Computer & Communications Industry Association
Open Markets. Open Systems. Open Networks.

# Making EU product liability rules fit for the digital age

## POSITION PAPER ON THE REVISION OF THE PRODUCT LIABILITY DIRECTIVE

December 2022

### Introduction

The Computer & Communications Industry Association (CCIA Europe) agrees that the European product liability regime should be adapted to new developments and to help improve consumer compensation for defective products.

CCIA Europe's Members have been driving many digital innovations over the past decades, with the safety of consumers always being of paramount importance. The revision of the EU Directive on Liability for Defective Products, also known as the Product Liability Directive (PLD), was initiated in order to tackle the alleged challenges linked to the digital age, the circular economy, and the globalisation of value chains.[1] While we commend the European Commission's work to update the PLD, the proposed text requires further improvements to remove the uncertainties the current draft poses to all businesses across the European Union.

Both the old and the (proposed) new PLD build on the same principle of creating an EU-wide system that enables Europeans to ask for compensation when a defective product leads to physical injury or property damage. The PLD creates a strict liability regime, meaning that liability does not depend on the fault of the manufacturer, but only on the observed defectiveness of the product.

Moreover, the PLD is non-contractual, so its strict liability cannot be undermined by contractual clauses and is additional to other contractual liabilities. This system also applies to all products in the Single Market. Therefore, any changes brought to the PLD need to be carefully considered as they can have serious ramifications with an extremely wide impact.

While the main goal of adapting the PLD to new developments is laudable, some of the changes proposed for this revision risk disincentivising innovation and digitalisation in Europe, which would be to the detriment of European consumers and businesses alike. In fact, so far the rationale behind the revision does not seem to be based on evidence of any major challenges faced on the ground across the EU that would justify such changes. The impact assessment of the revision indeed mostly relies on prediction and hypothetical assumptions.[2]

As the European Parliament and the Council are starting to discuss their positions on the PLD revision, CCIA Europe offers the following key recommendations to further improve the Directive:

I. Preserve innovation with narrower and clearer definitions
II. Clarify specific liability provisions to account for technological products

[1] European Commission, Proposal for a Directive on liability for defective products, 28 September 2022, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0495
[2] European Commission, Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, Impact assessment study on the revision of the Product Liability Directive (PLD) 85/374/EEC : No. 887/PP/GRO/IMA/20/1133/11700 : final report, Publications Office of the European Union, 2022, available at https://data.europa.eu/doi/10.2873/138110

## I. Preserve innovation with narrower and clearer definitions

The most significant change proposed for the PLD revision is the extension of the PLD's scope by widening the definition of "product" and additions to the list of damages. While it is claimed that the proposal remains technology-neutral, this extension of scope fails to recognise the specificities of new technologies. As a consequence, this would lead to legal uncertainty for businesses, a chilling effect on innovation, and ultimately less choice for European consumers.

### 1. Software cannot have the same liability as tangible goods

Article 4(2) of the PLD revision broadens the definition of a "product" from tangible goods only to also include software (whether embedded or standalone), artificial intelligence (AI) systems, as well as digital services necessary for the product's functioning. A strict liability regime usually applies to products that pose a significant risk, such as severe physical injury or damage to property, for example in the case of explosives.

While the purpose of the PLD is to be general, it is hard to imagine how software could physically act upon any person or physical property to provoke such injury or damage. Indeed, the nature and risk profile of software differ fundamentally from those of physical goods. This is particularly true as software simply cannot be completely bug-free. Software continuously evolves, even after being put on the market, which means that it is constantly improved and fixed as developers identify new risks. For example, developers identify bugs encountered by users and will prepare a software update to fix them. As it stands, this extension of the PLD's scope is not fit for purpose and does not account for the properties of software and technological products. It should also be noted that the proposed revision does not provide any precise definition of "software".

Embedded software is already covered by the current PLD, as underlined in the impact assessment conducted for this revision.[3] Hence, we fail to see the added value of including standalone software in the scope of the PLD as there are no liability gaps. Besides, if the software is defective, the EU's Sale of Goods Directive and the Digital Content and Digital Services Directive already offer a very high level of contractual protection to consumers.[4] Consumers can also seek remedies under fault-based liability regimes of Member States.

In fact, this extension of the product scope would discourage software developers from innovating, as they would be subject to a strict liability regime. Bringing non-embedded software within the scope of the PLD could thus have significant consequences.

Developers may be discouraged from developing, or releasing, software in the EU, or may raise the price of software for consumers to cover potential liability costs. This could result in the roll-out and uptake of digital technologies in the EU lagging behind the rest of the world. It would also discourage the sharing of security-related information across the developer ecosystem and would

[3] Impact assessment study on the revision of the Product Liability Directive, op. cit., p.23
[4] Directive (EU) 2019/771 on certain aspects concerning contracts for the sale of goods, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0771; Directive (EU) 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32019L0770

discourage all players along the supply chain to assist in providing security fixes, as they would try to avoid future liability. This is clearly detrimental to end-users, who may be exposed to security risks for longer. This would even be damaging to product safety itself, as software components are used to improve physical goods. Software developed for cars, or apps monitoring energy systems, would be negatively impacted for example.

While the proposal excludes services from the scope, "related services" are included to cover digital services without which a product would not function (Article 4(4)). The definition of related services should be further limited to avoid inadvertently covering a wide range of services under this strict liability regime. Indeed, including services in the scope of the PLD would be a shift in EU law and case law, both of which have recognised the separation of the liability regimes for goods and services.[5] Recital 15 of the proposal should at least mention that only digital services necessary to the core functionality of a product are in scope.

The proposal sets out an exemption for open-source software (OSS) in recital 13. This exemption would be strengthened if directly included in the main text. Furthermore, the current text limits the exemption as long as the OSS is not used commercially. As it stands, the manufacturer could face liability for the OSS elements of the product they sell. A broader exemption for all OSS and its uses would be welcomed to avoid situations where liability would be complex to establish. This would better reflect the reality of OSS development without undermining the manufacturer's liability.

Covering software, AI, and digital services under the exact same, strict liability regime as traditional products raises more questions than it solves. At the very minimum, the PLD should use narrower and clearer definitions to avoid overly-broad interpretations and uncertain implementation.

### 2. Scope of damages should remain limited to material harm

Article 4(6) of the proposal expands the list of damages to include both "psychological health" and "loss or corruption of data". While damages remain limited to material losses, this expansion creates uncertainty, especially in combination with the wide definition of "product" discussed above.

That is why the proposal needs to better outline what is meant by material losses resulting from harm to psychological health. While recital 17 implies that this addition is merely a clarification, current case law proves that this understanding varies greatly from one Member State to another. This is even more important as non-embedded software is now within the scope of the revised PLD. It will be difficult to clearly establish and quantify software's impact on psychological health.

For example, a wellness app might have warned its users of its indicative nature, but would still be held liable for a mental illness developed by one of its users. This type of damage is particularly unforeseeable. As psychological health is already tackled by standard liability regimes, including national liability rules, the appropriateness of this inclusion in the context of a strict liability regime should be reconsidered.

[5] Court of Justice of the European Union, Judgement of 10 June 2021, Case C65/20, VI v KRONE – Verlag Gesellschaft mbH & Co KG, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62020CJ0065

The inclusion of data loss provides for a separate and potentially overlapping basis for compensation with the EU's General Data Protection Regulation (GDPR).[6] While the impact assessment underlines that loss or corruption of data is an addition to the revised PLD in order to cover situations that the GDPR does not, the articulation of the two texts is still unclear.[7] A clear materiality threshold for a product would help to differentiate between the two regimes. Recital 16 could further specify that the PLD's liability only applies when the GDPR is not applicable. Otherwise, creating such a dual liability regime will confuse consumers, and could eventually lead to forum shopping and double claims for single harm.

Any extension of the scope of damages should be based on clear definitions. The proposal would benefit from well-defined concepts, especially when it comes to "psychological harm" and "data loss and corruption".

### 3. Removal of the thresholds

The combination of the removal of minimum and maximum thresholds (respectively €500 and €70 million) with the extension of the product definition and the scope of damages, upsets the careful balance of the current Directive. This overall balance needs to be carefully assessed when weighing the individual extensions being proposed.

The reasoning for having such thresholds remains true today. A minimum threshold prevents frivolous claims and maintains the back-stop nature of the regime, while an upper maximum allows for insurable risks. For SMEs in particular, persuading retailers to carry their products would become increasingly difficult under the revised PLD. These figures should be subject to maximum harmonisation in order to address the current issues with divergence across Member States as identified by the European Commission.

## II. Clarify specific liability provisions to account for technological products

Several additions to specific provisions on the liability of defective products, and their overall novelty, still require further clarity. The assessment of defectiveness, the disclosure of evidence, and the limitation period should take into account the particular nature of new technologies in order to keep a technology-neutral approach. The following suggestions (4-8) would improve the proportionality of the provisions when it comes to technological products; providing more predictability and ultimately benefiting consumers and businesses alike.

### 4. Refine the assessment of defectiveness

Article 6 of the PLD revision establishes a list of elements to take into account to assess the defectiveness of a product. Several of these elements refer to digital functionalities, such as

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[7] European Commission, Commission Staff Working Document, Impact Assessment Report, Proposal for a Directive of the European Parliament and of the Council on liability for defective products, 28 September 2022, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2022:0316:FIN:EN:PDF

cybersecurity, interconnectivity, or machine learning. Greater clarity on these aspects would be appreciated, especially as it would apply to software and AI applications.

For example, one of the criteria requires the intervention by a regulatory authority relating to product safety. This intervention could be a request to fix a bug, which is done quickly. In that case, however, it is not clear how it would be a relevant aspect to assess the defectiveness of the software in question. Other elements related to defectiveness that are being considered include "product safety requirements, including safety-relevant cybersecurity requirements". At the very least, such cybersecurity requirements should be made consistent with violations of the Cyber Resilience Act.[8]

### 5. Recognise the role of online marketplaces in the supply chain

The draft proposal continuously emphasises that producers and importers are the parties who should be considered liable in case of damages caused by defective products manufactured or imported into the EU. Indeed, these entities have control over the process influencing a product's safety. Article 7 establishes a clear chain of liability throughout the supply chain. Online marketplaces are only involved when no economic operator or authorised representative has been identified. The reference to the Digital Services Act's liability exemption in Article 7(6) of the revised PLD ensures coherence and consistency with recent EU legislative initiatives.[9] It is also worth noting that companies which operate an online marketplace as a hybrid business model (e.g. combining manufacturing and intermediating between traders and consumers) will be considered economic operators when relevant.

To ensure the effectiveness of this chain of liability, the role of the authorised representative should be better framed. Taking stock of the implementation of the Market Surveillance Regulation and the upcoming General Product Safety Regulation, this concept needs to be strengthened.[10] For example, this could be done through accreditation by public authorities.

### 6. Rebuttable presumptions

Easing the burden of proof with rebuttable presumptions as provided for in Article 9 would be disproportionate. In particular, most software and AI systems would automatically fall under Article 9(4) because of their technical complexity. This solution would therefore not be neutral.

The rebuttable presumption would generalise a worst-case scenario approach. Even if the defendant can contest this presumption, it creates a perspective of uncertainty and heavy legal fees for all businesses developing complex products. It would furthermore, de facto, amount to a reversal of

[8] European Commission, Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454
[9] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2065&qid=1666857517641
[10] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products (Market Surveillance Regulation), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32019R1020; European Commission, Proposal for a Regulation on general product safety (GPSR), available at: https://eurlex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0346&qid=1628522210573

the burden of proof rather than the intended alleviation. A more proportionate approach would further limit this rebuttable presumption to specific cases. The presumption of defectiveness in Article 9(2)(c) is also problematic, as no clarification of an "obvious malfunction" is given.

### 7. New disclosure obligations

The PLD revision would enable national courts to ask for the disclosure of evidence to defendants upon claimants' demand in Article 8. The threshold for ordering such disclosures is very low as the claimant only has to present facts and evidence sufficient to support the plausibility of the claim. Furthermore, the scope of information that can be disclosed is very broad as it covers "what is necessary and proportionate". This disclosure obligation should be better framed to avoid burdening defendants and prevent abusive demands early in the procedure.

### 8. Shorter limitation period for new technologies

The limitation period of 10 years (Article 14) proposed in the revision is not in line with the realities of software development or AI application. Under the revised PLD, software developers would have to provide updates for 10 years, which does not reflect how long software programs are usually used. The obligation to provide updates would be equal to imposing a product monitoring obligation on manufacturers, which is not the original goal of the PLD revision. The period of time during which software could potentially be considered to cause harm will typically be much shorter. It is also unclear if the limitation period would be renewed after every software update, which would unfairly extend the limitation period. Therefore, the limitation period should be adapted to reflect the reality of software development and ensure neutrality across products.

## Conclusion

The revision of the Product Liability Directive is an opportunity to adapt this decades-old EU framework to new developments, such as the digitalisation of society and (increasingly complex) global value chains. Nevertheless, each change brought about by this proposal should be carefully balanced to ensure the PLD continues to work for European consumers. Further reflection is needed to narrow the definitions and the scope of the proposal, as well as to improve specific liability provisions.

The European Parliament and the Council should amend the proposal to ensure it takes a more technology-neutral approach and better reflects how today's technologies actually work. This would provide greater legal certainty to businesses and better protect European consumers from defective products.

## About CCIA Europe

- The Computer & Communications Industry Association (CCIA) is an international, not-for-profit association representing a broad cross section of computer, communications, and Internet industry firms.
    - As an advocate for a thriving European digital economy, CCIA Europe has been actively contributing to EU policy making since 2009.
    - CCIA's Brussels-based team seeks to improve understanding of our industry and share the tech sector's collective expertise, with a view to fostering balanced and well-informed policy making in Europe.
- For more information, visit: twitter.com/CCIAeurope or www.ccianet.org