

Warszawa, 26 marca 2023 r.

Szanowny Pan  
Józef Orzeł  
Przewodniczący  
Rady do Spraw Cyfryzacji

## WEZWANIE DO ZANIECHANIA NARUSZEŃ DÓBR OSOBISTYCH

Działając w imieniu Huawei Polska sp. z o.o. związku z informacjami o planach przyjęcia *Stanowiska Rady ds. Cyfryzacji na temat nakazu usunięcia aplikacji TikTok przez urzędników i pracowników administracji publicznej z telefonów służbowych oraz zagrożeń ze strony Dostawców Wysokiego Ryzyka* (dalej „Stanowisko”),  
wzywam Pana na podstawie art. 24 w zw. z art. 43 kodeksu cywilnego (dalej „k.c.”) do natychmiastowego usunięcia i zaprzestania rozpowszechnienia nieprawdziwych informacji ze Stanowiska dotyczących Huawei, w szczególności odnoszących się do:

1. **wspierania przez Huawei władz Chin i ich służb wywiadowczych w gromadzeniu danych:** (...)  
*chińskie firmy technologiczne, w tym aplikacja TikTok, mogą wspierać władze Chin i ich służby wywiadowcze w gromadzeniu ogromnych ilości danych na całym świecie - ze szczególnym naciskiem na cele polityczne i bezpieczeństwa o wysokiej wartości. Udowodnione to zostało w raporcie ze śledztwa Kongresu USA dotyczącego Huawei i ZTE z 2012 r. (s. 1 Stanowiska);*
2. **niepokojących informacji o ekspansji chińskich firm technologicznych w Polsce (s.2 Stanowiska):**
  - a. *fakt zakupów przez firmę Cellnex, jakoby testowych, urządzeń Huawei;*
  - b. *a przez to oparcie danych polskich podatników na macierzy Huawei OceanStor Dorado 18000 V6, co rodzi ryzyko, że Chiny otrzymają dostęp do wszystkich istotnych operacji handlowych polskich przedsiębiorców;*
3. **ustawy Secure Equipment Act jakoby bezpośrednio zakazującej sprzedaży urządzeń Huawei (s. 3 Stanowiska):**  
*Na szczególną uwagę zasługuje również fakt, że Stany Zjednoczone podjęły szereg działań legislacyjnych (np. Secure Equipment Act), które doprowadziły do ograniczenia, a następnie zakazu sprzedaży chińskich urządzeń firm Huawei i (...) w USA również w sektorze prywatnym (s. 3 Stanowiska).*

Prezentowane w Stanowisku informacje są bezpodstawne i wprowadzające w błąd, przez co naruszają dobre imię (renomę) Huawei.

Aktualna treść Stanowiska zawiera nieuprawnione twierdzenia, narażające Spółkę na utratę reputacji wśród kontrahentów, co będzie skutkowało poważną i nieodwracalną szkodą po stronie Huawei. W przypadku nieuwzględnienia wezwania do zaprzestania naruszeń, Huawei zastrzega

możliwość skierowania sprawy do sądu cywilnego w celu zaprzestania dalszych naruszeń, usunięcia skutków tych naruszeń oraz złożenia oświadczenia odpowiedniej treści i w odpowiedniej formie, a także żądania zadośćuczynienia pieniężnego oraz dochodzenia naprawienia szkody na zasadach ogólnych.

## UZASADNIENIE

1. Zgodnie z przywołanymi przepisami, Huawei jako osobie prawnej przysługuje ochrona dobrego imienia (renomy), polegająca na żądaniu zaprzestania rozpowszechniania bezpodstawnych i wprowadzających w błąd informacji, a w przypadku naruszenia, żądanie usunięcia skutków naruszenia. Huawei może także żądać zapłaty określonej sumy pieniężnej na wskazany cel społeczny oraz odszkodowania w przypadku, gdy w następstwie tych działań została wyrządzona szkoda majątkowa.
2. Na s. 1 Stanowiska zawarte są wyłącznie rozważania dotyczące aplikacji TikTok (poza ostatnim akapitem). W rozważania te włączone jest zdanie dotyczące Huawei. Huawei jest przywołane w aspekcie TikTok. W Stanowisku są zawarte stwierdzenia, że aplikacja TikTok, może „wspierać władze Chin i ich służby wywiadowcze w gromadzeniu ogromnych ilości danych na całym świecie - ze szczególnym naciskiem na cele polityczne i bezpieczeństwa o wysokiej wartości. **Udowodnione to zostało w raporcie ze śledztwa Kongresu USA dotyczącego Huawei i ZTE z 2012 r.**” W ten sposób powiązanie w Stanowisku informacji o TikTok z Huawei sugeruje, że Huawei uczestniczy w praktykach, które zarzuca się TikTok. Po drugie, bezpodstawne jest przywoływanie dla uzasadnienia określonych zarzutów pod adresem TikTok, innego podmiotu (-ów), tylko dlatego, że pochodzą z tego samego kraju, tj. Chin. Po trzecie, przywołany raport ze śledztwa Kongresu USA dotyczący Huawei i ZTE z 2012 r. (*“Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE”*), wbrew twierdzeniu, że „**Udowodnione to zostało**” wszystko w tym raporcie tj. domniemane naruszenia, nie zawiera on takich dowodów. **Przedstawia jedynie rekomendacje i to tylko dla podmiotów prywatnych, w zakresie rozważenia długoterminowych ryzyk oraz zachęt do poszukiwania alternatywnych dostawców.**
3. W Stanowisku więc bezpodstawnie powiązано, czy wręcz wymieszano kwestie dotyczące TikTok z Huawei. Jedynym łącznikiem obu tych firm jest pochodzenie z tego samego kraju. Wprowadza to w błąd, że Huawei jakoby uczestniczyła w zarzucanych TikTok praktykach i że działania innych krajów w stosunku do TikTok przywołane w Stanowisku, powinny być także zastosowane w stosunku do Huawei, skoro jest z nimi powiązana i uczestniczy, jak „udowodnił” to przywołany raport. **Niewątpliwie taki opis godzi w renomę Huawei oraz może wywołać bardzo poważne, wymierne szkody majątkowe, np. poprzez zaprzestanie kupowania przez klientów produktów Huawei.**
4. W Stanowisku na s. 2 znajdują się informacje, że „*W opinii Rady ds. Cyfryzacji coraz bardziej niepokojące stają się informacje o ekspansji chińskich firm technologicznych w Polsce, tj. m.in.: - fakt zakupów przez firmę Cellnex, jakoby testowych, urządzeń Huawei”* - a przez to oparcie danych polskich podatników na macierzy Huawei OceanStor Dorado 18000 V6, co rodzi ryzyko, że Chiny otrzymają dostęp do wszystkich istotnych operacji handlowych polskich przedsiębiorców”;
5. W kwestiach dotyczących nowoczesnych technologii cyberbezpieczeństwa Rada opiera się na raporcie sprzed 11 lat. Rada dokonuje uogólnień, nieopartych żadnymi konkretnymi dowodami czy opracowaniami, **poprzestając na informacjach prasowych. Podstawą bardzo poważnych zarzutów w stosunku do firm technologicznych jest pochodzenie z Chin.**
6. Przykładem niepokojących zdaniem Rady informacji, jest „**fakt zakupów przez firmę Cellnex, jakoby testowych, urządzeń Huawei**”. Informacja ta ma budować w stosunku do Huawei negatywny przekaz („zaniepokojenie Rady”). Tymczasem, po pierwsze decyzja Cellnex, jest po

prostu jej autonomiczną decyzją gospodarczą. Po drugie, Rada sugeruje zaistnienie jakichś nieprawidłowości przy zakupie sprzętu przez Cellnex od Huawei, poprzez sformułowanie, że zakupiono urządzenia Huawei „jakoby testowe”. Z kontekstu całego Stanowiska łatwo wywnioskować, że chodzi o urządzenia, które mogą być używane w sposób nieprawidłowy i niezgodnie z ich przeznaczeniem.

7. Tego rodzaju twierdzenia są nieprawdziwe i bezpodstawnie naruszają dobre imię i renomę Huawei. Zwłaszcza, że Huawei otrzymał pierwszy na świecie certyfikat oceny zgodności (EAL) Common Criteria (CC) na poziomie 4+ za swoje produkty 5G. CCN (Centro Criptológico Nacional). Hiszpański urząd certyfikacji, wydał certyfikat dla oprogramowania Huawei 5900 Series 5G gNodeB 20 maja 2020 r. Ocena została przeprowadzona zgodnie z postanowieniami hiszpańskiego systemu oceny i certyfikacji bezpieczeństwa IT. **Oznacza to, że kod źródłowy dla kluczowego produktu do rozwoju sieci 5G jest przetestowany i certyfikowany.**
8. Oceny i opinie zawarte w Stanowisku nie mogą być formułowane w oderwaniu od obowiązującego w Polsce porządku prawnego, innymi słowy muszą uwzględniać obowiązujące powszechnie przepisy prawa. Tymczasem sformułowana w Stanowisku ocena zakupu przez firmę Cellnex urządzeń Huawei jest po prostu sprzeczna z szeregiem obowiązujących w polskim porządku prawnym zasad gospodarczych, a w szczególności ze: sformułowaną w art. 2 ustawy z dnia 6 marca 2018 r. prawa przedsiębiorców (dalej „p.p.”) zasadą wolności działalności gospodarczej; przewidzianą w art. 8 p.p. zasadą co nie jest prawem zabronione, jest dozwolone; sformułowaną w art. 10 p.p. zasadą domniemania uczciwości przedsiębiorcy czy przewidzianą w art. 12 p.p. zasadą pogłębiania zaufania, proporcjonalności, bezstronności i równego traktowania przedsiębiorców przez organy państwa.
9. Podobnie należy ocenić informacje w Stanowisku o *zakupie chińskich urządzeń do przetwarzania danych przez kluczowe podmioty w państwie, w tym wygrany przetarg na modernizację infrastruktury informatycznej w Centrum Informatyki Resortu Finansów (CIRF), a przez to oparcie danych polskich podatników na macierzy Huawei OceanStor Dorado 18000 V6, co rodzi ryzyko, że Chiny otrzymają dostęp do wszystkich istotnych operacji handlowych polskich przedsiębiorców.* Znowu tworzona jest nieprawdziwa i bezpodstawna informacja, naruszająca dobre imię i reputację Huawei, jakoby poprzez zakup urządzeń Huawei dojdzie do udostępnienia danych zgromadzonych w tych systemach odpowiednim instytucjom państwa chińskiego. W żaden sposób tego rodzaju twierdzenia nie są poparte dowodami czy faktami.
10. **Co więcej, sformułowane w ten sposób twierdzenia, stawiają także bezpodstawne zarzuty instytucjom państwa polskiego (ministerstwom), że uczestniczą w jakiś sposób w tym „negatywnie ocenianym procederze”. To bardzo poważne zarzuty, bo należy przypomnieć, że instytucje państwowe działają według określonych procedur jak przetargi publiczne i posiadają do dyspozycji wszystkie stosowne służby, które pomagają im ocenić zagrożenia i je uniknąć.** Dodatkowo wprost wskazuje się, że poprzez takie działania Huawei i instytucji rządowych szkody poniosą polscy podatnicy i przedsiębiorcy. To także niezwykle poważne zarzuty – znowu niepoparte żadnymi dowodami. Jeżeli Rada uważa, że takie nieprawidłowości wystąpiły, które należy zakwalifikować jako poważne przestępstwo, zgodnie z art. 304 § 2 kodeksu postępowania karnego jest obowiązana niezwłocznie o tym zawiadomić prokuratora lub Policję. W razie niezawiadomienia powinna zaprzestać rozpowszechnia takich informacji.
11. Warto w tym miejscu tj. odnośnie fragmentu Stanowiska, które wprost sugeruje możliwość przekazania danych dotyczących polskich przedsiębiorców chińskim instytucjom rządowym, że Huawei jako spółka technologiczna aktywnie działa w ponad 360 międzynarodowych organizacjach normalizacyjnych, w tym IIC, IEEE-SA, BBF, ETSI, TMF, WFA, OASIS, WWRF, OpenStack, Linaro, ONAP, IFAA. Huawei włączył się w uznawane na całym świecie standardy i wymagania dotyczące certyfikacji bezpieczeństwa cybernetycznego, takie jak CC i FIPS do badań i rozwoju produktów, a także proaktywnie zaprasza laboratoria zewnętrzne do ich certyfikacji.

Obecnie produkty i usługi Huawei uzyskały ponad 270 certyfikatów bezpieczeństwa (w tym CC, FIPS i CSA).

12. W Stanowisku na s. 3 znajduje się stwierdzenie, że *Na szczególną uwagę zasługuje również fakt, że Stany Zjednoczone podjęły szereg działań legislacyjnych (np. Secure Equipment Act), które doprowadziły do ograniczenia, a następnie zakazu sprzedaży chińskich urządzeń firm Huawei i ZTE w USA również w sektorze prywatnym.* Z tak sformułowanej wypowiedzi można wywnioskować, że w USA zostały przyjęte regulacje, np. wspomniany Secure Equipment Act, który był skierowany przeciwko konkretnym firmom, w tym Huawei. Tymczasem, jest to bardzo ogólny dokument, który nie jest skierowany przeciwko jakemukolwiek podmiotowi i ma zastosowanie w stosunku do wszystkich działających na rynku w USA firm.
13. Sformułowania zawarte w Stanowisku wskazujące konkretny podmiot, są bezpodstawne i nieuprawnione, godzące w nazwę i reputację Huawei. Należy zauważyć i podkreślić, że **odnośnie tzw. dostawców wysokiego ryzyka**, trwają obecnie prace nad nowelą ustawy o Krajowym systemie cyberbezpieczeństwa. Zmiana ustawy jest właściwą drogą prawną do ewentualnego wprowadzenia tego rodzaju regulacji. **Pomimo, że ukazało się już 9 wersji tej noweli, nigdy i to nie tylko w uzasadnieniach kolejnych wersji noweli, nie użyto nazwy Huawei jako podmiotu, którego ma dotyczyć lub przeciwko któremu miałyby być skierowane tego rodzaju regulacje.** Ze Stanowiska wynika więc, że wbrew intencjom i zapewnieniom projektodawców noweli ustawy o Krajowym systemie cyberbezpieczeństwa, jej uregulowania, w szczególności dotyczące dostawców wysokiego ryzyka, mają jednak być skierowane przeciwko dostawcom z Chin, w szczególności Huawei.
14. **Stanowisko Rady w zakresie sprzedaży sprzętu do budowy 5G, gdy chodzi o dostawców z Chin, nie może być zaakceptowane, gdyż jak wcześniej wspomniano, Huawei spełnia wymagania certyfikacyjne. Certyfikacja jest jednym z najskuteczniejszych sposobów usuwania wątpliwości związanych z bezpieczeństwem.** Przyznanie dla Huawei pierwszego na świecie certyfikatu 5G CC EAL4+ stanowi dowód, że rozwiązania Huawei w zakresie 5G spełniają najwyższe standardy bezpieczeństwa oraz pozwalają na przyznanie Huawei statusu zaufanego dostawcy 5G.
15. **Stanowisko Rady bezpodstawnie, przedstawia bardzo niekorzystnie firmę Huawei.** Warto więc przypomnieć i wskazać, że Huawei:
  - na całym świecie wspiera ponad 1500 operatorów sieci telekomunikacyjnych w 170 krajach
  - zainwestowała w ośrodki badawcze, innowacyjne i szkoleniowe w Polsce
  - stworzyła ponad 3000 miejsc pracy bezpośrednio i pośrednio
  - w odróżnieniu od konkurencyjnych dostawców pochodzących z państw UE płaci podatki w Polsce.

\*\*\*

Jak zostało wskazane na wstępie, w przypadku nieuwzględnienia wezwania do zaprzestania naruszeń, Huawei zastrzega możliwość skierowania sprawy do sądu cywilnego w celu zaprzestania dalszych naruszeń, usunięcia skutków tych naruszeń oraz złożenia oświadczenia odpowiedniej treści i w odpowiedniej formie, a także żądania zadośćuczynienia pieniężnego oraz dochodzenia naprawienia szkody na zasadach ogólnych.

W imieniu Huawei Polska sp. z o.o.

Zhang Jie – Dyrektor Zarządzający