PRZEWODNIK DLA PRZEDSIĘBIORCÓW SPOŁECZNYCH

O CZYM NALEŻY PAMIĘTAĆ PRZETWARZAJĄC DANE OSOBOWE

Każdy przedsiębiorca w czasie wykonywania swojej działalności przetwarza dane osobowe. Dane te mogą dotyczyć jego pracowników, klientów czy dostawców różnorodnych usług. Zgodne z prawem przetwarzanie danych wymaga jednak uwzględnienia szeregu wymogów wskazanych w regulacjach prawnych oraz wypracowania odpowiednich wewnętrznych procedur i wdrożenia środków zabezpieczających te dane przed nieuprawnionym dostępem. W przypadku nieodpowiedniego przetwarzania danych przedsiębiorca może ponieść odpowiedzialność prawną. Dlatego też kwestia ta, chociaż często traktowana jako stosunkowo mało istotna, w praktyce ma bardzo duże znaczenie.

Celem niniejszego przewodnika jest więc zapoznanie przedsiębiorców społecznych z podstawowymi zagadnieniami z zakresu ochrony danych osobowych.

SPIS TREŚCI

1. PODSTAWOWE POJĘCIA

Czym są dane osobowe?

Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Danymi osobowymi są zarówno takie informacje, które pozwalają na jednoznaczne określenie tożsamości konkretnej osoby (np. imię i nazwisko, numer PESEL), jak również takie, które nie pozwalają na jej bezpośrednią identyfikację, ale po podjęciu dodatkowych działań są wystarczające do jej ustalenia. W związku z tym danymi osobowymi nie będą informacje o dużym stopniu ogólności, np. nazwa ulicy i numer domu czy wysokość wynagrodzenia. Informacje takie będą jednak stanowić dane osobowe wówczas, gdy zostaną zestawione z dodatkowymi informacjami, które w konsekwencji można odnieść do konkretnej osoby (np. powiązać z jej imieniem i nazwiskiem, czy też numerem PESEL).

Czym jest "przetwarzanie danych" w rozumieniu ustawy?

Przetwarzaniem danych są wszelkie operacje wykonywane na danych osobowych, takie jak np. zbieranie, utrwalanie danych, ich opracowywanie, zmienianie, udostępnianie i usuwanie, w tym w szczególności operacje, które wykonuje się w systemach informatycznych.

Przetwarzanie w rozumieniu ustawy to nie tylko aktywne działanie, jakie przedsiębiorca podejmuje w stosunku do danych osobowych (np. analiza danych, przekazywanie ich innym podmiotom, publikacja danych w Internecie), ale także samo przechowywanie danych, np. na płycie CD, lub na serwerze zewnętrznej firmy informatycznej (tzw. hosting danych).

Dane jakich osób są chronione prawem?

Aktualnie, na gruncie przepisów chronione są dane osobowe wszystkich żyjących osób fizycznych, w tym także osób fizycznych prowadzących jednoosobową działalność gospodarczą. Przedsiębiorca powinien więc zapewnić ochronę danych m.in. swoich pracowników, współpracowników, klientów, jak również osób kontaktowych po stronie kontrahentów (np. podwykonawców, którym zleca świadczenie pewnych usług, w tym jednoosobowych przedsiębiorców). Osoby, których dane są przetwarzane określane są jako tzw. "osoby, których dane dotyczą" lub "podmioty danych".

Kiedy przedsiębiorca jest administratorem danych, a kiedy tzw. procesorem danych osobowych?

Administratorem danych jest każdy podmiot (przedsiębiorca), który decyduje o celach (tzn. po co dane osobowe mają być przetwarzane, np. na potrzeby reklamowania produktów i usług, na potrzeby rekrutacji, realizacji umowy, itp.) oraz o środkach (w szczególności używanym systemie informatycznym) przetwarzania danych osobowych. Na administratora danych ustawa nakłada wiele obowiązków związanych z przetwarzaniem danych.

Administrator danych może przetwarzać dane samodzielnie, bądź też korzystać z usług innego podmiotu, tzn. powierzyć przetwarzanie danych np. firmie informatycznej, agencji reklamowej, firmie świadczącej usługi księgowe. Taki podmiot określany jest mianem przetwarzającego dane na zlecenie (tzw. procesor danych). Procesor może przetwarzać powierzone mu dane tylko w takim zakresie i celach, jakie wynikają z umowy, którą administrator i procesor są zobowiązani zawrzeć (tzw. umowa powierzenia danych osobowych, wymagająca formy pisemnej).

Jakie przepisy regulują przetwarzanie danych osobowych?

Podstawowym aktem prawnym regulującym zasady przetwarzania danych osobowych w Polsce jest aktualnie ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Ponadto, podmioty przetwarzające dane osobowe powinny stosować się do przepisów zawartych w aktach wykonawczych do tej ustawy. Lista podstawowych regulacji dotyczących ochrony danych osobowych znajduje się pod adresem http://www.giodo.gov.pl/144/j/pl/.

Co istotne, w maju 2018 r. zacznie obowiązywać w Polsce unijna regulacja o ochronie danych osobowych (tzw. ogólne rozporządzenie o ochronie danych), która w istotnym zakresie zastąpi obowiązujące obecnie przepisy. Biorąc pod uwagę skalę zmian przedsiębiorcy powinni już teraz rozpocząć przygotowania do zmian.

2. OBOWIĄZKI ZWIĄZANE Z PRZETWARZANIEM DANYCH

Przedsiębiorca przetwarzający dane osobowe jest zobowiązany spełnić szereg wymogów prawnych oraz podjąć określone działania w celu zapewnienia bezpieczeństwa danych. Zakres tych obowiązków zależy od roli, w jakiej przedsiębiorca występuje, tzn. czy jest on administratorem danych, czy też podmiotem przetwarzającym dane osobowe na zlecenie (tj. procesorem danych) – przy czym ten sam podmiot może występować w obu tych rolach, w zależności od prowadzonych operacji na danych.

2.1 Obowiązki administratora danych

Znajdujące się poniżej zestawienie zawiera wykaz podstawowych obowiązków z zakresu ochrony danych osobowych, do których realizacji zobowiązany jest każdy przedsiębiorca będący **administratorem danych**.

Podstawy przetwarzania danych

- Administrator musi być w stanie wykazać, że przetwarzanie danych w konkretnym celu (np. marketingowym, rekrutacyjnym) jest uzasadnione i może zostać oparte na co najmniej jednej podstawie pozwalającej na przetwarzanie danych, które określone są w ustawie o ochronie danych osobowych ('**uodo**') (art. 23 oraz art. 27 uodo). Przesłanki te to np. zgoda osoby zainteresowanej (np. klienta lub użytkownika witryny internetowej) lub konieczność zawarcia i realizacji umowy (np. umowy sprzedaży zawartej z kontrahentem). Czasem to przepisy innych ustaw wprost dopuszczają przetwarzanie określonych danych, dla określonych celów (np. Kodeks pracy, ustawa o świadczeniu usług drogą elektroniczną).

- Pozyskanie zgody osoby, której dane dotyczą nie w każdym przypadku jest konieczne, aby legalnie przetwarzać dane osobowe w konkretnym celu. Wszystkie wskazane w przepisach prawa podstawy (przesłanki) stanowią równorzędną podstawę przetwarzania danych. Dlatego też w sytuacji gdy przetwarzanie danych jest niezbędne do zawarcia i realizacji umowy, nie ma potrzeby zbierania dodatkowej zgody od strony umowy, aby przetwarzać dotyczące jej dane osobowe w tym celu.

- W sytuacji gdy przetwarzanie danych oparte jest na zgodzie podmiotu danych, oświadczenie dotyczące wyrażenia zgody musi być sformułowane w zrozumiały i jednoznaczny sposób, a także musi zostać wyodrębnione od innych oświadczeń woli składanych przez tę osobę. W szczególności zgoda na przetwarzanie danych nie może być częścią umowy lub regulaminu, lecz musi stanowić odrębną deklarację zainteresowanej osoby (tzw. klauzulę zgody).

- Zbieranie oraz przetwarzanie tzw. danych wrażliwych ("sensytywnych"), tj. danych, o których mowa w art. 27 ust. 1 uodo, takich jak dane o stanie zdrowia czy o poglądach politycznych, jest co do zasady zabronione. Jeśli jednak dane takie muszą zostać zebrane dla potrzeb prowadzenia działalności gospodarczej przez administratora, można to zrobić pod warunkiem otrzymania zgody osoby, której dane dotyczą (która w tym przypadku wymaga formy pisemnej) lub spełnienia innej przesłanki legalności wskazanej w przepisach prawa (art. 27 ust. 2 uodo).

Podstawowe zasady przetwarzania danych osobowych

- Poza koniecznością wykazania właściwej podstawy prawnej dla operacji na danych, administrator musi również przez cały czas przetwarzać dane zgodnie z podstawowymi zasadami określonymi w przepisach prawa (art. 26 uodo).

- Zgodnie z tymi zasadami, dozwolone jest zbieranie wyłącznie tych rodzajów danych, które są ściśle związane z celem prowadzonej przez administratora działalności. Dane muszą być więc adekwatne do celu przetwarzania, np. w celu przesyłania newslettera drogą mailową nie będzie adekwatne przetwarzanie pełnych danych adresowych osoby, jej numeru telefonu, czy też numeru PESEL.

- Gromadzone dane muszą być potrzebne do realizacji istniejącego (znanego administratorowi) celu przetwarzania. Dlatego też zabronione jest zbieranie danych "na zapas", a więc wyłącznie z założeniem przyszłego ich wykorzystania.

- Administrator nie może uzależniać zawarcia umowy/realizacji usługi od wyrażenia przez podmiot danych zgody na ich przetwarzanie dla innych celów niż wykonanie umowy/realizacja usługi (np. dla celów marketingu towarów i usług podmiotów trzecich).

- Administrator jest zobowiązany do zweryfikowania, czy zbierane dane są dokładne, kompletne i aktualne, w szczególności gdy dane nie pochodzą bezpośrednio od podmiotu danych, ale np. gdy baza danych została nabyta od podmiotu trzeciego (tzw. brokera danych).

- Zabronione jest przechowywanie danych dłużej niż jest to konieczne dla osiągnięcia celu, dla którego dane zostały zebrane. Wymaga to określenia przez administratora tzw. okresów retencji (przechowywania) danych.

- W przypadku gdy cel przetwarzania zostanie osiągnięty (np. świadczenie na rzecz podmiotu danych zostanie wykonane), zebrane dane powinny zostać usunięte lub zanonimizowane (czyli pozbawione cech, które pozwalają na przypisanie ich konkretnej osobie), chyba że dopuszczalne jest dalsze ich przetwarzanie na podstawie obowiązujących przepisów prawa.

Obowiązek informacyjny

- Przed rozpoczęciem przetwarzania danych osobowych administrator jest zobowiązany przekazać osobie, której dane dotyczą, określone w przepisach prawa informacje, m.in. na temat danych adresowych administratora, celu zbierania danych, znanych administratorowi odbiorców danych (tj. o innych administratorach danych, którym dane mogą zostać przekazane), prawie dostępu do treści danych dotyczących określonej osoby oraz prawie ich poprawiania, itd. (art. 24 uodo).

- W przypadku gdy administrator nie uzyskał danych bezpośrednio od podmiotu danych (np. jeśli administrator nabył zbiór danych od brokera danych), wymagane jest poinformowanie osób, których dane dotyczą dodatkowo o fakcie przetwarzania danych oraz o tym, skąd pochodzą dane (art. 25 uodo).

Obowiązek informacyjny

- Przepisy prawa nie określają formy, w jakiej obowiązek informacyjny powinien być realizowany. Dopuszczalne jest więc poinformowanie podmiotu danych np. pisemnie, mailowo, czy też telefonicznie.
- Sposób poinformowania powinien pozwalać na wykazanie, iż administrator prawidłowo zrealizował swój obowiązek. W przypadku ewentualnego sporu dotyczącego wypełnienia obowiązku informacyjnego, to administrator danych zobowiązany będzie dostarczyć dowód, że został on spełniony.
- Podmiot danych ma prawo dostępu do treści swoich danych, prawo ich poprawiania, usuwania oraz żądania zaprzestania ich dalszego przetwarzania w określonych przypadkach.

Obowiązek rejestracyjny

- Administrator danych jest, co do zasady, zobowiązany zgłosić zbiór (zbiory) danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych ('**GIODO**').
- Obowiązkowi rejestracji zbioru danych osobowych nie podlega administrator danych, który powołał administratora bezpieczeństwa informacji ('**ABI**') i zgłosił go GIODO do rejestracji – jednakże wyłącznie w przypadku, gdy zbiór taki nie zawiera danych wrażliwych (art. 43 ust. 1a uodo).
- Przed zgłoszeniem zbioru do rejestracji, każdy administrator powinien zweryfikować, czy prowadzony przez niego zbiór danych nie jest zwolniony z obowiązku rejestracji na podstawie przepisu prawa (tj. art. 43 ust. 1 uodo).
- Administrator powinien dokonać zgłoszenia zbioru danych do rejestracji za pomocą formularza, którego wzór opublikowany został w przepisach wykonawczych do ustawy; może również skorzystać z formularza on-line dostępnego na stronie internetowej GIODO.
- Wszelkie zmiany dotyczące informacji zgłoszonych uprzednio do rejestracji należy zgłosić GIODO w ciągu 30 dni od daty ich wprowadzenia. Aktualizacji danych zawartych w zgłoszeniu należy dokonać w ten sam sposób, co samego zgłoszenia.
- W sytuacji gdy w zbiorze nie są przetwarzane dane wrażliwe, rozpoczęcie przetwarzania takich danych można rozpocząć już po zgłoszeniu zbioru do rejestracji GIODO, tj. po samym wysłaniu wniosku.
- W sytuacji natomiast przetwarzania danych wrażliwych administrator może rozpocząć ich zgodne z prawem przetwarzanie dopiero po dokonaniu rejestracji zbioru danych przez GIODO, tj. wpisaniu takiego zbioru do rejestru, który jest dostępny pod adresem https://egiodo.giodo.gov.pl/index.dhtml.

Zabezpieczenie danych

- Administrator powinien w ramach swojej organizacji (przedsiębiorstwa) wdrożyć stosowne techniczne oraz organizacyjne zabezpieczenia przetwarzanych danych osobowych, o których mowa w art. 36-39 uodo. Stosowane środki bezpieczeństwa powinny zostać dostosowane do istniejących zagrożeń i charakteru przetwarzanych danych.

- Dostęp do przetwarzanych danych mogą mieć jedynie osoby odpowiednio upoważnione przez administratora. Wiąże się z tym obowiązek wydawania osobom mającym dostęp do danych (np. pracownikom, współpracownikom) specjalnych pisemnych upoważnień.

- Każdy administrator danych jest zobowiązany do opracowania specjalnej dokumentacji wewnętrznej, w której należy opisać m.in. sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę danych (tzw. polityka bezpieczeństwa oraz instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych). Szczegółowy zakres informacji, które powinny zostać zawarte w tej dokumentacji określają przepisy prawa.

- Administrator oraz wszystkie osoby, które zostały przez niego upoważnione do przetwarzania danych osobowych zobowiązane są zachować w tajemnicy dane osobowe, do których mają dostęp oraz metody ich zabezpieczania.

- Administrator danych jest zobowiązany prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych, która powinna zawierać: imię i nazwisko osoby upoważnionej, datę nadania i ustania oraz zakres upoważnienia, a także identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

- Administrator danych może (lecz nie musi) powołać administratora bezpieczeństwa informacji, który będzie realizował część obowiązków związanych z ochroną danych, w imieniu administratora danych. Osoba taka musi spełniać określone wymogi, np. w zakresie wiedzy dotyczącej problematyki ochrony danych osobowych. Powołanie ABI-ego oraz zgłoszenie tego faktu GIODO pozwala administratorowi skorzystać z określonych w przepisach usprawnień (np. umożliwia w pewnych przypadkach na zwolnienie się z obowiązku zgłoszenia zbiorów danych osobowych GIODO). Powołanie ABI-ego przesądza jednak z drugiej strony o konieczności realizacji dodatkowych wymogów, np. prowadzenia wewnętrznego rejestru przetwarzanych zbiorów danych osobowych.

Udostępnianie i powierzanie danych do przetwarzania

- Udostępnianie danych (tj. przekazywanie ich innemu administratorowi danych, w celu ich przetwarzania przez tego administratora dla jego własnych celów) jest możliwe w przypadku spełnienia jednej z przesłanek legalizujących przetwarzanie danych. Udostępnianie jest bowiem jedną z form przetwarzania danych i podlega takim samym zasadom, jak inne działania podejmowane na danych.

- Powierzanie danych do przetwarzania (tzw. outsourcing przetwarzania) polega na przekazywaniu danych przez administratora innemu podmiotowi (tzw. procesorowi danych), który przetwarza te dane na rzecz i w imieniu administratora danych (np. powierzenie danych firmie hostingowej, która na zlecenie administratora przetwarza dane na swoich serwerach, korzystanie z usług kadrowo-księgowych świadczonych przez zewnętrzną firmę).

- Powierzenie danych do przetwarzania jest dopuszczalne wyłącznie w przypadku, gdy administrator zawrze z procesorem danych umowę powierzenia danych do przetwarzania. Umowa taka wymaga zawarcia w formie pisemnej i powinna określać ona co najmniej zakres powierzanych danych, zakres czynności na danych jakie realizować może procesor danych oraz wskazywać na cele, w których dane mogą być przetwarzane.

Przekazywanie danych do państw trzecich

- W przypadku gdy administrator przekazuje dane osobowe do innych podmiotów z państw *należących* do Europejskiego Obszaru Gospodarczego ('**EOG**') sytuację taką należy traktować tak samo jak przekazanie (powierzenie lub udostępnienie) wewnątrzkrajowe, w związku z czym nie jest konieczne spełnienie dodatkowych wymogów.

- Przekazywanie danych osobowych do tzw. państw trzecich (tj. państw, które *nie należą* do EOG) wymaga spełnienia dodatkowych wymogów i co do zasady jest możliwe, jeśli dane państwo zapewnia na swym terytorium odpowiedni poziom ochrony danych osobowych (co dotyczy jednak niewielkiej grupy państw, np. Kanady, Argentyny, Izraela, nie dotyczy zaś co do zasady USA, jak również Indii, Chin czy innych państw azjatyckich).

- Administrator danych może przekazać dane osobowe do państwa trzeciego, które nie zapewnia odpowiedniego poziomu ochrony danych, pod warunkiem, że spełniona jest jedna z ustawowych przesłanek dla takiego przekazania, np.: osoba, której dane dotyczą, udzieliła na to zgody na piśmie; przekazanie jest niezbędne do wykonania umowy pomiędzy administratorem danych a osobą, której dane dotyczą lub jest podejmowane na jej życzenie; czy też w sytuacji gdy dane są ogólnie dostępne (art. 47 uodo).

- Administrator danych może podpisać również specjalną umowę transferową, opartą na modelowych klauzulach opracowanych przez Komisję Europejską lub skorzystać z takich instrumentów, jak wiążące reguły korporacyjne (art. 48 uodo). Jeśli żadna z tych możliwości nie może być wykorzystana, niezbędne jest wówczas uzyskanie zgody GIODO na transfer danych, w postaci decyzji administracyjnej.

2.2 Obowiązki procesora danych

Procesor danych powinien przede wszystkim zadbać o zawarcie z administratorem, który zleca mu przetwarzanie danych, umowy powierzenia danych osobowych, zgodnej z wymogami prawnymi. Umowa taka – która stanowi podstawę zgodnego z prawem przetwarzania danych przez procesora – powinna precyzyjnie określać, jakie działania procesor powinien i może wykonywać na powierzonych danych. W sytuacji natomiast, gdyby procesor przetwarzał dane w zakresie szerszym niż przewidziany w umowie, lub też w innych celach niż określone przez administratora, należałoby traktować go w tym zakresie jako niezależnego administratora danych (z czym wiążą się dodatkowe obowiązki, wskazane powyżej). Przykładowo, gdyby dane osobowe klientów spółki A (tj. administratora danych) zostały powierzone w drodze umowy agencji reklamowej (tj. procesorowi) w celu wysłania do tych klientów treści marketingowych dotyczących spółki A, a agencja reklamowa skorzystałaby z tych danych, aby przesłać także informacje reklamowe dotyczące własnych usług, byłaby w tym zakresie administratorem danych (powinna więc np. zgłosić zbiór danych osobowych GIODO).

Co do zasady procesor nie jest zobowiązany do realizacji ustawowych obowiązków nałożonych na administratora danych (np. w zakresie obowiązku zgłoszenia zbioru danych osobowych). Procesor danych jest jednak zobowiązany zastosować te środki zabezpieczające, o których mowa w art. 36-39 u.o.d.o. Przy czym obowiązek ten powinien on zrealizować jeszcze przez rozpoczęciem przetwarzania danych na zlecenie administratora, a nie w trakcie prowadzonych operacji na danych.

3. KONTROLA Z GODNOŚCI PRZETWARZANIA DANYCH Z PRAWEM

Organem nadzorczym wyznaczonym do przeprowadzania kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych jest Generalny Inspektor Ochrony Danych Osobowych. Celem kontroli jest ustalenie stanu faktycznego w zakresie przestrzegania przez podmiot kontrolowany przepisów o ochronie danych osobowych oraz udokumentowanie dokonanych ustaleń.

W praktyce kontrole przeprowadzają inspektorzy GIODO w kilkuosobowych zespołach kontrolnych. Czynności kontrolne są dokonywane w siedzibie kontrolowanego podmiotu oraz ewentualnie także w innym miejscu (np. jednostce organizacyjnej) wskazanym jako obszar przetwarzania danych osobowych.

Kontrola przetwarzania danych osobowych obejmuje zarówno administratorów danych podlegających obowiązkowi zgłoszenia zbioru do rejestracji, jak też administratorów danych, którzy z mocy ustawy są z obowiązku rejestracji zwolnieni. Ponadto, w przypadku gdy administrator danych sam nie przetwarza danych, lecz zleca to innemu podmiotowi (procesorowi danych), kontroli podlegać może również ten podmiot. Zatem obowiązki związane z kontrolą ciążą nie tylko na administratorach danych, lecz także na podmiotach zajmującym się przetwarzaniem danych na podstawie tzw. umowy powierzenia.

Podczas kontroli przestrzegania przepisów o ochronie danych osobowych inspektor z biura GIODO zwraca szczególną uwagę na następujące kwestie: przesłanki legalności przetwarzania danych osobowych; przesłanki legalności przetwarzania danych szczególnie chronionych (tzw. danych wrażliwych); zakres i cele przetwarzania danych; merytoryczna poprawność danych i ich adekwatność do celu przetwarzania; realizacja obowiązku informacyjnego; zgłoszenie zbioru do rejestracji GIODO; obowiązki związane z przekazywaniem danych do państw trzecich, powierzeniem przetwarzania danych, zabezpieczeniem danych.

Co do zasady kontrole są zapowiadane z kilkudniowym wyprzedzeniem. Podmioty, które mają być poddane kontroli, informowane są w pierwszej kolejności telefonicznie, a następnie na piśmie (faksem) przedstawiany jest ogólny przedmiot kontroli, termin dokonania czynności oraz prośba o przygotowanie dokumentacji dotyczącej przetwarzania danych. Kontrola trwa zwykle kilka dni, jednak jeśli dotyczy dużych podmiotów, może zająć nawet kilka tygodni.

Więcej informacji o zakresie i przebiegu kontroli dostępnych jest pod adresem: http://www.giodo.gov.pl/487/id_art/3908/j/pl/.

4. ODPOWIEDZIALNOŚĆ ZA NARUSZENIE PRZEPISÓW

W przypadku naruszenia przepisów prawa z zakresu ochrony danych osobowych GIODO może nakazać podmiotowi przetwarzającemu dane (administratorowi lub procesorowi), w drodze decyzji administracyjnej, usunięcie naruszeń, a w szczególności:

1) usunięcie uchybień;

2) uzupełnienie, uaktualnienie, sprostowanie, udostępnienie lub nieudostępnienie danych osobowych;

3) zastosowanie dodatkowych środków zabezpieczających dane osobowe;

4) wstrzymanie przekazywania danych osobowych do państwa trzeciego;

5) zabezpieczenie danych lub przekazanie ich innym podmiotom;

6) w szczególnych przypadkach GIODO możne nakazać nawet usunięcie danych osobowych, co w przypadku wartościowych biznesowo zbiorów danych może być szczególnie kłopotliwe.

W sytuacji gdy podmiot, którego dotyczy decyzja GIODO nie podejmie kroków w celu usunięcia naruszeń, możliwe jest nałożenie na niego kar finansowych (grzywny).

Niektóre działania naruszające przepisy o ochronie danych osobowych (np. brak rejestracji zbioru lub też brak realizacji obowiązku informacyjnego) traktowane są jako przestępstwo karne. Osoba, która je popełniła (zazwyczaj członek zarządu spółki lub jednoosobowy przedsiębiorca) może zostać skazany na karę grzywny, ograniczenia wolności lub pozbawienia wolności do lat 3.

Opracowanie przygotował:
Damian Karwala, radca prawny
Paweł Tobiczyk, aplikant adwokacki

Stan prawny:
25 listopada 2016 r.

Niniejszy poradnik został stworzony przez DLA Piper w ramach projektu realizowanego we współpracy z NESsT.