

Kancelaria Gabrysiak i Wspólnicy

POLITYKA BEZPIECZEŃSTWA INFORMACJI

Grudzień 2018 r.

Gabrysiak i Wspólnicy s.k.a.
Ul. Puławska 257/71
02-769 Warszawa

t: +48 22 110 50 66
e: kancelaria@gnadwokaci.pl
www.gnadwokaci.pl

Member of the Banking Litigation Network

Spółka wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000737428. Kapitał zakładowy w kwocie 150 000 złotych w całości opłacony.

Wprowadzenie

Niniejsza *Polityka bezpieczeństwa*, zwana dalej Polityką, została sporządzona w celu wykazania, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymogami prawa, dotyczącymi zasad przetwarzania i zabezpieczenia danych w kancelarii, w tym z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej RODO).

Definicje:

1. **Administrator Danych:** kancelaria Gabrysiak i Wspólnicy spółka cywilna, dalej także „GiW”.
2. **Dane osobowe:** wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. **System informatyczny:** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji narzędzi programowych zastosowanych w celu przetwarzania danych.
4. **Użytkownik:** osoba upoważniona przez Administratora Danych do Przetwarzania danych osobowych.
5. **Zbiór danych:** każdy uporządkowany zestaw danych o charakterze osobowym, dostępny według określonych kryteriów.
6. **Przetwarzanie danych:** jakiegokolwiek operacje wykonywane na Danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie w formie tradycyjnej oraz w systemach informatycznych.
7. **Identyfikator użytkownika:** ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (Użytkownika) w razie Przetwarzania danych osobowych w takim systemie.
8. **Hasło:** ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym (Użytkownikowi) w razie, przetwarzania danych osobowych w takim systemie.
9. **Uwierzytelnianie:** działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu (Użytkownika)
10. **Pracownicy** – osoba(y) współpracująca z GiW w związku z działalnością przedsiębiorstwa GiW na podstawie umowy o pracę lub innego stosunku prawnego
11. **Serwer** – to jest urządzenie HPDL 160 G9, będące własnością GiW, umieszczone i pracujące w serwerowni przy ul. Konstruktorskiej 5, 02-673 Warszawa. Serwer ten znajduje się pod opieką Procesora, który w ramach świadczonych usług zapewnia jego obsługę, serwis i dostępność w ramach Systemu informatycznego GiW. Na tym serwerze pracują serwery wirtualne gromadzące dane GiW i udostępniające usługi w postaci: serwer plików, poczta e-mail, portale GiW.
12. **Procesor** – IT Kreator Sp. z o.o. ul. Bielawska 14A, 05-520 Konstancin Jeziorna, NIP 952-213-98-94, KRS 0000585019.

I. Postanowienia ogólne

1. Polityka dotyczy wszystkich Danych osobowych przetwarzanych w kancelarii Gabrysiak i Wspólnicy niezależnie od formy ich przetwarzania (przetwarzane tradycyjnie zbiory ewidencyjne, systemy informatyczne) oraz od tego, czy dane są lub mogą być przetwarzane w zbiorach danych.
2. Polityka jest przechowywana w wersji elektronicznej oraz w wersji papierowej w siedzibie Administratora.
3. Polityka jest udostępniana do wglądu osobom posiadającym upoważnienie do przetwarzania danych osobowych na ich wniosek, a także osobom, którym ma zostać nadane upoważnienie do przetwarzania danych osobowych, celem zapoznania się z jej treścią.
4. Zgodnie z art. 6 ustawy z 26 maja 1982 r. Prawo o Adwokaturze, Dane osobowe przetwarzane w kancelarii Gabrysiak i Wspólnicy, a uzyskane w związku z udzielaniem pomocy prawnej przez adwokata, objęte są tajemnicą adwokacką. Adwokata nie można zwolnić od obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę.
5. W zakresie przetwarzania danych pozyskanych w związku z wykonywaniem czynności objętych tajemnicą adwokacką Administrator stosuje się do wskazanych powyżej przepisów dotyczących zachowania tajemnicy zawodowej.
6. Dla skutecznej realizacji Polityki Administrator Danych zapewnia:
 - a) odpowiednie do zagrożeń i kategorii danych objętych ochroną środki techniczne i rozwiązania organizacyjne,
 - b) kontrolę i nadzór nad Przetwarzaniem danych osobowych,
 - c) monitorowanie zastosowanych środków ochrony.
7. Monitorowanie przez Administratora Danych zastosowanych środków ochrony obejmuje m.in. działania Użytkowników, naruszanie zasad dostępu do danych, zapewnienie integralności plików oraz ochronę przed atakami zewnętrznymi oraz wewnętrznymi.
8. Administrator Danych zapewnia, że czynności wykonywane w związku z przetwarzaniem i zabezpieczeniem danych osobowych są zgodne z niniejszą polityką oraz odpowiednimi przepisami prawa.

II. Dane osobowe przetwarzane u administratora danych

1. Dane osobowe przetwarzane przez Administratora Danych gromadzone są w zbiorach danych. Z uwagi na charakter działalności Administratora gromadzi on dane w zbiorach obejmujących osoby fizyczne uczestniczące w tzw. sądowych postępowaniach zbiorowych (postępowania prowadzone na podstawie „Ustawy o dochodzeniu roszczeń w postępowaniu grupowym”, Dz.U. 2010 nr 7 poz. 44 ze zmianami) oraz w zbiorze obejmującym osoby, dla których Kancelaria prowadzi indywidualne doradztwo prawne w tym postępowania sądowe lub inne. Administrator na bieżąco tworzy listę zbiorów danych, która stanowi załącznik do niniejszej polityki.
2. Administrator danych nie podejmuje czynności przetwarzania, które mogłyby się wiązać z poważnym prawdopodobieństwem wystąpienia wysokiego ryzyka dla praw i wolności osób.
3. W przypadku planowania takiego działania Administrator wykona czynności określone w art. 35 i nast. RODO.
4. W przypadku planowania nowych czynności przetwarzania Administrator dokonuje analizy ich skutków dla ochrony danych osobowych oraz uwzględnia kwestie ochrony danych w fazie ich projektowania.
5. Administrator danych prowadzi rejestr czynności przetwarzania.

III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem

1. Wszyscy Pracownicy zobowiązani są do przetwarzania danych osobowych zgodnie z obowiązującymi przepisami i zgodnie z ustaloną przez Administratora Danych Polityką Bezpieczeństwa, Instrukcją Zarządzania Systemem Informatycznym, a także innymi dokumentami wewnętrznymi i procedurami związanymi z Przetwarzaniem danych osobowych w kancelarii Gabrysiak i Wspólnicy.

2. Wszystkie dane osobowe w Kancelarii są przetwarzane z poszanowaniem zasad przetwarzania przewidzianych przez przepisy prawa:
 - a) w każdym wypadku występuje chociaż jedna z przewidzianych przepisami prawa podstaw dla przetwarzania danych;
 - b) dane przetwarzane są rzetelnie i w sposób przejrzysty;
 - c) dane osobowe zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
 - d) dane osobowe są przetwarzane jedynie w takim zakresie, jaki jest niezbędny dla osiągnięcia celu przetwarzania danych;
 - e) dane osobowe są prawidłowe i w razie potrzeby uaktualniane;
 - f) czas przechowywania danych jest ograniczony do okresu ich przydatności do celów, do których zostały zebrane, a po tym okresie są one anonimizowane bądź usuwane;
 - g) wobec osoby, której dane dotyczą, wykonywany jest obowiązek informacyjny zgodnie z treścią art. 13 i 14 RODO;
 - h) dane są zabezpieczone przed naruszeniami zasad ich ochrony.
3. Administrator danych nie przekazuje osobom, których dane dotyczą, informacji w sytuacji, w której dane te muszą zostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej (art. 14 ust 5 pkt d RODO).
4. Za naruszenie lub próbę naruszenia zasad przetwarzania i ochrony Danych osobowych uważa się w szczególności:
 - a) naruszenie bezpieczeństwa Systemów informatycznych, w których przetwarzane są dane osobowe, w razie ich przetwarzania w takich systemach;
 - b) udostępnianie lub umożliwienie udostępniania danych osobom lub podmiotom do tego nieupoważnionym;
 - c) zaniechanie, choćby nieumyślne, dopełnienia obowiązku zapewnienia danym osobowym ochrony;
 - d) niedopełnienie obowiązku zachowania w tajemnicy Danych osobowych oraz sposobów ich zabezpieczenia;
 - e) przetwarzanie Danych osobowych niezgodnie z założonym zakresem i celem ich zbierania;
 - f) spowodowanie uszkodzenia, utraty, niekontrolowanej zmiany lub nieuprawnione kopiowanie Danych osobowych;
 - g) naruszenie praw osób, których dane są przetwarzane.
5. W przypadku stwierdzenia okoliczności naruszenia zasad ochrony danych osobowych Użytkownik zobowiązany jest do podjęcia wszystkich niezbędnych kroków, mających na celu ograniczenie skutków naruszenia i do niezwłocznego powiadomienia Administratora Danych.
6. Do obowiązków Administratora Danych w zakresie zatrudniania, zakończenia lub zmiany warunków zatrudnienia Pracowników (osób podejmujących czynności na rzecz Administratora Danych na podstawie innych umów cywilnoprawnych) należy dopilnowanie, by:
 - a) Pracownicy byli odpowiednio przygotowani do wykonywania swoich obowiązków;
 - b) każdy z przetwarzających Dane osobowe był pisemnie upoważniony do przetwarzania zgodnie z „Upoważnieniem do przetwarzania danych osobowych”
 - c) każdy Pracownik zobowiązał się do zachowania danych osobowych przetwarzanych w Kancelarii w tajemnicy, podpisując „Oświadczenie i zobowiązanie osoby przetwarzającej dane osobowe do zachowania tajemnicy”.
7. Pracownicy zobowiązani są do:
 - a) ścisłego przestrzegania zakresu nadanego upoważnienia;
 - b) przetwarzania i ochrony danych osobowych zgodnie z przepisami;
 - c) zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia;
 - d) zgłaszania incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwym funkcjonowaniem systemu.

IV. Obszar przetwarzania danych osobowych

1. Obszar, w którym przetwarzane są Dane osobowe na terenie kancelarii Gabrysiak i Wspólnicy obejmuje pomieszczenie biurowe kancelarii zlokalizowane w siedzibie kancelarii przy ul. Puławskiej 257/71, 02-769 Warszawa.
2. Dodatkowo obszar, w którym przetwarzane są Dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych należące do kancelarii Gabrysiak i Wspólnicy znajdujące się poza obszarem wskazanym powyżej.

V. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności, rozliczalności i ciągłości Przetwarzanych danych.
2. Zastosowane środki ochrony (techniczne i organizacyjne) powinny być adekwatne do stwierdzonego poziomu ryzyka dla poszczególnych systemów, rodzajów zbiorów i kategorii danych. Środki obejmują:
 - a) ograniczenie dostępu do pomieszczeń, w których przetwarzane są dane osobowe, jedynie do osób odpowiednio upoważnionych. Inne osoby mogą przebywać w pomieszczeniach wykorzystywanych do przetwarzania danych jedynie w towarzystwie osoby upoważnionej.
 - b) zamykanie pomieszczeń tworzących obszar Przetwarzania danych osobowych określony w pkt IV powyżej na czas nieobecności Pracowników w sposób uniemożliwiający dostęp do nich osób trzecich;
 - c) zanonimizowane opisywanie akt poszczególnych spraw, które to akta zawierają dane osobowe, a w razie potrzeby używanie dodatkowo zamkniętych szafek i sejfów do zabezpieczenia dokumentów;
 - d) wykorzystanie niszczarki do skutecznego usuwania dokumentów zawierających dane osobowe;
 - e) ochronę sieci lokalnej przed działaniami inicjowanymi z zewnątrz przy użyciu sieci firewall;
 - f) wykonywanie kopii awaryjnych danych gromadzonych na Serwerze plików dostępnych dla Pracowników jako „dysk Z”
 - g) ochronę sprzętu komputerowego wykorzystywanego u Administratora przed złośliwym oprogramowaniem;
 - h) zabezpieczenie dostępu do urządzeń Kancelarii przy pomocy haseł dostępu;
 - i) wykorzystanie szyfrowanych kanałów transmisji przy przesyłaniu danych.

VI. Naruszenia zasad ochrony danych osobowych

1. W przypadku stwierdzenia naruszenia ochrony danych osobowych Administrator dokonuje oceny, czy zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.
2. W każdej sytuacji, w której zaistniałe naruszenie mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych, Administrator zgłasza fakt naruszenia zasad ochrony danych organowi nadzorcemu bez zbędnej zwłoki – jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia.
3. Jeżeli ryzyko naruszenia praw i wolności jest wysokie, Administrator zawiadamia o incydencie także osobę, której dane dotyczą.

VII. Powierzenie przetwarzania danych osobowych

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w drodze umowy zawartej w formie pisemnej, zgodnie z wymogami wskazanymi dla takich umów w art. 28 RODO i tylko jeżeli są to dane, które może ujawnić bez naruszenia adwokackiej tajemnicy zawodowej.
2. Przed powierzeniem przetwarzania danych osobowych Administrator w miarę możliwości uzyskuje informacje o dotychczasowych praktykach procesora dotyczących zabezpieczenia danych osobowych.

VIII. Przekazywanie danych do państwa trzeciego

1. Administrator Danych Osobowych nie będzie przekazywał danych osobowych do państwa trzeciego, poza sytuacjami w których następuje to na wniosek osoby, której dane dotyczą.

IX. Postanowienia końcowe

1. Za niedopełnienie obowiązków wynikających z niniejszego dokumentu Pracownik ponosi odpowiedzialność na podstawie Kodeksu pracy, Przepisów o ochronie danych osobowych oraz Kodeksu karnego w odniesieniu do danych osobowych objętych tajemnicą zawodową oraz innych przepisów prawa, mających zastosowanie do danego Pracownika.
2. Integralną część niniejszej Polityki bezpieczeństwa stanowią następujące Załączniki:
 - a) **Załącznik nr 1:** Rejestr czynności przetwarzania danych osobowych.
 - b) **Załącznik nr 2:** Wzór Upoważnienia do przetwarzania danych osobowych.
 - c) **Załącznik nr 3:** Wzór Oświadczenia i zobowiązania osoby przetwarzającej dane osobowe.
 - d) **Załącznik nr 4:** Wzór zgłoszenia naruszenia zasad ochrony danych do organu nadzorczego.
 - e) **Załącznik nr 5:** Lista zbiorów danych osobowych.

Załącznik 1. Rejestr czynności przetwarzania danych osobowych

| | |
|---|---|
| Nazwa oraz dane kontaktowe Administratora Danych | Kancelaria Gabrysiak i Wspólnicy spółka cywilna. ul. Puławska 257/71, 02-769 Warszawa, tel. +48 22 110 50 66 |
| Imię i nazwisko lub nazwa oraz dane kontaktowe Inspektora Ochrony Danych Osobowych | Nie ma zastosowania. |
| Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych | Osoby fizyczne – aktualni lub byli klienci Kancelarii Gabrysiak i Wspólnicy. |
| Cele przetwarzania danych osobowych | Prowadzenie obsługi prawnej klientów, w tym postępowań sądowych, informowanie klientów o zmianach w prawie, informowanie klientów o usługach prawnych świadczonych przez Kancelarię. |
| Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych | Odbiorcami, którym dane będą przekazywane są: <ul style="list-style-type: none"> • Procesor oraz ew. inni profesorzy, współpracujący z Kancelarią - na podstawie umów o powierzenie przetwarzania danych osobowych; • osoby współpracujące z Kancelarią w ramach jej przedsiębiorstwa, działające na podstawie umów i oraz upoważnień do przetwarzania danych osobowych. Kancelaria nie ujawnia danych odbiorcom w Państwach trzecich. |
| Informacja o przekazywaniu danych osobowych do państwa trzeciego | Kancelaria nie przekazuje danych do państw trzecich. |
| Planowane terminy usunięcia poszczególnych kategorii danych | 5 lat po zakończeniu świadczenia usług dla danego klienta. |
| Ogólny opis techniczny i organizacyjny środków bezpieczeństwa danych. | Serwer gromadzący dane przetwarzane przez GiW jest własnością GiW, znajduje się w serwerowni zewnętrznej przy ul. Konstruktorskiej 5 w Warszawie. Połączenie między serwerownią a biurem GiW zrealizowane za pomocą tunelu VPN site-to-site. System antywirusowy ESET ENDPOINT SECURITY zainstalowany na wszystkich komputerach GiW. Dodatkowo w biurze zastosowano FireWall CISCO ASA 5506 jako urządzenie zabezpieczające dostęp do Internetu. Spoza biura dostęp do danych na Serwerze jest możliwy jedynie za pośrednictwem szyfrowanego tunelu VPN. Laptopy, GiW, pracujące także poza biurem posiadają szyfrowane dyski. Poczta e-mail GiW znajduje się i jest obsługiwana przez Serwer GiW. Backup wirtualnych serwerów jest tworzony na dedykowanej dla GiW przestrzeni dyskowej Procesora. |

.....
[miejsowość, data sporządzenia]

**UPOWAŻNIENIE DO PRZETWARZANIA
DANYCH OSOBOWYCH**

nr

Działając w imieniu kancelarii Gabrysiak i Wspólnicy, Administratora Danych Osobowych niniejszym upoważniam:

Panią/Pana.
Stanowisko

do przetwarzania danych osobowych w kancelarii Gabrysiak i Wspólnicy

w następującym zakresie:

- bez ograniczeń
- podgląd danych
- wprowadzanie danych
- opracowywanie danych
- zmienianie danych
- usuwanie danych.

A. Okres upoważnienia: na cały okres zatrudnienia / na cały okres współpracy.

B. Zakres upoważnienia:

- dane przetwarzane na nośnikach papierowych,
- system informatyczny,
- dane osobowe objęte zbiorem:

- a)
- b)
- c)

.....
[administrator danych]

....., dn. r.
[miejsce i data sporządzenia]

.....
imię i nazwisko osoby upoważnionej

.....
stanowisko

.....
miejsce pracy

OŚWIADCZENIE

Oświadczam, że – w związku z wykonywaniem przeze mnie prac / świadczeniem przeze mnie usług na rzecz kancelarii Gabrysiak i Wspólnicy – administratora danych, i upoważnieniem mnie do przetwarzania danych osobowych – zapoznałem/łam się ze stosownymi przepisami i standardami ochrony danych osobowych, zobowiązuję się do przestrzegania:

- Polityki Bezpieczeństwa informacji w kancelarii Gabrysiak i Wspólnicy;
- Instrukcji zarządzania systemem Informatycznym w kancelarii Gabrysiak i Wspólnicy.
- przepisów o ochronie danych osobowych, w tym Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/ WE;
- przepisów o ochronie tajemnicy zawodowej adwokatów lub radców prawnych.

W związku z powyższym zobowiązuję się do:

- a) zapewnienia ochrony danych osobowych przetwarzanych w zbiorach administratora, a w szczególności zapewnienia ich bezpieczeństwa przed udostępnianiem osobom trzecim i nieuprawnionym, zabraniam, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem danych;
- b) zachowania w tajemnicy, także po zaprzestaniu wykonywania prac / świadczenia przeze mnie usług, wszelkich informacji dotyczących funkcjonowania systemów służących do przetwarzania danych osobowych we wszystkich zbiorach objętych udzielonym mi upoważnieniem;
- c) natychmiastowego zgłaszania do Administratora Danych zaobserwowanego zagrożenia danych;
- d) próby lub faktu naruszenia zabezpieczenia fizycznego pomieszczenia gdzie przetwarzane są dane oraz innych przypadków naruszenia lub podejrzenia naruszenia bezpieczeństwa danych lub systemów informatycznych administratora.

.....
[czytelny podpis osoby składającej oświadczenie]

Załącznik 4. Wzór zgłoszenia incydentu naruszenia ochrony danych osobowych

....., dn. r.
[miejsce i data sporządzenia]

Prezes Urzędu Ochrony Danych Osobowych
.....

ZGŁOSZENIE INCYDENTU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Działając na podstawie art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), niniejszym zgłaszam zajście incydentu naruszenia ochrony danych osobowych.

| | |
|---|--|
| Dane Administratora Danych Osobowych | |
| Miejsce i dzień naruszenia | |
| Kategoria i przybliżona liczba osób, których dane dotyczą | |
| Kategorie i przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie | |
| Opis charakteru naruszenia ochrony danych | |
| Możliwe konsekwencje naruszenia ochrony danych | |
| Środki zastosowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych | |

.....
[podpis osoby uprawnionej
do reprezentowania Administratora Danych]

Załącznik nr 5 Lista zbiorów danych osobowych

Na dzień 23 maja 2018 r. GiW dysponuje czterema zbiorami danych osobowych:

1. Zbiór danych osobowych osób uczestniczących w postępowaniu grupowym toczącym się aktualnie w Sądzie Apelacyjnym w Łodzi pod sygnaturą akt I ACa 1058/15. Zbiór ten jest określany w przedsiębiorstwie GiW jako „GNB”.
2. Zbiór danych osobowych osób uczestniczących w postępowaniu grupowym toczącym się aktualnie w Sądzie Okręgowym w Łodzi pod sygnaturą akr I C 519/16. Zbiór ten jest określany w przedsiębiorstwie GiW jako „GNMF”.
3. Zbiór danych osobowych osób, na rzecz których GiW świadczy usługi prawne, w tym reprezentuje te osoby w indywidualnych postępowaniach. Zbiór ten jest określany w przedsiębiorstwie GiW jako „Klienci Indywidualni” lub „KI”.
4. Zbiór danych osobowych Pracowników Kancelarii, który w przedsiębiorstwie funkcjonuje jako „Informacje o Pracownikach”.