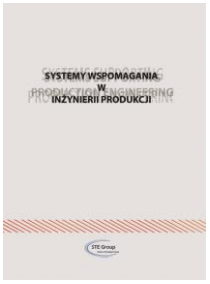
Naruszenie ochrony danych osobowych. Obowiązki administratora

Data wpłynięcia do Redakcji: 12/2021
Data akceptacji przez Redakcję do publikacji: 12/2021

2021, volume 10, issue 1, pp. 11-19



Marzena Smolarska
FAMUR S.A., **Poland**

Streszczenie: W artykule przedstawiono wytyczne unijnego rozporządzenia oraz stanowisko polskiego organu nadzorczego dotyczące naruszeń ochrony danych osobowych i sposobu postępowania z nimi. Zdefiniowano obowiązki administratora oraz określono jak należy rozpatrywać incydenty bezpieczeństwa informacji i jak należy definiować naruszenie bezpieczeństwa danych osobowych osób fizycznych. Przedstawiono przesłanki naruszenia ochrony danych osobowych, opisano typy naruszeń oraz wymieniono przykładowe naruszenia. Jak istotna dla administratora danych jest dokumentacja w postaci procedur i ewidencji naruszeń. W artkule przedstawiono również proces zgłaszania naruszeń oraz opisano przypadki w których dochodzi do naruszenia danych. Zwrócono uwagę na konieczność zindywidualizowanego podejścia do wyjaśniania incydentów bezpieczeństwa informacji. Incydenty bezpieczeństwa w wyniku przeprowadzonej analizy ryzyka i określeniu poziomu tego ryzyka, mogą okazać się naruszeniem, zagrażającym przysługującym prawom, wolności lub możliwości sprawowania kontroli nad danymi osób fizycznych. Przedstawiono jak ogromne znaczenie ma ciągły monitoring zastosowanych środków bezpieczeństwa poprzez cykliczne audyty i analizę ryzyka. Jaką wartość ma dobrze przeprowadzone postępowanie wyjaśniające incydentu bezpieczeństwa danych osobowych.

Słowa kluczowe: administrator, analiza ryzyka, incydent bezpieczeństwa, naruszenie, organ nadzorczy, osoba fizyczna, unijne rozporządzenie, RODO

WPROWADZENIE

Obowiązki dotyczące naruszeń można spotkać nie tylko w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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) zwanym RODO ale i w innych aktach prawnych takich jak: Ustawa z dnia 16 lipca 2004 roku Prawo telekomunikacyjne (Dz. U. 2004.171.1800 z późn. zm.), Ustawa z dnia 14 grudnia 2018 roku o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. 2019.0.125) Rozporządzenie eIDAS – Rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania z odniesieniu do transakcji elektronicznych na rynku wewnętrznym, Ustawa z dnia 15 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018.1560).

Contact address: msmolarska@famur.com

Powyższe akty prawne nakładają na administratorów konkretne obowiązki związane z zgłaszaniem naruszeń do organów nadzorczych, powiadamianiem osób których dane dotyczą, stosowaniem środków bezpieczeństwa minimalizujących ryzyko utraty danych i kontroli nad nimi.

Czym jest naruszenie ochrony danych osobowych? Zgodnie z art. 4 pkt 12 RODO jest to „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych" [1].

O naruszeniu mówimy wtedy, kiedy spełnione są łącznie trzy przesłanki:

- naruszenie musi dotyczyć danych osobowych osoby fizycznej, które przetwarzane są przez administratora;
- skutkiem naruszenia może być zniszczenie, utrata, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych;
- naruszenie jest skutkiem niedostosowania się do przyjętych zasad bezpieczeństwa danych osobowych w przedsiębiorstwie [2].

Wyróżniamy trzy typy naruszeń ochrony danych osobowych:

- naruszenie poufności – polega na ujawnieniu danych osobowych nieuprawnionej osobie;
- naruszenie dostępności – polega na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych;
- naruszenie integralności – polega na zmianie treści danych osobowych w sposób nieautoryzowany [3].

Unijne rozporządzenie nakłada na administratora danych pewne obowiązki związane z naruszeniem ochrony danych osobowych a mianowicie:

- wprowadzenie procedur umożliwiających stwierdzenie i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych;
- prowadzenie rejestru naruszeń;
- zgłaszanie naruszeń organowi nadzorczemu jakim jest Prezes Urzędu Ochrony Danych Osobowych (PUODO);
- powiadomienie osoby, której dane dotyczą, o naruszeniu;
- podjęcie działań mających na celu przeciwdziałanie skutkom naruszenia i zapobieganie im w przyszłości.

Najistotniejszym elementem całego procesu związanego ze zgłaszaniem naruszeń ochrony danych odosobowych, jest niezwłoczne podjęcie działań, zarówno wobec osób, których dane dotyczą jak i wobec organu nadzorczego [2].

ZGŁASZANIE NARUSZEŃ ORGANOWI NADZORCZEMU

Zanim administrator podejmie decyzję, czy zgłaszać naruszenie ochrony danych osobowych do PUODO, czy nie musi przede wszystkim zastanowić się czy doszło do naruszenie praw i wolności osoby fizycznej, której naruszenie dotyczy. Analizując definicję naruszenia ochrony danych osobowych należy zwrócić uwagę że nie każde zdarzenie, które uznane zostanie za incydent bezpieczeństwa

informacji będzie naruszeniem. Zatem w jakich sytuacjach dochodzi do naruszenia ochrony danych osobowych osoby fizycznej:

- osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw lub wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi;
- przetwarzaniu podlegają dane szczególnie chronione, czyli dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie, przekonania światopoglądowe lub przynależność do związków zawodowych, a także dane genetyczne, dotyczące zdrowia, seksualności, wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa;
- dochodzi do zautomatyzowanego przetwarzania danych, w tym profilowania;
- przetwarzane są dane osób wymagających szczególnej opieki, zwłaszcza dzieci;
- przetwarzanie danych odbywa się na dużą skalę i wpływa na znaczną liczbę osób, których dane dotyczą.

Ustalając, czy ryzyko naruszenia praw lub wolności osób fizycznych jest niskie czy wysokie, należy uwzględnić: charakter, zakres, kontekst i cele przetwarzania danych osobowych [4].

Pewien katalog naruszeń zawiera formularz zgłoszeniowy na stronie PUODO, który można wykorzystać zgłaszając naruszenie ochrony danych osobowych.

Wśród naruszeń ochrony danych autorzy formularza wymieniają:

- zgubienie lub kradzież nośnika lub urządzenia;
- zgubienie, kradzież lub pozostawienie w niezabezpieczonej lokalizacji dokumentacji papierowej, która zawiera dane osobowe;
- utratę przez operatora pocztowego korespondencji papierowej lub otwarcie jej przed zwróceniem nadawcy;
- nieuprawnione uzyskanie dostępu do informacji;
- nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń;
- pojawienie się złośliwego oprogramowania, które ingeruje w poufność, integralność i dostępność danych;
- uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, tj. drogą e-mailową lub za pomocą komunikatora internetowego (phishing);
- nieprawidłową anonimizację danych osobowych w dokumencie;
- nieprawidłowe usunięcie lub zniszczenie danych osobowych z nośnika lub urządzenia elektronicznego przed jego zbyciem przez administratora;
- niezamierzoną publikację;
- wysłanie danych osobowych do niewłaściwego odbiorcy;
- ujawnienie danych niewłaściwej osoby;
- ustne ujawnienie danych osobowych [4].

Wytyczne co do zgłaszania naruszeń wynikają z art. 33 RODO – Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu.

1. Administrator danych bez zbędnej zwłoki, nie później niż w terminie 72 h po stwierdzeniu naruszenia zobligowany jest dokonać zgłoszenia organowi nadzorczemu. Jeżeli zgłoszenie nastąpi po tym czasie administrator musi dołączyć wyjaśnienie przyczyn opóźnienia.

Zgłoszenie musi co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
3. Jeżeli administrator nie jest w stanie dostarczyć informacji w tym samym czasie w pełnym zakresie może to zrobić sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze [1].

Administrator danych chcąc zapewnić odpowiedni poziom bezpieczeństwa danych oraz sposobu postępowania z naruszeniami danych osobowych zobligowany jest do wdrożenia procedury zarządzania naruszeniami ochrony danych osobowych oraz prowadzenia rejestru naruszeń. Celem procedury powinno być całościowe przedstawienie procesu zarządzania naruszeniami w organizacji oraz zapewnienie, że

- analiza każdego naruszenia będzie realizowana w terminie nieprzekraczającym 72 godzin od powzięcia informacji o wystąpieniu naruszenia ochrony danych osobowych;
- informacja o wystąpieniu Naruszenia ochrony danych osobowych będzie przekazywana niezwłocznie niezależnie od źródła;
- wyniki oceny naruszenia ochrony danych osobowych będą wykorzystywane do doskonalenia mechanizmów ochrony danych osobowych w organizacji;
- w stosownych przypadkach informacja o wystąpieniu naruszenia ochrony danych osobowych będzie przekazywana do organu nadzorczego ds. ochrony danych osobowych oraz podmiotu danych.

Procedura powinna określać role i zadania osób odpowiedzialnych za proces zarządzania naruszeniami ochrony danych osobowych jak i pracowników zgłaszających incydenty bezpieczeństwa informacji, opis zdarzeń naruszających

ochronę danych oraz opis postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych.

Szczególnie istotnym elementem regulacyjnym obszar naruszeń jest ich ewidencjonowanie

i monitorowanie wdrożonych środków ochrony. W rejestrze naruszeń zapisuje się wszystkie naruszenia ochrony danych wskazując następujące informacje:

- numer naruszenia,
- data wystąpienia naruszenia,
- data i czas stwierdzenia naruszenia,
- data powiadomienia przez podmiot przetwarzający,
- data zakończenia naruszenia,
- źródło informacji/sposób zgłoszenia,
- kategoria danych których dotyczy naruszenie,
- kategoria osób których dane dotyczą,
- charakter naruszenia (poufność, integralność, dostępność),
- na czym polegało naruszenie,
- przyczyna naruszenia,
- środki bezpieczeństwa zastosowane przed naruszeniem,
- konsekwencje naruszenia,
- ryzyko naruszenia praw i wolności osób fizycznych (niskie, średnie, wysokie),
- komunikacja z osobami, których dane dotyczą,
- środki zaradcze – termin realizacji/osoby odpowiedzialne,
- ocena skuteczności wdrożenia środków zaradczych,
- treść decyzji narządu/administratora,
- zgłoszenie naruszenia do organu nadzorczego ds. ochrony danych osobowych.

Procedura naruszeń ochrony danych osobowych powinna również uwzględniać sposób raportowania naruszeń do administratora danych. Należy pamiętać, że zalecenia wskazywane w ramach wydawanych rekomendacji podlegają monitorowaniu i powinny być weryfikowane niezwłocznie po wskazanym terminie implementacji.

Obowiązek zgłaszania naruszeń do organu nadzorczego ma wyłącznie administrator. Natomiast podmiot przetwarzający zobligowany jest do zawiadomienia o zdarzeniu właściwego administratora, którego dane przetwarza na podstawie umowy powierzenia przetwarzania danych osobowych. Ponadto podmiot przetwarzający ma obowiązek ustalenia okoliczności naruszenia i niezwłocznego przekazania tych informacji administratorowi, na którego zlecenie dokonuje przetwarzania.

Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

Zgłoszenia można dokonać na 4 sposoby:

1. Elektronicznie poprzez wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie biznes.gov.pl.,

2. Elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP – UODO/SkrytkaESP,
3. Elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl lub platformie epuap.gov.pl,
4. Tradycyjną pocztą wysyłając wypełniony formularz na adres Urzędu.

Jeżeli naruszenie dotyczy danych osób w różnych krajach UE, Prezes UODO może być, ale nie musi być wiodącym (czyli właściwym dla administratora lub podmiotu przetwarzającego) organem nadzorczym. W przypadku transgranicznego naruszenia danych administrator powinien dokonać analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem jest Prezes UODO, czy też może inny europejski organ nadzorczy [5].

ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ

Administrator podczas postępowania wyjaśniającego zaistniałego incydentu za pomocą dostępnych mu środków zobligowany jest podjąć decyzję co do zgłoszenia naruszenia do PUODO jak i powiadomienia osoby, której naruszenie dotyczy. Jeżeli incydent może skutkować wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, administrator musi dokonać takiego zgłoszenia nie tylko do organu nadzorczego ale i powiadomić osobę której dane dotyczą. Zawiadomienie o naruszeniu ochrony danych osobowych powinno zawierać opis zdarzenia, jaki zakres danych został ujawniony, możliwe konsekwencje dla osoby fizycznej, której dane zostały ujawnione, jakie działania podjął administrator aby zminimalizować negatywne skutki naruszenia oraz wskazówki dla osoby poszkodowanej co może zrobić.

W zawiadomieniu należy również podać dane kontaktowe inspektora ochrony (jeżeli został on wyznaczony) lub wskazać inny punkt kontaktowy, od którego osoba zainteresowana będzie mogła uzyskać więcej informacji.

Prezes UODO w zawiadomieniu osoby, której dane dotyczą kładzie szczególny nacisk na szczegółowe wyjaśnienie tej osobie ewentualnych konsekwencji naruszenia bezpieczeństwa jej danych osobowych, np. m. in.:

- uzyskanie przez osoby trzecie kredytów w instytucjach poza bankowych;
- dokonanie zakupów w systemie ratalnym;
- uzyskanie dostępu do danych o stanie zdrowia, w przypadku przełamania zabezpieczeń do systemu świadczeń opieki zdrowotnej lub korzystania ze świadczeń opieki zdrowotnej;
- założenie konta internetowego (np. w serwisach społecznościowych);
- korzystanie z praw obywatelskich np. wykorzystanie pozyskanych danych do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego;
- wyłudzenie ewentualnego ubezpieczenia lub środków z ubezpieczenia;
- zawarcie umów cywilno-prawnych, np. najmu nieruchomości;
- możliwość uzyskania tzw. dowodu kolekcjonerskiego, który na pierwszy rzut oka trudno odróżnić od dowodu będącego autentycznym dokumentem

tożsamości, co w konsekwencji może skutkować przejęciem karty SIM do telefonu, a co za tym idzie umożliwia uzyskanie dostępu do konta bankowego bądź innych usług powiązanych z numerem telefonu;
- wykorzystanie danych do zarejestrowania karty telefonicznej typu pre-paid, która może posłużyć do celów przestępczych.

Prezes UODO zwraca również uwagę na konieczność używania prostego i jasnego języka w korespondencji pomiędzy administratorem danych a osoba fizyczną do której adresowane jest zawiadomienie o naruszeniu danych. Jest to organ który badając zgłoszenie o naruszeniu w każdej chwili może zobligować swoim wystąpieniem administratora danych do ponownego zawiadomienia osoby, której dotyczy naruszenie i doprecyzowania ewentualnych konsekwencji naruszenia oraz propozycji działań w celu zaradzenia naruszeniu i zminimalizowaniu jego negatywnych skutków.

Zgodnie z art. 34 ust. 3 RODO zawiadomienie osób, których dane dotyczą, nie jest konieczne jeżeli:
- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie,

w szczególności środki takie jak szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
- administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób [1].

Jeżeli administrator nie zawiadomił osoby (której dane dotyczą), o naruszeniu ochrony danych osobowych, Prezes UODO może od niego tego zażądać, w przypadku gdy stwierdzi, że incydent może skutkować wysokim ryzykiem naruszenia praw lub wolności osób fizycznych. Organ nadzorczy może również stwierdzić, że spełniony został jeden z warunków, o których mowa powyżej.

Ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono, np. dyskryminacją, kradzieżą tożsamości lub oszustwo dotyczące tożsamości, nadużyciami finansowymi, stratami finansowymi, nieuprawnionym cofnięciem pseudonimizacji, utratą poufności danych osobowych chronionych tajemnicą zawodową, naruszeniem dobrego imienia lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej. Ponadto wysokie prawdopodobieństwo takiej szkody występuje jeżeli naruszenie dotyczy danych osobowych szczególnie chronionych, ujawniających: pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane dotyczące zdrowia, dane dotyczące życia seksualnego [1].

WNIOSKI

RODO wymaga podjęcia konkretnych kroków w związku z naruszeniem ochrony danych osobowych. W przypadku każdego incydentu bezpieczeństwa informacji administrator powinien podjąć działania, które będą zapobiegać ewentualnym naruszeniom w przyszłości, a mianowicie: oszacować ryzyko utraty przysługujących praw i wolności osób fizycznych, których dotyczy naruszenie, zbadać czy naruszenie było wynikiem świadomej, czy nieświadomej działalności człowieka, czy też przyczyną naruszenia były problemy systemów informatycznych w których dane są przetwarzane. Analizując powyższe działania administrator powinien wdrożyć odpowiednie środki prawne, organizacyjne oraz techniczne w tym informatyczne i fizyczne, które w sposób zadawalający zminimalizują ryzyko bezprawnego zniszczenia, utraty, zmiany, nieuprawnionego dostępu do przetwarzanych danych osobowych. Wdrożone zabezpieczenia powinny być efektywne dlatego też muszą być na bieżąco sprawdzane i monitorowane aby móc zachować poufność, integralność i dostępność danych osobowych. Doskonałym narzędziem monitoringu ochrony danych osobowych w przedsiębiorstwie jest audyt. Wyniki z audytu powinny być przedstawione administratorowi danych a działania poaudytowe doskonalące istniejące zabezpieczenia wdrożone bez zbędnej zwłoki. Nie należy zapominać również o analizie ryzyka. Przeprowadzona analiza ryzyka podczas wyjaśniania incydentu bezpieczeństwa informacji pozwala nie tylko na jego sklasyfikowanie jako naruszenie ochrony danych osobowych ale przede wszystkim umożliwia zidentyfikowanie podatności w systemie zabezpieczeń.

Warto wskazać na edukacyjną rolę postępowania wyjaśniającego incydenty bezpieczeństwa danych osobowych, przeprowadzonego w sposób prawidłowy i transparentny. Tak przeprocedowany incydent jest wartością umożliwiającą nie tylko poprawę systemu ochrony danych osobowych ale i stanowi materiał na budowanie szeroko pojętej świadomości wśród pracowników i kadry kierowniczej organizacji.

LITERATURA

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 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).
[2] Obowiązki administratorów związane z naruszeniami ochrony danych osobowych. Urząd Ochrony Danych Osobowych, wersja 1.0, 2019.
[3] Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP rev.01).
[4] https://gdpr.pl/naruszenie-ochrony-danych-osobowych
[5] https://uodo.gov.pl/pl/134/233

Breach of personal data protection. Administrator's obligations

Abstract: The article presents the guidelines of the EU regulation and the position of the Polish supervisory authority regarding personal data breaches and the manner of dealing with them. The article points out Controller's responsibilities, manners to handle information about security incidents and ways to define a personal data breach. The article also presents reasons that cause violation of personal data protection, the types of violations and examples of such violations. Importance of documentation and the form of procedures is pointed, as a basic obligation for the Controller (for ex. records of violations). The article also covers the breach notification process and describes the cases of data breaches. The necessity of an individualized approach to explaining information security incidents was emphasized. Security incidents as a result of the conducted risk analysis and determination of the level of this risk may turn out to be a violation, that threatens the rights, freedoms or the ability to exercise control over the data of natural persons. It is accentuated how important is the continuous monitoring of the applied security measures through periodic audits and risk analysis. What is the value of a well-conducted investigation of a personal data security incident.

Keywords: controller, risk analysis security incident, breach, supervisory authority, natural person, EU regulation, GDPR

mgr Marzena Smolarska
FAMUR S.A.
ul. Armii Krajowej 51
40-698 Katowice, Poland
tel.: +48 781 550 418
e-mail: msmolarska@famur.com