Lista lektur prawniczych Inspektora Ochrony Danych

Inspektor Ochrony Danych to bardzo „młody" zawód. Oczekiwania co do zakresu wiedzy i kompetencji IODa bywają diametralnie różne. W dzisiejszym wpisie przyjrzymy się wiedzy i umiejętnościom, które powinien posiadać IOD.

Co na temat kompetencji IODa mówi RODO?

„Art. 37 ust. 1 pkt. 4

Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39."

Autorzy RODO użyli sformułowania o fachowej wiedzy na temat prawa. Wykształcenie prawnicze wydaje się być preferowane przez twórców RODO.

Prawo to jednak zdecydowanie nie wszystko!

Czy nie-prawnik może być dobrym IODem?

Zdecydowanie TAK! Warunkiem jest jednak to, że nasz Inspektor uzyska wsparcie prawników.

Od czasów Administratora Bezpieczeństwa Informacji, niewiele się zmieniło. Odwieczna dyskusja odnośnie tego czy ABI powinien być:

1) Prawnikiem,
2) Informatykiem,
3) Specjalistą od ISO,
4) Czy jeszcze kimś innym...

Trwa po dziś dzień. Ta dyskusja jest według mnie całkowicie jałowa. Obecnie modeli sprawowania funkcji IOD jest bardzo wiele.

Bo prawo to nie wszystko!

Poza wskazaną w RODO wiedzą prawniczą, IOD powinien także:

1) Posiadać wiedzę informatyczną,
2) Dysponować umiejętnościami miękkimi (w tym prowadzenia szkoleń),
3) Być dobrym managerem i organizatorem,
4) Dysponować szeroką wiedzą na temat branży, w której działa jego organizacja.

Idealny IOD jest więc wziętym prawnikiem, informatykiem, szkoleniowcem i jednocześnie dobrym managerem.

Czy ktoś z Państwa zna osoby o tak szerokiej wiedzy i kompetencjach? Ja nie znam. I sam nie czuje się komfortowo we wszystkich tych obszarach łącznie.

Co więc powinien zrobić wystarczająco dobry IOD?

Wystarczająco dobry IOD, jest w pełni świadom niemożliwości bycia ekspertem, we wszystkich obszarach, o których pisałem w poprzednim akapicie.

To niemożliwe!

Możliwe jest za to takie ułożenie sobie współpracy wewnątrz organizacji, aby obszary w których IOD czuje się mniej pewnie, powierzyć innym osobom.

Jeśli IOD nie jest prawnikiem – sugeruję powierzyć prace nad umowami powierzenia czy klauzulami zgód, działowi prawnemu.

Jeśli IOD nie jest informatykiem, niech za obszar bezpieczeństwa IT odpowiada odpowiednio kompetentny informatyk.

Jeśli IOD ma lęk przed wystąpieniami publicznymi i nie chce szkolić pracowników – niech powierzy to działanie zewnętrznym lub wewnętrznym trenerom.

Rozwiązań i sposobów poradzenia sobie z brakiem wiedzy i umiejętności w poszczególnych obszarach jest bardzo dużo.

Największym błędem jest próba bycia ekspertem w każdej sferze, na którą oddziałuje RODO.

Co IOD prawnik powinien przeczytać?

W dzisiejszym wpisie przygotowałem coś dla wszystkich IODów, specjalizujących się w obszarze prawniczym.

Poniższa tabela zawiera ważne akty prawne/rekomendacje/opinie/publikacje, które powinien znać każdy IOD – prawnik.

Wykaz podstawowych aktów prawnych / wytycznych / innych materiałów dla Inspektora Ochrony Danych

Lp.	Nazwa	Liczba stron	Link
Akty prawne			
1.	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)	88	Tekst uchwalony: https://uodo.gov.pl/pl/131/224
			Skonsolidowany tekst (po sprostowaniu): https://uodo.gov.pl/pl/131/539

2.	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.)	58	http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001000
3.	Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn. Dz.U. z 2019 r. poz. 123, 730, ze zm.)	2	http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20021441204
4.	Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (tekst jedn. Dz.U. z 2018 r. poz. 1954 ze zm.)	10	http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041711800
5.	Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (tekst jedn. Dz.U. z 2019 r. poz. 1040,1043)	6	http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19740240141
6.	Rozporządzenie Ministra Pracy i Polityki Socjalnej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej (tekst jedn. Dz.U. z 2018 r. poz. 2369)	9	http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180002369/O/D20182369.pdf
Wytyczne / poradniki Prezesa Urzędu Ochrony Danych Osobowych			
7.	Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony	5	http://monitorpolski.gov.pl/MP/2019/666
8.	*Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców* – poradnik przygotowany przez Prezesa Urzędu Ochrony danych Osobowych	44	https://uodo.gov.pl/pl/138/545
9.	*Jak rozumieć podejście oparte na ryzyku według RODO?* – poradnik przygotowany przez Prezesa Urzędu Ochrony danych Osobowych (część I)	21	https://giodo.gov.pl/pl/1520282/10294
10.	*Jak stosować podejście oparte na ryzyku?* – poradnik przygotowany przez Prezesa Urzędu Ochrony danych Osobowych (część II)	42	https://giodo.gov.pl/pl/1520282/10294
11.	Wskazówki i wyjaśnienia Prezesa Urzędu Ochrony Danych Osobowych dotyczące obowiązku rejestrowania czynności i kategorii	16	https://www.giodo.gov.pl/pl/1520281/10449

	czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO		
12.	Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego	28	https://uodo.gov.pl/pl/138/354
Decyzje Prezesa Urzędu Ochrony Danych Osobowych			
13.	Decyzje Prezesa Urzędu Ochrony Danych Osobowych (opublikowane na stronie www.uodo.gov.pl, wg. stanu na 12.08.2019 r. publikowanych jest 113 decyzji)	...	https://uodo.gov.pl/pl/p/decyzje
Opinie i wytyczne Europejskiej Rady Ochrony Danych / Grupy Roboczej Art. 29			
14.	Wytyczne 1/2018 dotyczące certyfikacji i określania kryteriów certyfikacji zgodnie z artykułami 42 i 43 rozporządzenia 2016/679	18	https://uodo.gov.pl/pl/10/540
15.	Wytyczne 2/2018 w sprawie wyjątków określonych w art. 49 rozporządzenia 2016/679	18	https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_pl.pdf
16.	Wytyczne 3/2018 dotyczące terytorialnego zakresu stosowania RODO (język angielski)	23	https://uodo.gov.pl/pl/138/584
17.	WP 262 Wytyczne dotyczące art. 49 (język angielski)	17	https://uodo.gov.pl/pl/11/23
18.	WP 261 Wytyczne dotyczące akredytacji podmiotów certyfikujących (język angielski)	12	https://uodo.gov.pl/pl/11/24
19.	WP 260 Wytyczne dotyczące przejrzystości na podstawie rozporządzenia 2016/679	45	https://uodo.gov.pl/pl/10/434
20.	WP 259 Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679	35	https://uodo.gov.pl/pl/10/428
21.	WP 257 Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych dla podmiotów przetwarzających (język angielski)	22	https://uodo.gov.pl/pl/11/19

22.	WP 256 Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które mają zostać uwzględnione w wiążących regułach korporacyjnych (język angielski)	20	https://uodo.gov.pl/pl/11/18
23.	WP 254 Dokument dotyczący adekwatności (język angielski)	9	https://uodo.gov.pl/pl/11/21
24.	WP 253 Wytyczne w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679	18	https://uodo.gov.pl/pl/10/13
25.	WP 251 Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE	44	https://uodo.gov.pl/pl/10/11
26.	WP 250 Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzenia 2016/679	39	https://uodo.gov.pl/pl/10/12
27.	WP 249 Opinia 2/2017 na temat przetwarzania danych w miejscu pracy	28	https://uodo.gov.pl/pl/10/10
28.	WP 248 Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679	29	https://uodo.gov.pl/pl/10/9
29.	WP 244 Wytyczne dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmioty przetwarzającego	14	https://uodo.gov.pl/pl/10/5
30.	WP 243 Wytyczne dotyczące inspektorów ochrony danych	26	https://uodo.gov.pl/pl/10/7
31.	WP 242 Wytyczne dotyczące prawa do przenoszenia danych	24	https://uodo.gov.pl/pl/10/6
32.	WP 169 Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"	38	https://giodo.gov.pl/pl/1520057/3595
33.	WP 89 Opinia 4/2004 w sprawie przetwarzania danych osobowych przy nadzorze z użyciem kamer video	33	https://giodo.gov.pl/pl/1520189/7146

Materiały pomocnicze			
34.	P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018	923	
35.	E. Bielak-Jomaa (red.), D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz,* Warszawa 2017	1168	
36.	M. Sakowska-Baryła (red), Ogólne rozporządzenie o ochronie danych osobowych. Komentarz	684	
37.	P. Litwiński (red.), P. Barta / D. Dörre-Kolasa, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018	648	
PODSUMOWANIE		**ŁĄCZNIE 4 264 stron**	

Wyliczona przez z nas powyżej, liczba stron jest mocno szacunkowa. Podobnie jak zaprezentowany wykaz „lektur", który w konkretnym przypadku może być krótszy, ale też i dłuższy. Każdy Inspektor Ochrony Danych powinien bowiem zapoznać się także z przepisami sektorowymi dotyczącymi obszaru działalności podmiotu, który go wyznaczył na tę funkcję np. medycyna, oświata, samorząd terytorialny itp. Ostateczna ilość i obszerność materiałów z którymi będzie musiał zaznajomić się IOD zależeć będzie od branży, w której działa administrator i przedmiotu jego działalności, a także zakresu obowiązków IOD.

Ponadto wytycznych EROD czy UODO cały czas przybywa. Powyższe zestawienie rośnie z miesiąca na miesiąc.

Wnioski

Mam kilka wniosków, płynących z lektury powyższej tabeli:

1) Jeśli jesteś początkującym prawnikiem i właśnie zostałeś człowiekiem od RODO w swojej organizacji, to potrzebujesz dużo czasu, aby rzetelnie zapoznać się z powyższą listą.

2) Profesjonalne pełnienie funkcji IODa w dużej organizacji na doczepkę, obok 20 innych ważnych obszarów, jest niemożliwe.

3) Bycie dobrym prawnikiem w obszarze RODO wymaga specjalizacji. Nie wyobrażam sobie naszych ekspertów zajmujących się równocześnie prawem nowych technologii czy zamówień publicznych.

A jak z ilością potrzebnej do przyswojenia wiedzy radzi sobie nasz ekspert?

Ewelina Rećko, ekspert ds. ochrony danych osobowych

Sprawowanie funkcji IOD to duże wyzwanie. Żeby się z niego wywiązać konieczne jest ciągłe dokształcanie, śledzenie bieżących zmian (w tym roku zmianie uległo blisko 170 aktów prawnych!), czytanie wielu, często sprzecznych opinii ekspertów z branży, żeby ostatecznie przyjąć rozwiązanie bezpieczne i pro-biznesowe.
Przy wypracowaniu odpowiedniej koncepcji przetwarzania danych niezwykle cenne okazuje się posiadania kilkuosobowego Zespołu IOD, który wspiera się nawzajem specjalistyczną wiedzą.

Podsumowanie

Lista lektur obowiązkowych z samego obszaru prawnego jest pokaźna. I wciąż rośnie. Jako IODowie potrzebujemy czasu na zapoznanie się z ww. pozycjami. Potrzebujemy się nieustannie doskonalić i aktualizować naszą wiedzę.

Jeśli ktoś trywializuję naszą pracę do poziomu jednego Rozporządzenia (RODO), liczącego sobie zaledwie 99 artykułów – niech załączona tabela będzie krótką i celną ripostą.

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu

Źródła:

- 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)
- praktyczne doświadczenie budowania systemów ochrony danych osobowych od 2008 roku (jako ABI) i po 2018 (jako IOD).