

The background of the slide shows a blurred office setting with people sitting at a table. A large, semi-transparent purple shape is overlaid on the left side of the image, containing the text.

NIS-2 — kogo dotyczą nowe regulacje i jakie są kary za ich niestosowanie?

Magdalena Bilicka
Counsel
Grant Thornton

Karolina Idziak
Associate
Grant Thornton

Agenda

- I. Wprowadzenie – implementacja i ogólne informacje o Dyrektywie NIS-2
- II. Kary i sankcje za naruszenie obowiązków
- III. Podmioty zobowiązane – kwalifikacja przedmiotowa i wielkościowa
- IV. Sektory ważne
- V. Sektory kluczowe
- VI. Zakończenie – podsumowanie najważniejszych zagadnień

1. Wprowadzenie – implementacja i ogólne informacje o Dyrektywie NIS-2

NIS-2*

- państwa członkowskie Unii Europejskiej mają 21 miesięcy na wprowadzenie postanowień dyrektywy do prawa krajowego
- nowe przepisy powinny być stosowane we wszystkich krajach Unii Europejskiej od 18 października 2024 r.

* Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)



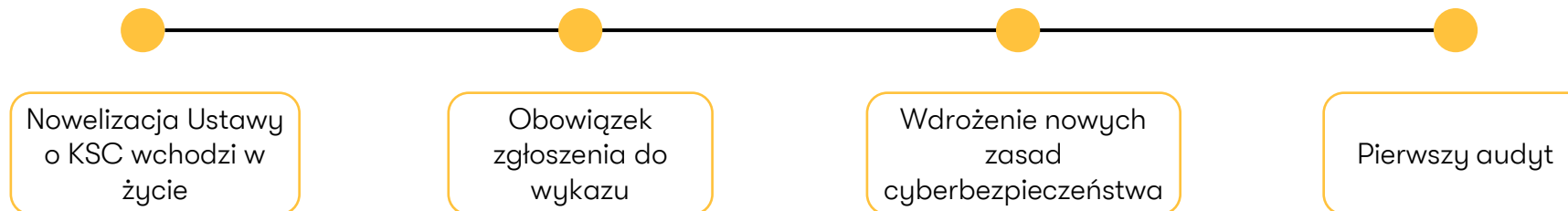
Projekt nowelizacji Ustawy o KSC*

- opublikowany dnia 3 października 2024 r. (wcześniejsza wersja z 24 kwietnia 2024 r.)
- planowany termin wejścia w życie: koniec 2024 r.

Art. 16. 1. Podmiot kluczowy i podmiot ważny:

- 1) realizuje obowiązki, o których mowa w niniejszym rozdziale, **w terminie 6 miesięcy**,
- 2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy **w terminie ~~12~~ 24 miesięcy** – od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny. ”;

~~17.10.2024~~ **początek 2025** Po ~~2~~ **3** miesiącach Po **6** miesiącach Po ~~12~~ **24** miesiącach



* Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tekst jednolity: Dz. U. z 2023 r. poz. 913 ze zmianami)



1. Zgłoszenia lobbingowe

Data ostatniej modyfikacji: 11-09-2024



2. Uzgodnienia

Data ostatniej modyfikacji: 07-10-2024



3. Konsultacje publiczne

Data ostatniej modyfikacji: 11-10-2024



4. Opiniowanie

Data ostatniej modyfikacji: 07-10-2024



5. Komitet Rady Ministrów do Spraw Cyfryzacji



6. Komitet do Spraw Europejskich



7. Komitet Społeczny Rady Ministrów



8. Komitet Ekonomiczny Rady Ministrów



9. Stały Komitet Rady Ministrów



10. Komisja Prawnicza



11. Potwierdzenie projektu przez Stały Komitet Rady Ministrów



12. Rada Ministrów

13. Notyfikacja

14. Skierowanie projektu ustawy do Sejmu



Minister
Cyfryzacji

DP.MC.WL.0211.16.2024

Warszawa, 07 października 2024 r.

wg rozdzielnika

Szanowni Państwo,

uprzejmie informuję, że w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny, zostały udostępnione dokumenty dotyczące **projektu ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32)**, tj. zestawienie uwag z etapu uzgodnień, konsultacji publicznych i opiniowania – wraz ze stanowiskiem Ministra Cyfryzacji.

Większość uwag została uwzględniona albo wyjaśniona.

Projekt ustawy zostanie niezwłocznie skierowany do dalszych prac legislacyjnych.

Z wyrazami szacunku

z up. Ministra Cyfryzacji
Dariusz Standerski
Sekretarz Stanu
w Ministerstwie Cyfryzacji
/dokument podpisany elektronicznie/

Artykuł 5

Harmonizacja minimalna

Niniejsza dyrektywa nie uniemożliwia państwom członkowskim przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, pod warunkiem że takie przepisy są spójne z obowiązkami państw członkowskich, ustanowionymi w prawie Unii.

2. Kary i sankcje za naruszenie obowiązków

Kary wg NIS-2

Podmiot ważny

Maksymalnie 7 mln euro lub 1,4% łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa

Podmiot kluczowy

Maksymalnie 10 mln euro lub 2% łącznego rocznego światowego obrotu w poprzednim roku obrotowym przedsiębiorstwa

Kary wg projektu Ustawy o KSC

Podmiot ważny

Od 15 tys. zł do 7 mln euro
lub 1,4% łącznego rocznego
światowego obrotu w
poprzednim roku obrotowym
przedsiębiorstwa

Podmiot kluczowy

Od 20 tys. zł do 10 mln euro
lub 2% łącznego rocznego
światowego obrotu w
poprzednim roku obrotowym
przedsiębiorstwa

“5. Jeżeli podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, powodując:

1) bezpośrednio i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi;

2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług

– organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości **do 100 000 000 zł”;**

Inne sankcje



zawieszenie, ograniczenie zakresu albo cofnięcie koncesji do czasu gdy podmiot podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń



wykreślenie podmiotu z rejestru działalności regulowanej



cofnięcie zezwolenia do czasu gdy podmiot podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń



w celu przymuszenia do wykonania nałożonych obowiązków można nałożyć okresową karę pieniężną, w wysokości od 500 zł do 100 000 złotych za każdy dzień opóźnienia

Kary personalne



Niezależnie od kary nałożonej na spółkę, karę pieniężną można nałożyć również na kierownika podmiotu kluczowego lub podmiotu ważnego za niedokonanie obowiązków.

Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki zostały powierzone innej osobie za jej zgodą.



Kara pieniężna może być wymierzona w kwocie nie większej niż 600% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop



Organ właściwy do spraw cyberbezpieczeństwa może zwrócić się do sądu o nałożenie tymczasowego zakazu zajmowania stanowiska przez osoby kierujące podmiotem kluczowym

3. Podmioty zobowiązane – kwalifikacja przedmiotowa i wielkościowa

Kwalifikacja podmiotu



1. Czy spełniam kryteria podlegania przepisom niezależnie od wielkości?



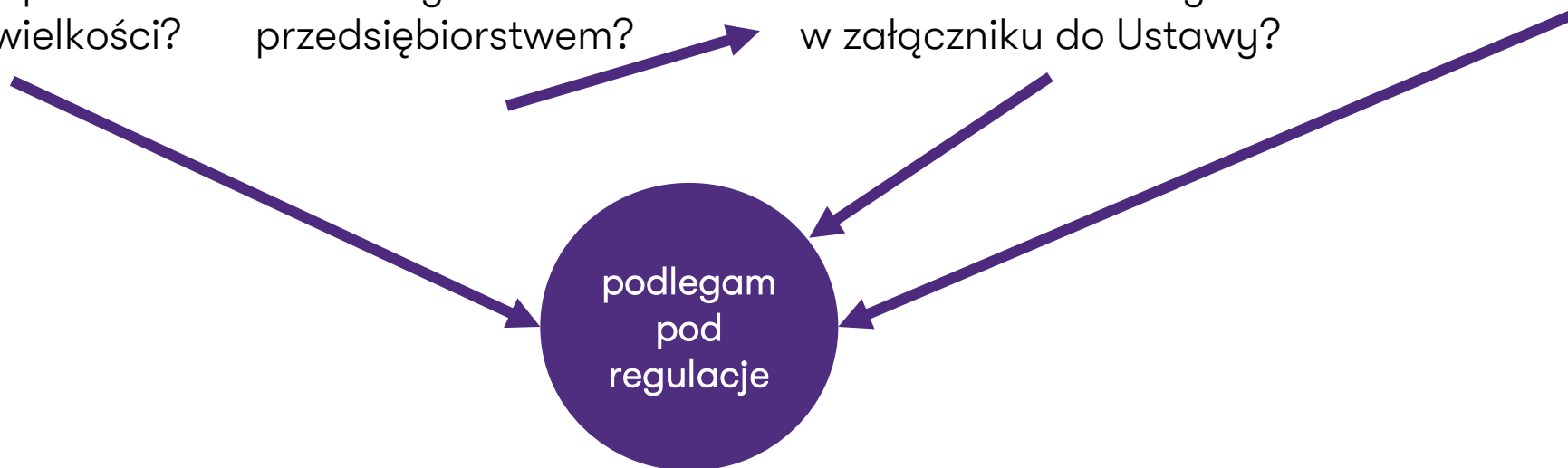
2. Czy jestem średnim albo dużym przedsiębiorstwem?



3. Czy działam w jednym z sektorów wskazanych w załączniku do Ustawy?



4. Czy świadczę usługę ICT?



Niezależnie od wielkości

dostawca usług DNS

~~dostawca usług zarządzanych w zakresie cyberbezpieczeństwa~~

kwalifikowany i niekwalifikowany dostawca usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia 910/2014

podmiot krytyczny

podmiot publiczny

podmiot zidentyfikowany jako podmiot kluczowy albo ważny na podstawie art. 71

podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 1 do ustawy z nazwy albo poprzez określenie jego rodzaju,

podmiot będący operatorem obiektu energetyki jądrowej

rejestr nazw domen najwyższego poziomu (TLD).

podmiot będący inwestorem obiektu energetyki jądrowej, który uzyskał decyzję zasadniczą

przedsiębiorca komunikacji elektronicznej

podmiot leczniczy, jeżeli zatrudnia min. 50 osób

w tym w szczególności:

- 1) organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i **ochrony prawa oraz sądy i trybunały;**
- 2) **jednostki samorządu terytorialnego oraz ich związki;**
- 3) **uczelnie publiczne**
- 4) **państwowe i samorządowe instytucje kultury;**

prowadzi działalność w określonym sektorze oraz:

- 1) jako jedyny świadczy, **za pomocą systemu informacyjnego**, usługę, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej,
- 2) zakłócenie świadczenia, **za pomocą systemu informacyjnego**, usługi spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności albo ryzyko systemowe zaprzestania **lub zdrowia publicznego** świadczenia usług przez podmioty kluczowe lub podmioty ważne lub
- 3) Świadczenie, **za pomocą systemu informacyjnego**, usług ma istotne znaczenie na poziomie krajowym lub województwa

“Do celów niniejszej dyrektywy następujące podmioty uznaje się za podmioty kluczowe:

a) podmioty w rodzaju tych, o których mowa w załączniku I, przekraczające pułapy dla średnich przedsiębiorstw, określone w art. 2 ust. 1 załącznika do zalecenia 2003/361/WE; (...)”

“Podmiotem kluczowym jest:

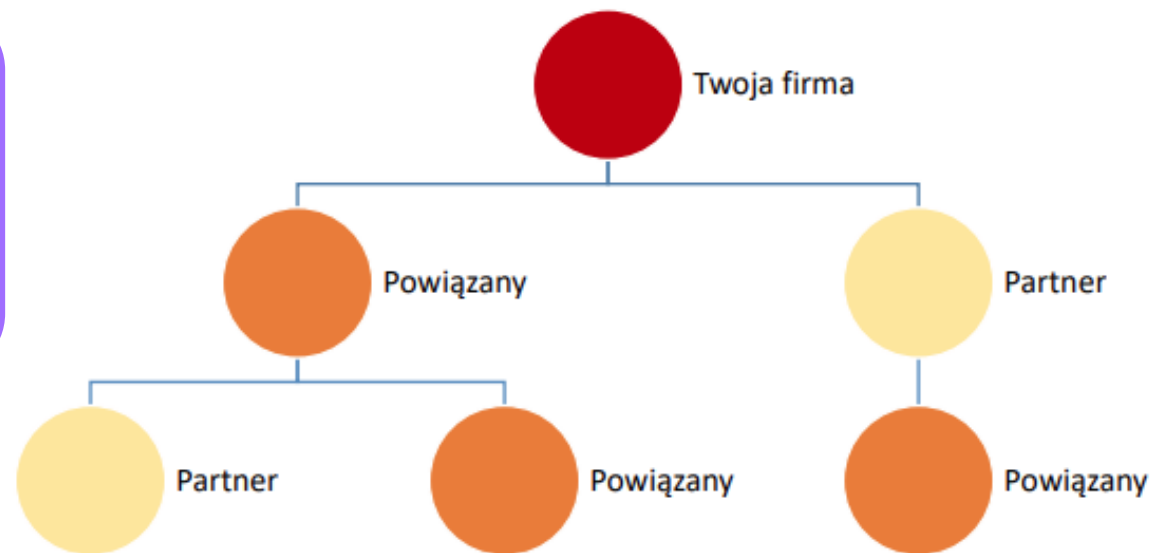
- 1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 ~~in~~ ~~2~~ do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1),1, z późn. zm.)), zwanego dalej „rozporządzeniem 651/2014/UE”;**
- 2) przedsiębiorca komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w rozporządzeniu art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa;**
- 3) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, który co najmniej spełnia wymogi dla małego albo średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa;**

Wielkość przedsiębiorstwa

Wielkość przedsiębiorstwa	Zatrudnienie (RJR)		Roczny obrót		Roczna suma bilansowa
Mikro	< 10	i	≤ 2 mln euro	lub	≤ 2 mln euro
Małe	< 50		≤ 10 mln euro	lub	≤ 10 mln euro
<u>Średnie</u>	<u>< 250</u>		<u>≤ 50 mln euro</u>	<u>lub</u>	<u>≤ 43 mln euro</u>

Jeżeli podmiot spełnia wymogi do uznania za podmiot kluczowy ponieważ przewyższa kryteria dla średniego przedsiębiorstwa zgodnie z art. 6 ust. 2–4 załącznika I do rozporządzenia 651/2014/UE, ale jego system informacyjny jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich, to nie jest podmiotem kluczowym.

Źródło: PARP



Sektory kluczowe

	Wydobywanie kopalin
	Energia elektryczna
	Ciepło
	Ropa i paliwa
Energia	Gaz
	Energetyka jądrowa
	Dostawy i usługi dla sektora energii
	Jednostki nadzorowane i podległe
	Wodór
Transport	Transport lotniczy
	Transport kolejowy
	Transport wodny
	Transport drogowy
Bankowość i infrastruktura rynków finansowych	
Ochrona zdrowia	
Zaopatrzenie w wodę pitną i jej dystrybucja	
Ścieki	
Infrastruktura cyfrowa	Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej
	Komunikacja elektroniczna
Zarządzanie usługami ICT	
Przestrzeń kosmiczna	
Podmioty publiczne	

np. przedsiębiorstwa energetyczne posiadające koncesję na wykonywanie działalności gospodarczej w zakresie: wytwarzania/ przesyłania/ dystrybucji/ obrotu energią elektryczną/ ciepłem/ paliwami ciekłymi/ gazem

np. przewoźnik lotniczy, zarządzający lotniskiem, zarządca infrastruktury kolejowej, przewoźnik kolejowy, armator, podmioty zarządzające drogami

np. banki, instytucja kredytowa, SKOK-i, biura maklerskie

np. podmioty lecznicze, laboratoria referencyjne UE, podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych zdefiniowanych, podmioty produkujące podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, **hurtownie farmaceutyczne, apteki**

np. dostawca usług DNS, dostawca chmury obliczeniowej, dostawca usług zaufania, dostawca usług centrum przetwarzania danych, rejestracja nazw domen, dostawca usług zarządzanych

Sektory **kluczowe** ważne (1/2)

Produkcja, wytwarzanie i dystrybucja chemikaliów

Produkcja, przetwarzanie i dystrybucja żywności

produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro

produkcja komputerów, wyrobów elektronicznych i optycznych

produkcja urządzeń elektrycznych

Produkcja

produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana

produkcja pojazdów samochodowych, przyczep i naczep

produkcja pozostałego sprzętu transportowego

np. przedsiębiorstwo zajmujące się produkcją substancji oraz wytwarzaniem i dystrybucją substancji lub mieszanin

np. przedsiębiorstwa spożywcze, prowadzące jakąkolwiek działalność związaną z jakimkolwiek etapem produkcji, przetwarzania i dystrybucji żywności

np. produkcja rur, drutów, metali szlachetnych, aluminium, odlewnictwo metali, żeliwa

np. produkcja metalowych elementów konstrukcyjnych, metalowych elementów stolarki budowlanej, zbiorników, cystern i pojemników metalowych, kucie, prasowanie, wyłaczanie i walcowanie metali, obróbka metali, produkcja narzędzi, produkcja zamków i nawiasów, produkcja pojemników metalowych, produkcja wyrobów z drutu, produkcja opakowań z metali lekkich, produkcja złączy, śrub, tańcuchów i sprężyn

np. produkcja pojazdów silnikowych, części i akcesoriów do pojazdów silnikowych, produkcja rowerów i wózków inwalidzkich, produkcja wózków dziecięcych, produkcja pomp i sprężarek, kurków i zaworów, łożysk, kół zębatych, pieców, palenisk, urządzeń dźwigowych, chwytaków, maszyn dla rolnictwa i leśnictwa, ciągników rolniczych, narzędzi mechanicznych, broni i amunicji, maszyn do przemysłu włókienniczego i papierniczego, produkcja elektrycznego sprzętu gospodarstwa domowego, produkcja nonelektrycznego sprzętu gospodarstwa domowego

Sektory ważne (2/2)

Usługi pocztowe

Zbieranie odpadów

Transport odpadów

Przetwarzanie odpadów, w tym sortowanie, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów

Gospodarowanie odpadami

Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami

Dostawy i usługi dla sektora gospodarowania odpadami

Jednostki nadzorowane i podległe

Zbieranie odpadów

Dostawcy usług cyfrowych

Badania naukowe

np. operator pocztowy

np. podmioty świadczące usługi zbierania, transportu, przetwarzania, sprzedaży odpadów

np. podmioty świadczące usługi zbierania, transportu, przetwarzania, sprzedaży odpadów

np. podmioty prowadzące działalność gospodarczą dostaw usług zarządzanych w zakresie cyberbezpieczeństwa dla podmiotów kluczowych lub podmiotów ważnych

np. podmioty prowadzące działalność gospodarczą dostaw usług zarządzanych w zakresie cyberbezpieczeństwa dla podmiotów kluczowych lub podmiotów ważnych

np. dostawca internetowej platformy handlowej, dostawca wyszukiwarki internetowej, dostawca platformy sieci usług społecznościowych

np. organizacja badawcza

“Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług przez ten podmiot, zapewniający:

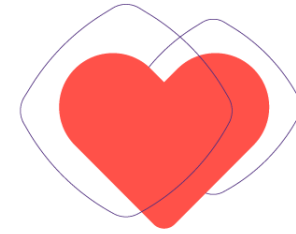
(...)

d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy **bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym, (...)**

BEZPŁATNA ANKIETA

Czy moja firma podlega pod NIS2?
SPRAWDŹ w 2 minuty - Grant
Thornton

Zapraszam do kontaktu



CLIENT WEEK
z Grant Thornton



Magdalena Bilicka

Counsel

M +48 661 538 507

E magdalena.bilicka@pl.gt.com



Karolina Idziak

Associate

M +48 885 887 294

E karolina.idziak@pl.gt.com