KOMISJA EUROPEJSKA

DYREKCJA GENERALNA DS. KONKURENCJI

Ostatnia aktualizacja: marzec 2024 r.

Nota objaśniająca na temat kontroli przeprowadzanych przez Komisję na podstawie art. 20 ust. 4 rozporządzenia Rady (WE) nr 1/2003

Nota ma jedynie charakter informacyjny i pozostaje bez uszczerbku dla formalnej wykładni uprawnień Komisji Europejskiej w zakresie prowadzenia postępowań.

1) Przedsiębiorstwa ([1]) są prawnie zobowiązane do podporządkowania się kontroli zarządzonej decyzją Komisji zgodnie z art. 20 ust. 4 rozporządzenia Rady (WE) nr 1/2003. Pisemne upoważnienia służą do wskazania nazwisk urzędników i innych osób towarzyszących upoważnionych przez Komisję do przeprowadzenia kontroli („inspektorzy"). Każdy z inspektorów zobowiązany jest przedstawić dokument tożsamości.

2) Od inspektorów nie można wymagać dodatkowych informacji na temat przedmiotu kontroli, który określono w decyzji, ani jakiegokolwiek uzasadnienia decyzji. Mogą oni jednak wyjaśniać kwestie proceduralne, na przykład w odniesieniu do poufności lub danych osobowych, oraz ewentualne konsekwencje odmowy poddania się kontroli.

3) Poświadczona kopia decyzji powinna zostać przekazana przedsiębiorstwu. Protokół z powiadomienia o decyzji służy jedynie do potwierdzenia jej doręczenia, a podpisanie go przez odbiorcę nie oznacza podporządkowania się kontroli.

4) Zgodnie z art. 20 ust. 2 rozporządzenia (WE) nr 1/2003 inspektorzy mają prawo do:

   a) wchodzenia do wszelkich pomieszczeń, na teren i do środków transportu należących do przedsiębiorstwa;

   b) sprawdzania ksiąg i innych rejestrów dotyczących działalności przedsiębiorstwa, bez względu na sposób ich przechowywania;

   c) pobierania lub uzyskiwania w każdej formie kopii lub wyciągów z tych ksiąg lub rejestrów;

   d) pieczętowania wszelkich pomieszczeń, ksiąg lub rejestrów przedsiębiorstwa na czas i w zakresie koniecznym do przeprowadzenia kontroli;

   e) zadawania pytań przedstawicielom pracowników lub pracownikom przedsiębiorstwa w celu uzyskania wyjaśnień co do faktów lub dokumentów dotyczących przedmiotu kontroli oraz do rejestrowania odpowiedzi.

([1]) Pojęcie „przedsiębiorstwo" obejmuje zarówno przedsiębiorstwa, jak i związki przedsiębiorstw.

5) Urzędnicy i inne osoby towarzyszące upoważnieni lub wyznaczeni przez organ ochrony konkurencji państwa członkowskiego, na którego terytorium jest przeprowadzana kontrola, mogą aktywnie pomagać inspektorom w wypełnianiu ich obowiązków. W tym celu, zgodnie z art. 20 ust. 2 rozporządzenia (WE) nr 1/2003, przysługują im te same uprawnienia co inspektorom (zob. pkt 4 powyżej).

6) Przedsiębiorstwo może podczas kontroli **konsultować się z zewnętrznym radcą prawnym**. Obecność radcy prawnego w miejscu kontroli nie jest jednak warunkiem zgodności z prawem takiej kontroli. Inspektorzy mogą wchodzić do pomieszczeń, powiadamiać o decyzji nakazującej kontrolę i zajmować wybrane przez siebie biura, nie czekając, aż przedsiębiorstwo skonsultuje się ze swoim radcą prawnym. Niezależnie od przypadku, inspektorzy będą godzić się tylko na niewielkie opóźnienie w oczekiwaniu na konsultacje z radcą prawnym przed rozpoczęciem badania ksiąg i innych rejestrów dotyczących działalności, sporządzaniem kopii lub wyciągów z tych dokumentów, pieczętowaniem w razie potrzeby pomieszczeń, ksiąg lub rejestrów przedsiębiorstwa lub zwracaniem się o przedstawienie ustnych wyjaśnień. Wszelkie tego rodzaju opóźnienie musi być ograniczone do absolutnego minimum.

7) Jeżeli na żądanie inspektorów przedstawiciel lub pracownik przedsiębiorstwa składa, zgodnie z art. 4 ust. 1 rozporządzenia Komisji (WE) nr 773/2004, **ustne wyjaśnienia** na miejscu dotyczące faktów lub dokumentów związanych z przedmiotem kontroli, wyjaśnienia te mogą być rejestrowane w dowolnej formie. Kopia takiego zapisu zostanie udostępniona zainteresowanemu przedsiębiorstwu po zakończeniu kontroli, zgodnie z art. 4 ust. 2 rozporządzenia (WE) nr 773/2004.

8) W przypadkach, gdy o wyjaśnienia został poproszony pracownik przedsiębiorstwa, który nie jest lub nie był upoważniony przez przedsiębiorstwo do składania wyjaśnień w imieniu przedsiębiorstwa, Komisja wyznacza termin, w którym przedsiębiorstwo może zgłosić Komisji dowolne sprostowanie, zmianę lub uzupełnienie do wyjaśnień złożonych przez takiego pracownika, które następnie zostaną dodane do wyjaśnień zarejestrowanych podczas kontroli.

9) Inspektorzy są uprawnieni do badania wszelkich ksiąg i rejestrów dotyczących działalności, niezależnie od nośnika, na jakim są one przechowywane, oraz do pobierania lub uzyskiwania, w dowolnej formie, kopii lub wyciągów z tych ksiąg lub rejestrów. Obejmuje to badanie informacji elektronicznych oraz sporządzanie elektronicznych lub papierowych kopii takich informacji. Przedstawiciele przedsiębiorstwa są uprawnieni do obserwowania działań podejmowanych przez inspektorów bez ingerowania w ich pracę.

10) Inspektorzy mogą przeszukiwać środowisko informatyczne (np. usługi chmury, serwery, komputery stacjonarne, laptopy, tablety i inne urządzenia mobilne) przedsiębiorstwa oraz wszystkie należące do niego nośniki danych (np. zewnętrzne urządzenia pamięciowe, taśmy zapasowe, klucze USB, płyty CD-ROM, DVD). Ma to również zastosowanie do urządzeń oraz nośników prywatnych wykorzystywanych w celach zawodowych (według modelu BYOD – Przynieś własny sprzęt), jeśli takowe znaleziono na miejscu. W tym celu inspektorzy mogą korzystać z wszelkich wbudowanych funkcji w systemach informatycznych i infrastrukturze informatycznej przedsiębiorstwa. Mogą także korzystać z własnego specjalistycznego oprogramowania lub sprzętu komputerowego

(„narzędzia informatyki śledczej”). Narzędzia te umożliwiają Komisji, zgodnie z art. 20 ust. 2 lit. b) rozporządzenia (WE) nr 1/2003, kontrolę systemów i danych przedsiębiorstwa, w szczególności poprzez tworzenie dokładnych duplikatów danych, w tym danych odzyskanych, oraz przeszukiwanie takich duplikatów przy jednoczesnym poszanowaniu integralności systemów i danych przedsiębiorstw.

11) Przedsiębiorstwo jest zobowiązane do pełnej i aktywnej współpracy z inspektorami. Oznacza to, że przedsiębiorstwo może zostać poproszone o oddelegowanie przedstawicieli pracowników lub pracowników do pomocy inspektorom. Obejmuje to nie tylko obowiązek udzielania wyjaśnień na temat organizacji przedsiębiorstwa i jego środowiska informatycznego, ale również wykonywanie konkretnych zadań, takich jak wprowadzanie specjalnych poleceń do systemów informatycznych w celu zgromadzenia informacji, wykorzystywanie wbudowanych narzędzi typu „Litigation hold”, czasowe blokowanie indywidualnych kont użytkowników, czasowe odłączanie komputerów od sieci, usuwanie i ponowna instalacja napędów w komputerach oraz udzielanie wsparcia na poziomie praw dostępu administratora. Jeżeli takie działania są podejmowane, przedsiębiorstwo nie może w żadnym wypadku przeszkadzać w ich realizacji; jego obowiązkiem jest także poinformowanie pracowników, dla których działania te mogą mieć jakieś następstwa. Inspektorzy mogą wystąpić do przedsiębiorstwa o skorzystanie z jego sprzętu (np. nośników pamięci, kluczy USB, kabli przyłączeniowych, skanerów, drukarek, ekranów), ale nie mogą być zobowiązani do korzystania z takiego sprzętu. Na żądanie kontrolowane przedsiębiorstwo informuje inspektorów o sposobie realizacji ich wniosków, przekazując rejestry lub informując inspektorów o instrukcjach wydawanych pracownikom przedsiębiorstwa odpowiedzialnym za realizację wniosków inspektorów.

12) Nośniki danych, które zostały wybrane do zbadania, mogą pozostawać pod kontrolą inspektorów do czasu zakończenia kontroli w pomieszczeniach przedsiębiorstwa. Mogą one zostać zwrócone wcześniej, np. po wykonaniu czytelnej i dokładnej kopii binarnej danych objętych postępowaniem. Kopia taka stanowi dokładny duplikat (części lub wszystkich) danych przechowywanych na oryginalnym nośniku. Zbadanie dokładnego duplikatu jest równoważne zbadaniu oryginalnego nośnika.

13) Od momentu powiadomienia o decyzji w sprawie kontroli przedsiębiorstwo działa ze szczególną starannością i podejmuje wszelkie właściwe środki w celu zabezpieczenia dostępnych mu dowodów. Informowanie pracowników i przedstawicieli pracowników o podejmowanych działaniach należy do obowiązków przedsiębiorstwa. Usunięcie dokumentacji przedsiębiorstwa (lub manipulowanie nią), zarówno umyślne, jak i przypadkowe, może być uznane za utrudnianie Komisji przeprowadzenia kontroli. Jeśli dochodzi do takiego utrudniania, Komisja może nałożyć na przedsiębiorstwo grzywnę w wysokości do 1 % jego całkowitego obrotu w poprzednim roku obrotowym.

14) Obowiązek zabezpieczenia dowodów wykracza poza sam czas trwania kontroli na miejscu ([2]).

([2]) Zob. w tym kontekście wyrok z dnia 9 kwietnia 2019 r. w sprawie T-371/17, Qualcomm i Qualcomm Europe/Komisja, EU:T:2019:232, pkt 136, utrzymany w mocy w postępowaniu odwoławczym w sprawie C-466/19 P, Qualcomm i Qualcomm Europe/Komisja, EU:C:2021:76, pkt 114.

15) Na zakończenie kontroli inspektorzy dokładnie czyszczą ([3]) wszystkie nośniki danych Komisji, na których były przechowywane dane przedsiębiorstwa. Sprzęt komputerowy udostępniany przez przedsiębiorstwo nie jest czyszczony przez inspektorów, ale zwracany przedsiębiorstwu.

16) Jeżeli w planowanym terminie zakończenia kontroli w pomieszczeniach przedsiębiorstwa nie zakończono wyboru dokumentów na potrzeby postępowania, Komisja może mieć uzasadnione powody, by zdecydować, również w interesie zainteresowanego przedsiębiorstwa, o kontynuowaniu kontroli danych, które zgromadziła od przedsiębiorstwa, w siedzibie Komisji w Brukseli. W takim przypadku, oprócz zbioru danych już zbadanych, pobrana może zostać kopia niezbadanych jeszcze danych w celu przeprowadzenia kontroli w późniejszym terminie. Kopia ta zostanie zabezpieczona poprzez umieszczenie w opieczętowanej kopercie, która zostanie zabrana do siedziby Komisji w Brukseli. Komisja zaprosi przedsiębiorstwo do: (i) uczestniczenia w otwarciu opieczętowanej koperty oraz (ii) w dalszej kontroli w pomieszczeniach Komisji. Jeżeli kontynuacja kontroli oznacza dodatkowe koszty dla kontrolowanego przedsiębiorstwa, wynikające wyłącznie z takiej kontynuacji, przedsiębiorstwo to może domagać się zwrotu tych kosztów w drodze należycie uzasadnionego wniosku. Komisja może również zwrócić przedsiębiorstwu opieczętowaną kopertę bez jej otwierania. Komisja może także zwrócić się do przedsiębiorstwa o przechowanie zapieczętowanej koperty w bezpiecznym miejscu, tak aby móc kontynuować proces przeszukiwania w pomieszczeniach przedsiębiorstwa w trakcie kolejnej zapowiedzianej wizyty.

17) Przedsiębiorstwo będzie miało możliwość dokonania przeglądu tymczasowych zbiorów danych wybranych przez inspektorów, które mają zostać dodane do akt sprawy, w celu ustalenia, czy chce podnosić roszczenia dotyczące np. danych potencjalnie chronionych przez prawniczą tajemnicę zawodową lub szczególnych kategorii danych osobowych ([4]). Na tym etapie przedsiębiorstwo może również zgłosić uwagi, jeżeli uważa, że dane wybrane przez inspektorów, które mają zostać dodane do akt sprawy, nie mają związku z przedmiotem decyzji w sprawie kontroli. Jeśli chodzi o zbiory danych ostatecznie wybrane przez inspektorów podczas kontroli na miejscu (lub w ramach kontynuacji kontroli), które zostają włączone do gromadzonych przez Komisję akt sprawy, przedsiębiorstwo otrzyma nośnik danych (np. klucz USB), na którym wszystkie te zbiory danych są zarejestrowane. Przedsiębiorstwo zostanie poproszone o podpisanie ostatecznych list eksportowych wybranych danych. Inspektorzy zabierają ze sobą dwie identyczne kopie takich zbiorów danych zarejestrowane na zakodowanych nośnikach danych.

18) Elementy materiału dowodowego wybrane w toku kontroli mogą zostać pobrane w całości (jeżeli wybrany jest np. tylko jeden załącznik do wiadomości elektronicznej, wówczas ostateczny eksport obejmuje samą wiadomość wraz ze

([3]) Technicznym terminem na określenie takiego czyszczenia jest „sanityzacja” (zwana również „bezpiecznym wymazywaniem”). Celem sanityzacji jest całkowite usunięcie danych z nośnika danych, tak aby niemożliwe było ich odzyskanie za pomocą jakichkolwiek znanych technik.

([4]) Zob. art. 10 ust. 1 rozporządzenia (UE) 2018/1725, w którym „szczególne kategorie danych osobowych” zdefiniowano jako dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne lub biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia lub dane dotyczące życia seksualnego lub orientacji seksualnej osoby fizycznej. Zob. również art. 9 ust. 1 rozporządzenia (UE) 2016/679.

wszystkimi załącznikami, które są do niej załączone). W trakcie ostatecznego przetworzenia danych w celu umieszczenia w aktach sprawy każdy element materiału dowodowego może zostać podzielony na części składowe (np. główna wiadomość elektroniczna, załączniki lub inne wbudowane dane), które mogą zostać ujęte w wykazie oddzielnie i otrzymać odpowiednie indywidualne numery referencyjne.

19) Jeżeli przedsiębiorstwo udostępnia na wniosek inspektorów materiały do sporządzania kopii, wówczas Komisja, na wniosek przedsiębiorstwa, zwróci koszty materiałów wykorzystanych do sporządzenia kopii dla Komisji.

20) Do dokumentów skopiowanych podczas kontroli mają zastosowanie przepisy art. 28 rozporządzenia (WE) nr 1/2003 dotyczące tajemnicy służbowej. Jeżeli na późniejszym etapie postępowania zajdzie konieczność udostępnienia tych dokumentów osobom trzecim, np. w celu zapewnienia dostępu do akt, przedsiębiorstwo zostanie poproszone o zidentyfikowanie ewentualnych tajemnic handlowych lub innych informacji poufnych zawartych w dokumentach, uzasadnienie swojej decyzji oraz przekazanie wersji dokumentów nieobjętych klauzulą poufności.

21) W przypadku opieczętowania pomieszczeń, ksiąg lub rejestrów przedsiębiorstwa przez inspektorów sporządzany jest protokół. Przedsiębiorstwo zobowiązane jest dopilnować, by założone pieczęci pozostały nienaruszone do czasu ich usunięcia przez inspektorów. W momencie zdjęcia pieczęci sporządzony zostanie odrębny protokół, w którym umieszczona zostanie informacja o stanie pieczęci na ten moment.

22) Rozporządzenie (UE) 2018/1725 ma zastosowanie do danych osobowych zgromadzonych przez Komisję podczas postępowań z zakresu ochrony konkurencji. Ponieważ unijne zasady ochrony konkurencji mają zastosowanie jedynie do przedsiębiorstw, dane osobowe osób fizycznych jako takich nie są objęte postępowaniami ani kontrolami prowadzonymi przez Komisję w celu ochrony konkurencji. Dane osobowe pracowników przedsiębiorstwa (np. imiona i nazwiska, numery telefonów, adresy poczty elektronicznej) mogą jednak znaleźć się w dokumentach biznesowych związanych z takimi postępowaniami i mogą być w związku z tym kopiowane lub uzyskiwane podczas kontroli oraz mogą zostać włączone do akt Komisji.

23) Wszystkie dane osobowe z akt Komisji w sprawach z zakresu ochrony konkurencji mogą być wykorzystywane wyłącznie do celów, dla których zostały zgromadzone (wykonanie art. 101 lub art. 102 TFUE) i będą przetwarzane zgodnie z przepisami rozporządzenia (UE) 2018/1725, jak określono w oświadczeniu DG ds. Konkurencji o ochronie prywatności ([5]).

24) Jeżeli zestaw(-y) danych udostępniany(-e) inspektorom obejmuje(-ą) szczególne kategorie danych osobowych ([6]), przedsiębiorstwo powinno powiadomić inspektorów o obecności takich szczególnie chronionych danych osobowych, wskazując w szczególności, o które akta lub dane chodzi. Inspektorzy dołożą

([5]) Zob. https://competition-policy.ec.europa.eu/system/files/2021-05/privacy_statement_antitrust_pl.pdf

([6]) Zob. przypis 4 powyżej.

starań, aby przegląd takiej dokumentacji odbywał się w ramach odrębnej procedury ze względu na wrażliwość takich danych.