Brussels, 26 October 2023

Re: The Revision of the Directive on Liability for Defective Products should strike a fair balance to support innovation

Our associations represent a broad coalition of global and European companies, from startups and SMEs to leading technology companies.

Following the discussions in the Council of the EU and the European Parliament, the interinstitutional negotiations on the revision of the EU Directive on Liability for Defective Products, also known as the Product Liability Directive (PLD), are starting this month. As negotiations seem to be likely to go at a rapid pace, we urge the policymakers to allow enough time to discuss the possible consequences of the suggested provisions and include stakeholders in those discussions.

The tech sector, along with others, has been vocal throughout the legislative scrutiny to ensure that policymakers are aware of the unintended consequences of certain provisions of the revised PLD. While the European Parliament and the Council introduced changes to the text under revision, we invite policymakers to take the utmost prudence on certain elements which could impact the competitiveness of the European economy in the long run. As software is set to be part of the definition of a "product", other parts of the revision need to be refined to support innovation in the software sector and avoid overburdening developers. For emerging technologies like AI, which are also being regulated under the AI Act and AI Liability Directive, it will be crucial to strike the right balance and avoid an excessively restrictive legal framework which would hinder AI development and use in Europe. To do so, we suggest:

- **The revised PLD should only cover software proportionately** to the extent to which software is essential to the functioning of a product into which it is embedded or with which it is inter-connected, as proposed in the Parliament's mandate. Also, information should not be considered a product, and therefore product liability rules should not apply to the content of digital files, such as media files or ebooks or the mere source code of software.

- **The definitions of the new harms in the scope of the PLD need to be measurable** so that judicial authorities and companies avoid facing excessive legal action. Data loss and corruption of data are already covered under other liability

regimes, such as the GDPR. In addition, damage to data usually would not be of the same severity as damages to health or property which are the cornerstones of the original PLD. Data loss and corruption, if not deleted altogether, should at minimum be limited to irreversible damages amounting to over 1,000 euros. Psychological harm should be certified by doctors where serious adverse effects on the victim's psychological integrity are demonstrated.

- **The conditions for disclosure obligations should meet a higher threshold** to protect trade secrets and limit excessive litigation. To do so, the request for evidence should be open to all parties once the proceedings have started. The relevance of the evidence and unintended consequences of disclosures should be taken into account in the assessment of the necessity and proportionality of the request.

- **The alleviation of the burden of proof cannot be solely based on the complexity of a product**, as it would amount to a *de facto* reversal of the burden of proof for technological products or AI. Introducing safeguards to the presumption of defectiveness is necessary to preserve the neutrality of the Directive. Therefore, the claimant should demonstrate excessive technical or scientific complexity and a strong possibility of defectiveness exists. Also, the courts should limit access to only information which is necessary and proportionate to support a claim and prove defectiveness or causal link.

- **Cybersecurity flaws should not be considered a defect unless there is a breach of relevant EU and national law**. In this way, complex cybersecurity efforts, being an ongoing struggle against existing and evolving threats, would be given the needed flexibility in the landscape of constantly evolving malicious actors. Therefore, considerations of cybersecurity-related defectiveness need to be based on the concrete requirements under the law.

- **Software manufacturers should not be liable beyond the expected lifecycle of the software**. Software can have a widely varying lifecycle (e.g. gaming apps and operating systems) and limiting software manufacturer's liability to the intended software lifecycle is needed to preserve innovation in Europe. In addition, installation of upgrades and updates by users should be a condition to trigger any liability of the software producer.

We encourage policymakers to reach a necessary balance between the protection of consumers and the ability of companies to offer innovative products to consumers in this final stretch of the negotiations.

Signatories (in alphabetical order):

- Alliance Française des Industries du Numérique (AFNUM) - HATVP
- American Chamber of Commerce to the EU (AmCham EU) - 5265780509-97
- BSA | The Software Alliance - 75039383277-48
- Computer & Communications Industry Association (CCIA Europe) - 15987896534-82
- Developers Alliance - 135037514504-30
- DOT Europe - 53905947933-43
- Information Technology Industry Council (ITI) - 061601915428-87
- European Semiconductor Industry Association (ESIA) - under the EECA umbrella: 22092908193-23