firmom prawniczym zidentyfikowanie i podjęcie działań ograniczających w odniesieniu do ryzyka, które w przeciwnym razie pozostałoby niezauważone oraz przeciwdziałanie naruszeniom, które w przeciwnym razie mogłyby wystąpić.

Przeciwnie do przypadku zgłoszenia naruszenia ochrony danych, nie istnieją żadne przeszłe przypadki czy wytyczne regulacyjne, które określałyby w jaki sposób kancelarie prawne czy osoby wykonujące podobne profesje powinny przeprowadzać ocenę skutków.

Obecnie oceny skutków dla ochrony danych przeprowadza się w różny sposób i z wykorzystaniem różnych metod; oceny te są najbardziej popularne w krajach posiadających tradycję prawa precedensowego.[6] W Europie, Biuro Komisarza ds. Informacji Zjednoczonego Królestwa (ang. Information Commissioner's Office of the United Kingdom) wydało w 2014 r. Kodeks dobrych praktyk w zakresie oceny skutków dla ochrony prywatności (ang. *Privacy Impact Assessment Code of Practice*)[7] (w następstwie Instrukcji oceny skutków dla ochrony prywatności (ang. *Privacy Impact Assessment Manual*) wydanej w 2007 r.), natomiast w 2015 r. francuski organ ochrony danych (CNIL) wydał Instrukcję oceny skutków dla ochrony prywatności (ang. *Privacy Impact Assessment Manual*).[8] Także Komisja Europejska wydała zalecenie, w którym wzywała do przeprowadzania ocen skutków dla chipów RFID[9] i które skutkowało publikacją w dniu 12 stycznia 2011 r. Propozycji sektora w sprawie ram oceny skutków w zakresie ochrony danych i prywatności w zastosowaniach RFID (ang. *Privacy and Data Protection Impact Assessment Framework for RFID Applications*). Ta ostatnia propozycja została zatwierdzona przez Grupę roboczą artykułu 29 i służyła także jako wzór do opracowania podobnego „szablonu" dla inteligentnych liczników.[10]

---

[6] Przyjmuje się, że wywodzące się ze Stanów Zjednoczonych oceny oddziaływania na środowisko stanowią podstawy przeprowadzania oceny skutków dla prywatności, zob. raport PIAF (ang. *Deliverable D1 of PIAF*) na stronie http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf.

[7] Zob. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

[8] Zob. https://www.cnil.fr/fr/node/15798.

[9] Zob. Zalecenie Komisji 2009/387/WE, na stronie http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:EN:PDF.

[10] Zob. Zalecenie Komisji 2012/148/WE i jego zatwierdzenie przez przez Grupę roboczą artykułu 29 na stronie http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_en.pdf.

Niestety zalecenia te dotyczą tylko omawianych przez nie kwestii i raczej nie przydadzą się jako praktyczne wskazówki przy przeprowadzaniu ocen skutków przez prawników lub osoby wykonujące podobne profesje w kontekście zgłoszeń naruszenia ochrony danych. Więcej informacji należy oczekiwać na poziomie krajowych szczegółowych regulacji sektorowych, jeżeli takie zostaną opracowane.

Wyniki zleconej przez Komisję analizy ocen skutków dla prywatności (Ramy oceny skutków dla prywatności w zakresie praw do ochrony danych i prywatności, (ang. *Privacy Impact Assessment Framework for data protection and privacy rights*)) mogą okazać się przydatne dla prawników zainteresowanych historią ocen skutków dla prywatności.[11]

Podsumowując, chociaż rozporządzenie jako takie przedstawia pewne informacje szczegółowe na temat ocen skutków, faktyczne wymogi praktyczne nie są jeszcze znane. Oczekuje się, że organy nadzorcze i Rada wskazana powyżej zapewnią dalsze wskazówki w zakresie brakujących informacji takich jak informacje dotyczące rodzaju przetwarzania, dla którego taka ocena skutków może być wymagana.

E. Przenoszenie danych

Osoby, których dane dotyczą mają prawo otrzymać od administratora kopię danych osobowych ich dotyczących, które są lub były przetwarzane. Art. 20 Rozporządzenia wymaga przekazania takich danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, ale jest to tylko wymóg bardzo ogólny.

Zgodnie z Wytycznymi Grupy roboczej artykułu 29 dotyczącymi prawa do „przenoszenia danych" (ang. *WP29 Guidelines on the right to "data portability"*) terminy „ustrukturyzowany", „powszechnie używany" i „nadający się do odczytu maszynowego" stanowią zbiór minimalnych wymogów, które powinny ułatwić interoperacyjność formatu danych dostarczanych przez administratora danych. Wytyczne Grupy roboczej artykułu 29 wskazują ponadto, że mając na uwadze szeroki zakres potencjalnych rodzajów danych, które mogą być przetwarzane przez administratora danych, Rozporządzenie nie wprowadza szczegółowych zaleceń w zakresie formatu dostarczanych danych osobowych.

[11] http://www.piafproject.eu/About%20PIAF.html.

Chociaż wymóg powszechnie używanego formatu nadającego się do odczytu maszynowego jest prosty do spełnienia, kwestia „ustrukturyzowanego” formatu może okazać się istotnym problemem. Dokumenty, na których pracują prawnicy są zazwyczaj nieustrukturyzowane jeżeli chodzi o zawarte w nich treści (np. formaty Microsoft Word czy PDF). Nie istnieje jeden powszechnie przyjęty format obsługi wszystkich dokumentów czy spraw sądowych, który stanowiłby format ustrukturyzowany.

Wszyscy prawnicy wiedzą w jaki sposób należy przekazywać dokumenty do nowych kancelarii prawnych, wybranych przez ich poprzednich klientów, ale czasem dokładny format i układ takich przekazywanych dokumentów może już sam w sobie stanowić przedmiot sporu prawnego. W przyszłości, problem ten może wymagać dalszego uregulowania przez Adwokatury i Stowarzyszenia Prawnicze.

F. Możliwość ustalenia odbiorców danych osobowych

Administratorzy danych mają obowiązek zapewnienia możliwości ustalenia odbiorców danych osobowych dotyczących określonej osoby (przynajmniej w zakresie nazwy/imienia i nazwiska oraz elektronicznych danych kontaktowych). To też jest obowiązek, który często mógłby zostać spełniony przez firmy prawnicze, gdyby wprowadziły one pewne zmiany w swoich systemach informatycznych (np. skonfigurowały system w taki sposób, aby zapewniał wiarygodny i możliwy do ustalenia zapis odbiorców danych osobowych).