

Warszawa, 6 września 2023 r.
KL/340/163/AM/2023

Pan
Janusz Cieszyński
Pełnomocnik Rządu ds. Cyberbezpieczeństwa
Minister Cyfryzacji

Szanowny Panie Ministrze,

Mając na uwadze prace toczące się na poziomie UE, skoncentrowane wokół wypracowania tekstu aktu delegowanego, który ma być wydany na podstawie art. 40 ust. 13 Aktu o Usługach Cyfrowych (*Digital Services Act*), poniżej przedstawiam uwagi Konfederacji Lewiatan wobec wypracowywanego projektu regulacji.

Mam nadzieję, że materiał będzie pomocny w rozmowach Ministerstwa Cyfryzacji na temat kształtu reformy rynku cyfrowego w Europie.

Z poważaniem



Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:

Pani Katarzyna Bis-Płaza – Dyrektorka Departamentu Projektów i Strategii, Ministerstwo Cyfryzacji

Załącznik: Stanowisko Konfederacji Lewiatan wobec aktu delegowanego, wydawanego na podstawie art. 40 Digital Services Act

**Stanowisko Konfederacji Lewiatan wobec aktu delegowanego, wydawanego na podstawie art. 40
ust. 13 Digital Services Act**

In its call for evidence on the DSA Art 40, the EC is asking views on what provisions could be useful to help balance the new data access rights and the protection of users' and business rights, as well as their views on the necessary safeguards to minimise the risk of abuses of data access. In our view, the recently adopted Data Act, which provides a framework that allows access to data, includes appropriate safeguards on trade secrets, data protection rights and users' security. The same guardrails should be incorporated in the planned delegated act to ensure consistency when it comes to data access provisions, to ensure that businesses can legitimately protect their proprietary information and to guarantee that innovation incentives are kept. More concretely, like the Data Act, the future delegated act should guarantee that:

- Trade secrets are preserved and only disclosed if all necessary measures are ensured before disclosure, otherwise access can be withheld.
- There is full alignment with the GDPR, particularly in what concerns sharing of personal data.
- Data holders can restrict further sharing / data access if processing by third parties could compromise the product or services' security requirements.

KL/340/163/AM/2023

member of



member of

