KINGFISHER PLC

Norma ochrony danych

Właściciel dokumentacji:	Inspektor Ochrony Danych Grupy
Dokument przeznaczony do wiadomości:	Wszystkie spółki Kingfisher
Polityka generalna	Polityka ochrony danych
Kolejna aktualizacja:	9 stycznia 2019 r.
Powiązane dokumenty:	Polityka ochrony danych, Polityka prowadzenia dokumentacji i przechowywania dokumentów, Norma prowadzenia dokumentacji i przechowywania dokumentów, Polityka bezpieczeństwa informacyjnego, Polityka dopuszczalnego użytkowania

Spis treści

1. Podsumowanie i cel(-e)

Celem niniejszej Normy Polityki jest zapewnienie zgodności z przepisami prawnymi dotyczącymi ochrony danych i prywatności oraz zapewnienie, że dane naszych klientów, pracowników i dostawców są zbierane i wykorzystywane zawsze zgodnie z jurysdykcją, której podlegają Spółki Grupy Kingfisher.

W niniejszej Normie Polityki „**Dane osobowe**" oznaczają informacje pozyskane indywidualnie lub wraz z innymi informacjami, które pozwalają na identyfikację osób („**Osoba fizyczna**"). Obejmują one na przykład: firmowy adres e-mail Osoby fizycznej, jej imię w połączeniu z adresem pocztowym lub datą urodzenia, zdjęciem itp.

Dane osobowe należy zawsze przechowywać bezpiecznie oraz przetwarzać rzetelnie,~~i traktować sprawiedliwie~~, przejrzyście i zgodnie z przepisami prawa.

Każda Spółka Grupy musi być świadoma ram regulacyjnych, które obowiązują na terytorium, w którym działa spółka.

- W Unii Europejskiej od 25 maja 2018 r. obowiązuje Ogólne rozporządzenie o ochronie danych (GDPR) (Rozporządzenie Unii Europejskiej 2016/679) oraz inne przepisy dotyczące prywatności i lokalne zasady ochrony danych;
- Poza Unią Europejską Spółki Grupy obowiązują wszelkie lokalne i regionalne przepisy prawne, których spółki muszą przestrzegać w swojej działalności.

Inspektor Ochrony Danych Grupy ustali i wdroży obowiązujące procedury zgodności z pomocą osoby, która w każdym kraju działalności Kingfisher jest odpowiedzialna za kwestie dotyczące ochrony danych („**Krajowy Delegat ds. Ochrony Danych**").

2. Odpowiedzialność i kierownictwo

2.1 INSPEKTOR OCHRONY DANYCH GRUPY jest odpowiedzialny za niniejszą Normę Polityki i jej wdrożenie w całej Grupie.

Rola i odpowiedzialność Inspektora Ochrony Danych są następujące:

- bieżące informowanie Rady Dyrektorów o odpowiedzialności, zagrożeniach i problemach związanych z ochroną danych;
- regularne aktualizowanie i zatwierdzanie procedur i polityk ochrony danych;
- monitorowanie zgodności z procedurami, politykami i obowiązującymi przepisami w zakresie ochrony danych i prywatności;
- zorganizowanie szkolenia na temat ochrony danych i doradzanie pracownikom i osobom objętym niniejszymi zasadami;
- udzielanie odpowiedzi na pytania o ochronę danych pracowników, członków zarządu i innych partnerów;
- udzielanie odpowiedzi osobom takim, jak klienci i pracownicy, którzy chcą wiedzieć, które z ich danych są przechowywane, a także zatwierdzanie ze stronami trzecimi,

które obsługują dane spółki, wszelkich kontraktów lub umów dotyczących przetwarzania danych;
- nadzorowanie i aktualizowanie ~~ocen wpływu na prywatność~~ oceny skutków dla ochrony danych;
- bycie punktem kontaktu dla głównego organu nadzorczego oraz współpraca z lokalnymi organami nadzorczymi.

Z Inspektorem Ochrony Danych można skontaktować się, wysyłając wiadomość e-mail na adresdpo@kingfisher.com

Pamiętaj, że wszystkie spółki Kingfisher oraz wszystkie piony w Grupie są zobowiązane do ujawnienia wszelkich informacji, których może potrzebować Inspektor Ochrony Danych w celu realizacji swoich obowiązków bez zbędnej zwłoki.

2.2 KRAJOWY DELEGAT DS. OCHRONY DANYCH jest odpowiedzialny za:
- pomoc Inspektorowi Ochrony Danych w zrozumieniu lokalnych przepisów prawnych dotyczących prywatności lub ustaw o ochronie danych;
- pomoc Inspektorowi Ochrony Danych w definiowaniu zasad i procesów ochrony danych w kraju lub na terytorium działania Spółek Grupy Kingfisher;
- pośredniczenie pomiędzy Inspektorem Ochrony Danych a odpowiednimi Spółkami Grupy Kingfisher w kraju w kwestiach związanych z ochroną danych lub prywatnością.

Lista Krajowych Delegatów ds. Ochrony Danych jest dostępna w Intranecie, a informacje o zmianach będą regularnie podawane przez Komunikację Wewnętrzną.

2.3 ZESPÓŁ ZARZĄDCZY IT jest odpowiedzialny za zapewnianie bezpieczeństwa danych w systemach Kingfisher i stron trzecich.

Przed przetwarzaniem danych przez Spółkę Grupy lub stronę trzecią należy skonsultować się z Zespołem Zarządczym IT. Informacje o osobach kontaktowych z Zespołu Zarządczego IT są podane w Intranecie, a informacje o zmianach będą regularnie podawane przez Komunikację Wewnętrzną.

Role i odpowiedzialność Zespołu Zarządczego IT:
- zapewnienie, że wszystkie systemy, usługi, oprogramowanie i sprzęt spełniają dopuszczalne standardy bezpieczeństwa;
- zapewnienie, że wszystkie systemy, usługi, oprogramowanie i sprzęt umożliwiają zachowanie zgodności z politykami, standardami, procesami, wytycznymi i przepisami prawnymi odpowiednich krajów w zakresie ochrony danych;
- sporządzanie systemów i polityk bezpieczeństwa informacyjnego oraz dokumentów związanych z umowami;
- przeprowadzanie oceny należytej staranności stron trzecich.

3. Minimalne standardy Grupy

O ile przepisy prawne obowiązujące w Spółkach Operacyjnych Grupy Kingfisher nie nakładają bardziej rygorystycznych wymogów (w którym to przypadku takie wymogi są obowiązujące), w Grupie Kingfisher podczas przetwarzania Danych osobowych pracowników, klientów i dostawców zawsze obowiązują poniższe standardy. Bardziej szczegółowe zasady obowiązujące w poszczególnych krajach zostaną podane do wiadomości każdej Spółki Grupy Kingfisher przez Inspektora Ochrony Danych lub Krajowego Delegata ds. Ochrony Danych.

3.1 Zbieranie danych:

Przez zebraniem Danych osobowych:

- musimy upewnić się, że zbieramy tylko Dane osobowe konieczne do realizacji celu;
- musimy upewnić się, że cel zbierania danych ma uzasadnienie i nie narusza praw Osób fizycznych;
- musimy w jasny sposób poinformować Osoby fizyczne o tym, w jakim sposób i dlaczego zamierzamy wykorzystać ich Dane osobowe;
- musimy zapewnić, że Dane osobowe zostaną zebrane w sposób bezpieczny i że zostaną podjęte odpowiednie środki bezpieczeństwa, które mają na celu zapobiec nieautoryzowanemu dostępowi do Danych osobowych, ich zniszczeniu i utracie.

3.2 Operowanie danymi:

- musimy zapewnić, że Dane osobowe nie są dostępne osobom, które nie potrzebują do nich dostępu;
- musimy zapewnić, że Dane osobowe są wykorzystywane wyłącznie w celach, do jakich zostały zebrane, czego Osoby fizyczne, których dane są wykorzystywane, mogłyby oczekiwać;
- musimy regularnie sprawdzać i potwierdzać, że dane są przetwarzane i przechowywane w sposób bezpieczny oraz chronione przed nieuprawnionym~~ch~~ dostępem, zniszczeniem oraz utratą;
- musimy rozpoznać poniższe informacje oraz zapisać je w formacie, o którym poinformuje Inspektor Ochrony Danych: (i) kategorie zbieranych i przetwarzanych danych, (ii) kategorie Osób fizycznych, których dane są przetwarzane, (iii) kategorie odbiorców, którym zostały lub będą udostępnione Dane osobowe, (iv) adresy miejsc przechowywania danych.
- Za każdym razem przed użyciem automatycznego narzędzia przetwarzania, którego użycie skutkuje podjęciem automatycznych decyzji w sprawie Osoby fizycznej, np. oceną określonych aspektów personalnych Osoby fizycznej do analizy lub prognozy określonych aspektów jej wyników pracy, sytuacji ekonomicznej, zdrowia, indywidualnych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczenia się, należy skontaktować się z Inspektorem Ochrony Danych lub Krajowym Delegatem ds. Ochrony Danych.

3.3 Przekazywanie danych:

Przed~~z~~ wydaniem zgody na udzielenie dostępu (poprzez transfer lub dostęp zdalny) do Danych osobowych jakiemukolwiek podmiotowi przetwarzającemu dane spoza Grupy Kingfisher:

- musimy zapewnić, że podmiot przetwarzający dane, któremu przekazujemy Dane osobowe, spełnia wymogi niniejszej Normy oraz obowiązujących przepisów prawa;
- musimy rozpoznać i zapisać poniższe informacje: (i) imię, nazwisko i dane kontaktowe przedstawiciela podmiotu przetwarzającego dane oraz inspektora ochrony danych, (ii) kategorie przetwarzanych danych, (iv) kategorie osób, których dane będą przetwarzane, (v) adresy miejsc, do których zostaną przekazane dane i z których nastąpi dostęp do danych, (vi) lista i dane korporacyjne dotyczące podwykonawców przetwarzania (vi) kategorie odbiorców, którym zostały lub będą udostępnione Dane osobowe;
- musimy zapewnić, że żadne Dane osobowe nie zostaną przekazane do i nie będą dostępne z innego kraju lub terytorium, jeżeli ten kraj lub to terytorium nie zapewnia odpowiedniego poziomu ochrony praw i wolności Osób fizycznych w związku z przetwarzaniem danych osobowych lub że zostanie zawarta pomiędzy stronami pisemna umowa zawierająca odpowiednie zapewnienia (lub że istnieją ważne alternatywne ustalenia, zgodne z obowiązującymi przepisami prawnymi o ochronie danych osobowych, które zawierają takie zapewnienia).

3.4 Przechowywanie danych

Nie należy przechowywać Danych dłużej, niż jest to konieczne dla~~w~~ celu, w jakim zostały zebrane (ustęp 3.1 powyżej). Oznacza to, że dane muszą zostać zniszczone lub bezpiecznie usunięte z systemów spółki, jeżeli ich przechowywanie nie jest dłużej wymagane.

Przykład: Klient wziął udział w konkursie, w którym do wygrania były elektronarzędzia. W tym celu wypełnił formularz, wpisując swoje imię i nazwisko, adres i ~~number~~ numer telefonu i zaznaczył, że nie chce otrzymywać żadnych dalszych wiadomości od Spółki Grupy. Po rozlosowaniu nagród Spółka Grupy powinna usunąć dane klienta podane w formularzu, ponieważ nie muszą być dłużej przechowywane w celu, w jakim zostały zebrane.

Należy zapewniać zgodność z polityką Kingfisher w zakresie przechowywania dokumentów oraz z przepisami prawnymi określającymi okres przechowywania.

3.5 Prawa Osób fizycznych

Dane należy przetwarzać z poszanowaniem praw Osób fizycznych. Prawa Osób fizycznych różnią się w zależności od kraju. W ogólnym ujęciu, w Unii Europejskiej Osoby fizyczne mają prawo:

(a) wycofać zgodę na przetwarzanie ich Danych osobowych (jeżeli dane są przetwarzane w oparciu o zgodę);
(b) sprzeciwić się przetwarzaniu swoich Danych osobowych (jeżeli dane są przetwarzane w uzasadnionym interesie);
(c) uzyskać dostęp do wszelkich przechowywanych Danych osobowych na ich temat;
(d) zażądać ~~skorygowania~~ poprawienia nieprawidłowości w Danych osobowych;

(e) zażądać usunięcia swoich Danych osobowych z systemów spółki;
(f) zażądać przesłania swoich danych osobowych do innych spółek;
(g) nie dopuścić do przetwarzania danych, jeżeli może to spowodować szkody lub stworzyć niebezpieczeństwo zagrażające im samym lub innym osobom.

3.6 Zażalenia i naruszenia

Wszelkie zażalenia i naruszenia, w tym naruszenia ochrony danych osobowych~~bezpieczeństwa, które mają wpływ na Dane osobowe~~, muszą zostać bezzwłocznie zgłoszone do Inspektora Ochrony Danych i/lub delegata.

Wszelkie zażalenia w sprawie naruszeń ochrony danych osobowych~~bezpieczeństwa, które mają wpływ na Dane osobowe~~ muszą zostać bezzwłocznie zgłoszone do Kierownika Zespołu Zarządczego IT.

Jakakolwiek kradzież, niewłaściwe użycie lub naruszenie bezpieczeństwa, które skutkuje zniszczeniem, utratą, zmianą, niepowołanym ujawnieniem lub dostępem do Danych osobowych, muszą zostać bezzwłocznie (w każdym wypadku w ciągu nie dłużej niż 2 godzin) zgłoszone do Inspektora Ochrony Danych oraz Kierownika Zespołu Zarządczego IT.

4. Monitorowanie i audyt

Aby zapewnić zgodność z niniejszą Normą Polityki, co jakiś czas zostanie przeprowadzony audyt zgodności z niniejszą Normą Polityki i innymi procesami związanymi z ochroną danych wydanymi przez Inspektora Ochrony Danych lub Krajowych Delegatów ds. Ochrony Danych.

Jeżeli masz wątpliwości co do przedmiotu niniejszej Normy Polityki, zwróć się o pomoc do Inspektora Ochrony Danych Grupy lub swojego Krajowego Delegata ds. Ochrony Danych.

Możesz również zadzwonić na infolinię, aby zgłosić swoje wątpliwości.

5. Zestawienie zgód i zatwierdzeń

Działanie/sytuacja	Wiadomość		Do/od kogo?
	(Uprzednie) Powiadomienie	Uprzednie zatwierdzenie	
Naruszenie ~~danych~~ochrony danych osobowych	X		Inspektor Ochrony Danych Grupy* + Kierownik Zarządczy
Zautomatyzowane podejmowanie decyzji (w tym Profilowanie)	X	X	Inspektor Ochrony Danych Grupy + Kierownik Zarządczy
Zażalenia ~~podmiotów danych~~osób, których dane dotycza	X		Inspektor Ochrony Danych Grupy

Zapytania organów regulacyjnych	X		Inspektor Ochrony Danych Grupy* + Dyrektor ds. Prawnych Grupy
Działanie egzekwujące rozporządzenie	X		Inspektor Ochrony Danych Grupy* + Dyrektor ds. Prawnych Grupy
Wykonanie praw ~~podmiotów danych~~ osób, których dane dotyczą	X		Inspektor Ochrony Danych Grupy
Nowe operacje przetwarzania, które uruchamiają wymóg Oceny ~~wpływu na prywatność danych~~skutków dla ochrony danych	X	X	Inspektor Ochrony Danych Grupy + Kierownik Zarządczy

*W każdym przypadku bezpośrednio lub za pośrednictwem Krajowego Delegata ds. Ochrony Danych.