

# Kary organów nadzorczych w Unii Europejskiej



Kraj oraz organ nadzorczy

**Włochy**

Italian Data Protection Authority (Garante)



Data wydania decyzji

**06 październik 2022 r.**



Podmiot kontrolowany

**Alpha Exploration**



Wysokość kary

**2 000 000 EUR**

**FORSAFE**  
BEZPIECZEŃSTWO PONAD WSZYSTKO



## Rodzaj naruszenia

Art. 5 (1) a), e), f) RODO, Art. 6 RODO, Art. 7 RODO, Art. 12 (1) RODO, Art. 13 RODO, Art. 14 RODO, Art. 27 (4) RODO, Art. 28 RODO, Art. 32 RODO, Art. 35 RODO.  
Nieprzestrzeganie ogólnych zasad przetwarzania danych.



## Przedmiot decyzji

### Źródło postępowania:

Włoski organ nadzorczy w wyniku doniesień prasowych, zdecydował o dokonaniu czynności kontrolnych w Alpha Exploration (Spółka), który obsługuje portal społecznościowy Clubhouse.

### Opis wydarzeń:

**1)** Przedmiotem kontroli była weryfikacja realizacji zasad ochrony danych osobowych w Clubhouse.

**2)** W trakcie czynności kontrolnych włoski organ nadzorczy ustalił, iż Clubhouse to serwis społecznościowy oparty wyłącznie na interakcjach głosowych, odbywających się w pokojach konwersacyjnych, który dostępny jest publicznie za pośrednictwem aplikacji mobilnej.

**3)** W marcu 2021 r. Clubhouse posiadał ok. 16 mln użytkowników.

**4)** W trakcie czynności kontrolnych włoski organ nadzorczy uznał, że naruszono:

**a)** zasadę legalizacji – Spółka przetwarzała dane w celach marketingowych, nagrywała i udostępniała dźwięk podmiotom trzecim, profilowała i udostępniała informacje o kontaktach bez adekwatnej podstawy prawnej,

**b)** zasadę przejrzystości – Spółka nie realizowała obowiązku informacyjnego wobec użytkowników oraz wobec osób niebędących użytkownikami, a pozyskanymi z książek telefonicznych użytkowników,

**c)** zasadę ograniczenia przechowywania – Spółka w błędny sposób określiła okresy przechowywania danych osobowych,

**d)** obowiązek podania danych kontaktowych do wyznaczonego przedstawiciela – Spółka tego nie uczyniła,

**e)** obowiązek wskazania pełnomocnika i określenia jego funkcji i obowiązków – Spółka tego nie uczyniła,

**f)** obowiązek podpisania umów powierzenia przetwarzania danych osobowych – Spółka nie opracowała rejestru podmiotów przetwarzających,

**g)** obowiązek przeprowadzenia oceny skutków dla ochrony danych – Spółka tego nie uczyniła.

### Przyczyna naruszenia:

Spółka nie dopełniła obowiązku realizacji podstawowych zasad ochrony danych osobowych.

### Decyzja:

**1)** Kara pieniężna w wysokości 2 000 000 EUR.

**2)** Zakaz dalszego przetwarzania dokonywanego na potrzeby marketingu bezpośredniego, profilowania i udostępniania informacji o koncie, ze względu na nieodpowiednią podstawę prawną.

**3)** Nakaz zapewnienia zgodności przetwarzania poprzez:

**a)** aktualizację regulaminu usługi poprzez wstawienie opisu funkcji Clips & Replays (funkcja nagrywania),

**b)** przypisanie podstaw prawnych do każdego celu przetwarzania danych osobowych,

**c)** wprowadzenie funkcji umożliwiającej poinformowanie użytkownika, że wejście do pokoju wiąże się z ewentualnym nagraniem czatu,

**d)** wdrożenie mechanizmu informowania osób niebędących użytkownikami Clubhouse, a pozyskanymi z książek telefonicznych użytkowników o przetwarzaniu ich danych osobowych,

**e)** wskazanie okresów przechowywania danych osobowych w zależności od ich rodzaju,

**f)** wskazanie kontaktowego adresu e-mail wyznaczonego przedstawiciela,

**g)** umieszczenie linku odsyłającego do wykazu podmiotów przetwarzających dane osobowe oraz bieżące aktualizowanie tego wykazu,

**h)** określenie funkcji pełnomocnika oraz opisanie jej w akcie jego wyznaczenia,

**i)** przeprowadzenie oceny skutków przetwarzania danych osobowych prowadzonego za pośrednictwem platformy Clubhouse,

**j)** zawiadomienie organu nadzorczego o podjętych działaniach wynikających z wydanej decyzji – w terminie 30 dni od jej dostarczenia.

### Źródło:

<https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9828901>



## Kompas FORSAFE

### JAK UNIKAĆ TAKICH NARUSZEŃ?

**1)** Realizuj zasadę przejrzystości przetwarzania danych osobowych poprzez wykonanie obowiązku informacyjnego.

**2)** Informacje lub komunikaty opracuj tak, aby treści:

**a)** miały zwięzłą formę (osoba nie może być przytłoczona informacjami),

**b)** miały przejrzystą formę (informacje należy odróżnić od innych informacji niezwiązanych z prywatnością),

**c)** miały zrozumiałą formę (informacje powinny być możliwe do zrozumienia przez przeciętnego przedstawiciela grupy docelowych odbiorców),

**d)** miały łatwo dostępną formę (osoba nie powinna być zmuszona do wyszukiwania informacji – miejsce i sposób dostępu do informacji powinien być oczywisty),

**e)** były napisane jasnym i prostym językiem (informacji udzielaj w możliwie najprostszym sposób, bez stosowania złożonych struktur zdaniowych i językowych; informacji udzielaj w sposób konkretny i jednoznaczny pamiętając o wskazaniu celu i podstawy prawnej przetwarzania danych osobowych; unikaj wyrazów takich, jak: „może”, „niektóre”, „często”, „możliwe”),

**f)** były przekazane na piśmie lub w formie elektronicznej oraz ustnie – na żądanie osoby, której dane dotyczą.

**3)** Realizację zasady przejrzystości możesz oprzeć o warstwowe podejście do udzielania informacji osobie, której dane dotyczą. Pamiętaj, aby w pierwszej warstwie uwzględnić informacje na temat celów przetwarzania, tożsamości administratora i opisu praw osoby, której dane dotyczą, a także informacje na temat najważniejszych skutków przetwarzania danych osobowych.

**4)** Rekomendowane jest, aby administratorzy działający w środowisku cyfrowym/online, przekazywali informacje dotyczące prywatności poprzez elektroniczne oświadczenie o ochronie prywatności lub elektroniczną informację o polityce prywatności.

**5)** Wykonaj ocenę skutków dla ochrony danych, gdy:

**a)** przetwarzanie danych osobowych z dużym prawdopodobieństwem może powodować wysokie naruszenie praw lub wolności osób fizycznych,

**b)** przetwarzanie danych osobowych opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu,

**c)** dane osobowe szczególnej kategorii oraz dane dotyczące wyroków sądowych i czynów zabronionych są przetwarzane na dużą skalę,

**d)** operacje przetwarzania danych osobowych zawarte są w wykazie upublicznionym przez organ nadzorczy.

**6)** Jeśli jako Administrator nie masz swojej jednostki organizacyjnej na terenie Unii Europejskiej, ale obowiązują Ciebie przepisy RODO, wówczas Twoim obowiązkiem jest wyznaczenie na piśmie przedstawiciela, który będzie mieć swoją siedzibę na terenie Unii Europejskiej.

