

WYTYCZNE DOTYCZĄCE TARCZY POUFNOŚCI UE-USA

Wprowadzenie

Czym jest Tarcza Prywatności UE-USA i dlaczego jest nam potrzebna?

Unię Europejską (UE) i Stany Zjednoczone (USA) łączą silne powiązania handlowe. Przekazywanie danych osobowych jest ważnym i niezbędnym aspektem stosunków transatlantyckich, zwłaszcza w dzisiejszej zglobalizowanej gospodarce cyfrowej. Wiele transakcji obejmuje gromadzenie i wykorzystywanie danych osobowych, na przykład imienia i nazwiska, numeru telefonu, daty urodzenia, adresu zamieszkania i poczty elektronicznej, numeru karty kredytowej, numeru ubezpieczenia społecznego lub numeru pracownika, nazwy użytkownika, płci i stanu cywilnego lub innego rodzaju informacji, które umożliwiają identyfikację danej osoby. Na przykład nasze dane mogą zostać zebrane w UE przez oddział lub kontrahenta amerykańskiej firmy, który po otrzymaniu tych danych wykorzysta je w Stanach Zjednoczonych.

Może do tego przykładowo dochodzić, gdy kupujemy towary lub usługi w internecie lub korzystamy z mediów społecznościowych bądź usług przechowywania danych w chmurze albo gdy jesteśmy pracownikiem firmy mającej siedzibę w UE, która korzysta z usług spółki z USA (np. spółki dominującej) do przetwarzania danych pracowników. Prawo UE wymaga, by w przypadku przekazywania danych osobowych do Stanów Zjednoczonych, dane te były nadal objęte wysokim poziomem ochrony.

Tarcza Prywatności UE-USA pomaga zapewnić ten cel. Zezwala ona na przekazywanie naszych danych osobowych z UE przedsiębiorstwu ze Stanów Zjednoczonych pod warunkiem, że będzie ono przetwarzało te dane (np. korzystało z nich, przechowywało je i przekazywało dalej) z zachowaniem ściśle określonych przepisów i gwarancji ochrony danych. Ochrona danych przysługuje niezależnie od tego, czy jesteśmy obywatelem UE.

Jak działa Tarcza Prywatności?

Ochronę danych przekazywanych z UE do USA zapewniają różne narzędzia, między innymi postanowienia umowne, wiążące uregulowania wewnętrzne przedsiębiorstw oraz Tarcza Prywatności. W przypadku stosowania Tarczy Prywatności dane przedsiębiorstwo musi w pierwszej kolejności zobowiązać się przed Departamentem Handlu USA do przestrzegania obowiązujących w jej ramach zasad. Obowiązki mające zastosowanie wobec przedsiębiorstw stosujących zasady Tarczy Prywatności są określone w „Zasadach ochrony prywatności” (ang. *Privacy Principles*). Departament Handlu odpowiada za zarządzanie i administrowanie Tarczą Prywatności oraz dopilnowanie, by przedsiębiorstwa wywiązywały się ze swoich zobowiązań. Aby uzyskać certyfikat w ramach Tarczy POUFNOŚCI, dane przedsiębiorstwo musi stosować politykę ochrony prywatności zgodną z Zasadami ochrony prywatności. Przedsiębiorstwa mają ponadto obowiązek przedłużania swojego „członkostwa” w Tarczy Prywatności co roku. Jeżeli tego nie uczynią, nie będą mogły otrzymywać i używać danych osobowych z UE w ramach Tarczy.

Aby dowiedzieć się, czy konkretne przedsiębiorstwo z USA uczestniczy w Tarczy Prywatności, można sprawdzić wykaz podmiotów uczestniczących w programie Tarczy Prywatności (w skrócie „wykaz Tarczy Prywatności”) zamieszczony na stronach Departamentu Handlu (<https://www.privacyshield.gov/welcome>). Wykaz ten zawiera szczegółowe informacje na temat wszystkich przedsiębiorstw biorących udział w Tarczy Prywatności, rodzaju danych osobowych, z jakich przedsiębiorstwa te korzystają oraz charakteru oferowanych przez nie usług. Można również zapoznać się z wykazem przedsiębiorstw, które przestały uczestniczyć w programie Tarczy Prywatności. Oznacza to, że utraciły one możliwość otrzymywania naszych danych osobowych w ramach Tarczy Prywatności. Ponadto przedsiębiorstwa te mogą przechowywać nasze dane osobowe, tylko pod warunkiem złożenia w Departamencie Handlu oświadczenie, że będą nadal stosowały Zasady ochrony prywatności.

Obowiązki przedsiębiorstwa w ramach Tarczy Prywatności oraz prawa, z jakich możemy skorzystać w związku z przetwarzaniem naszych danych osobowych

Dzięki Tarczy Prywatności uzyskujemy szereg uprawnień, a przedsiębiorstwa mają obowiązek ochrony naszych danych osobowych zgodnie z „Zasadami ochrony prywatności”.

1. Prawo do informacji

Przedsiębiorstwo stosujące zasady Tarczy Prywatności musi poinformować nas:

- jakiego rodzaju dane osobowe przetwarza;
- jakie jest uzasadnienie przetwarzania naszych danych osobowych;
- czy zamierza przekazać nasze dane osobowe innemu przedsiębiorstwu oraz przedstawić stosowne uzasadnienie;
- o naszym prawie żądania od przedsiębiorstwa dostępu do naszych danych osobowych;
- o przysługującym nam prawie do decydowania, czy zezwolić przedsiębiorstwu na używanie naszych danych osobowych w „istotnie odmienny” sposób lub na ujawnienie tych danych innemu przedsiębiorstwu (tzw. prawo „opt-out”). W przypadku danych wrażliwych (tj. danych ujawniających na przykład nasze pochodzenie etniczne lub stan zdrowia) przedsiębiorstwo stosujące zasady Tarczy Prywatności ma obowiązek poinformowania nas o tym, że może wykorzystać lub ujawnić te dane tylko za naszą zgodą (tzw. prawo „opt-in”);
- jak możemy skontaktować się z przedsiębiorstwem, jeżeli zechcemy złożyć skargę na sposób, w jaki nasze dane osobowe zostały wykorzystane;
- o niezależnym organie właściwym do rozstrzygania sporów, przed którym będziemy mogli wnieść skargę w UE lub USA;
- o organie administracji publicznej w USA, który odpowiada za prowadzenie dochodzeń w sprawie przestrzegania przez przedsiębiorstwa obowiązków w ramach Tarczy Prywatności oraz ich egzekwowanie;
- o możliwości wystąpienia sytuacji, w której przedsiębiorstwo będzie musiało odpowiedzieć na żądanie ujawnienia informacji o nas wystosowane przez organy publiczne USA.

Przedsiębiorstwo stosujące zasady Tarczy Prywatności ma obowiązek udostępnić nam link do swojej polityki ochrony prywatności zamieszczonej na ogólnie dostępnej stronie internetowej lub udostępnić tę politykę w inny sposób. Ma również obowiązek udostępnienia nam linku do wykazu Tarczy Prywatności zamieszczonego na stronach internetowych Departamentu Handlu, na której będziemy mogli sprawdzić, czy dane przedsiębiorstwo stosuje zasady Tarczy Prywatności.

2. Ograniczenia dotyczące korzystania z danych do różnych celów. Co do zasady przedsiębiorstwo stosujące zasady Tarczy Prywatności może wykorzystywać nasze dane osobowe wyłącznie w celu, w jakim je pierwotnie pozyskało lub w innym celu, na który później wyraziliśmy zgodę. Możliwość wykorzystania naszych danych osobowych w innym celu będzie zależała od tego, jak bardzo nowy cel odbiega od pierwotnego:

- Nigdy nie jest dozwolone wykorzystanie naszych danych w celu, który jest niezgodny z pierwotnym celem;
- Jeżeli nowy cel jest inny, ale powiązany z pierwotnym (tj. „istotnie odmienny”), przedsiębiorstwo stosujące zasady Tarczy Prywatności może wykorzystać nasze dane, tylko jeżeli się temu nie sprzeciwimy, a w przypadku danych wrażliwych – tylko jeżeli wyrazimy na to zgodę;
- Jeżeli nowy cel jest odmienny od pierwotnego, ale na tyle zbliżony, żeby nie uznać go za istotnie odmienny, wówczas użycie danych osobowych jest dopuszczalne.

Na przykład, jeżeli nasz pracodawca przekazał nasze dane do USA w celu ich przetwarzania, przedsiębiorstwo z USA będzie mogło wykorzystać te dane w celu zaoferowania nam polisy ubezpieczeniowej albo planu emerytalnego, o ile się temu nie sprzeciwimy. Nie będzie mu również wolno sprzedać naszych danych przedsiębiorstwu będącemu osobą trzecią, aby przedsiębiorstwo to mogło oferować nam towary lub usługi niezwiązane z naszym zatrudnieniem.

Mamy również prawo do decyzji, czy zezwolić przedsiębiorstwu stosującemu zasady Tarczy Prywatności na przekazanie naszych danych osobowych innemu przedsiębiorstwu, czy to z USA, czy z innego kraju spoza UE. Mimo że nie będziemy mieli tego prawa w przypadku, gdy nasze dane będą przesyłane innemu przedsiębiorstwu (zwanemu również „agentem”) w celu ich przetworzenia w imieniu, na rzecz i zgodnie z instrukcjami przedsiębiorstwa stosującego zasady Tarczy Prywatności, przedsiębiorstwo to będzie musiało podpisać z agentem umowę zobowiązującą go do zapewnienia takich samych gwarancji ochrony danych, jakie są wymagane w ramach Tarczy Poufności. Ponadto przedsiębiorstwo stosujące zasady Tarczy Prywatności może być pociągnięte do odpowiedzialności za działania swojego agenta, jeżeli agent nie przestrzega zasad.

3. Minimalizacja danych i obowiązek przechowywania danych tylko przez niezbędny okres

Przedsiębiorstwo stosujące zasady Tarczy Prywatności może wyłącznie otrzymywać i przetwarzać dane osobowe w zakresie, w jakim są one istotne w świetle celu przetwarzania, i

musi dopilnować, by przetwarzane dane były ściśle, wiarygodne, kompletne i aktualne. Może przechowywać nasze dane osobowe tylko tak długo, jak jest to niezbędne na potrzeby przetwarzania. Wolno mu przechowywać nasze dane przez dłuższy okres tylko wówczas, gdy potrzebuje ich do ściśle określonych celów, takich jak archiwizacja w interesie publicznym, dziennikarstwo, literatura i sztuka, badania naukowe lub historyczne bądź analizy statystyczne. Jeżeli nasze dane są nadal przetwarzane w tych celach, przedsiębiorstwo musi przestrzegać Zasad ochrony prywatności.

4. Obowiązek zabezpieczenia danych

Przedsiębiorstwo musi dopilnować, by nasze dane osobowe były przechowywane w bezpiecznym miejscu i zabezpieczone przed utratą, niewłaściwym wykorzystaniem, nieuprawnionym dostępem, ujawnieniem, zmianą lub zniszczeniem, z należyтым uwzględnieniem charakteru danych i ryzyka związanego z ich przetwarzaniem.

5. Obowiązek ochrony danych w przypadku ich przekazywania innemu przedsiębiorstwu

Jak zauważono powyżej (pkt 2), w niektórych warunkach i uwzględniając cel, w którym przedsiębiorstwo stosujące zasady Tarczy Prywatności otrzymało nasze dane osobowe, przedsiębiorstwo to może przekazać te dane innemu przedsiębiorstwu. Na przykład, przedsiębiorstwo może przekazać nasze dane (innemu przedsiębiorstwu, które samo decyduje, jak korzystać z danych – tzw. „administrator danych”) bez naszego sprzeciwu, bądź też zawiera umowę o świadczenie usług z podwykonawcą przetwarzania danych (tzw. „agentem”). Przedsiębiorstwo otrzymujące dane, niezależnie od tego, czy jest zlokalizowane w USA, czy poza USA, ma obowiązek zapewnienia takiego samego poziomu ochrony naszych danych osobowych, jaki gwarantuje Tarcza Prywatności. Wymaga to zawarcia umowy między przedsiębiorstwem stosującym zasady Tarczy Prywatności a osobą trzecią, określającej warunki, na jakich ta osoba trzecia może wykorzystywać nasze dane osobowe, oraz jej obowiązki w zakresie ochrony naszych danych. Umowa musi zobowiązywać tę osobę trzecią do poinformowania przedsiębiorstwa stosującego zasady Tarczy Prywatności o zaistnieniu sytuacji, w której utraci ona możliwość wywiązywania się ze swoich obowiązków, w którym to przypadku będzie ona musiała zaprzestać wykorzystywania danych. W przypadku gdy osoba trzecia działa jako agent przedsiębiorstwa stosującego zasady Tarczy Prywatności, obowiązują surowsze zasady. Wówczas przedsiębiorstwo stosujące zasady Tarczy Prywatności może być pociągnięte do odpowiedzialności za działania agenta niedopełniającego swojego obowiązku ochrony naszych danych osobowych.

6. Prawo dostępu do danych i ich poprawienia

Mamy prawo żądania od przedsiębiorstwa stosującego zasady Tarczy Prywatności dostępu do naszych danych osobowych. Oznacza to, że mamy prawo zapoznać się ze swoimi danymi, ale również otrzymać informację o celu, w jakim dane te są przetwarzane, kategoriach przechowywanych danych osobowych oraz odbiorcach, którym dane te są ujawniane. Możemy następnie zażądać od przedsiębiorstwa skorygowania, zmiany lub usunięcia danych, jeżeli są nieścisłe, nieaktualne lub były przetwarzane z naruszeniem zasad Tarczy

Prywatności. Przedsiębiorstwo ma również obowiązek potwierdzenia, czy jest w posiadaniu naszych danych osobowych i je przetwarza.

Z reguły nie musimy podawać powodu, dla którego chcemy uzyskać dostęp do swoich danych osobowych. Przedsiębiorstwo będzie mogło jednak poprosić o ich podanie, jeżeli nasz wniosek będzie zbyt uogólniony lub niejednoznaczny. Przedsiębiorstwo ma obowiązek odpowiedzieć w rozsądnym terminie na nasz wniosek o udzielenie dostępu. Przedsiębiorstwo może być uprawnione do ograniczenia naszego prawa dostępu, ale tylko w określonych sytuacjach, na przykład jeżeli zapewnienie dostępu mogłoby zagrozić poufności, tajemnicy adwokackiej lub byłoby sprzeczne z obowiązkami prawnymi.

Prawo dostępu może być szczególnie przydatne, jeżeli nasze dane osobowe są używane w celu podjęcia decyzji, która może mieć na nas istotny wpływ. W typowych sytuacjach, w których staje się to istotne (np. gdy podejmowana jest decyzja dotycząca zatrudnienia, udzielenia kredytu itp.), amerykańskie prawo przewiduje dodatkowe prawa, które umożliwiają nam lepsze zrozumienie zakresu uwzględnienia naszych danych.

7. Prawo do wniesienia skargi i ochrony prawnej

Jeżeli dane przedsiębiorstwo nie przestrzega zasad Tarczy Prywatności i nie wywiązuje się ze swojego obowiązku ochrony naszych danych osobowych, przysługuje ci, nieodpłatnie, prawo do wniesienia skargi i zadośćuczynienia. Przedsiębiorstwa stosujące zasady Tarczy Prywatności mają obowiązek zapewnienia niezależnego mechanizmu badania nierozstrzygniętych skarg. Mogą na przykład zdecydować się na pozasądowe rozstrzygnięcie sporu (ADR) lub poddać nadzorowi krajowego organu ochrony danych (OOD).

A zatem istnieje kilka możliwości wniesienia skargi:

1. do samego przedsiębiorstwa stosującego zasady Tarczy Prywatności z USA;
2. za pomocą niezależnego mechanizmu dochodzenia praw, np. do organu pozasądowego rozstrzygania sporów (ADR) lub organu ochrony danych (OOD);
3. do amerykańskiego Departamentu Handlu, wyłącznie poprzez ODD;
4. do amerykańskiej Federalnej Komisji Handlu (lub amerykańskiego Departamentu Transportu, jeżeli skarga dotyczy linii lotniczej lub agenta sprzedaży biletów);
5. do Organu Arbitrażowego Tarczy Prywatności, tylko po wyczerpaniu pozostałych możliwości dochodzenia praw.

- **Organ pozasądowego rozstrzygania sporów (ADR)**

Organ pozasądowego rozstrzygania sporów jest podmiotem prywatnym rozpatrującym skargi na przedsiębiorstwa. Decydując się na ten sposób rozstrzygnięcia sporu, przedsiębiorstwo stosujące zasady Tarczy Prywatności musi zdecydować, czy sprawę ma rozstrzygnąć organ z UE, czy z USA. Tryb, w jakim będzie przebiegać alternatywne rozstrzygnięcie sporu, zależy od organu, do którego skierowano sprawę.

- **Krajowy organ ochrony danych**

Organ ochrony danych funkcjonuje w każdym państwie członkowskim UE, odpowiadając za ochronę i egzekwowanie przepisów dotyczących ochrony danych na szczeblu krajowym.

- **Organ Arbitrażowy Tarczy Prywatności**

Organ Arbitrażowy Tarczy Prywatności (Privacy Shield Panel) jest ciałem składającym się z trzech niezależnych arbitrów, co oznacza, że rozstrzyga spory w drodze pozasądowej. Jego decyzje są jednak wiążące i wykonalne w sądach USA. Tylko ty możesz skierować sprawę do Organu Arbitrażowego Tarczy Prywatności, pod pewnymi warunkami (w szczególności po uprzednim wyczerpaniu pozostałych środków prawnych). Przedsiębiorstwo stosujące zasady Tarczy Prywatności nie ma takiego prawa, ponieważ ten rodzaj arbitrażu jest przewidziany z myślą o tobie.

8. Ochrona prawna w przypadku dostępu do danych przez organy publiczne USA

Wreszcie wpływ na ochronę naszych danych osobowych może mieć dostęp, jaki posiadają do nich organy publiczne USA. Tarcza Prywatności zapewnia, by organy te miały wgląd w nasze dane osobowe tylko w zakresie niezbędnym do realizacji celu związanego z ochroną interesu publicznego, np. ochrony bezpieczeństwa narodowego lub ścigania przestępstw. Chociaż obowiązujące amerykańskie prawo zapewnia już indywidualnym osobom mechanizmy ochrony i dochodzenia praw w ramach funkcjonowania wymiaru sprawiedliwości, Tarcza Prywatności ustanawia specjalny instrument kontroli dostępu do danych ze względów na bezpieczeństwo narodowe – tak zwany mechanizm Rzecznika Ochrony Danych (zob. część C).

B) Jak wnieść skargę przeciwko przedsiębiorstwu stosującemu zasady Tarczy Prywatności?

Jeżeli uznasz, na przykład, że dane przedsiębiorstwo nie korzysta z naszych danych osobowych w odpowiedni sposób lub nie przestrzega przepisów, skargę w ramach Tarczy Prywatności będziesz mógł złożyć na kilka sposobów.

Będziesz mógł wybrać mechanizm dochodzenia praw, który jest dla ciebie najodpowiedniejszy i najlepiej dopasowany do charakteru naszej skargi.

Poniżej przedstawiono możliwości złożenia skargi:

1. Przedsiębiorstwo stosujące zasady Tarczy Prywatności z USA. Przedsiębiorstwo musi zawsze przekazać nam dane osoby, z którą będziemy się mogli bezpośrednio skontaktować w razie pytań lub skarg. Przedsiębiorstwo ma obowiązek przesłania odpowiedzi na naszą skargę w terminie 45 dni od jej otrzymania. W odpowiedzi przedsiębiorstwo musi oświadczyć, czy uznaje naszą skargę, a jeżeli tak, jakie działanie naprawcze podejmie. Przedsiębiorstwo jest zobowiązane rozpatrzyć każdą otrzymaną skargą, chyba że skarga jest w sposób oczywisty bezzasadna.

2. Niezależny organ pozasądowego rozstrzygania sporów (ADR) w przypadku, gdy przedsiębiorstwo stosujące zasady Tarczy Prywatności wybrało ADR jako swój niezależny mechanizm rozwiązywania sporów. Na swojej stronie internetowej przedsiębiorstwo ma obowiązek zamieszczenia informacji dotyczących organu ADR oraz linku do jego strony internetowej. Informacje te powinny zawierać szczegóły dotyczące usług oferowanych przez ten organ oraz trybu postępowania. Organy ADR muszą mieć możliwość stosowania skutecznych środków prawnych i kar w celu zapewnienia, by przedsiębiorstwo stosujące zasady Tarczy Prywatności przestrzegało obowiązku ochrony naszych danych osobowych. Mechanizm ten jest dostępny bezpłatnie.

3. Krajowy organ ochrony danych. Co do zasady przedsiębiorstwo stosujące zasady Tarczy Prywatności ma swobodę wyboru, czy poddać się właściwości organu ochrony danych z UE pełniącego funkcję niezależnego mechanizmu rozstrzygania sporów. Jeżeli jednak dane przedsiębiorstwo przetwarza dane dotyczące zasobów ludzkich (pracowników), ma obowiązek poddania się nadzorowi organu ochrony danych (OOD). Oznacza to, że jako pracownik możemy zawsze zwrócić się do swojego OOD w przypadku jakiegokolwiek skargi dotyczącej danych związanych z naszym zatrudnieniem, przekazanych przedsiębiorstwu stosującemu zasady Tarczy Prywatności. Ponadto, nawet jeżeli OOD nie ma uprawnień do sprawowania nadzoru nad danym przedsiębiorstwem stosującym zasady Tarczy Prywatności, możemy zawsze zwrócić się do swojego OOD, który następnie przekaze naszą skargę właściwemu organowi z USA (zob. poniżej).

OOD przekaze przedsiębiorstwu swoje zalecenie niezwłocznie, nie później niż w terminie 60 dni od otrzymania skargi. Zostaniemy poinformowani o przesłanym zaleceniu, które zostanie upublicznione w dopuszczalnym zakresie. Następnie przedsiębiorstwo będzie miało 25 dni na zastosowanie się do zalecenia, a jeżeli tego nie uczyni, OOD może skierować sprawę do Federalnej Komisji Handlu USA w celu ewentualnego wyegzekwowania przepisów. Może również poinformować Departament Handlu o odmowie zastosowania się do zalecenia OOD przez przedsiębiorstwo, co może doprowadzić do jego usunięcia z wykazu Tarczy Prywatności, o ile nie zaprzestanie ono naruszeń.

Dodatkowo, jeżeli na podstawie naszej skargi OOD stwierdzi, że przekazanie naszych danych osobowych przedsiębiorstwu stosującemu zasady Tarczy Prywatności narusza unijne przepisy dotyczące danych osobowych, może również podjąć kroki wobec unijnego przedsiębiorstwa przekazującego dane, a w razie konieczności, podjąć decyzję o wstrzymaniu przekazywania danych. Dotyczy to, między innymi, przypadków, w których przedsiębiorstwo z UE ma podstawy sądzić, że przedsiębiorstwo uczestniczące w Tarczy Prywatności nie przestrzega Zasad ochrony prywatności.

4. Departament Handlu. Nawet jeżeli OOD nie ma uprawnień nadzorczych nad przedsiębiorstwem stosującym zasady Tarczy Prywatności, którego dotyczy nasza skarga, może mimo to przekazać tę skargę Departamentowi Handlu USA. Będzie się to odbywało za pośrednictwem nowo utworzonego, specjalnego punktu kontaktowego, który odpowiada za bezpośrednie kontakty z organami ochrony danych. Departament Handlu rozpatrzy skargę i

przekazuje naszemu OOD odpowiedź w terminie 90 dni. Departament Handlu może również przekazywać skargi Federalnej Komisji Handlu (lub Departamentowi Transportu).

4. Federalna Komisja Handlu. Możemy wnieść skargę bezpośrednio do amerykańskiej Federalnej Komisji Handlu w ramach tego samego systemu skarg, z jakiego korzystają obywatele USA: www.ftc.gov/complaint. Federalna Komisja Handlu rozpatruje również skargi otrzymywane od Departamentu Handlu USA, unijnych organów ochrony danych i organów zajmujących się pozasądowym rozstrzygnięciem sporów. Podobnie jak Departament Handlu Federalna Komisja Handlu również utworzyła specjalny punkt kontaktowy, za pomocą którego może bezpośrednio kontaktować się z unijnymi OOD w sposób ułatwiający kierowanie skarg i współpracę w ramach ich rozpatrywania.

5. Organ Arbitrażowy Tarczy Prywatności Jeżeli po wyczerpaniu pozostałych możliwości dochodzenia praw nasza skarga pozostanie w całości lub w części nierozstrzygnięta albo nie będziemy zadowolony ze sposobu, w jaki ją rozpatrzono, możemy skorzystać z innego środka: wiążącego arbitrażu.

Kto może skorzystać z arbitrażu?

Należy pamiętać, że tylko my – jako osoba fizyczna – możemy skierować do wiążącego i podlegającego wykonaniu arbitrażu sprawę przeciwko przedsiębiorstwu stosującemu zasady Tarczy Prywatności.

Kiedy możemy skorzystać z arbitrażu?

Przedsiębiorstwo stosujące zasady tarczy poufności jest zobowiązane przystąpić do arbitrażu, jeżeli zdecydujemy się skierować do niego sprawę. Możemy to jednak uczynić dopiero po wyczerpaniu innych dróg dochodzenia swoich praw, tzn. po zwróceniu się do samego przedsiębiorstwa, organu pozasądowego rozstrzygania sporów lub Departamentu Handlu. Są inne sytuacje, w których nie będziemy mogli skorzystać z Organu Arbitrażowego Tarczy Prywatności, a mianowicie wówczas, gdy nasza skarga była już uprzednio przedmiotem postępowania arbitrażowego; sąd już rozpatrzył naszą skargę, a my byliśmy stroną tego postępowania sądowego; strony już rozstrzygnęły spór polubownie; lub gdy OOD jest w stanie rozstrzygnąć naszą skargę, kontaktując się bezpośrednio z przedsiębiorstwem. Przy tym równoległe z arbitrażem mogą się toczyć dochodzenia prowadzone przez Federalną Komisję Handlu.

Jak można wystąpić o arbitraż?

Aby wszcząć postępowanie arbitrażowe, musimy najpierw formalnie zawiadomić przedsiębiorstwo o tym, że zamierzamy to uczynić. Zawiadomienie musi zawierać skrócony opis kroków, jakie już podjęliśmy w celu zapewnienia rozstrzygnięcia naszej skargi, oraz opis domniemanego naruszenia. Możemy również załączyć dowolne dokumenty potwierdzające lub teksty prawne związane z naszą skargą.

Gdzie będzie toczyć się postępowanie arbitrażowe? Jakie są jego korzyści?

Arbitraż będzie się toczył w USA, ponieważ tam ma swoją siedzibę przedsiębiorstwo, którego dotyczy skarga. Jednocześnie arbitraż ma kilka „przyjaznych konsumentom” elementów, które dają nam istotne atuty:

- prawo do zwrócenia się do OOD o pomoc w przygotowaniu naszego roszczenia;
- możliwość uczestniczenia w postępowaniu telefonicznie lub poprzez wideokonferencję – a zatem nie obowiązuje wymóg fizycznej obecności w USA;
- możliwość uzyskania bezpłatnego tłumaczenia ustnego lub pisemnego dokumentów z języka angielskiego na inny język;
- koszty arbitrażu (z wyjątkiem kosztów prawnika) zostaną pokryte ze środków specjalnego funduszu założonego przez Departament Handlu i finansowanego z rocznych składek przedsiębiorstw stosujących zasady Tarczy Prywatności.

Jak długo trwa postępowanie arbitrażowe?

Postępowanie arbitrażowe zakończy się w terminie 90 dni od dnia, w którym przesłaliśmy zawiadomienie przedsiębiorstwu.

Jakie działania naprawcze zostaną podjęte?

Jeżeli Organ Arbitrażowy Tarczy Prywatności znajdzie dowody naruszenia Zasad ochrony prywatności, może wydać postanowienie nakazujące przedsiębiorstwu przyznanie nam prawa dostępu do naszych danych osobowych, ich poprawienia, usunięcia lub zwrócenia.

Mimo że Organ Arbitrażowy Tarczy Prywatności nie może zasądzić na naszą rzecz odszkodowania pieniężnego, będziemy mogli go dochodzić w sądzie. Jeżeli decyzja wydana w wyniku postępowania arbitrażowego nie będzie dla nas zadowalająca, będziemy mogli ją zaskarżyć zgodnie z amerykańskim prawem, na podstawie przepisów federalnej ustawy o arbitrażu (ang. Federal Arbitration Act).

C) Instytucja Rzecznika Ochrony Danych: jak wnieść skargę na amerykański organ władz publicznych

W ramach Tarczy Prywatności ustanowiono nowy niezależny mechanizm dochodzenia praw w dziedzinie bezpieczeństwa narodowego: instytucję Rzecznika Ochrony Danych.

Czym jest instytucja Rzecznika Ochrony Danych?

Rzecznik Ochrony Danych Tarczy Prywatności jest urzędnikiem wysokiego szczebla Departamentu Stanu USA, który jest niezależny od agencji wywiadu USA. Rzecznik, który korzysta ze wsparcia liczego personelu, zapewnia prawidłowe i terminowe rozpatrywanie skarg i dopilnowuje, by stosowano odpowiednie amerykańskie przepisy, a w przypadku ich naruszenia – by wdrożono środki zaradcze.

Wypełniając swoje obowiązki i rozpatrując otrzymywane skargi, Rzecznik Ochrony Danych będzie ściśle współpracował z pozostałymi niezależnymi organami nadzoru i dochodzeniowymi oraz uzyskiwał od nich wszelkie informacje niezbędne do podjęcia

stosownych kroków w odpowiedzi na skargę dotyczącą tego, czy obserwacja osoby kierującej skargę jest zgodna z amerykańskim prawem. Mowa tu o organach odpowiedzialnych za nadzorowanie poszczególnych agencji wywiadu USA.

Czy Rzecznik Ochrony Danych rozpatruje wyłącznie skargi dotyczące przekazywania danych osobowych przedsiębiorstwom stosującym zasady Tarczy Prywatności?

Nie, właściwość Rzecznika nie ogranicza się do Tarczy Prywatności. Obejmuje ona wszystkie skargi dotyczące wszelkich danych osobowych i wszystkich rodzajów przekazywania danych z UE przedsiębiorstwom w USA w celach handlowych, w tym przekazywania danych z wykorzystaniem narzędzi alternatywnych, takich jak standardowe klauzule umowne lub wiążące uregulowania wewnętrzne przedsiębiorstw.

Jak wnieść skargę do Rzecznika Ochrony Danych?

Należy najpierw przesłać skargę na piśmie organowi nadzoru w swoim państwie członkowskim sprawującemu nadzór nad krajowymi służbami bezpieczeństwa lub swojemu OOD. Innymi słowy mamy możliwość zwrócenia się do organu, który udzieli nam pomocy w naszym języku.

W swoim pisemnym wniosku należy podać takie informacje jak przyczyny złożenia wniosku, rodzaj oczekiwanej reakcji lub zadośćuczynienia, organy administracji USA, które zdaniem wnioskodawcy mogą być zaangażowane w działania związane z jego obserwacją, a także informacje o innych krokach, które wnioskodawca już podjął, aby wyegzekwować swoje prawa, oraz o otrzymanych już odpowiedziach. W swoim wniosku nie musimy jednak wykazywać, że agencje wywiadu USA faktycznie uzyskały dostęp do naszych danych.

Przed przekazaniem do Rzecznika Ochrony Danych nasz wniosek zostanie sprawdzony w celu zweryfikowania naszej tożsamości, stwierdzenia, że działamy wyłącznie w swoim imieniu, a nie w imieniu rządu lub organizacji międzyrządowej, że nasz wniosek zawiera wszystkie istotne informacje, że dotyczy danych osobowych przekazanych do USA i że nasz wniosek nie jest niepoważny, złośliwy lub złożony w złej wierze, tj. że jest wyrazem rzeczywistych obaw.

Co następuje po przekazaniu naszego wniosku Rzecznikowi Ochrony Danych?

Rzecznik Ochrony Danych rozpatrzy nasz wniosek oraz – jeżeli będzie miał pytania lub będzie wymagał dodatkowych informacji – skontaktuje się z organem, który przesłał wniosek.

Po ustaleniu, że nasz wniosek jest kompletny, Rzecznik Ochrony Danych, przekaże go odpowiednim organom USA. Jeżeli wniosek dotyczy zgodności obserwacji z amerykańskim prawem, Rzecznik będzie mógł współpracować z jednym z niezależnych organów nadzoru mających uprawnienia dochodzeniowe. Aby odpowiednio zareagować, Rzecznik Ochrony Danych będzie musiał uzyskać niezbędne informacje. Stwierdzi, czy nasz wniosek został prawidłowo zbadany i czy przestrzegano amerykańskiego prawa, a jeżeli nie, dopilnuje, by naprawiono jego wszelkie naruszenia tego prawa. W odpowiedzi nie znajdzie się informacja, czy byliśmy obiektem obserwacji amerykańskich służb wywiadu.

Wnioski o udzielenie informacji

Na podstawie amerykańskiej ustawy o swobodzie informacji (ang. Freedom of Information Act, FOIA) możemy złożyć wniosek o dostęp do dokumentów będących w posiadaniu amerykańskiego rządu. Informacje na temat tego, jak złożyć wniosek, można znaleźć na stronach www.FOIA.gov oraz <http://www.justice.gov/oip/foia-resources>. Na ogólnie dostępnych stronach każdego departamentu znajdują się informacje, jak można złożyć wniosek o dostęp do dokumentów.

Nie można jednak uzyskać dostępu do informacji niejawnych chronionych ze względów bezpieczeństwa narodowego, danych osobowych osób trzecich, a także informacji dotyczących dochodzeń organów ścigania. Ograniczenia te odnoszą się zarówno do Amerykanów, jak i osób innej narodowości.

Spory dotyczące wniosków o dostęp do dokumentów na podstawie FOIA są rozstrzygane w postępowaniu administracyjnym, a w następnej instancji – w sądach federalnych USA. Sąd może zdecydować, czy odmowa dostępu do żądanych przez nas dokumentów była uzasadniona albo może zmusić rząd do udostępnienia tych dokumentów. Sąd może postanowić o zwrocie kosztów pełnomocnictwa, ale nie może zasądzić odszkodowania pieniężnego.

Szczególne procedury wnoszenia skargi opisane w niniejszym przewodniku nie zastępują przysługującego nam prawa do skorzystania, w celu wyegzekwowania naszych praw, z porady i wsparcia krajowych organów ochrony danych.