Wdrożenie RODO, czyli kto jest kim na RODO szachownicy?

Każde wdrożenie RODO napotyka na kilka punktów szczególnego oporu. Tak nazywam kluczowe momenty, które wymagają podjęcia decyzji biznesowych, interpersonalnych i są po prostu ważne dla Twojej organizacji.

O jednym z takich momentów właśnie czytasz. Jest nim zbudowanie struktury organizacyjnej, które zapewni rozliczalność RODO w Twojej organizacji.

Skąd się bierze opór przy budowaniu struktury?

Na początku odpowiedzmy sobie na pytanie - czym w ogóle jest struktura organizacyjna RODO?

Na potrzeby tego tekstu, zdefiniuję ją jako: *podział ról i obowiązków, związanych z prawidłowym funkcjonowaniem RODO w organizacji*.

Do konkretnych ról (np. Administratora Systemów Informatycznych), zostaną przypisane konkretne obowiązki.

Prawie każde wdrożenie RODO, które realizujemy, traci rozpęd w momencie ustalania struktury organizacyjnej. Czasem może to budzić pewną frustrację ze strony osób wdrażających. Jednak jeśli przyjrzymy się bliżej przyczynom oporu wdrożeniowego, to okaże się, że warto na chwile zwolnić. Dzięki temu mamy szansę poznać konkretne obawy osób, które przejmą nowe role i nowe obowiązki. Jeśli w żaden sposób nie odpowiemy na te obawy czy wątpliwości, to wdrożenie prawdopodobnie zakończy się tzw. „papierowym wdrożeniem".

Poprzez papierowe wdrożenie RODO, rozumiem sytuację, kiedy co prawda role są obsadzone i zdefiniowane, polityka ochrony danych osobowych jest podpisana, ale w praktyce… to wszystko nie działa. Jeśli nie przyjrzymy się konkretnym obawom Zespołu, związanym z nową rolą i odpowiedzialnością, to ryzykujemy właśnie „papierowe wdrożenie RODO". W skrajnych przypadkach nie dojdzie nawet do „wdrożenia papierowego". Wydarzy się tak np. wtedy, kiedy ważną funkcję będzie miał sprawować wspólnik lub wspólniczka czy inna osoba funkcyjna w organizacji. Taka osoba zaniepokojona nową rolą i obowiązkami z niej wynikającymi, po prostu nie podpisze polityki ochrony danych osobowych. A jak już wielokrotnie pisaliśmy na łamach naszego bloga, brak polityki podpisanej przez osobę uprawnioną do reprezentacji Administratora danych, jest tożsamy z brakiem tej polityki w oczach regulatora. Przypominam, że w PODO znajdują się najczęściej wszystkie kluczowe, wymagane przez RODO procedury.

Król, czyli Administrator danych osobowych

Rozstawiamy zatem nasze figury na szachownicy! Administrator danych to nasza organizacja. Spółka prawa handlowego, osoba fizyczna prowadząca działalność gospodarczą, organizacja pozarządowa czy

jednostka administracji publicznej. Na naszej szachownicy, podobnie jak w grze w szachy, rola ADO będzie z jednej strony kluczowa, z drugiej strony dość ograniczona.

Administratorem danych osobowych się po prostu jest. W tym miejscu nie ma pola do dyskusji czy wyboru. Jeśli Twoja organizacja przetwarza dane osobowe (jak 99,9% organizacji), to staje się Administratorem danych osobowych. Wszystkie RODO obowiązki są adresowane do Administratora danych osobowych. Z kolei ADO jest reprezentowany najczęściej przez Zarząd. W dużych organizacjach, Zarząd nie angażuje się osobiście w obszary związane z RODO. Deleguje je na zewnątrz (outsourcing) lub do wewnątrz organizacji. Jeśli Zarząd nie angażuje się w kwestie związane z RODO, powinien przynajmniej raz do roku przeanalizować raport z audytu i usłyszeć osobiście, od osoby zajmującej się RODO, jaki jest status wdrożenia. Zdecydowanie zalecam, przynajmniej minimalny poziom wiedzy Zarządów o tym co dzieje się na RODO szachownicy w zarządzanych przez nich organizacjach.

Poza przyjmowaniem raportów, Zarząd powinien być włączany w sytuacje podejmowania kluczowych decyzji, związanych z RODO. Może zdarzyć się tak, że ważna opinia IOD lub innej kluczowej osoby, nie jest jednoznaczna. Obrazując to przykładem. Firma z branży IT zastanawia się nad zmianą framework'u swojego kluczowego systemu informatycznego. Dotychczasowy framework przestał otrzymywać wsparcie od producenta. Co teraz? Wymiana frameworku systemu to ogromne koszty finansowe. Z drugiej strony opinie dotyczące bezpieczeństwa dotychczasowego framework'u, są mocno podzielone. Część specjalistów jest zdania, że system będzie bezpieczny. Część uważa, że framework powinien zostać wymieniony. IOD lub inna osoba odpowiedzialna za RODO widzi rozsądne argumenty po obu stronach dyskusji.

To jest właśnie moment, kiedy do gry powinien wejść król, to znaczy Administrator danych osobowych. To ADO powinien podjąć finalną biznesową decyzję w oparciu o rzetelne i wiarygodne informacje zgromadzone przez osoby zajmujące się RODO w organizacji.

Oczywiście tak to wygląda w dużych organizacjach. W małych kilkuosobowych firmach, Zarządy będą osobiście zaangażowane w kwestie związane z RODO na poziomie operacyjnym.

Królowa, czyli osoba realnie zarządzająca RODO

Jeśli Zarząd opowiada jedynie za odbieranie raportów i podejmowanie kluczowych decyzji biznesowych, to ktoś musi jeszcze monitorować całą resztę. A więc badać poziom faktycznej realizacji obowiązków prawno-organizacyjnych, wynikających z RODO, takich jak:

- prowadzenie RCP,

- prowadzenie RKPC,

- wdrożenie i przestrzeganie procedur: reagowania na incydenty, realizacji praw osób, szkoleń, szacowanie ryzyka, DPIA,

- podpisywanie umów powierzenia,

- zadania bieżące – przygotowanie klauzul zgód, obowiązków informacyjnych, etc.

W dobrze działającej strukturze, ktoś musi wziąć na siebie odpowiedzialność za powyższe obszary. To nie znaczy, że nasza królowa, musi samodzielnie prowadzić RCP. Może zlecić prowadzenie RCP dla konkretnych procesów, innym osobom (np. Zarządzającym).

Niemniej jednak, potrzebne jest ogólne wzięcie odpowiedzialności za całokształt funkcjonowania RODO w organizacji. Bez tego wzięcia odpowiedzialności, system skończy jako kolejne „papierowe wdrożenie RODO".

W naszej systematyce, najczęściej osobą odpowiedzialną za bieżące monitorowanie wdrożenia, będzie Inspektor Ochrony Danych. IOD nie musi, a nawet nie powinien wykonywać samodzielnie wszystkich ww. zadań. O samym zakresie obowiązków IOD, pisaliśmy już obszernie na naszym blogu.

Jeśli Twoja organizacja nie wyznacza Inspektora Ochrony Danych, to uważam, że i tak powinna ustanowić jedną, konkretną osobę, odpowiedzialną za kwestie związane z prawno-organizacyjnymi aspektami RODO. My taką osobę nazywamy Oficerem Bezpieczeństwa Danych Osobowych (OBDO). Z naszych doświadczeń wynika jednoznacznie – jeśli nikt nie weźmie odpowiedzialności za ww. obszar to murowany efekt wdrożenia będzie tylko jeden – „papierowe wdrożenie".

Wieże, czyli Administrator Systemów Informatycznych

Kolejną ważną figurą na naszej szachownicy będzie Administrator Systemów Informatycznych (ASI), w niektórych organizacjach zwany Administratorem Bezpieczeństwa Systemów (ABS). Ktoś musi wziąć odpowiedzialność za obszar IT security. Jak pokazała bardzo głośna sprawa kary dla Morele.net (pisaliśmy o niej szeroko na naszym blogu) organ nadzorczy może ocenić adekwatność naszych zabezpieczeń IT security. Jeśli ocena będzie negatywna, to grozi nam kara. Nasza infrastruktura IT sama się nie zabezpieczy. Potrzebny jest ktoś, kto skoordynuje zabezpieczenia. Kto będzie koordynatorem w sytuacji naruszenia związanego bezpośrednio z funkcjonowaniem infrastruktury IT.

Rola ASI będzie bardzo różna w zależności od wielkości organizacji i stopnia skomplikowania zabezpieczeń IT. Duże banki czy inne organizacje bazujące na wielkiej ilości danych i równie dużej ilości SI, mogą wyznaczać osoby odpowiedzialne za bezpieczeństwo odrębnie dla każdego systemu. Jednak nawet w takiej sytuacji, jeden z ASIch, powinien sprawować nadzór nad IT sec globalnie, dla całej organizacji.

Organizacje, które nie przetwarzają tak dużej ilości informacji jak np. banki, mogą budować strukturę nieco inaczej. Na przykład poprzez wyznaczenie jednego ASI, który będzie utrzymywał bieżący kontakt z dostawcami zabezpieczeń IT. ASI sam nie musi wprowadzać konkretnych zabezpieczeń. Powinien jednak czuwać nad całością i koordynować prace dostawców, którzy wdrażają zabezpieczenia IT.

Jak to może wyglądać w u mikroprzedsiębiorcy zatrudniającego ok. 10 osób? Podzielę się naszym „Lex Artistowym" przykładem. Funkcję ASI pełni Wiceprezes Zarządu, Łukasz. Łukasz nie jest informatykiem, jednak posiada dużą wiedzę dotyczącą systemów informatycznych i ich zabezpieczeń. Łukasz we współpracy z naszym dostawcą IT, wspólnie ustalają poziomy zabezpieczeń adekwatne do naszych potrzeb, a następnie je wdrażają.

W ten sposób, wspólnie z naszym dostawcą wsparcia IT, wdrożyliśmy w Lex Artist na przykład: VPN, szyfrowanie dysków twardych, SSO.

Nasz ASI na bieżąco analizuje aktualnie dostępne na rynku zabezpieczenia i w razie potrzeby, wspólnie z dostawcą IT, wdraża je w praktyce.

Często zdarza się, że w firmie nikt nie chce zostać ASI. W wielu przypadkach, nasz organizacyjny informatyk i tak jest osobą, która wdraża zabezpieczenia IT. Chodzi jedynie o oficjalne przypisanie mu takiej roli.

Patrząc na tę sytuację ze strony ASI, opór jest sprawą naturalną. Otrzymuje nową listę obowiązków. Nie zawsze czuje się w nich kompetentny. Jeśli poczucie braku kompetencji, jest przyczyną odmowy przyjęcia funkcji ASI, pomóż informatykowi uzyskać kompetencje. Możesz zainwestować w szkolenie, możesz zatrudnić zewnętrzną firmę IT, która wesprze Twojego ASI w tych obszarach, w których nie czuje się pewnie.

Jedno jest pewne – ASI to niezbędna figura na Twojej RODO szachownicy. Bez ASI, nie masz szans na pozytywne przejście kontroli UODO. Bez ASI Twoje zabezpieczenia IT sec, a raczej ich brak, mogą skutkować nałożeniem wysokiej kary przez regulatora.

Gońce i skoczki, czyli zarządzający zbiorami i procesami

W większych organizacjach potrzebne jest jeszcze ogniwo pośrednie między decyzyjnymi osobami (Zarząd, IOD, ASI), a pracownikami po prostu przetwarzającymi dane osobowe. Takimi osobami na naszej RODO szachownicy będą Zarządzający zbiorami/procesami. Czasem nazywani opiekunami zbiorów lub procesów. Nomenklatura bywa różna. Zasada funkcjonowania jest dość podobna.

Zarządzający procesami są w sposób szczególny zobowiązani do opieki nad konkretnymi procesami przetwarzania danych osobowych. Ich rolą może być na przykład dbanie o aktualność rejestru czynności przetwarzania w zakresie procesów, którymi się opiekują. Chodzi o to, żeby IOD czy OBDO mieli pewność i gwarancję, że otrzymają informację o każdej istotnej zmianie przetwarzania danych osobowych. W większej organizacji, IOD czy OBDO nie mają możliwości codziennego sprawdzania i badania aktualności RCP czy RKCP. Musza opierać się na wiedzy osób pracujących przy konkretnych procesach przetwarzania danych osobowych. Wyznaczenie Zarządzających też czasem bywa bardzo problematyczne. Kandydaci i kandydatki najczęściej przeceniają swój poziom RODO odpowiedzialności. Wydaje im się, że muszą precyzyjnie znać przepisy RODO i podejmować kluczowe decyzje związane z przetwarzaniem danych osobowych.

Cel i idea tej funkcji są zupełnie inne. Chodzi o szybkie i sprawne przekazywanie informacji osobom decyzyjnym. Dzięki dobrze funkcjonującym Zarządzającym zbiorami/procesami, nie będzie szansy na to, że np. organizacja postawi nową stronę internetową zbierającą dane osobowe, a IOD/OBDO nigdy się o tym nie dowiedzą. W efekcie na stronie nie będzie np. obowiązków informacyjnych, a klauzula zgody na przetwarzanie danych osobowych będzie wadliwa.

Jak więc nawiązać współpracę z Zarządzającym i pokazać im, że nie mają się czego obawiać? Najlepiej zrobić to w formie szkolenia lub spotkania, na którym istota funkcji zostanie precyzyjnie wyjaśniona i opisana.

Pionki... czyli upoważnieni pracownicy

Bycie pionkiem co prawda ma w naszym języku negatywne konotacje. Niemniej jednak, na RODO szachownicy mamy figury ważne i ważniejsze. Rolę pionków zarezerwowałem dla osób, które nie pełnią żadnej roli w strukturze, poza przetwarzaniem danych osobowych. No właśnie... więc ta rola wcale nie jest taka nieistotna. W prawdziwych szachach nie da się wygrać bez pomocy pionków.

Przetwarzający dane pracownicy, czasem nie chcą przyjmować upoważnień. Takie sytuacje zdarzają się bardzo rzadko, ale zdarzają się. Jak ich przekonać do zajęcia swojego miejsca na naszej szachownicy?

Podobnie jak w poprzednich przypadkach; Kluczowe jest zrozumienie przyczyny obaw pracowników. Z reguły będzie to obawa przed podpisaniem (lub przyjęciem) dokumentu, który ma wygenerować dla nich dodatkową odpowiedzialność. W tym przypadku przeważnie pomaga argument, że upoważnienie jest obowiązkiem prawnym, nałożonym na ADO, wynikającym bezpośrednio z treści RODO.

To nie jest nieformalny dokument wymyślony przez sztab prawników ADO, żeby narazić pracownika na dodatkowe ryzyka prawne. Inne obawy pracowników przeważnie będą podobne, do tych które wyrażają Zarządzający zbiorami. Może je generować przede wszystkim niejasny poziom oczekiwań i odpowiedzialności. Sposobem na zaangażowanie pracowników i ich uspokojenie, będzie szkolenie. Na szkoleniu pracownicy powinni poznać precyzyjny zakres własnej odpowiedzialności i obowiązków.

Podsumowanie

Brak odpowiedniego określenia wszystkich ról na Twojej RODO szachownicy, jest jedną z najczęstszych przyczyn „papierowego wdrożenia RODO". Zgodność z RODO wymaga połączenia dobrych i skutecznych procedur z ich przyswojeniem przez pracowników. Ludzie muszą identyfikować się z wdrożonymi procedurami i rozumieć je. Jeśli uda Ci się połączyć wysokiej jakości procedury z odpowiednim ich zakomunikowaniem Twojemu Zespołowi, to znaczy, że osiągnąłeś/aś duży sukces.

Poniżej dołączam tabelę, która stanowi podsumowanie najczęstszych obaw, konkretnych kategorii osób:

Rola w organizacji:	Jakie może mieć obawy?	Jak zmniejszyć poziom niepokoju?
Zarząd	Najczęstszą obawą będzie obawa przed podpisaniem samej polityki ochrony danych. Zarząd może obawiać się, że podpisanie błędnie przygotowanego dokumentu doprowadzi do poważnych konsekwencji dla organizacji.	Podpisanie polityki nie jest jednorazową czynnością, wykluczającą jakiekolwiek zmiany. PODO może być w dowolnym momencie zmieniona przez Zarząd. Zdecydowanie większym ryzykiem niż błędna PODO, jest brak jej podpisania i przyjęcia przez Zarząd.
Inspektor Ochrony Danych	Obawy IOD są bardzo różnej natury. W większości przypadków IOD myśli, że bierze na siebie odpowiedzialność za wszystko co dzieje się w obszarze ODO. Niektórzy IOD, którzy równolegle pełnią inne role w organizacji, mogą obawiać się braku czasu na zajęcie się nowymi obowiązkami.	IOD nie bierze odpowiedzialności za całokształt RODO w organizacji. Rolą IOD jest doradzanie i opiniowanie. Ostateczne decyzje podejmuje Administrator danych i to on ponosić będzie odpowiedzialność za stwierdzone niezgodności z RODO. Jeśli chodzi o brak czasu na pełnienie funkcji IOD, to tutaj może pomóc transparenty podział RODO obowiązków. Na przykład rolą IOD wcale nie musi być opiniowanie umów powierzenia przetwarzania DO. Tym niech zajmie się dział prawny.
Administrator Systemów Informatycznych	ASI będzie odpowiadał za obszar IT security w Organizacji. W większości przypadków informatycy nie specjalizują się w temacie IT sec. Trudno im więc wziąć odpowiedzialność za coś, na czym się nie znają.	Jeśli ASI nie ma wiedzy i kompetencji z zakresu IT sec., powinien móc je pozyskać na zewnątrz. Na przykład w formie współpracy z zewnętrznymi specjalistami lub poprzez dodatkowe szkolenia. W takiej sytuacji ASI powinien przede wszystkim zarządzać obszarem IT sec, a niekoniecznie osobiście znać się na szczegółach.
Zarządzający zbiorami/procesami	Zarządzający zbiorami lub procesami przeważnie obawiają się, że nakłada się na nich całkowitą odpowiedzialność za procesy, którymi zarządzają.	Zarządzający powinni zostać przeszkoleni. Powinni wiedzieć, że ich rola polega przede wszystkim na informowaniu IOD lub innej osoby o zmianach w przetwarzaniu DO, o

		incydentach etc. Zarządzający nie musi znać precyzyjnie przepisów RODO. Zarządzający musi wiedzieć kiedy i z kim konsultować zmiany czy niestandardowe sytuacje.
Osoby upoważnione	Upoważnieni pracownicy często obawiają się, że wymagać się od nich będzie precyzyjnej znajomości RODO.	Pracownicy powinni wiedzieć, że ich rola sprowadza się do respektowania procedur ustanowionych przez ADO. W większości przypadków będzie to po prostu informowanie IOD czy innej osoby o różnych zdarzeniach. Na przykład o incydencie, wdrażaniu nowego projektu czy o planowanym zawarciu umowy z kontrahentem, kiedy potrzebne będzie przygotowanie umowy powierzenia.

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu Lex Artist

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)