

Trade Secrets under the Data Act: call for a balanced and enforceable approach

Key messages:

1. Trade-secret protection should remain an exceptional safeguard, not a broad new ground for refusing data access.
2. Any refusal must be based on objective evidence of a high likelihood of serious economic damage, including where third-country risks are invoked.
3. Whenever a data holder refuses access on trade-secret grounds, the refusal should be reviewed by the competent authority and be subject to a binding decision.

The Issue

1st October 2026

The Data Act already provides strong safeguards for the protection of trade secrets. At the same time, it was adopted to ensure that users and authorised third parties can effectively access and use data generated by connected products.

The challenge is therefore not whether trade secrets should be protected, but how to prevent the trade-secret exception from becoming a broad and easily invoked reason to refuse access by the data holder. It should also be recognised that most data-driven services in the automotive sector are developed by third parties rather than by data holders themselves. This is why trade-secret provisions must not become a blanket mechanism for refusing access.

ISP Position

The ISP coalition supports a balanced approach that protects genuine trade secrets while preserving the Data Act's **core objective of effective data access**. Trade secret protection should remain an **exceptional safeguard** rather than a general right to refuse access. Any refusal should be based on objective and verifiable evidence, with the data holder demonstrating a concrete and specific risk of serious economic damage. While risks associated with third countries may be taken into account, they should form part of the overall assessment and should not constitute an automatic or standalone justification for refusing access.

The proposed third-country ground could allow access to be refused merely because a recipient has a parent company, shareholder or other corporate link outside the EU. This could affect legitimate EU businesses operating within international corporate structures, even where no concrete risk of unlawful disclosure exists.

Why a review mechanism is essential

The most important safeguard is an **independent review by the competent authority**. Today, the Data Act requires a data holder to notify the competent authority when refusing access on trade-secret grounds, but **it does not clearly require the authority to assess whether that refusal is justified**. ISP's proposed amendment closes this gap by requiring the competent authority to review the evidence and issue a binding decision.

This review mechanism would help prevent unjustified or overly broad refusals, ensure that the trade secret exception remains limited to genuine cases, and provide greater legal certainty for both data holders and users. It would also reduce the need for costly litigation while promoting a more consistent application and enforcement of the Data Act across the European Union.

Trade secrets must be protected, but no company should be able to act as judge of its own refusal. Independent review by the competent authority is therefore essential.