# ROZPORZĄDZENIE O OGÓLNEJ OCHRONIE DANYCH

Analiza z dnia 3 września 2012 r.

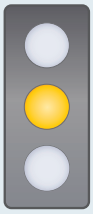
Centrum für Europäische Politik

FORUM OBYWATELSKIEGO ROZWOJU

## NAJWAŻNIEJSZE ZAGADNIENIA

**PRZEDMIOT ROZPORZĄDZENIA:** Komisja zamierza przystosować przepisy dotyczące ochrony danych do wymagań ery Internetu.

**STRONY ZAANGAŻOWANE:** Wszyscy obywatele i przedsiębiorstwa oraz władze publiczne.



**ZA:**
- Ujednolicenie przepisów o ochronie danych oraz przyznanie krajowym organom kompetencji obejmujących całą UE zmniejszy koszty ponoszone przez przedsiębiorstwa oraz zapewni wszystkim podmiotom równe szanse.

**PRZECIW:**
- Rodzaj i liczba kompetencji przyznanych Komisji jest nie do zaakceptowania z punktu widzenia zasady podziału władz. Decyzje o istotnym znaczeniu dla danej dziedziny prawa powinny być podejmowane przez samego prawodawcę europejskiego.
- Przepisy dotyczące nieważności zgody są niejasne, uwzględnić trzeba również konieczność przetwarzania danych dotyczących zdrowia.
- Przepisy dotyczące ochrony danych pracowników nie służą budowie zaufania do prawa.

## TREŚĆ

### Tytuł

**Wniosek** dotyczący **Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych** i swobodnym przepływem takich danych **(Rozporządzenie o Ogólnej Ochronie Danych). Sygnatura COM(2012) 11** z 25 stycznia 2012 r.

### Streszczenie

Uwaga! Wskazane numery artykułów i stron odnoszą się do wniosku (2012) 11.

#### › Tło i cel

- Unijne przepisy dotyczące ochrony danych powstały w połowie lat 90. (Dyrektywa o Ochronie Danych 95/46/EC, zmieniona ostatnio Rozporządzeniem (EC) nr 1882/2003) – czyli w czasach, gdy Internet dopiero „raczkował" [COM(2012) 9, s. 3].
- Unijne przepisy o ochronie danych muszą zostać dostosowane do wymagań ery Internetu. Ich nowelizacja polegać ma przede wszystkim na stworzeniu - poprzez pełne ujednolicenie - „nowoczesnych, silnych, spójnych i wszechstronnych ram prawnych UE w dziedzinie ochrony danych" [COM (2012) 9, s. 12]. Kluczowym elementem harmonizacji ma być Rozporządzenie o Ogólnej Ochronie Danych (dalej zwane GDPR).

#### › Zakres

- Mówiąc najprościej, zakres materialny obejmuje wszelkie zautomatyzowane przetwarzanie indywidualnych danych oraz ich przechowywanie w zbiorach danych (art. 2 (1); wyjątki: art. 2 (2)).
- Zakres personalny obejmuje w szczególności:
  - „administratora", którym jest każda osoba, samodzielnie lub wspólnie z innymi ustalająca cele, warunki i sposoby przetwarzania danych osobowych (art. 4 (5));
  - „podmiot przetwarzający", którym jest każdy, kto przetwarza dane osobowe w imieniu administratora (art. 4 (6)).
- Zasięg terytorialny obejmuje:
  - administratorów zarejestrowanych w UE (art. 3 (1)), niezależnie od tego, czy dane przetwarzane są w granicach czy poza granicami UE (preambuła nr 19);
  - administratorów zarejestrowanych poza UE (art. 3 (2)), pod warunkiem, że:
    - przetwarzane są dane osobowe „podmiotów danych mających siedzibę w Unii" (a nie tylko obywateli Unii, art. 9 TEU), oraz
    - przetwarzanie danych „wiąże się" z oferowaniem towarów lub usług podmiotom danych w Unii lub też z monitorowaniem ich zachowań, np. poprzez tworzenie profilów użytkownika (preambuła nr 21; tzw. profilowanie).
  - Państwa Członkowskie mogą po spełnieniu określonych warunków w dalszym ciągu stanowić przepisy w sprawie przetwarzania danych, dotyczące m.in.:
    - danych związanych ze zdrowiem (art. 81 w połączeniu z art. 9 (2) lit. h);
    - danych osobowych pracowników gromadzonych przez pracodawców „w granicach określonych niniejszym Rozporządzeniem" (art. 82);
    - przetwarzania danych przez władze publiczne lub w powiązaniu z usługami świadczonymi w interesie publicznym (por. art. 6 (1) lit. e, (3) lit. b, preambuła nr 36).

#### › Legalność przetwarzania danych

- Przetwarzanie danych osobowych jest zgodne z prawem (art. 6 (1) lit. b-f);
  - gdy jest niezbędne do wykonania umowy, w której podmiot danych jest stroną;
  - gdy jest niezbędne do wypełnienia obowiązków prawnych administratora;
  - gdy wymaga tego „istotny" interes podmiotu danych;
  - gdy jest to niezbędne do wykonywania obowiązków publicznych;
  - gdy jest to w inny sposób „niezbędne" do realizacji „słusznych interesów" administratora, a interesy lub podstawowe prawa i wolności podmiotu danych nie mają charakteru nadrzędnego.

**Autor:** Oliver Sauer
**CEP** | Kaiser-Joseph-Straße 266, 79098 Freiburg | Niemcy | tel. +49 (0)761 38693-105 | www.cep.eu
**Polska wersja analizy powstała dzięki Fundacji FOR**
**FOR** | Al. Szucha 2/4 lok. 20, 00-582 Warszawa | Polska | tel. +48 22 427 40 10 | www.for.org.pl
**Tłumaczenie:** Krzysztof Szwałek

- Przetwarzanie tzw. danych wrażliwych, takich jak dane osobowe związane z wyznawaną religią lub przekonaniami, zdrowiem lub wyrokami skazującymi (art. 9 (1)) jest do co zasady niezgodne z prawem. W przypadku zawierania umowy o pracę (art. 9 (2) lit. b) lub w postępowaniu przed władzami publicznych (por. art. 9 (2) lit. g) mogą być jednak stosowane inne rozwiązania.

### › Zgoda na przetwarzanie danych osobowych

- Przetwarzanie danych osobowych jest zgodne z prawem również na podstawie zgody podmiotu danych (art. 6 (1) lit. a).
- Zgoda nie legitymizuje przetwarzania danych osobowych w przypadku:
  - gdy istnieje „znacząca nierównowaga" pomiędzy pozycją podmiotu danych i administratora (art. 7 (4)), „szczególnie" w „sytuacji zależności", np. takiej jak pomiędzy pracownikiem a pracodawcą (preambuła nr 34);
  - gdy przetwarzanie danych jest generalnie zakazane (por. art. 9 (1)), a prawo UE inne niż GDPR lub prawo krajowe wyklucza udzielenie zgody (art. 9 (2) lit. a).
- Obowiązek przedstawienia dowodu uzyskania zgody spoczywa na administratorze (art. 7 (1)). W przypadku deklaracji pisemnej, zgodna musi jasno wynikać z jej tekstu (art. 7 (2)).

### › Proces przetwarzania danych

- Z przetwarzaniem wiążą się m.in. następujące obowiązki:
  - obowiązek stosowania procedur technicznych, chroniących podmioty danych w najszerszym możliwym zakresie („ochrona danych w fazie projektowania"), takich jak „zasada domyślnej ochrony danych" np. w przypadku sieci społecznościowych (art. 23);
  - obowiązek (stałego) wszechstronnego dokumentowania [operacji przetwarzania danych – przyp. tłum.] (szczegóły w art. 28), które zastąpi obowiązek (uprzedniego) zawiadamiania organu nadzoru o przetwarzaniu danych (art. 18 i 19 Dyrektywy 95/46/EC); nie dotyczy to przedsiębiorstw zatrudniających mniej niż 250 pracowników, które przetwarzają dane w ramach działalności „podrzędnej" w stosunku do głównej działalności (art. 28 (4) lit. b);
  - obowiązek zachowania zgodności ze standardami ochrony danych (szczegóły: art. 30);
  - obowiązek informowania organu nadzoru (art. 31) i podmiotu danych (art. 32) o naruszeniu ochrony danych;
  - obowiązek sporządzania w sytuacji szczególnego ryzyka „oceny wpływu na ochronę danych" (szczegóły: art. 33);
  - obowiązek wyznaczenia inspektora ochrony danych (art. 35), w sytuacji, gdy:
    - przetwarzanie danych prowadzone jest w przedsiębiorstwach zatrudniających 250 lub więcej osób;
    - „główna działalność" administratora wymaga regularnego i systematycznego „nadzorowania podmiotów danych" (tu różnica pomiędzy wyjaśnieniem ze s. 12 i punktem 75 preambuły: tam jest mowa o sytuacji, gdy „operacje przetwarzania" wymagają regularnego i systematycznego „nadzorowania");
    - przetwarzanie danych jest prowadzone przez władze publiczne lub instytucje publiczne.
  - W zakres praw podmiotu danych wchodzi m.in.:
    - „prawo do bycia zapomnianym i wymazanym": podmiot danych może w określonych przypadkach domagać się wymazania jego danych osobowych i wnosić o wstrzymanie się od dalszego rozpowszechniania takich danych (art. 17 (1) oraz o podjęcie „wszelkich racjonalnych kroków" by poinformować [o tym fakcie – przyp. tłum.] osoby trzecie (art. 17 (2)).
    - „prawo do przenoszenia danych": podmiot danych ma prawo do uzyskania od administratora kopii swoich danych osobowych „w powszechnie używanym formacie elektronicznym", np. w celu przeniesienia ich do innego dostawcy np. usług internetowych (szczegóły art. 18).
    - „prawo wniesienia sprzeciwu", który powoduje obowiązek uzasadnienia przez administratora [prawa do przetwarzania – przyp. tłum.] (art. 19).
  - Adresatem zobowiązań zwykle jest administrator, ale również – w zależności od rodzaju zobowiązania – podmiot przetwarzający dane.

### › Krajowe organy ochrony danych

- Każde Państwo Członkowskie musi podjąć działania w kierunku stworzenia efektywnego nadzoru nad ochroną danych (art. 46 (1)).
- Przy wykonywaniu swoich obowiązków (art. 52) oraz wyżej wymienionych uprawnień (art. 53), organ nadzoru powinien cieszyć się „całkowitą" niezależnością (art. 47 (1)). W szczególności nie może być związany jakimikolwiek instrukcjami (por. art. 47 (2)).
- Kompetencje każdego organu nadzoru obejmują jedynie kraj jego siedziby (art. 51 (1)). Jeśli administrator lub podmiot przetwarzający dane ma siedziby w więcej niż jednym Państwie Członkowskim, organ nadzoru w państwie, w którym znajduje się „główna siedziba" tego administratora lub podmiotu (art. 4 (13), preambuła nr 27) zyskuje kompetencje obejmujące również inne Państwa Członkowskie (art. 51 (2), tzw. zasada „punktu kompleksowej obsługi").

### › Ochrona prawna

- Prawo do wnoszenia skarg do organu nadzoru przysługuje:
  - każdej zainteresowanej osobie fizycznej (art. 73 (1));
  - organom, organizacjom lub stowarzyszeniom, których celem jest ochrona danych w imieniu zainteresowanych osób fizycznych (art. 73 (2)) i ich własnym imieniu (art. 73 (3)).
- Prawo do podejmowania środków prawnych przeciwko organowi nadzoru przysługuje:
  - co do zasady każdej zainteresowanej osobie fizycznej lub prawnej (por. art. 74 (1), (2));
  - organom, organizacjom lub stowarzyszeniom, których celem jest ochrona danych w imieniu zainteresowanych osób fizycznych (art. 76 (1), art. 73 (2) w powiązaniu z art. 74).
- Prawo do podejmowania środków prawnych przeciwko administratorom i podmiotom przetwarzającym dane przysługuje:
  - każdej zainteresowanej osobie fizycznej (art. 75 (1));
  - organom, organizacjom lub stowarzyszeniom, których celem jest ochrona danych w imieniu zainteresowanych osób fizycznych (art. 76 (1), art. 73 (2) w powiązaniu z art. 75).

### › Zobowiązania i sankcje

- Administratorzy i podmioty przetwarzające dane odpowiadają solidarnie, przy czym możliwe jest uwolnienie od odpowiedzialności (art. 77).
- Państwa Członkowskie ustalają przepisy dotyczące kar, stosownie do skali naruszenia prawa (art. 78 (1)).
- Każdy organ nadzoru jest upoważniony do bezpośredniego nakładania grzywien (art. 79 (1)). W zależności od skali naruszenia przepisów mogą one wynosić do miliona euro, a w przypadku przedsiębiorstw - do 2 proc. całkowitego rocznego obrotu (szczegóły: art. 79 (3)-(6)).

**Autor:** Oliver Sauer
**CEP** | Kaiser-Joseph-Straße 266, 79098 Freiburg | Niemcy | tel. +49 (0)761 38693-105 | www.cep.eu
**Tłumaczenie:** Krzysztof Szwałek
**Polska wersja analizy powstała dzięki Fundacji FOR**
**FOR** | Al. Szucha 2/4 lok. 20, 00-582 Warszawa | Polska | tel. +48 22 427 40 10 | www.for.org.pl

› **Uprawnienia regulacyjne Komisji**
Rozporządzenie wymienia 26 uprawnień do przyjęcia aktów delegowanych (art. 290 TFEU) oraz 25 uprawnień do przyjęcia aktów wykonawczych (art. 291 TFEU).

### Stanowisko Komisji wobec zasady pomocniczości

Zdaniem Komisji, ujednolicenie na obszarze Unii ochrony danych jest niezbędne, by umożliwić ponadgraniczny przepływ danych osobowych oraz by zagwarantować wszystkim podmiotom danych skuteczną ochronę w całej UE (s. 6).

### Tło polityczne

Pakiet przepisów dotyczących ochrony danych osobowych ze stycznia 2012 r. obejmuje Komunikat [COM(2012) 9], niniejsze Rozporządzenie, zastępujące w dużej mierze obowiązującą dotychczas Dyrektywę o Ochronie Danych 95/46/EC (art. 88) i tworzące „ogólne unijne ramy dla ochrony danych" [zob. COM(2012) 9, s. 4], oraz Dyrektywę [COM(2012) 10] w sprawie współpracy polityczno-prawnej w dziedzinie przestępczości kryminalnej (PJCCM), zastępującą istniejącą Decyzję Ramową 2008/977/JI.

### Procedura prawna

| | |
|---|---|
| 25 stycznia 2012 r. | Przyjęcie przez Komisję |
| 16 lutego 2012 r. | Przesłanie do Komisji PE |
| 23 maja 2012 r. | Swoje opinie nt. pomocniczości wraz z uzasadnieniem przedstawiły: senat Francji (6 marca 2012 r.), Belgijska Izba Reprezentantów (27 marca 2012 r.), niemiecki Bundesrat (30 marca 2012 r.), szwedzki Riksdag (30 marca 2012 r.) oraz włoska Izba Deputowanych (4 kwietnia 2012 r.). |
| 15 stycznia 2013 r. | Opinia Europejskiego Komitetu Ekonomiczno-Społecznego (EESC) |
| 5 lutego 2013 r. | Pierwsze czytanie w Parlamencie Europejskim (EP) |
| | Przyjęcie przez EP i Radę, publikacja w Dzienniku Urzędowym Unii Europejskiej, wejście w życie |

### Podmioty uczestniczące w procesie politycznym

| | |
|---|---|
| Prowadząca Dyrekcja Generalna: | Dyrekcja generalna ds. sprawiedliwości |
| Komisja Parlamentu Europejskiego: | Komisja ds. swobód obywatelskich, sprawiedliwości i spraw wewnętrznych (prowadząca), sprawozdawca Jan Philipp Albrecht (Frakcja Zielonych/EFA, Niemcy) |
| Sposób decyzji w Radzie Unii Europejskiej | Większość kwalifikowana (do przyjęcia konieczna jest zgoda większości Państw Członkowskich oraz 255 z 345 głosów). |

### Szczegóły legislacyjne

| | |
|---|---|
| Kompetencje prawne | Art. 16 (2) TFEU (Ochrona danych), art. 114 TFEU (jednolity rynek) |
| Forma kompetencji prawnych | Kompetencje dzielone (art. 4 (1), (2) TFEU) |
| Procedura legislacyjna | Art. 294 TFEU (zwykła procedura legislacyjna) |

## OCENA

### Ocena wpływu na gospodarkę

**Ujednolicenie prawa dotyczącego ochrony danych oraz przyznanie krajowym organom kompetencji obejmujących całą UE oznaczać będzie dla zmniejszenie obciążeń i kosztów ponoszonych przez przedsiębiorców, a także stworzenie równych szans do konkurowania.**

### Ocena prawna

Kompetencje

Nie budzą wątpliwości. Podstawą prawną są przede wszystkim nowe uprawnienia UE w zakresie ochrony danych (art. 16 (2) TFEU).

Pomocniczość

Przyjmowanie rozporządzeń na szczeblu UE jest uzasadnione, gdy sprawa dotyczy kwestii ponadgranicznych, a już szczególnie regulowanie funkcjonowania tak „bezdomnego" medium jak Internet może być skuteczne tylko poprzez tworzenie ponadnarodowych ram prawnych. Gdy problem ma wymiar wyłącznie krajowy, ogólnoeuropejskie regulacje przewidujące ujednolicenie przepisów budzą wątpliwości. Argumentem na korzyść ogólnounijnej regulacji jest to, że jej brak oznaczać będzie obowiązywanie w przypadku bardzo podobnych transakcji dwóch różnych porządków prawnych dotyczących ochrony danych. Dzięki Internetowi - uregulowanie którego jest głównym celem reformy – kwestia przekraczania granicy traci na znaczeniu - zarówno dla dostawców, jak i użytkowników ma wymiar wirtualny.

Proporcjonalność

Forma prawna rozporządzenia ma uchronić unijne prawo o ochronie danych przed sytuacją, w której zostałoby ono wdrożone w każdym Państwie Członkowskim w nieco innym kształcie. Dla skutecznego uregulowania Internetu może mieć to kluczowe znaczenie, inaczej

**Autor:** Oliver Sauer
**CEP** | Kaiser-Joseph-Straße 266, 79098 Freiburg | Niemcy | tel. +49 (0)761 38693-105 | www.cep.eu
**Tłumaczenie:** Krzysztof Szwałek
**Polska wersja analizy powstała dzięki Fundacji FOR**
**FOR** | Al. Szucha 2/4 lok. 20, 00-582 Warszawa | Polska | tel. +48 22 427 40 10 | www.for.org.pl

bowiem powstanie niebezpieczeństwo, że przedsiębiorstwa będą przenosić się do krajów nakładających najmniejsze wymagania w tym zakresie. Z drugiej strony, pełna harmonizacja obejmująca również kwestie o wymiarze krajowym nie jest konieczna, mamy więc do czynienia z nieproporcjonalnością inicjatywy. Istniejąca Dyrektywa o Ochronie Danych – w interpretacji ETS – już teraz doprowadziła jednak do dużego stopnia harmonizacji, dlatego zmiana status quo może się wydawać bardziej problematyczna niż będzie w rzeczywistości.

Zgodność z prawem UE

Rodzaj i liczba uprawnień przyznanych Komisji jest nie do zaakceptowania z punktu widzenia zasady podziału władz. Kluczowe dla danej gałęzi prawa decyzje muszą być podejmowane przez samego ustawodawcę europejskiego (por. art. 290 TFEU). Co więcej, obecnie trudno jest przewidzieć dokładnie skutki reformy, biorąc pod uwagę liczne „luki" w tekście rozporządzenia.

Objęcie rozporządzeniem podmiotów przetwarzających dane osobowe spoza UE z prawnego punktu widzenia nie budzi wątpliwości. Państwa – w tym również UE – mogą stanowić podobne regulacje, pod warunkiem, że istnieje wystarczająco mocny materialny związek z ich terytorium. Praktyka prawa międzynarodowego oraz jego doktryna, podobnie jak rozstrzygnięcia ETS, pozwalają w tej kwestii na bardzo wiele (zobacz ostatni ETS, C-366/10, Stowarzyszenie Transportu Lotniczego Ameryki i inni, paragrafy 110, 121 i kolejne). Przewidziane w rozporządzeniu powiązanie kwestii regulowania działań tego rodzaju administratorów danych z kwestią siedziby podmiotów tych danych – szczególnie w przypadku wykorzystywania Internetu – nie wydaje się więc problematyczne. Wątpliwości nie budzi również rozszerzenie zakresu rozporządzenia na administratorów działających w UE, a przetwarzających dane poza jej granicami. Zupełnie inną kwestią jest egzekwowanie unijnych norm dotyczących ochrony praw w takich sytuacjach.

To, w jakich sytuacjach przetwarzanie danych przez administratora spoza UE „wiąże" się z oferowaniem dóbr i usług użytkownikom mającym siedzibę w UE, wymaga wyjaśnienia, szczególnie w odniesieniu do rzeczywistości internetowej. Podobne kłopoty sprawia określenie różnic w zakresie jurysdykcji nad umowami konsumenckimi (por. ECJ, C-585/08 i inne, Pammer).

„Prawo do przenoszenia danych" stworzono głównie w związku z rzeczywistością internetową (np. sieciami społecznościowymi), jego zakres niepotrzebnie sięga jednak dużo dalej.

**Zasada, zgodnie z którą zgoda podmiotu danych nie uprawnia do przetwarzania danych w sytuacji, gdy mamy do czynienia ze „znaczącą nierównowagą" pomiędzy pozycją administratora i podmiotu danych jest nieprecyzyjna, budzi więc wątpliwości. Nie jest na przykład jasne, czy taka „znacząca nierównowaga" występuje w relacjach pomiędzy towarzystwem ubezpieczeniowym i jego klientami. W praktyce – poza uzyskaną zgodą - często nie będzie istnieć żadna inna podstawa prawna do przetwarzania danych związanych ze zdrowiem** (por. art. 81, art. 9 (2) lit. h), choć przetwarzanie tych danych jest ważne w przypadku wielu ubezpieczeń. Dlatego też wspomniany przepis powinien zostać zrewidowany – powinno się co najmniej wymienić przykłady [nierównowagi – przyp. tłum.], bowiem za przetwarzanie danych bez zgody grożą wysokie grzywny (art. 79 (6) lit. a). To samo dotyczy niejasnych i niespójnych przepisów o wyznaczeniu inspektora ochrony danych w przedsiębiorstwach zatrudniających mniej niż 250 pracowników (art. 79 (6), lit. j). Rozporządzenie dopuszcza doprecyzowanie przepisów przez samą Komisję (art. 35 (11) w powiązaniu z art. 86).

Przepisy dotyczące ochrony danych osobowych pracowników są dość tajemnicze: z jednej strony Komisja podkreśla, że celem jest harmonizacja, podczas gdy z drugiej strony postanawia złagodzić istniejące przepisy dotyczące harmonizacji w tej dziedzinie (por. ETS, C-468 i inne, ASNEF) – chociaż „tylko w granicach niniejszego Rozporządzenia", a nawet przyznaje sobie prawo wydawania aktów delegowanych (art. 82 (3)). Z tego względu w przyszłości krajowe prawodawstwo w tej dziedzinie napotka na poważne kłopoty.

Kwestia pozwów zbiorowych też budzi wątpliwości – uprawnione do ich składania organy, organizacje i stowarzyszenie nie muszą bowiem spełniać żadnych warunków (poza raczej nieokreślonym obowiązkiem działania w celu ochrony danych i zarejestrowania zgodnego z prawem Państwa Członkowskiego).

## WNIOSKI

Ujednolicenie prawa o ochronie danych i przyznanie krajowym władzom publicznym kompetencji obejmujących całą UE zmniejszy koszty ponoszone przez zainteresowanych przedsiębiorców i stworzy równe warunki konkurowania. Rodzaj i liczba kompetencji przyznanych Komisji jest nie do zaakceptowania z punktu widzenia zasady podziału władz. Decyzje o kluczowym znaczeniu dla danej gałęzi prawa muszą być podejmowane przez sam europejski organ ustawodawczy. Przepisy dotyczące nieważności zgody są niekonkretne, co więcej, konieczne jest uwzględnienie konieczności przetwarzania danych dotyczących zdrowia. Regulacje dotyczące ochrony danych pracowników nie spowodują wzrostu zaufania do prawa.



**Autor:** Oliver Sauer
**CEP** | Kaiser-Joseph-Straße 266, 79098 Freiburg | Niemcy | tel. +49 (0)761 38693-105 | www.cep.eu
**Tłumaczenie:** Krzysztof Szwałek

**Polska wersja analizy powstała dzięki Fundacji FOR**
**FOR** | Al. Szucha 2/4 lok. 20, 00-582 Warszawa | Polska | tel. +48 22 427 40 10 | www.for.org.pl