PFP
POLSKA FUNDACJA
PRZEDSIĘBIORCZOŚCI

Za co Prezes UODO nakłada kary finansowe –

czyli jakich praktyk należy się wystrzegać

Radca prawny Maja Grzegorczyk

październik 2020r.

Kary finansowe w RODO – krótkie przypomnienie

Podstawę do nakładania kar finansowych za naruszenie regulacji dotyczących ochrony danych osobowych stanowi art. 83 RODO.

Przepis ten reguluje:

- kto może zostać ukarany;
- za jakie naruszenia kara finansowa może zostać nałożona;
- przesłanki ustalania wysokości kar finansowych;
- progi kar finansowych;
- modyfikacje karania dla podmiotów publicznych;
- odesłania proceduralne.

Charakter kar finansowych w RODO

(!) Skuteczność kary:

ma ona przede wszystkim doprowadzić do zaprzestania trwania naruszenia ochrony danych osobowych, a zatem musi być wystarczająco dotkliwa, aby zmusić podmiot, który dopuszcza się naruszenia do realizacji obowiązków wynikających z RODO.

Nie może ona być zbyt niska, aby podmiot ten nie wkalkulował jej w koszty prowadzonej działalności i tzw. ryzyko biznesowe.

(!) Odstraszający charakter kary:

Kara ma spełniać funkcję wychowawczą. Ma powstrzymać ukarany podmiot przed ponownym naruszaniem prawa oraz nakłonić inne podmioty do przestrzegania zasad ochrony danych osobowych.

(!) Represyjny oraz prewencyjny charakter kary:

Kara ma mieć także charakter represyjny - za naruszenie przepisów ochrony danych, oraz prewencyjny – powstrzymać zarówno podmiot ukarany, jak i wszystkie inne podmioty przed naruszaniem przepisów w przyszłości.

(???) Kto może zostać ukarany …

- administrator danych;
- Współadministrator;
- procesor;
- subprocesor (dalsze powierzenie przetwarzania);
- podmiot certyfikujący;
- podmiot monitorujący przestrzeganie kodeksów tzw. branżowych.

(???) A ile to kosztuje …

RODO wyróżnia dwa przedziały kar pieniężnych:

- **do 10 mln euro**, a w przypadku przedsiębiorstwa do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego;
- **do 20 mln euro**, a w przypadku przedsiębiorstwa do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

- Nasza ustawa o ochronie danych osobowych przewiduje jednak mniejsze kary dla podmiotów sektora finansów publicznych:

- jednostki sektora finansów publicznych (np. szkoły, uczelnie, szpitale, ZUS, gminy, NFZ, sądy), instytuty badawcze i Narodowy Bank Polski – w wysokości do 100 000 złotych;

- jednostki sektora finansów publicznych z dziedziny kultury (np. teatry, opery, filharmonie, kina, muzea, biblioteki, domy kultury, galerie sztuki) – w wysokości do 10 000 złotych.

(!!!) Pamiętaj

Nałożenie kary łączy się z wydaniem decyzji administracyjnej wraz z uzasadnieniem, od której przysługuje prawo wniesienia skargi do sądu administracyjnego.

(!!!) Pamiętaj

Jakie czynniki brane są pod uwagę przy nakładaniu kar finansowych:

- charakter, waga i czasu trwania naruszenia – który obowiązek administratora/ względnie prawo osoby, której dane dotyczą, został naruszony;
- jak poważne jest naruszenie, związane z nim zagrożenia i skala tj. liczba pokrzywdzonych osób;
- umyślny lub nieumyślny charakter naruszenia – czy jest to celowe działanie ADO, czy też zachodzi brak zamiaru z jego strony, bo jest to np. błąd ludzki;
- czy zostały podjęte / względnie jakie działania minimalizujące szkody poniesione przez osoby, których dane dotyczą zostały podjęte – czy administrator podjął wszelkie możliwe starania celem ograniczenia skutków naruszenia dla danej osoby (danych osób).

Co na przykład??

Odpowiednio szybki kontakt z osobami, których dane dotyczą i wskazanie co się stało.

(!!!) Pamiętaj

Jakie czynniki brane są pod uwagę przy nakładaniu kar finansowych:

- czy administrator wdrożył odpowiednie systemy bezpieczeństwa;
- czy administrator już wcześniej dopuszczał się naruszeń, czy też jest to tzw. pierwszy raz;
- stopień współpracy administratora z organem nadzorczym – czy administrator współpracuje w toku postępowania, czy raczej ignoruje organ nadzorczy. Ta druga postawa z pewnością przełoży się na wysokość kary, o czym niektórzy już się przekonali;
- kategorie danych osobowych, których dotyczyło naruszenie – dane zwykłe, dane szczególnych kategorii, tzw. dane o karalności, czy zachodzi możliwość identyfikacji osób fizycznych;

(!!!) Pamiętaj

Jakie czynniki brane są pod uwagę przy nakładaniu kar finansowych:

- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu – to, czy administrator sam zgłosił naruszenie ma znaczący wpływ na ocenę zasadności karania;
- czy administrator stosował się do tzw. kodeksów branżowych określających pewne branżowe wytyczne dla przetwarzania i ochrony danych osobowych;
- z pewnością znaczenie ma także to, czy oraz jakie korzyści osiągnął podmiot, który dopuścił się naruszenia.
- I wiele innych obciążających lub łagodzących w zależności od okoliczności konkretnego przypadku.

Przegląd wybranych kar nałożonych przez organ nadzorczy

Za co i dlaczego aż tyle …

Decyzja Prezesa UODO z dnia 15 marca 2019r. ZSPR.421.3

Kwota kary: 943 470 PLN

Naruszone przepisy RODO

- **14 ust. 1 – 3 RODO** – obowiązki w zakresie przekazywania informacji o przetwarzaniu danych osobowych w przypadku pozyskiwania danych osobowych w sposób inny niż bezpośrednio od osoby, której dane dotyczą (tzw. wtórny obowiązek informacyjny)

A jak do tego doszło…

- Spółka pozyskiwała dane osobowe ze źródeł publicznie dostępnych, m. in. z Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEiDG) i przetwarzała je w celach zarobkowych.

- Organ nadzorczy kontrolował niedopełnienie obowiązku informacyjnego wobec osób fizycznych prowadzących działalność gospodarczą – przedsiębiorców, którzy aktualnie ją prowadzą bądź tę działalność tą zawiesili, jak i tych, którzy prowadzili ją w przeszłości.

- Spółka spełniła obowiązek informacyjny jedynie wobec tych osób, co do których posiadała adresy e-mail. W przypadku pozostałych osób spółka odstąpiła od spełnienia obowiązku informacyjnego tłumacząc się zbyt wysokimi kosztami takiej operacji – szacowanymi na ok. 34 mln złotych.

- Treść klauzuli informacyjnej została jedynie opublikowana na stronie internetowej spółki.

- W ocenie Prezesa UODO takie działanie było niewystarczające. Mając dane kontaktowe do poszczególnych osób spółka powinna spełnić wobec nich obowiązek informacyjny tj. poinformować m. in. o: swoich danych, skąd ma dane tych osób, w jakim celu i jak długo zamierza je przetwarzać oraz o przysługujących tym osobom prawach wynikających RODO.

- Spółka dysponując adresami korespondencyjnymi i numerami telefonów mogła spełnić obowiązek informacyjny wobec osób, których dane przetwarza.

- Organ uznał, że naruszenie miało charakter umyślny, ponieważ spółka miała świadomość istnienia obowiązku informacyjnego.

- Nakładając karę finansową, organ wziął pod uwagę również fakt, że spółka nie podjęła żadnych działań zmierzających do usunięcia naruszenia, ani nie zadeklarowała takiego zamiaru.

(!!!) Wnioski

Obowiązek informowania osób fizycznych o przetwarzaniu ich danych osobowych jest jednym z podstawowych obowiązków administratora danych i należy realizować go w taki sposób, by osoba fizyczna miała faktyczną możliwość zapoznania się z treścią tejże informacji.

Administrator nie może zatem zasłaniać się niedogodnościami i kosztami.

(???) A co na to sąd….

- w ocenie sądu administracyjnego jawność rejestru (CEiDG) nie daje prawa do dowolnego przetwarzania danych z niego, w tym nie wyłącza obowiązku informacyjnego. Co więcej powinien on zostać spełniony niezależnie od daty pozyskania danych. Niewspółmiernie duży wysiłek nie może być utożsamiany z wysokością kosztów.

- Sąd podzielił pogląd UODO, że spełnienie obowiązku informacyjnego przez wysłanie tradycyjną pocztą listu lub w drodze kontaktu telefonicznego, nie jest czynnością niemożliwą oraz nie wymaga niewspółmiernie dużego wysiłku.

- **W ocenie Sądu pojęcie niewspółmiernie dużego wysiłku nie może być utożsamiane z wysokością kosztów.** Sąd nie zgodził się również z poglądem, że ryzyko dla osób, których dane zostały pozyskane jest w "najgorszym wypadku" bardzo niskie. Co więcej sąd uznał, że obowiązek informacyjny należy też spełnić wobec osób, których dane zostały pozyskane przed 25 maja 2018 roku, a więc przed dniem w którym zaczęto stosować RODO.

(???) A co na to sąd….

- prawo do ponownego wykorzystywania informacji sektora publicznego nie oznacza, że dane osób fizycznych prowadzących aktualnie jednoosobową działalność gospodarczą oraz osób fizycznych, które zawiesiły jej wykonywanie wyłączone są z zakresu stosowania RODO.

(!!!) Pamiętaj

Sąd wskazał również, że zgodnie z motywem 171 RODO przetwarzanie, które w dniu rozpoczęcia stosowania RODO już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów.

A zatem najwyższy czas na audyt.

(wyrok WSA w Warszawie z 11 grudnia 2019 r., sygn. akt: II SA/WA 1030/19)

Decyzja Prezesa UODO z dnia 25 kwietnia 2019 r. ZSPR.440.43.2019

Kwota kary: 55 750,50 PLN

Naruszone przepisy RODO

- ✓ **5 ust. 1 lit. f RODO** – zasada integralności i poufności;
- ✓ **32 ust. 1 lit. b RODO** – zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- ✓ **32 ust. 2 RODO** – obowiązek oceny stopnia bezpieczeństwa przetwarzania przy uwzględnieniu ryzyka wiążącego się z przetwarzaniem, w szczególności wynikającego z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

A jak do tego doszło…

- Organizacja upubliczniła w sieci dane osobowe sędziów, którym przyznano licencje sędziowskie w 2015 roku (585 osób). Opublikowano nie tylko ich imiona i nazwiska, ale także adresy zamieszkania oraz numery PESEL.

- Nie ma przy tym żadnych podstaw prawnych, by w Internecie dostępny był aż tak szeroki zakres danych sędziów. Upubliczniając je, administrator stwarzał potencjalne ryzyko ich bezprawnego wykorzystania – taki zestaw danych osobowych ułatwia zaciągnięcie np. pożyczki podszywając się pod inną osobę.

- Organizacja dostrzegła swój błąd i sama zgłosiła naruszenie ochrony danych osobowych Prezesowi UODO, ale próby usunięcia naruszenia były nieskuteczne – nieskutecznie próbowano usunąć dane, stąd takie działanie przesądziło o nałożeniu kary.

- Definitywne usunięcie naruszenia nastąpiło dopiero po wszczęciu postępowania przez Prezesa UODO.

- Ustalając wysokość kary Prezes UODO wziął pod uwagę czas trwania naruszenia oraz fakt, że dotyczyło ono dużej grupy osób. Uznał, że mimo iż ostatecznie naruszenie zostało usunięte, to miało poważny charakter.

- Prezes UODO uwzględnił również okoliczności łagodzące, którymi były m.in. dobra współpraca administratora z organem nadzoru czy brak dowodów na to, że powstały szkody po stronie osób, których dane ujawniono.

(!!!) Wnioski

Zanim opublikujemy (szczególnie w Internecie) dane osób fizycznych, należy się dobrze zastanowić, czy istnieje ku temu podstawa prawna, a także jakie mogą być tego skutki.

Dodatkowo należy zawsze przemyśleć, czy zakres publikowanych danych nie jest zbyt obszerny.

Bardzo ciekawa historia

Decyzja Prezesa UODO z dnia 18 lutego 2020 r. ZSZZS.440.768.2018

Kwota kary: 20 000 PLN

Naruszone przepisy RODO

- ✓ **art. 5 ust. 1 lit. c RODO** – zasada minimalizacji danych;
- ✓ **art. 9 ust. 1 RODO** – zakaz przetwarzania szczególnych kategorii danych osobowych.

A jak do tego doszło…

- Prezes UODO nałożył karę w związku z naruszeniem polegającym na przetwarzaniu danych biometrycznych dzieci podczas korzystania przez nie ze szkolnej stołówki.

- Szkoła przetwarzała dane szczególnych kategorii (dane biometryczne) 680 dzieci bez podstawy prawnej, mogąc jednocześnie zastosować inne formy identyfikacji uczniów.

- Postępowanie wykazało, że szkoła pozyskuje te dane i przetwarza je na podstawie pisemnej zgody rodziców lub opiekunów prawnych.

- Prezes UODO uznał, że przetwarzanie danych biometrycznych dzieci nie jest niezbędne dla osiągnięcia celu, jakim jest identyfikacja uprawnienia dziecka do odebrania obiadu. Szkoła może przeprowadzić identyfikację za pomocą innych środków, które nie ingerują tak dalece w prywatność dziecka.

- Prezes UODO w uzasadnieniu swojej decyzji podkreślił, że szczególnej ochrony danych osobowych wymagają dzieci. Dane biometryczne zaś, mają wyjątkowy charakter w świetle podstawowych praw i wolności osób fizycznych.

- W toku postępowania szkoła całkowicie zignorowała fakt przetwarzania danych biometryczny dzieci poprzez stwierdzenie, że nie przetwarza takich danych, co dodatkowo przemówiło za zastosowaniem kary pieniężnej.

- W tym przypadku kara pieniężna miała także spełnić funkcję represyjną, jako że stanowi odpowiedź na naruszenie przez szkołę przepisów RODO, ale i prewencyjną, jako że sama szkoła będzie skutecznie zniechęcona do naruszania w taki sposób przepisów ochrony danych osobowych w przyszłości.

(!!!) Wnioski

Należy zachować szczególną ostrożność przy przetwarzaniu danych osobowych dzieci.

Udzielona zgoda na przetwarzanie danych nie uratuje nas w przypadku, gdy organ dojdzie do wniosku, że takich danych w ogóle nie powinniśmy przetwarzać.

Uwaga na dane biometryczne – zawsze należy zastanowić się, czy celu przetwarzania nie jesteśmy w stanie osiągnąć wykorzystując inne dane, które już posiadamy.

Decyzja Prezesa UODO z dnia 16 lipca 2020 r. DKE.561.2.2020

Kwota kary: 5 000 PLN

Naruszone przepisy RODO

- ✓ **art. 58 ust. 1 lit. e RODO** – uprawnienia organu nadzorczego w zakresie uzyskiwania od administratora dostępu do wszelkich danych osobowych i informacji

Kara nałożona na osobę fizyczną prowadzącą działalność gospodarczą!!!

A jak do tego doszło…

- Przedsiębiorca prowadzący niepubliczny żłobek i przedszkole nie zapewnił Prezesowi UODO dostępu do danych osobowych i innych informacji niezbędnych do realizacji jego zadań – w tym przypadku do oceny czy administrator w sposób zgodny z przepisami RODO zawiadomił osoby, których dane dotyczą, o naruszeniu.

- Przedsiębiorca zgłosił do Prezesa UODO naruszenia ochrony danych osobowych, polegające na utracie dostępu do danych osobowych przechowywanych w prowadzonym niepublicznym żłobku i przedszkolu.

- W związku z brakiem w ww. zgłoszeniu informacji niezbędnych do oceny tego naruszenia, organ nadzorczy trzykrotnie skierował do przedsiębiorcy wezwania do złożenia stosownych wyjaśnień – przedsiębiorca nie udzielił Prezesowi UODO żadnej odpowiedzi na wezwania.

- Wydając decyzję o nałożeniu administracyjnej kary pieniężnej oraz określając jej wysokość, Prezes UODO wziął pod uwagę jako okoliczności obciążające przedsiębiorcę:

  - charakter, wagę i czas trwania naruszenia;
  - umyślny charakter naruszenia oraz
  - brak współpracy z organem nadzorczym.

Nałożona kara jest w ocenie Prezesa UODO proporcjonalna do wagi stwierdzonego naruszenia oraz do możliwości jej poniesienia przez przedsiębiorcę bez dużego uszczerbku dla prowadzonej przez niego działalności.

(!!!) Wnioski

Nawet mały przedsiębiorca musi liczyć się z możliwością wymierzenia kary finansowej.

W toku postępowania zawsze warto współpracować z UODO, by nie narażać się na bardziej dotkliwe sankcje.

Brak współpracy może skutkować nałożeniem albo podwyższeniem wysokości kary finansowej.

A zatem

Poprawne wdrożenie RODO to klucz do sukcesu

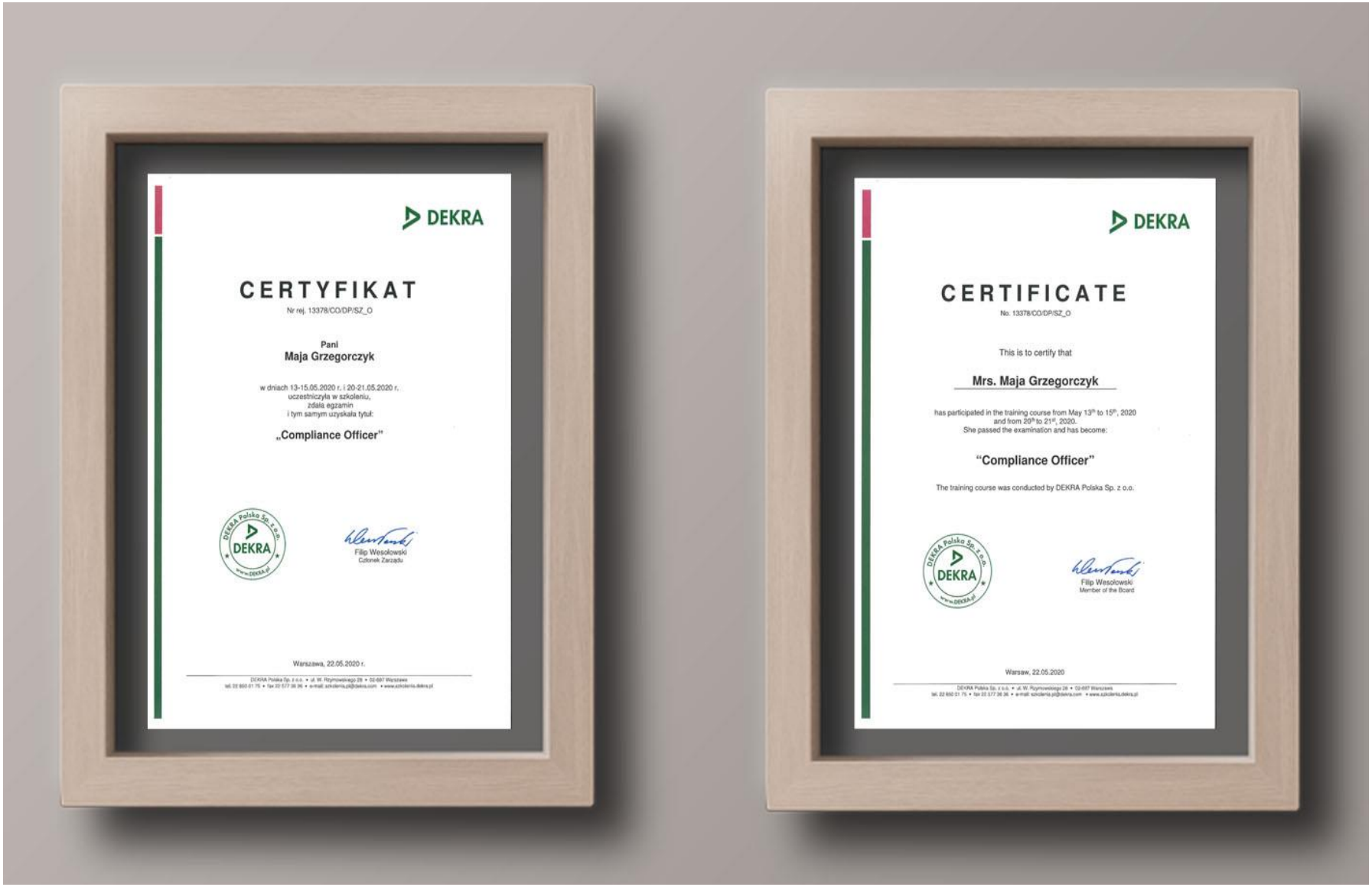
Zweryfikuj, czy spełniasz podstawowe obowiązki nałożone na podmioty przetwarzające dane

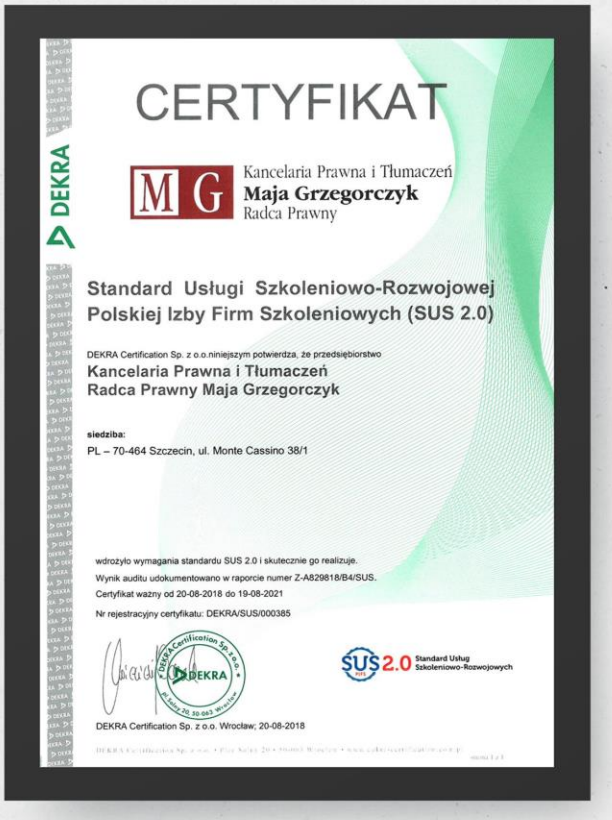
Pamiętaj, że obowiązek informacyjny jest bardzo ważny

oceń, czy nie przetwarzasz danych w nadmiarze i czy adekwatnie je chronisz

Uważaj na to jakie dane i gdzie publikujesz

Współpracuj z organem nadzorczym





CERTYFIKAT

Kancelaria Prawna i Tłumaczeń
Maja Grzegorczyk
Radca Prawny

Standard Usługi Szkoleniowo-Rozwojowej Polskiej Izby Firm Szkoleniowych (SUS 2.0)

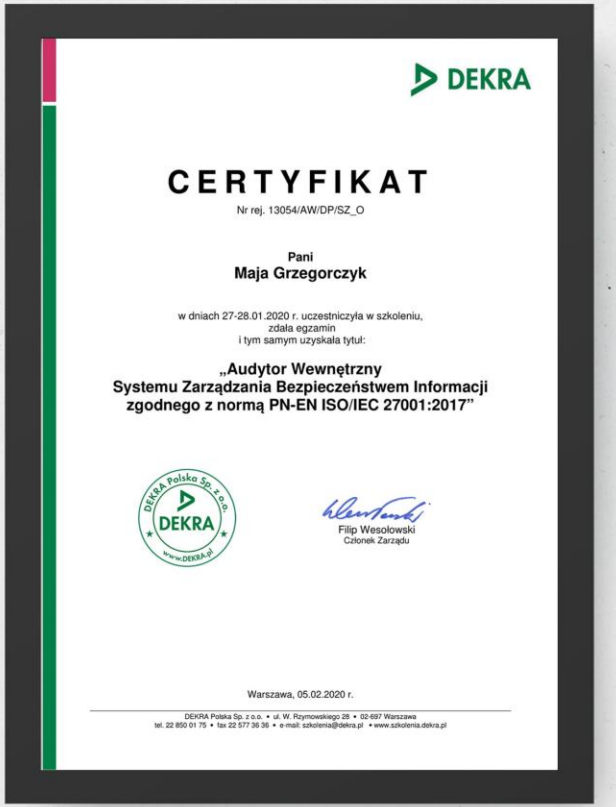
DEKRA Certification Sp. z o.o.niniejszym potwierdza, że przedsiębiorstwo
Kancelaria Prawna i Tłumaczeń
Radca Prawny Maja Grzegorczyk

siedziba:
PL – 70-464 Szczecin, ul. Monte Cassino 38/1

wdrożyło wymagania standardu SUS 2.0 i skutecznie go realizuje.
Wynik auditu udokumentowano w raporcie numer Z-A829818/B4/SUS.
Certyfikat ważny od 20-08-2018 do 19-08-2021
Nr rejestracyjny certyfikatu: DEKRA/SUS/000385

DEKRA Certification Sp. z o.o. Wrocław; 20-08-2018

SUS 2.0 Standard Usług Szkoleniowo-Rozwojowych



DEKRA

CERTYFIKAT

Nr rej. 13054/AW/DP/SZ_O

Pani
Maja Grzegorczyk

w dniach 27-28.01.2020 r. uczestniczyła w szkoleniu,
zdała egzamin
i tym samym uzyskała tytuł:

„Audytor Wewnętrzny
Systemu Zarządzania Bezpieczeństwem Informacji
zgodnego z normą PN-EN ISO/IEC 27001:2017"

DEKRA Polska Sp. z o.o. DEKRA www.DEKRA.pl

Filip Wesołowski
Członek Zarządu

Warszawa, 05.02.2020 r.

DEKRA Polska Sp. z o.o. • ul. W. Rzymowskiego 28 • 02-697 Warszawa
tel. 22 850 01 75 • fax 22 577 36 36 • e-mail: szkolenia@dekra.pl • www.szkolenia.dekra.pl

Kancelaria Prawna
Maja Grzegorczyk
Radca Prawny

kancelaria@maja-grzegorczyk.com
www.maja-grzegorczyk.com

tel./fax 91 434 13 67
kom. 501 148 704

ul. Monte Cassino 38/1; 70-764 Szczecin

facebook.com/MajaGKancelaria

Dziękujemy za uwagę

PFP
POLSKA FUNDACJA PRZEDSIĘBIORCZOŚCI

www.pfp.com.pl