

# Do I need to worry about Antitrust Laws when sharing data on Open Supply Hub?

## Memo for OS Hub Stakeholders

April 2025

This is a memo to support stakeholders of Open Supply Hub (OS Hub) in understanding the relationship between antitrust issues and supply chain transparency. This memo has been developed by the OS Hub Team based on analysis conducted by an external law firm with expertise on this subject.

Please note that this memo does not constitute legal advice, but rather serves as a starting place for your own decision-making, based on your region, business, and developments in the regulatory environment that may not have existed when this analysis was conducted.

**Open Supply Hub** is a non-profit powering the transition to safe and sustainable production with the world's most complete, open and accessible global supply chain map. It shows where global production locations are and who is connected to them and makes that data easy for anyone to work with. In doing so, OS Hub is opening doors to new solutions, targeted investment, and more effective collaborations. Open Supply Hub itself—as a 501(c)(3) organization without revenue-generating market activities—has minimal exposure to antitrust risk. The purpose of this memo is to support stakeholders with market activities and a higher antitrust risk exposure.

### What is Antitrust Law?

Antitrust laws seek to maintain fair competition in the marketplace. These laws generally comprise two sets of rules:

- Antitrust/competition laws prohibit agreements and concerted practices between independent companies which restrict competition unless they can be justified by efficiency gains.
- Antitrust laws also prohibit a company in a dominant market position from abusing that market position to exclude competitors and/or exploit consumers.

Violating antitrust laws can result in penalties, fines, and follow-on damage claims. Currently, over 100 jurisdictions have competition or antitrust laws. Many of those, including the EU and the US, enforce these laws based on the “effects doctrine”. This means that any agreement or action is subject to EU or US law if it has an effect in those regions, regardless of where it occurs or where the parties are located.

Agreements and concerted practices between competitors can give rise to the most serious violations of antitrust laws. Examples of generally prohibited activities involving competitors include fixing prices (including

price components); allocating markets or customers; engaging in bid-rigging; limiting output or technical development; boycotting third parties (customers, competitors, suppliers); and/or exchanging commercially sensitive information.

### Antitrust Law and the OS Hub Platform

**Antitrust risks related to information exchanges:** The OS Hub platform discloses information that it gathers from publicly available sources and directly from individual companies, including competitors that are active in the same market. Antitrust risks could arise where the information provided by competitors and disclosed on the OS Hub platform is commercially sensitive in nature. Commercially sensitive information typically includes information which is recent, current and/or future and which concerns prices, costs, capacity, production, quantities, market shares, customers, plans to enter or exit the market, or other important elements of a firm's competitive strategy. In contrast, publicly available information or information that is sufficiently aggregated so that it does not reveal a competitor's individual commercial strategy is not commercially sensitive.

**No commercially sensitive information disclosed on OS Hub:** The data shared on OS Hub is open and includes a map of production sites worldwide, along with profiles for each site. These profiles show the name\*, address\*, country\*, GPS coordinates, data sources, OS ID, parent company, and other details like facility type, product type, and number of workers (data points with an \* are mandatory, the rest are optional). However, it does not contain commercially sensitive information, including specific commercial information about suppliers or the details of their contracts with customers, such as prices, costs, production capacity, volumes, market shares, or other key strategic details that businesses in a competitive market would not want to share. All information disclosed on OS Hub serves the purpose to enable cooperation between companies and organisations to achieve their sustainability goals with regards to their supply chains.

### Antitrust considerations on how OS Hub users convene and collaborate around the data on the platform

At the heart of OS Hub's strategy and theory of change, is the notion that transparent supply chain data enables and facilitates positive action to make improvements in supply chains.

This does not mean that stakeholders shall not respect antitrust laws when convening and collaborating around the OS Hub data. Projects involving competitors bear the highest antitrust risk and require attention to ensure they do not involve the exchange of commercially sensitive information or any other form of collusion, such as fixing prices, allocating markets or customers, bid rigging, limiting of output or technical development, and/or boycotting third parties (customers, competitors, suppliers). In certain circumstances precautionary measures are advisable to avoid antitrust risk.

Below are a number of examples, or ways that the data on the platform can be used, to illustrate how they should be viewed in relation to antitrust laws.

***Collaborating around supply chain improvements:*** Antitrust laws do not generally prevent companies, including competitors, from engaging in such action. For example:

- Taking joint action for social or environmental improvements, e.g.: to reduce water risk in a region
- Co-investing in sustainability initiatives, like renewable technology at supplier production sites;
- Liaising with one another to identify partners or facilities for new program pilots;
- Collaborating to resolve violations of a supplier;
- Sharing information to enable businesses to take individual action such as interrupting purchases from a given supplier or ceasing operations in a given country; or
- Facilitating the coming together of collaborators not just around a specific shared supplier, but also around a shared region.

This is all not raising antitrust risks provided that it does not involve competitors exchanging commercially sensitive information and/or aligning their commercial actions and strategy, including agreeing to boycott or stop purchasing from their common supplier for whom certain violations have been reported (antitrust laws generally require competitors to take purchase decisions unilaterally and independently from competitors).

***Building collaborative grievance mechanisms:*** Antitrust laws do not generally prevent companies, including competitors, from cooperating when building a collaborative grievance mechanism under the applicable legislation. To avoid the risk of exchanging commercially sensitive information in projects involving competitors, the operation of the joint grievance mechanism can be delegated to a third party or to a Clean Team (i.e., a restricted group of individuals within an undertaking that are not involved in the competitors' commercial operations) bound by strict confidentiality obligations. This is to ensure that the third party or the dedicated Clean Team do not share commercially sensitive information relating to one competitor with another competitor, and that no such information is included in the reports prepared for competitors. Antitrust risks can also arise where competitors agree to boycott or stop purchasing from their common supplier for whom certain violations have been reported (antitrust laws generally require competitors to take purchase decisions unilaterally and independently from competitors).

***Shared auditing, due diligence & reporting:*** Shared supplier auditing, due diligence and reporting can significantly lower the burden for companies to comply with supply chain reporting requirements. However, sharing results of a supplier audit or a joint supplier due diligence / auditing raises antitrust risks where this involves the disclosure of commercially sensitive information amongst competitors. Similarly, discussions between competitors relating to any commercially sensitive information contained in any audit results/reports, and any coordinated conduct based on those discussions is prohibited under antitrust laws. To mitigate this risk, the preparation of a joint audit report or the supplier due diligence could be outsourced to a third party (provided this is permitted under the applicable supply-chain-specific legislation) or operated by a Clean Team bound by strict confidentiality obligations.

***Sharing information and resources in crisis moments:*** Sharing information and resources, including amongst competitors, is often necessary and indispensable for companies to deal with a crisis.

It's crucial for businesses not to think that a crisis allows them to engage in anti-competitive practices with competitors, by exchanging commercially sensitive information or aligning their commercial actions and behaviour in the market, including through fixing/aligning prices, limiting output, allocating markets/customers, organising boycotts. Antitrust laws still apply and violating them can lead to serious penalties. Depending on the crisis at stake, the antitrust risk may in practice be higher as crisis moments often increase interactions between companies and competitors in particular, at times with the objective to deal with the crisis through concerted, anti-competitive behaviour. Special attention is therefore warranted when competitors interact in crisis moments to avoid antitrust risk. In rare crisis situations, governments or antitrust regulators might approve certain collaborations between competitors, to help deal with the crisis. However, companies need to ensure that their actions strictly follow the specific rules and time limits set by the government. If they don't, they risk facing consequences from regulators or courts once the crisis is over.

**If you have questions or would like to discuss anything further,  
please get in touch with us at [info@opensupplyhub.org](mailto:info@opensupplyhub.org).**

**To learn more about OS Hub and access additional resources relevant for brands and retailers  
interested in supply chain transparency, visit <https://info.opensupplyhub.org/resources>.**