LEWIATAN

oraz

e-COMMERCE POLSKA
IZBA GOSPODARKI ELEKTRONICZNEJ

przedstawiają

KONSEKWENCJE EKONOMICZNE DLA MŚP UNIJNEGO PROJEKTU ROZPORZĄDZENIA O OCHRONIE DANYCH OSOBOWYCH wg projektu zatwierdzonego przez komisję LIBE[i]

LEWIATAN

e-COMMERCE POLSKA
IZBA GOSPODARKI ELEKTRONICZNEJ

Szanowni Państwo,

Po dwóch latach dyskusji, 4000 zgłoszonych poprawek i burzliwej debacie publicznej komisja Parlamentu Europejskiego LIBE przyjęła sprawozdanie do projektu rozporządzenia o ochronie danych osobowych[ii]. Przyjęte stanowisko było wyrazem zgody parlamentarzystów co do tego, że dane osobowe są wartością, w sensie ekonomicznym i społecznym, w związku z czym wymagają należytej ochrony.

Popierając w pełni takie podejście, Konfederacja Lewiatan i Izba Gospodarki Elektronicznej postanowiły sprawdzić jak zaproponowane przez Parlament przepisy działałyby w praktyce. Jak wpłynęłyby na codzienność przeciętnego przedsiębiorcy, który przetwarza dane przy okazji prowadzenia działalności, na umiarkowaną lub niewielką skalę. Chcieliśmy sprawdzić czy obowiązki, które administrator danych będzie musiał spełnić są proporcjonalne, a ograniczenia w przetwarzaniu danych nie utrudnią realizowania jego słusznych interesów. Spróbowaliśmy wreszcie oszacować jakie będą związane z tym koszty.

Dla uzyskania pełniejszego obrazu wybraliśmy bardzo różne profile działalności. Przeanalizowaliśmy sprawozdanie pod kątem obowiązków, jakie musiałby spełnić przedsiębiorca sprzedający swoje produkty przez Internet (księgarnia internetowa), świadczący usługi poza środowiskiem cyfrowym (gabinet kosmetyczny) oraz administrator prowadzący działalność niekomercyjną (poseł).

Konkluzje z tej analizy wskazują, że proponowane przez LIBE przepisy są oparte na niewłaściwych założeniach. Niedostatecznie różnicują one nakładane obowiązki w zależności od charakteru i skali przetwarzania danych oraz ewentualnych związanych z tym zagrożeń. Nawet administratorzy przetwarzający dane w minimalnym zakresie będą musieli stosować się do rozbudowanej listy obowiązków, zaprojektowanych z myślą o najbardziej zaawansowanych i ryzykownych procesach przetwarzania. Poniosą oni także koszty związane z zapewnieniem zgodności i wymaganych rozwiązań organizacyjnych. **Według naszej analizy, łączne koszty realizacji obowiązków dokumentacyjnych wynikających z rozporządzenia, w okresie pierwszych dwóch lat prowadzenia działalności przez każdego z analizowanych przedsiębiorców można szacować na nie mniej niż 66.600 złotych + VAT**. Suma ta obejmuje jedynie koszty sporządzenia dokumentacji oraz klauzul informacyjnych, w tym koszty związanej z tymi działaniami obsługi prawnej oraz koszty nabycia usług ABI. Nie uwzględnia kosztów działań niezbędnych do rzeczywistego zabezpieczenia danych osobowych przed ich utratą i zniszczeniem. Szokujący wydaje się fakt, iż koszt wdrożenia nowego prawa dla przedsiębiorców dokonujących minimalnych i społecznie niegroźnych operacji na danych osobowych będzie dziewięciokrotnie wyższy niż dotychczas.

Prawdą jest, że już obecnie firmy ponoszą koszty związane z zapewnieniem zgodności z przepisami, które niejednokrotnie przekraczają wskazane wyżej sumy. Istotnym i zobrazowanym w załączonym materiale problemem jest jednak to, że w razie przyjęcia przepisów rozporządzenia w wersji LIBE wskazane koszty poniosą niemal wszyscy.

Załączony materiał ma za zadanie pomóc w wyeliminowaniu zbędnych obciążeń. Zdaniem Konfederacji Lewiatan i e-Izby rozporządzenie nie powinno zostać przyjęte dopóki wszystkie postanowienia rodzące nieuzasadnione koszty nie zostaną usunięte. W przeciwnym razie szansa na wykorzystanie potencjału gospodarki internetowej dla powstawania i rozwoju innowacyjnych i konkurencyjnych przedsiębiorstw w Polsce i Unii Europejskiej zostanie zaprzepaszczona.

W imieniu Konfederacji Lewiatan:

Henryka Bochniarz
Prezydent

W imieniu Izby Gospodarki Elektronicznej:

Grzegorz Wójcik
Członek Zarządu

LEWIATAN

e-COMMERCE POLSKA
IZBA GOSPODARKI ELEKTRONICZNEJ

SPIS TREŚCI

MODEL nr 1 KSIĘGARNIA INTERNETOWA

Opis działalności

Osoba fizyczna prowadząca działalność gospodarczą zamierza otworzyć księgarnię internetową. Oferta ma obejmować: (1) sprzedaż wysyłkową książek oraz (2) udostępnianie e-booków w serwisie internetowym lub za pośrednictwem aplikacji umożliwiającej korzystanie z zasobów księgarni także za pośrednictwem urządzeń mobilnych, takich jak telefony i tablety.

Właściciel księgarni (zwany dalej Księgarnią) będzie prowadzić marketing ograniczony jedynie do newslettera, zawierającego informacje o ofertach dostosowanych do zainteresowań klienta.

Księgarnia będzie przetwarzać dane osobowe swych: (1) klientów, tj. osób, które dokonały zakupu i z konieczności podały swe dane, aby otrzymać przesyłkę oraz (2) osób zainteresowanych ofertą Księgarni.

Księgarnia będzie korzystała z usług kilku firm świadczących typowe i występujące powszechnie usługi dla przedsiębiorców, np.: hostingodawcy, firmy kurierskiej, dostawcy oprogramowania. Ponieważ Księgarnia będzie chciała udostępnić klientom aplikację mobilną na tablety i telefony komórkowe, będzie musiała korzystać z usług dwóch podmiotów, które dostarczają systemy operacyjne stanowiące środowisko pracy takich aplikacji tj. Google (system Android) oraz Apple. Podmioty te będą przetwarzać dane osobowe, których administratorem będzie Księgarnia na podstawie powierzenia.

Księgarnia postanowiła dokonywać minimum operacji na danych osobowych, aby maksymalnie ograniczyć zakres swych obowiązków wynikających z przepisów o ochronie danych osobowych.

Konsekwencje w zakresie ochrony danych osobowych

Ogólne obowiązki związane z przetwarzaniem danych[iii]

Obecnie w związku z rozpoczęciem działalności Księgarnia musi przygotować dwa dokumenty: Politykę bezpieczeństwa danych osobowych i Instrukcję zarządzania systemem informatycznym. Dokumenty te opisują zbiory danych osobowych i sposób zabezpieczenia tych danych. Księgarnia musi ponadto zawrzeć proste umowy powierzenia, z których wynika cel i zakres przetwarzania danych. Umowy powinny zostać zawarte na piśmie, ale wymóg ten jest ustanowiony jedynie dla celów dowodowych.

Po wprowadzeniu rozporządzenia w wersji LIBE konieczne będzie przygotowanie o wiele obszerniejszej dokumentacji. Księgarnia będzie musiała:

1) sporządzić *„zwięzłe, przejrzyste, jasne i łatwo dostępne polityki"* dotyczące przetwarzania danych osobowych i ochrony praw podmiotów danych (art. 11(1) LIBE) Treść LIBE sugeruje, że polityki będą musiały zostać opublikowane przez Księgarnię (*easily accessible*).

2) sporządzić i wdrożyć właściwe polityki oraz wdrożyć właściwe i możliwe do udowodnienia środki techniczne i organizacyjne (art. 22(1) LIBE) oraz towarzyszące im *compliance policies*, które powinny podlegać weryfikacji co dwa lata (art. 22(1a) LIBE). Księgarnia będzie musiała być w stanie wykazać adekwatność i skuteczność zastosowanych środków;

3) sporządzić dokumentację realizacji obowiązków wynikających z postanowień rozporządzenia (art. 28 (1) LIBE). Wszystkie działania związane z przetwarzaniem danych (np. instalacja oprogramowania antywirusowego lub kryptograficznego) będą musiały być rejestrowane i dokumentowane przez Księgarnię;

4) przeprowadzić analizę ryzyka (obowiązek wynika z przekroczenia limitu 5000 rekordów, co w środowisku cyfrowym jest niskim pułapem - art. 32a(2) lit. (b) LIBE). Analiza będzie musiała zostać udokumentowana na piśmie i będzie musiała raz do roku podlegać weryfikacji (art. 32a (4) LIBE);

5) przeprowadzić ocenę skutków w zakresie ochrony danych osobowych (*data protection impact assesment*) (art. 33(1) w zw. z art. 32a (3) LIBE);

6) zatrudnić (zawrzeć umowę) osobę świadczącą profesjonalne usługi *ABI (art. 32a(3) lit. (b) LIBE)* – obowiązek ten dotyczy administratora, który zgromadzi dane co najmniej 5.000 rekordów, czyli liczbę niewielką z punktu widzenia przedsiębiorcy prowadzącego księgarnię internetową.

7) wprowadzić środki weryfikujące wiek użytkowników podających swoje adresy e-mailowe na potrzeby otrzymywania newslettera oraz - w razie użytkowników młodszych niż 13 lat- mechanizmy uzyskiwania zgody rodziców/opiekunów prawnych.

Dodatkowo, po dwóch latach działalności Księgarnia będzie musiała:

1) przeprowadzić weryfikację zastosowanych polityk (art. 22(1) LIBE); weryfikacja będzie musiała zostać udokumentowana (art. 28 (1) LIBE);

2) przeprowadzić i udokumentować przegląd zgodności (*compliance review*) (art. 33a LIBE);

3) umożliwiając dostęp do danych osobowych firmom zewnętrznym, z których usług będzie korzystać (na przykład firmie świadczącej usługi hostingowe), Księgarnia będzie zmuszona zawierać szczególne umowy dotyczące powierzenia danych osobowych.

Wszystkie zawarte umowy powierzenia będą musiały być sporządzone na piśmie (art. 26 (3) LIBE) – elektroniczne zawarcie umowy powierzenia nie będzie spełniać wymogów.

Trudno sobie wyobrazić, aby dostawcy środowisk dla aplikacji mobilnych (tj. Google i Apple) zawierali umowy powierzenia z małymi przedsiębiorcami takimi jak Księgarnia w formie pisemnej. Co więcej, nawet, jeżeli takie umowy będą zawierane (w jakiejkolwiek formie), Księgarnia nie będzie miała w praktyce żadnych możliwości negocjowania ich treści. Wszelkie braki w tym zakresie będą mogły być sankcjonowane karami finansowymi, a odpowiedzialność za nie będzie ponosić przede wszystkim administrator danych osobowych, czyli Księgarnia.

Pozyskanie danych osobowych

W chwili, w której klient Księgarni będzie przekazywał jakiekolwiek swoje dane osobowe np. podawał mail umożliwiający wysyłanie newslettera lub podawał dane korespondencyjne przeznaczone do realizacji wysyłki, Księgarnia będzie musiała przedstawić na swojej stronie internetowej w formie graficznej i tekstowej następujące informacje:

1) czy dane osobowe są gromadzone poza minimum niezbędne dla każdego konkretnego celu przetwarzania;
2) czy dane osobowe są przechowywane poza minimum niezbędne dla każdego konkretnego celu przetwarzania;
3) czy dane osobowe są przetwarzane do celów innych niż cele, dla których zostały zgromadzone;
4) czy dane osobowe są przekazywane innym przedsiębiorcom;
5) czy dane osobowe są sprzedawane lub wynajmowane;
6) czy dane osobowe są przechowywane w postaci zaszyfrowanej (art. 13a LIBE)

Na wszystkie powyższe pytania, w przypadku Księgarni, odpowiedź jest przecząca. Księgarnia nie jest w szczególności zobowiązania do szyfrowania przechowywanych danych. Szyfrowanie danych wiąże się z koniecznością zakupu odpowiedniego oprogramowania i nie jest w przypadku Księgarni niezbędne. Księgarnia będzie musiała jednak ujawnić, że nie szyfruje przechowywanych danych. Podważy to zaufanie potencjalnych klientów do Księgarni, choć Księgarnia będzie przetwarzać i zabezpieczać dane osobowe zgodnie z zasadami wynikającymi z rozporządzenia.

Gdyby Księgarnia chciała dokonywać cesji wierzytelności firmom windykacyjnym, co jest powszechną praktyką w wypadku niewielkich roszczeń, Księgarnia musiałaby informować o tym klientów (pkt 3). Byłby to kolejny czynnik, który zniechęcałby klientów do korzystania z usług Księgarni.

W dalszej kolejności Księgarnia będzie musiała wyświetlić klientowi informacje, które obecnie muszą być przedstawiane klientom tj. informacje o:

1) tożsamości i danych kontaktowych administratora;
2) celach przetwarzania danych, do których przeznaczone są dane,
3) prawie do żądania dostępu do danych i ich poprawiania lub usunięcia danych, prawie do sprzeciwu wobec przetwarzania tych danych, lub uzyskania danych;
4) odbiorcach lub kategoriach odbiorców danych.

Księgarnia będzie musiała przedstawić również szereg nowych informacji, które dotychczas nie były publikowane. Konieczne będzie w szczególności przedstawienie informacji:

5) o tożsamości i danych kontaktowych ABI;
6) o bezpieczeństwie przetwarzania danych, w tym o warunkach umowy, na podstawie której będą przetwarzane dane, oraz sposobie ich realizacji lub o spełnieniu wymagań wskazanych w art. 6 (1) (f) LIBE, w wypadku prowadzenia wysyłki newslettera;
7) o okresie, w którym dane osobowe będą przechowywane, lub jeśli nie jest to możliwe, o kryteriach stosowanych do określenia tego okresu;
8) o prawie do złożenia skargi do organu nadzoru oraz danych kontaktowych organu nadzoru;
9) o profilowaniu, środkach opierających się na profilowaniu, oraz przewidywanym wpływie profilowania na prawa osoby, której dane dotyczą;
10) o algorytmach związanych z każdym automatycznym przetwarzaniem danych;
11) o tym, czy dane osobowe były dostarczone do władz publicznych w ciągu ostatnich 12 miesięcy;
12) dodatkowe inne informacje niezbędne w celu zagwarantowania rzetelnego przetwarzania danych, uwzględniające szczególne okoliczności, w których dane osobowe są gromadzone i przetwarzane, w szczególności istnienie niektórych czynności przetwarzania, których ocena wskazuje, że mogą wiązać się z wysokim ryzykiem w zakresie ochrony danych.

[za: art. 14 LIBE]

Przedstawienie informacji o bezpieczeństwie przetwarzania danych, por. pkt 6) powyżej, nie jest konieczne dla ochrony praw klientów Księgarni. Przeciwnie, realizacja tego obowiązku może prowadzić do publikacji informacji, których ujawnienie spowoduje obniżenie poziomu bezpieczeństwa danych.

Automatyczne przetwarzanie danych, o którym mowa w pkt 10), to każde przetwarzanie danych w systemach informatycznych (np. na serwerze), algorytmy wykorzystuje zaś każdy program komputerowy. Księgarnia będzie musiała zatem wymienić wszystkie, nawet najbardziej oczywiste funkcje oprogramowania przetwarzającego dane osobowe.

Informację, o której mowa w pkt 11), trzeba będzie przedstawić również wtedy, gdy Księgarnia będzie dochodziła należności w postępowaniu sądowym. Wysyłając pozew Księgarnia dostarcza dane osobowe do władz publicznych.

Pomimo że opisany powyżej katalog jest bardzo szeroki, nie jest on zamknięty i w praktyce może się okazać, że Księgarnia może zostać zobowiązana do przedstawienia dodatkowych informacji, o których mowa w pkt 12) powyżej.

Klient będzie musiał zapoznać się z opisanymi powyżej informacjami przed przekazaniem Księgarni własnych danych osobowych. Wskazanie linku do zawierającej te informacje podstrony nie będzie wystarczające. Konieczne będzie zaprezentowanie wskazanych informacji klientowi tak, aby zapoznał się z nimi przed podaniem danych osobowych. Otwarte pozostaje pytanie, w jaki sposób zredagować i przedstawić tak wielką ilość informacji tak, aby możliwe było ich przedstawienie klientowi, który wprowadza dane osobowe np. za pomocą aplikacji mobilnej w swoim telefonie komórkowym lub tablecie.

Profilowanie i dane wrażliwe

1) Księgarnia zamierza dostosowywać do oczekiwań klienta ofertę przedstawianą klientowi na stronie głównej, na profilu klienta, oraz informacje o ofercie wysyłane za pomocą newslettera. Przykładowo, klient, który przeglądał pozycje książkowe z działu „kryminały", otrzyma w newsletterze informację o nowych kryminałach w ofercie Księgarni. Dostosowanie oferty Księgarni do zainteresowań klienta wymaga przedstawienia klientowi dodatkowej informacji o podejmowanym profilowaniu, niezależnie od tego, czy Księgarnia będzie przetwarzać dane osobowe klienta, czy też dane te będą miały charakter danych pseudozanonimizowanych (art. 20 LIBE).

2) Księgarnia nie będzie jednakże mogła tworzyć profilowanych ofert, jeżeli lektury, którymi są zainteresowani klienci będą dotyczyły np. oferty prasy katolickiej, książek o określonej tematyce religijnej, politycznej lub filozoficznej, literatury kobiecej, czy tytułów dotyczących określonych chorób i problemów zdrowotnych. Przedstawienie przedmiotowych ofert będzie mogło zostać uznane za tworzenie profilów wyłącznie w oparciu o dane wrażliwe, a w konsekwencji prowadzić będzie do naruszenia przepisów o profilowaniu i ochronie danych wrażliwych (por. art. 9 i 20(3) LIBE).

3) Ponieważ za daną wrażliwą uważana jest płeć (*gender identity*), sposób adresowania przez Księgarnię korespondencji do danego klienta będzie mógł zostać objęty zakazem przetwarzania danych wrażliwych (art. 9(1) LIBE).

Przetwarzanie danych dzieci i zgoda na przetwarzanie danych

1) Księgarnia, aby móc oferować książki dla dzieci i młodzieży, będzie musiała weryfikować, czy zgoda na zakup książki przez dziecko została udzielona przez jego opiekuna (art. 8(1) LIBE). Księgarnia nie będzie mogła jednak w żaden sposób dokonać weryfikacji takiej zgody. Checkbox ze stosownym oświadczeniem nie będzie wystarczający. Ponieważ konsekwencją niezrealizowania tego obowiązku może być sankcja finansowa (art. 79 LIBE), Księgarnia będzie musiała zrezygnować z prowadzenia tego typu sprzedaży.

2) Adresy email stanowią, co do zasady dane osobowe. Przetwarzanie adresu email w celu wysyłania newslettera zawierającego materiały promocyjne innych podmiotów, nie będzie dopuszczalne bez zgody osoby przesyłającej dane. Ponieważ jednak zgoda na przetwarzanie danych musi być wyraźna (art. 4 (8) LIBE), samo przekazanie adresu email nie będzie uważane za wyrażenie zgody. Osoba zainteresowana otrzymywaniem newslettera będzie musiał zaznaczyć dodatkowy checkbox, w którym wyrazi zgodę na przetwarzanie danych w celu prowadzenia wysyłki newslettera.

3) Księgarnia nie będzie mogła oferować klientom, którzy wyrażą zgodę na otrzymywanie informacji handlowej, dodatkowych darmowych usług. Zgoda na przetwarzanie danych osobowych nie będzie bowiem mogła być warunkiem świadczenia usługi (art. 7(4) LIBE).

Zamówienie na rzecz osoby trzeciej

Jeżeli klient złoży zamówienie i poda dane osoby trzeciej, do której ma zostać wysłana książka (np. w charakterze prezentu), podstawą przetwarzania danych będzie prawnie usprawiedliwiony cel administratora (art. 6(1)(f) LIBE). Osoba trzecia będzie jednakże mogła w każdej chwili złożyć sprzeciw, a Księgarnia będzie musiała usunąć dane niezależnie od tego, że mogą być one niezbędne do udowodnienia wykonania przez Księgarnię usługi (art. 19 (2) LIBE).

Windykacja należności. Przekazanie danych osobowych firmie windykacyjnej

Przepisy rozporządzenia nie dają jednoznacznej odpowiedzi, czy istnieje podstawa prawna do prowadzenia windykacji należności przez Księgarnię po zrealizowaniu umowy. Wydaje się, że Księgarnia nie będzie mogła przekazać danych osobowych dłużników firmie windykacyjnej, która nabędzie od Księgarni wierzytelności z tytułu zrealizowanych dostaw oraz świadczonych usług i będzie we własnym imieniu dochodziła tych należności (por. art. 5 (b) LIBE). Ponieważ Księgarnia nie posiada środków na obsługę procesu windykacji, może to znacznie utrudnić dochodzenie przez Księgarnię należności.

Zmiana celu przetwarzania

Księgarnia nie będzie mogła sporządzić własnych zestawień opisujących proces sprzedaży np. wyjaśniających, w jaki sposób klienci dokonują zakupów, z jakich regionów kraju lub UE dokonywane są zamówienia. Przykładowo tabela Excel zawierająca jedynie kwoty zamówień i miejsca dostawy będzie zawierała dane pseudozanonimizowane, traktowane w tym zakresie w taki sam sposób jak dane osobowe (art. 20(1) LIBE). Jej sporządzenie będzie się wiązać z niedopuszczalną zmianą celu przetwarzania danych osobowych.

Przetwarzanie danych osobowych w celach dokumentacyjnych

Księgarnia będzie musiała zakupić i wdrożyć oprogramowanie, które zagwarantuje usunięcie danych po zrealizowaniu celu przetwarzania (art. 17(8b) lit. (b) LIBE).

Sankcje

1) Naruszenie jakichkolwiek ze wskazanych powyżej postanowień rozporządzenia będzie mogło wiązać się z nałożeniem na Księgarnię kary finansowej (art. 79 LIBE). Sankcje będą grozić za zrealizowanie wszystkich obowiązków wynikających z rozporządzenia, nawet tych których realizacja może budzić praktyczne wątpliwości (np. dotyczących ochrony danych osobowych dzieci) oraz tych, których realizacja nie wpływa bezpośrednio na stopień ochrony praw osób, których dane dotyczą (np. obowiązków dokumentacyjnych).

2) Kary finansowe będą mogły być nakładane niezależnie od stopnia winy (art. 79 LIBE). Ograniczenie odpowiedzialności finansowej Księgarni do winy umyślnej i niedbalstwa, będzie możliwe jedynie w wypadku posiadania "*European Data Protection Seal*" – art. 79(2b). Uzyskanie takiej gwarancji wymaga poniesienia przez Księgarnię dodatkowych kosztów audytu – art. 39 (2a).

Koszty

Księgarnia będzie musiała w celu spełnienia opisanych powyżej wymagań związanych z realizacją przepisów rozporządzenia ponieść istotne koszty związane z tworzeniem i utrzymaniem wymaganej dokumentacji i podejmowaniem działań organizacyjnych, do których zobowiązuje rozporządzenie.

Koszty zostały obliczone z uwzględnieniem stawek rynkowych obowiązujących obecnie, konieczności skorzystania z wyspecjalizowanych firm doradczych, poważnego ryzyka prawnego i finansowego obciążającego zarówno Księgarnię, jak i usługodawcę Księgarni (na przykład ABI), które to ryzyko zawsze przekłada się na wzrost cen usług.

Wysokość przedmiotowych wydatków, zważywszy na konieczność skorzystania z usług profesjonalnej firmy doradczej (realizacja obowiązków wymaga specjalistycznej wiedzy prawniczej, a często także technicznej, której Księgarnia nie posiada), można szacować w następujący sposób:

1) sporządzenie polityk dotyczących przetwarzania danych osobowych i ochrony praw podmiotów danych (art. 11(1) LIBE) – 6.000 złotych netto,

2) przygotowanie klauzul informacyjnych (art. 13a i 14 LIBE) – 600 złotych netto,
3) sporządzenie polityk zgodności (art. 22(1a) LIBE) – minimum 6.000 złotych netto,
4) przeprowadzenie i udokumentowanie analizy ryzyka (art. 32a (4) LIBE) – minimum 6.000 złotych netto
5) przeprowadzenie oceny skutków w zakresie ochrony danych osobowych (*data protection impact assesment*) (art. 33(1) w zw. z art. 32a (3) LIBE) – minimum 6.000 złotych netto,
6) sporządzenie pisemnych umów powierzenia przetwarzania danych osobowych dla co najmniej dwóch podmiotów (hostingodawców i dostawcy oprogramowania) – 1.500 złotych netto.

Księgarnia będzie musiała zawrzeć umowę z osobą świadczącą usługi ABI (art. 32a(3) lit. (b) LIBE). Umowa będzie musiała zostać zawarta na czas określony. Koszt takiej stałej obsługi Księgarni można szacować na (zważywszy na minimalny zakres przetwarzania danych przez Księgarnię) na około 1.500 złotych netto **miesięcznie, czyli 18.000 złotych netto w skali roku**.

Co roku Księgarnia będzie musiała ponieść koszt weryfikacji analizy ryzyka i udokumentowania tego procesu (art. 32a (4) LIBE). Działanie to będzie miało charakter rutynowy jego koszt można szacować na około 1.500 złotych netto.

Po dwóch latach działalności Księgarnia będzie musiała ponieść wydatki niezbędne do nabycia usług:

1) przeprowadzenia i udokumentowania weryfikacji zastosowanych polityk (art. 22(1) LIBE); – 1.500 złotych netto.
2) przeprowadzenia i udokumentowania przeglądu zgodności (*compliance review*) (art. 33a LIBE) – 1.500 złotych netto.

Łączne koszty realizacji obowiązków dokumentacyjnych wynikających z rozporządzenia w okresie pierwszych dwóch lat prowadzenia działalności przez Księgarnię można szacować na nie mniej niż 66.600 złotych + VAT.

Powyższa kalkulacja została sporządzona w oparciu o wiedzę dotyczącą cen usług prawniczych na rynku polskim.

Suma ta obejmuje jedynie koszty sporządzenia i realizacji dokumentacji oraz klauzul informacyjnych, w tym koszty związanej z tymi działaniami obsługi prawnej oraz koszty nabycia usług ABI.

Powyższy kosztorys nie obejmuje kosztów działań niezbędnych do rzeczywistego zabezpieczenia danych osobowych przed ich utratą i zniszczeniem.

Wskazane powyżej zestawienie pomija w szczególności koszty zakupu oprogramowania służącego do ochrony danych w tym oprogramowania antywirusowego i szyfrującego, koszty nabycia usług hostingowych we właściwie zabezpieczonych serwerach, koszty tworzenia kopii zapasowych, czy wreszcie koszty zabezpieczeń fizycznych, które powinny zostać zastosowane w siedzibie Księgarni.

MODEL nr 2 POSEŁ DO PARLAMENTU EUROPEJSKIEGO

Opis działalności

Poseł do Parlamentu Europejskiego (dalej: Poseł) w ramach działalności biura poselskiego prowadzi stronę internetową, w ramach której umożliwia użytkownikom zamówienie newslettera, wysyłanego na adres email. Zebrane adresy poczty elektronicznej odbiorców newslettera gromadzone są w bazie mailingowej.

Poseł organizuje również we własnym imieniu konkursy, w których nagrodą jest staż w biurze poselskim albo wizyta w Parlamencie Europejskim. W ramach organizacji konkursów Poseł zbiera dane osobowe ich uczestników (imię, nazwisko, adres email, adresy korespondencyjne).

Poseł organizuje wizyty w Parlamencie Europejskim. W związku z tym Poseł otrzymuje od szkół i innych zaprzyjaźnionych organizacji listy uczestników wycieczek. Poseł jako organizator przekazuje te listy podmiotom, które na jego zlecenie świadczą usługi niezbędne do obsługi wizyty (np. usługi transportowe).

Poseł rozważa możliwość wykorzystania, w niektórych wypadkach, zbieranych danych osobowych, do informowania o własnej działalności, w szczególności informowania o organizowanych konferencjach i działaniach związanych z kolejną kampanią do Parlamentu Europejskiego.

Do biura Posła jest kierowana korespondencja. Nadawcy przedstawiają problemy i proszą o interwencję w konkretnych sprawach. W treści pism często ujawniają swoje poglądy polityczne lub - prosząc o pomoc - dane dotyczące ich sytuacji materialnej, stanu zdrowia itp. Często są to więc dane wrażliwe. Korespondencja jest drukowana i gromadzona w dokumentacji prowadzonej przez personel biura poselskiego na potrzeby zajęcia się daną sprawą. Biuro Posła prowadzi w formie elektronicznej w arkuszu Excel rejestr spraw, w którym znajdują się między innymi dane osobowe nadawców.

Konsekwencje w zakresie ochrony danych osobowych[1]

Ogólne obowiązki związane z przetwarzaniem danych:

Obecnie Poseł musi przygotować dwa dokumenty: Politykę bezpieczeństwa danych osobowych i Instrukcję zarządzania systemem informatycznym. Dokumenty te opisują zbiory danych osobowych i sposób zabezpieczenia tych danych. Poseł musi ponadto zawrzeć proste umowy powierzenia, z których wynika cel i zakres przetwarzania danych. Umowy powinny zostać zawarte na piśmie, ale wymóg ten jest ustanowiony jedynie dla celów dowodowych.

Po wprowadzeniu rozporządzenia w wersji LIBE konieczne będzie przygotowanie o wiele obszerniejszej dokumentacji. Poseł będzie musiał:

1) sporządzić *„zwięzłe, przejrzyste, jasne i łatwo dostępne polityki"* dotyczące przetwarzania danych osobowych i ochrony praw podmiotów danych (art. 11(1) LIBE). Treść sprawozdania LIBE sugeruje, że polityki będą musiały zostać opublikowane;

2) sporządzić i wdrożyć właściwe polityki oraz wdrożyć właściwe i możliwe do udowodnienia środki techniczne i organizacyjne (art. 22(1) LIBE) oraz towarzyszące im *compliance policies*, które powinny podlegać weryfikacji co dwa lata (art. 22(1a) LIBE). Poseł będzie musiał być w stanie wykazać adekwatność i skuteczność zastosowanych środków;

3) sporządzić dokumentację realizacji obowiązków wynikających z postanowień rozporządzenia (art. 28 (1) LIBE)- trybu realizacji prawa do bycia zapomnianym, prawa do sprzeciwu itd. Wszystkie działania związane z przetwarzaniem

[1] Przy założeniu, że do Instytucji UE rozporządzenie będzie miało zastosowanie.

danych (np. instalacja oprogramowania antywirusowego lub kryptograficznego) będą musiały być rejestrowane i dokumentowane przez personel biura Poselskiego;

4) przeprowadzić analizę ryzyka (obowiązek wynika z przekroczenia limitu 5000 rekordów - art. 32a(2) lit. (b) LIBE). Analiza będzie musiała zostać udokumentowana na piśmie i będzie musiała raz do roku podlegać weryfikacji (art. 32a (4) LIBE);

5) przeprowadzić ocenę skutków w zakresie ochrony danych osobowych (*data protection impact assesment*) (art. 33(1) w zw. z art. 32a (3) LIBE);

Dodatkowo, po dwóch latach od rozpoczęcia przetwarzania danych Poseł będzie musiał:

1) przeprowadzić weryfikację zastosowanych polityk (art. 22(1) LIBE); weryfikacja będzie musiała zostać udokumentowana (art. 28 (1) LIBE).

2) przeprowadzić i udokumentować przegląd zgodności (*compliance review*) (art. 33a LIBE).

3) Jeżeli Poseł będzie umożliwiał dostęp do danych osobowych firmom zewnętrznym, z których usług będzie korzystał (na przykład firmie świadczącej usługi hostingowe, firmie organizującej przewozy osób uczestniczących w wizytach w Parlamencie Europejskim), Poseł będzie zmuszony zawrzeć szczegółowe umowy dotyczące powierzenia danych osobowych. Wszystkie zawarte umowy powierzenia będą musiały zostać sporządzone na piśmie (art. 26 (3) LIBE) – elektroniczne zawarcie umowy powierzenia nie będzie spełniać wymogów LIBE.

4) Wprowadzić środki weryfikujące wiek użytkowników podających swoje adresy e-mailowe na potrzeby otrzymywania newslettera oraz - w razie użytkowników młodszych niż 13 lat - mechanizmy uzyskiwania zgody rodziców/opiekunów prawnych.

Newsletter

Adres mailowy stanowi, co do zasady, danę osobową. Dlatego też w chwili, w której osoba zainteresowana otrzymaniem od Posła newslettera przekaże adres poczty elektronicznej, będzie przekazywała swoje dane osobowe. Poseł na stronie internetowej, przed otrzymaniem danych, będzie musiał przedstawić w formie graficznej i tekstowej następujące informacje:

1) czy dane osobowe są gromadzone poza minimum niezbędne dla każdego konkretnego celu przetwarzania;
2) czy dane osobowe są przechowywane poza minimum niezbędne dla każdego konkretnego celu przetwarzania;
3) czy dane osobowe są przetwarzane do celów innych niż cele, dla których zostały zgromadzone;
4) czy dane osobowe są przekazywane przedsiębiorcom;
5) czy dane osobowe są sprzedawane lub wynajmowane;
6) czy dane osobowe są przechowywane w postaci zaszyfrowanej (art. 13a LIBE)

Na wszystkie powyższe pytania, w przypadku Posła, odpowiedź powinna być co do zasady przecząca. Jeśli poseł nie będzie szyfrował danych lub z uzasadnionych względów wykorzysta zebrane dane do innych, słusznych celów, będzie musiał zaznaczyć niespełnienie tego obowiązku.

W dalszej kolejności wciąż na formularzu zamówienia newslettera przed podaniem danych osobowych, Poseł będzie musiał wyświetlić informacje o:

1) tożsamości i danych kontaktowych administratora;
2) celach przetwarzania danych, do których przeznaczone są dane;
3) prawie do żądania dostępu do danych i ich poprawiania lub usunięcia danych, prawie do sprzeciwu wobec przetwarzania tych danych, lub uzyskania danych;
4) odbiorcach lub kategoriach odbiorców danych;

Poseł będzie musiał przedstawić również szereg informacji, które dotychczas nie musiały być publikowane. Konieczne będzie w szczególności przedstawienie informacji:

5) o bezpieczeństwie przetwarzania danych, w tym o warunkach umowy, na podstawie której będą przetwarzane dane, oraz sposobie ich realizacji lub o spełnieniu wymagań wskazanych w art. 6 (1) (f) LIBE;
6) o okresie, w którym dane osobowe będą przechowywane, lub jeśli nie jest to możliwe, o kryteriach stosowanych do określenia tego okresu;
7) o prawie do złożenia skargi do organu nadzoru oraz danych kontaktowych organu nadzoru;
8) o profilowaniu, środkach opierających się na profilowaniu, oraz przewidywanym wpływie profilowania na prawa osoby, której dane dotyczą;
9) o algorytmach związanych z każdym automatycznym przetwarzaniem danych;
10) o tym, czy dane osobowe były dostarczone do władz publicznych w ciągu ostatnich 12 miesięcy;
11) dodatkowe inne informacje niezbędnye w celu zagwarantowania rzetelnego przetwarzania danych, uwzględniające szczególne okoliczności, w których dane osobowe są gromadzone i przetwarzane, w szczególności istnienie niektórych czynności przetwarzania, których ocena wskazuje, że mogą wiązać się z wysokim ryzykiem w zakresie ochrony danych.

[za: art. 14 LIBE]

Przedstawienie informacji o bezpieczeństwie przetwarzania danych, por. pkt 6) powyżej, nie jest konieczne dla ochrony praw podmiotów danych. Przeciwnie, realizacja tego obowiązku może prowadzić do publikacji informacji, których ujawnienie spowoduje obniżenie poziomu bezpieczeństwa danych osobowych (np. informacja o sposobie zabezpieczenia danych).

Automatyczne przetwarzanie danych, o którym mowa w pkt 10), oznacza każde przetwarzanie danych w systemach informatycznych (np. na serwerze). Algorytmy wykorzystuje zaś każdy program komputerowy. Poseł będzie musiał zatem wymienić wszystkie, nawet najbardziej oczywiste funkcje oprogramowania przetwarzającego dane osobowe.

Adresy email stanowią, co do zasady, dane osobowe. Przetwarzanie adresu email w celu wysyłania newslettera zawierającego materiały promocyjne innych podmiotów (np. partii politycznej, do której należy Poseł), nie będzie dopuszczalne bez zgody osoby przesyłającej dane. Ponieważ jednak zgoda na przetwarzanie danych musi być wyraźna (art. 4 (8) LIBE), samo przekazanie adresu email nie będzie uważane za wyrażenie zgody. Osoba zainteresowana otrzymywaniem newslettera będzie musiała zaznaczyć dodatkowy checkbox, w którym wyrazi zgodę na przetwarzanie danych w celu prowadzenia wysyłki newslettera.

Organizacja konkursu

1) Poseł będzie musiał przedstawić uczestnikom konkursu większość informacji opisanych powyżej.

2) Konkurs w wielu wypadkach nie jest umową, ale ma charakter przyrzeczenia publicznego. Dlatego Poseł będzie mógł przetwarzać dane osobowe w celu organizacji konkursu na podstawie przesłanki uzasadnionego celu administratora danych (art. 6 (1) (f) LIBE). Jednakże uczestnik konkursu będzie mógł w każdej chwili (np. po odebraniu nagrody) wyrazić sprzeciw wobec przetwarzania jego danych. W takiej sytuacji Poseł będzie musiał niezwłocznie usunąć jego dane (art. 19 (2) LIBE). Obowiązek usunięcia danych jest bezwarunkowy. Poseł utraci prawo do przetwarzania danych osobowych np. w celach dowodowych dla udokumentowania przebiegu konkursu, lub w celu publikacji wyników konkursu. Poseł nie będzie mógł przetwarzać danych uczestnika, który wyraził sprzeciw, w celu rozliczenia środków wydatkowanych na organizację konkursu.

Organizacja wizyt w Parlamencie Europejskim

1) Poseł jako organizator wizyt w Parlamencie będzie administratorem danych osobowych ich uczestników. Jednakże Poseł nie będzie z reguły zawierał odpowiednich umów z uczestnikami wizyt. Uczestnicy będą często przedstawiani

przez współpracujące z Posłem podmioty (szkoły, stowarzyszenia, partie polityczne). Poseł po otrzymaniu listy uczestników będzie musiał niezwłocznie przekazać uczestnikom wizyty obszerne informacje, o których mowa powyżej.

2) Poseł będzie mógł umożliwić udział w wizycie opierając przetwarzanie danych na podstawie przesłanki uzasadnionego celu administratora danych (art. 6 (1) (f) LIBE). W wypadku przyjęcia takiej podstawy prawnej przetwarzanie danych nie będzie możliwe po złożeniu sprzeciwu przez uczestnika. Poseł może odebrać od uczestnika wizyty zgodę na przetwarzanie danych osobowych. Zgoda taka będzie musiała jednak zostać odebrana wprost od każdego uczestnika wycieczki, w formie pisemnej lub elektronicznej. Udział uczestnika w wizycie w Parlamencie Europejskim sugerujący zgodę uczestnika na przetwarzanie jego danych osobowych nie będzie wystarczający. Poseł będzie musiał bowiem udokumentować fakt udzielenia zgody przez osobę, której dane dotyczą (art. 7 (1) LIBE).

Wysyłanie informacji o działalności Posła

1) Poseł nie będzie mógł wysłać osobom, które podały swoje dane osobowe w związku z organizacją wizyt lub konkursów, informacji o własnej działalności lub zawiadomień o innych organizowanych przez siebie przedsięwzięciach, nawet jeżeli zdaniem Posła osoby te mogłyby być bezpośrednio zainteresowane otrzymaniem takich informacji (art. 5 lit. (b) LIBE).

2) Poseł nie będzie mógł przekazać zebranych danych osobowych innym podmiotom np. partii politycznej, do której należy Poseł, w celu promowania (marketingu) działalności tej partii. Takie działanie będzie bowiem wykraczało poza cel przetwarzania danych przez Posła (art. 5 lit. (b) LIBE).

Obsługa obywateli

1) Jeżeli w treści korespondencji od obywateli zawarte będą dane wrażliwe, poseł - chcąc zająć się zgłoszoną sprawą - będzie musiał odesłać do obywatela pismo prosząc o przesłanie wyraźnej zgody na przetwarzanie danych wrażliwych do celu załatwienia sprawy. Poseł nie będzie mógł wskazać innej podstawy prawnej przetwarzania danych, nawet jeżeli dane przetwarzane byłyby w interesie osoby, która podała swoje dane, a Poseł działałby wyłącznie w celu udzielenie odpowiedzi na otrzymaną korespondencję (art. 9 (2) LIBE).

2) Poseł nie będzie mógł w ramach swojego biura przygotowywać statystyki spraw (np. w celu sporządzenia zestawienia obrazującego skąd pochodzą zgłaszający się do niego obywatele). Przetwarzanie danych w celach statystycznych ograniczone jest bowiem do prowadzenia badań statystycznych (art. 83 LIBE).

3) Poseł będzie musiał usunąć dane po zrealizowaniu celu przetwarzania danych, co najczęściej będzie wiązać się z koniecznością zakupu i wdrożenia stosownego oprogramowania (art. 17(8b) LIBE).

MODEL nr 3 SALON KOSMETYCZNY

Opis działalności

Absolwentka studium kosmetycznego (dalej: Kosmetyczka) chciałaby otworzyć własny salon kosmetyczny.
W ramach swojej działalności przetwarzać będzie dane swoich klientów. Ze względu na konieczność zapewnienia bezpieczeństwa (wykluczenia reakcji alergicznej, przeciwwskazań) przed wykonaniem niektórych zabiegów konieczne będzie przeprowadzenie ankiety o stanie zdrowia. Przetwarzane przez nią dane klientów będą więc zawierać także dane wrażliwe. Dane są przechowywane także po zabiegu w dokumentacji klientów na potrzeby ewentualnych reklamacji oraz zw. na bezpieczeństwo klientów.

Chcąc promować swój salon w ankiecie na temat stanu zdrowia zawarta będzie klauzula zgody na przetwarzanie danych w celach marketingowych. Pozwoli to Kosmetyczce na informowanie o promocjach dotychczasowych klientów.

Aby móc pozyskać nowych klientów, Kosmetyczka będzie korzystać z usług firmy marketingowej. W tym celu kupi bazę danych (zawierającą powyżej 5000 rekordów), formalnie stając się jej administratorem. Firma marketingowa, która bazę sprzeda (udostępni) i zajmie się promocją jej salonu będzie w tym układzie przetwarzającym.

Konsekwencje w zakresie ochrony danych osobowych

Ogólne obowiązki związane z przetwarzaniem danych[2]

Obecnie w związku z rozpoczęciem działalności Kosmetyczka musi przygotować dwa dokumenty: Politykę bezpieczeństwa danych osobowych i Instrukcję zarządzania systemem informatycznym. Dokumenty te opisują zbiory danych osobowych i sposób zabezpieczenia tych danych.

Po wprowadzeniu rozporządzenia konieczne będzie przygotowanie o wiele obszerniejszej dokumentacji. Kosmetyczka będzie musiała:

1) sporządzić *„zwięzłe, przejrzyste, jasne i łatwo dostępne polityki"* dotyczące przetwarzania danych osobowych i ochrony praw podmiotów danych (art. 11(1) LIBE). Będą one dużo bardziej obszerne niż obecnie. Ponieważ mają one być „łatwo dostępne" powinny one zostać umieszczone na stronie internetowej oraz zapewne wydrukowane i udostępniane w salonie.

2) sporządzić i wdrożyć właściwe polityki oraz wdrożyć właściwe i nadające się do udowodnienia środki techniczne i organizacyjne (art. 22(1) LIBE) oraz towarzyszące im *compliance policies*, które powinny podlegać weryfikacji co dwa lata (art. 22(1a) LIBE). Kosmetyczka będzie musiała być w stanie wykazać adekwatność i skuteczność zastosowanych środków;

3) sporządzić dokumentację realizacji obowiązków wynikających z postanowień rozporządzenia (art. 28 (1) LIBE);

4) przeprowadzić analizę ryzyka (ze względu na przetwarzanie danych wrażliwych należałoby stwierdzić, że naruszenie bezpieczeństwa danych mogłoby niekorzystnie wpłynąć na prywatność podmiotów danych, art. 32a(2) lit. (g) LIBE. Analiza będzie musiała zostać udokumentowana na piśmie i będzie musiała raz do roku podlegać weryfikacji (art. 32a (4) LIBE);

[2] Analiza obowiązków przewidzianych w Sprawozdaniu LIBE przyjętym 20 października 2013r.

5) przeprowadzić ocenę skutków w zakresie ochrony danych osobowych (*data protection impact assesment*) (art. 33(1) w zw. z art. 32a (3) LIBE);

6) zatrudnić osobę świadczącą profesjonalne usługi *ABI (art. 32a(3) lit. (b) LIBE)* – obowiązek ten dotyczy administratora, który zgromadzi dane co najmniej 5.000 rekordów. Jeśli kosmetyczka skorzysta z usług firmy marketingowej formalnie stanie się administratorem bazy danych zawierającej powyżej 5 tysięcy rekordów.

Po dwóch latach działalności Kosmetyczka będzie musiała:

1) przeprowadzić weryfikację zastosowanych polityk (art. 22(1) LIBE); weryfikacja będzie musiała zostać udokumentowana (art. 28 (1) LIBE);

2) przeprowadzić i udokumentować przegląd zgodności (*compliance review*) (art. 33a LIBE);

3) udostępniając lub umożliwiając dostęp do danych osobowych firmom zewnętrznym (na przykład firmie świadczącej usługi hostingowe), z których usług będzie korzystała, Kosmetyczka będzie zmuszona zawierać szczegółowe umowy dotyczące powierzenia danych osobowych. Wszystkie zawarte umowy powierzenia będą musiały być sporządzone na piśmie (art. 26 (3) LIBE) – elektroniczne zawarcie umowy powierzenia nie będzie spełniać wymogów.

Pozyskanie danych osobowych

W chwili, w której klient będzie przekazywał Kosmetyczce jakiekolwiek swoje dane osobowe (np. przed wypełnieniem ankiety dotyczącej zdrowia) będzie ona musiała przedstawić, w formie graficznej i tekstowej następujące informacje:

1) czy dane osobowe są gromadzone poza minimum niezbędne dla każdego konkretnego celu przetwarzania;
2) czy dane osobowe są przechowywane poza minimum niezbędne dla każdego konkretnego celu przetwarzania;
3) czy dane osobowe są przetwarzane do celów innych niż cele, dla których zostały zgromadzone; Zbierając dane , np. dla celów realizacji umowy kosmetyczka nie może wykluczyć, że ze względu na nieuregulowanie rachunku przez klienta nie zostaną one wykorzystane do celów dochodzenia roszczeń. W takim wypadku- mimo tego, że dochodzenie roszczeń jest prawnie usprawiedliwionym celem, Kosmetyczka będzie musiała zaznaczyć, że nie spełnia tego obowiązku.
4) czy dane osobowe są przekazywane innym przedsiębiorcom; Jeśli dane zostaną przekazane hosting provider'owi lub w przypadku dochodzenia roszczeń- firmie, która zajmuje się egzekwowaniem długów- będzie musiała zaznaczyć nie spełnienie tego obowiązku"
5) czy dane osobowe są sprzedawane lub wynajmowane;
6) czy dane osobowe są przechowywane w postaci zaszyfrowanej.
(art. 13a LIBE)- szyfrowanie nie wydaje się w tym przypadku niezbędne. Kosmetyczka będzie musiała wskazać na niewypełnienie tego obowiązku, co podważy zaufanie potencjalnych klientów, mimo przetwarzania danych zgodnie z prawem.

W dalszej kolejności Kosmetyczka będzie musiała wyświetlić klientowi informacje o:

1) tożsamości i danych kontaktowych administratora oraz ABI;
2) celach przetwarzania danych, do których przeznaczone są dane;
3) bezpieczeństwie przetwarzania danych, w tym o warunkach umowy, na podstawie której będą przetwarzane dane, a także informacje na temat sposobu ich realizacji i spełnienia wymagań wskazanych w art. 6 (1) (f) LIBE;
4) okresie, w którym dane osobowe będą przechowywane, lub jeśli nie jest to możliwe, o kryteriach stosowanych do określenia tego okresu;
5) prawie do żądania dostępu do danych i ich poprawiania lub usunięcia danych, prawie do sprzeciwu wobec przetwarzania tych danych, lub uzyskania danych;
6) prawie do złożenia skargi do organu nadzoru oraz danych kontaktowych organu nadzoru;
7) odbiorcach lub kategoriach odbiorców danych;

8) o profilowaniu, środkach opierających się na profilowaniu, oraz przewidywanym wpływie profilowania na prawa osoby, której dane dotyczą ;
9) o algorytmach związanych z każdym automatycznym przetwarzaniem danych;
10) wszelkie inne informacje, które są niezbędne w celu zagwarantowania rzetelnego przetwarzania danych, uwzględniające szczególne okoliczności, w których dane osobowe są gromadzone i przetwarzane, w szczególności istnienie niektórych czynności przetwarzania, których ocena wskazuje, że mogą wiązać się z wysokim ryzykiem w zakresie ochrony danych;
11) w stosownych przypadkach, informację, czy dane osobowe były dostarczone do władz publicznych w ostatnim okresie kolejnych 12 miesięcy.
(art. 14 LIBE)

Ze względu na obszerność tego katalogu spełnienie obowiązku informacyjnego będzie wymagało odesłania do polityk przetwarzania. Sporządzenie tak obszernego i złożonego dokumentu wymaga wiedzy o zasadach i praktyce przetwarzania danych, której przeciętny przedsiębiorca nie posiada.
W praktyce - jeszcze przed rozpoczęciem działalności - Kosmetyczka będzie musiała ponieść koszty związane z zatrudnieniem prawnika/ABI, który opracuje dla niej polityki prywatności, klauzule zgody, formularz realizujący obowiązek informacyjny itd.

Przetwarzanie danych osobowych w celach dokumentacyjnych

1) Po zrealizowaniu umowy Kosmetyczka będzie mogła przetwarzać dane osobowe klientów w celach dowodowych (art. 17(4) lit. (b) LIBE). Kosmetyczka nie będzie mogła jednak prowadzić rejestru (np. w formacie Excel) wizyt klientów do celów np. ustalenia rabatów dla regularnych klientów, uwag co do przebiegu zabiegów (np. reakcji alergicznych, jakie wystąpiły). Zrealizowane zamówienia nie będą mogły być dostępne w ramach normalnej pracy i będą musiały być utrwalone w sposób, który uniemożliwia ich zmianę (art. 17(4) LIBE).

2) Kosmetyczka będzie musiała usunąć dane po zrealizowaniu celu przetwarzania danych, co najczęściej będzie wiązać się z koniecznością zakupu i wdrożenia stosownego oprogramowania (art. 17(4) lit. (b) LIBE.

Sankcje

Naruszenie jakichkolwiek ze wskazanych powyżej postanowień rozporządzenia będzie mogło wiązać się z nałożeniem na Kosmetyczkę kary finansowej, niezależnie od stopnia winy - art. 79 (2a). Ograniczenie odpowiedzialności finansowej Kosmetyczki do winy umyślnej i niedbalstwa, będzie możliwe jedynie w wypadku posiadania "*European Data Protection Seal*" – art. 79(2b). Uzyskanie takiej gwarancji wymaga poniesienia przez Kosmetyczkę dodatkowych kosztów audytu – art. 39 (2a). Ze względu na przetwarzanie danych wrażliwych i ewentualne związane z tym ryzyko Kosmetyczka będzie chciała uzyskać taką pieczęć. Musi uwzględnić ten koszt jako dodatkowy koszt prowadzenia działalności .

Koszty

Kosmetyczka będzie musiała w celu spełnienia opisanych powyżej wymagań związanych z realizacją przepisów rozporządzenia ponieść istotne koszty związane z tworzeniem i utrzymaniem wymaganej dokumentacji i podejmowaniem działań organizacyjnych, do których zobowiązuje rozporządzenie.

Koszty zostały obliczone z uwzględnieniem stawek rynkowych obowiązujących obecnie, konieczności skorzystania z wyspecjalizowanych firm doradczych, poważnego ryzyka prawnego i finansowego obciążającego zarówno Kosmetyczkę, jak i usługodawcę Kosmetyczki (na przykład ABI), które to ryzyko zawsze przekłada się na wzrost cen usług.

Wysokość przedmiotowych wydatków, zważywszy na konieczność skorzystania z usług profesjonalnej firmy doradczej (realizacja obowiązków wymaga specjalistycznej wiedzy prawniczej, a często także technicznej, której Kosmetyczka nie posiada), można szacować w następujący sposób:

1) sporządzenie polityk dotyczących przetwarzania danych osobowych i ochrony praw podmiotów danych (art. 11(1) LIBE) – 6.000 złotych netto,
2) przygotowanie klauzul informacyjnych (art. 13a i 14 LIBE) – 600 złotych netto,
3) sporządzenie polityk zgodności (art. 22(1a) LIBE) – minimum 6.000 złotych netto,
4) przeprowadzenie i udokumentowanie analizy ryzyka (art. 32a (4) LIBE) – minimum 6.000 złotych netto
5) przeprowadzenie oceny skutków w zakresie ochrony danych osobowych (*data protection impact assesment*) (art. 33(1) w zw. z art. 32a (3) LIBE) – minimum 6.000 złotych netto,
6) sporządzenie pisemnych umów powierzenia przetwarzania danych osobowych dla co najmniej dwóch podmiotów (hostingodawców i dostawcy oprogramowania) – 1.500 złotych netto.

   Kosmetyczka będzie musiała zawrzeć umowę z osobą świadczącą usługi ABI (art. 32a(3) lit. (b) LIBE). Umowa będzie musiała zostać zawarta na czas określony. Koszt takiej stałej obsługi Kosmetyczki można szacować na (zważywszy na minimalny zakres przetwarzania danych przez Kosmetyczkę) na około 1.500 złotych netto **miesięcznie, czyli 18.000 złotych netto w skali roku**.

Co roku Kosmetyczka będzie musiała ponieść koszt weryfikacji analizy ryzyka i udokumentowania tego procesu (art. 32a (4) LIBE). Działanie to będzie miało charakter rutynowy jego koszt można szacować na około 1.500 złotych netto.

Po dwóch latach działalności Kosmetyczka będzie musiała ponieść wydatki niezbędne do nabycia usług:

1) przeprowadzenia i udokumentowania weryfikacji zastosowanych polityk (art. 22(1) LIBE); – 1.500 złotych netto.
2) przeprowadzenia i udokumentowania przeglądu zgodności (*compliance review*) (art. 33a LIBE) – 1.500 złotych netto.

Nie można wykluczyć, że ze względu na przetwarzanie danych wrażliwych koszt tych usług będzie wyższy.

Łączne koszty realizacji obowiązków dokumentacyjnych wynikających z rozporządzenia w okresie pierwszych dwóch lat prowadzenia działalności przez Kosmetyczkę można szacować na nie mniej niż 66.600 złotych + VAT.

Suma ta obejmuje jedynie koszty sporządzenia i realizacji dokumentacji oraz klauzul informacyjnych, w tym koszty związanej z tymi działaniami obsługi prawnej oraz koszty nabycia usług ABI.

Powyższy kosztorys nie obejmuje kosztów działań niezbędnych do rzeczywistego zabezpieczenia danych osobowych przed ich utratą i zniszczeniem.

Wskazane powyżej zestawienie pomija w szczególności koszty zakupu oprogramowania służącego do ochrony danych w tym oprogramowania antywirusowego i szyfrującego, koszty nabycia usług hostingowych we właściwie zabezpieczonych serwerach, koszty tworzenia kopii zapasowych, czy wreszcie koszty zabezpieczeń fizycznych, które powinny zostać zastosowane w siedzibie Kosmetyczki.

[i] Komisja ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych
[ii] Analiza obowiązków przewidzianych w Sprawozdaniu LIBE przyjętym 20 października 2013 r.
[iii] Analiza obowiązków przewidzianych w Sprawozdaniu LIBE przyjętym 20 października 2013 r.